



Cisco Catalyst IR8340 Rugged Series Router Software Configuration Guide, Cisco IOS XE Release 17.7.x

First Published: 2022-04-07

Last Modified: 2022-08-11

Americas Headquarters

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

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

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

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 NON-INFRINGEMENT 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)

© 2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1

Overview 1

Introduction 1

Accessing the CLI Using a Router Console 2

Using the Console Interface 5

Initial Bootup Security 6

Enforce Changing Default Password 6

Telnet and HTTP 7

Accessing the CLI from a Remote Console 8

Preparing to Connect to the Router Console 8

Setting Up the IR8340 to Run SSH 9

Using Telnet to Access a Console Interface 10

CLI Session Management 11

Information About CLI Session Management 11

Changing the CLI Session Timeout 11

Locking a CLI Session 11

Communications, services, and additional information 12

Cisco Bug Search Tool 12

Documentation feedback 12

CHAPTER 2

Using Cisco IOS XE Software 13

Understanding Command Modes 13

Keyboard Shortcuts 15

Using the no and default Forms of Commands 15

Using the History Buffer to Recall Commands 16

Managing Configuration Files	16
Saving Configuration Changes	16
Filtering Output from the show and more Commands	17
Finding Support Information for Platforms and Cisco Software Images	18
Using Cisco Feature Navigator	18
Getting Help	18
Finding Command Options: Example	19
Using Software Advisor	24
Using Software Release Notes	24

CHAPTER 3

Basic Router Configuration	25
IR8340 Interface Naming	25
Basic Configuration	26
Configuring Global Parameters	31
Configuring the Gigabit Ethernet Interface	32
Support for sub-interface on GigabitEthernet0/0/0	33
Configuring a Loopback Interface	33
Configuring CPU Allocation	34
Enabling Cisco Discovery Protocol	35
Configuring Command-Line Access	35
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 4

Configuring Secure Shell	41
Information About Secure Shell	41
Prerequisites for Configuring Secure Shell	41
Restrictions for Configuring Secure Shell	41
SSH And Router Access	42
SSH Servers, Integrated Clients, and Supported Versions	42
SSH Configuration Guidelines	43
How to Configure Secure Shell	43

Setting Up the IR8340 to Run SSH	43
Configuring the SSH Server	44
Monitoring the SSH Configuration and Status	46
Configuring the Router for Local Authentication and Authorization	46
Information about Secure Copy	47
Prerequisites for Secure Copy	48
Restrictions for Configuring Secure Copy	48
Configuring Secure Copy	48
Additional References	49

CHAPTER 5

Installing the Software 51

Installing the Software	51
Cisco Software Licensing	51
Consolidated Packages	51
Network-Essentials	52
Network-Advantage	52
Related Documentation	52
Installing the Cisco IOS XE Release	52
ROMMON Images	53
File Systems	53
Option to Enable or Disable USB Access	54
Autogenerated File Directories and Files	55
Flash Storage	56
Related Documentation	56

CHAPTER 6

Software Maintenance Upgrade (SMU) 57

Software Maintenance Upgrade (SMU)	57
SMU Workflow and Basic Requirements	58
SMU Example	58
Installing a Patch Image	58
Uninstalling the Patch Image	60
Uninstalling the Patch Image Using Rollback	60
Uninstalling the Patch Image Using Deactivate, Commit, and Remove	62

CHAPTER 7	Smart Licensing Using Policy (SLP)	65
	Smart Licensing Using Policy	65
CHAPTER 8	Configuring Ethernet Switch Ports	67
	Configuring VLANs	67
	Creating a VLAN	68
	Configuring LAN Ports for Layer 2 Switching	69
	Layer 2 LAN Port Modes	69
	Default Layer 2 LAN Interface Configuration	70
	Configuring LAN Interfaces for Layer 2 Switching	71
	IEEE 802.1x Protocol	71
	Configuring IEEE 802.1X Port-Based Authentication	71
	Enabling AAA Authorization for VLAN Assignment	71
	Enabling IEEE 802.1X Authentication and Authorization	72
	Spanning Tree Protocol Overview	74
	Default STP Configuration	75
	Enabling STP	76
	Configuring Optional STP Features	78
	Enabling PortFast	78
	Configuring PortFast BPDU Filtering	78
	Enabling BPDU Guard	80
	Enabling UplinkFast	81
	Enabling BackboneFast	82
	MAC Table Manipulation	83
	Creating a Static Entry in the MAC Address Table	83
	MAC Address-Based Traffic Blocking	83
	Configuring and Verifying the Aging Timer	84
	MAC Learning on a Vlan	85
	Assigning IP Addresses to Switch Virtual Interfaces	86
	SVI Supported Features	86
	IGMP Snooping for IPv4	88
	MLD Snooping	88
	MLD Snooping Configuration Guidelines	89

Default MLD Snooping Configuration	89
Enabling or Disabling MLD Snooping on a VLAN	90
Configuring UniDirectional Link Detection	91
Enabling UDLD Globally	91
Enabling UDLD on an Interface	92
Configuring the Switched Port Analyzer	92
SPAN and RSPAN	93
Creating a Local SPAN Session	93
Creating a Local SPAN with Incoming Traffic Allowed on Destination	95
Specifying VLANs to Filter	97
Verifying the SPAN Session	99
Removing a SPAN Session	99
Configuring a VLAN as an RSPAN VLAN	100
Creating an RSPAN Source Session	101
Specifying VLANs to Filter on RSPAN Source Session	103
Creating an RSPAN Destination Session and Configuring Incoming Traffic	104
EtherChannel Overview	106
Channel Groups and Port-Channel Interfaces	107
Port Aggregation Protocol	107
Link Aggregation Control Protocol	107
Configuring Layer 2 EtherChannels	107
Configuring EtherChannel Load-Balancing	109
Configuring the PAgP Learn Method and Priority	110
Configuring the LACP Port Channel Min-Links Feature	111
Configuring LACP Fast Rate Timer	112
Modular Quality of Service Command-Line Interface	113
Creating a Traffic Class	114
Creating a Traffic Policy	116
Configuring Class-Based Packet Marking	119
Attaching a Traffic Policy to an Interface	124
Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps	125

CHAPTER 9
Power over Ethernet 129

Power over Ethernet	129
---------------------	-----

Device Detection and Power Allocation	130
Configuring Power Over Ethernet	130
Configuring Universal PoE	131
PoE Debug Commands	132

CHAPTER 10

Configuring the T1/E1 Network Interface Module	133
Information About T1/E1 Network Interface Module	133
Configuring T1/E1 Network Interface Module	133
Configuring the Card Type	133
Changing the Card Type	134
Configuring the T1/E1 Network Interface Module for Data Support	135
Example of T1/E1 Network Interface Module Configuration	138

CHAPTER 11

Configuring the Serial Network Interface Module	141
About the Asynchronous/Synchronous Serial Network Interface Module	141
Configuring the Serial Interface to Sync or Async Mode	141
Configuring Synchronous Serial Ports	142
Checking DCE and DTE Cable Type	142
Specifying Synchronous Serial Encapsulation	142
DCE and DTE Configuration for HDLC Encapsulation	143
DCE and DTE Configuration for PPP (CHAP) Encapsulation	144
DCE and DTE Configuration for PPP (PAP) Encapsulation	145
DCE and DTE Configuration for Frame Relay Encapsulation	146
Serial Synchronous Show and Debug Commands	148
Configuring Asynchronous Serial Ports	149
Specifying Asynchronous Serial Encapsulation	149

CHAPTER 12

Cellular Pluggable Interface Module Configuration Guide	151
--	------------

CHAPTER 13

Information About SCADA	153
SCADA Overview	153
Role of the IR8340	153
Key Terms	154
Protocol Translation Application	154

Prerequisites	155
Guidelines and Limitations	156
Default Settings	156
Configuring Protocol Translation	156
Enabling the IR8340 Serial Port and SCADA Encapsulation	157
EXAMPLE	157
Configuring T101 and T104 Protocol Stacks	157
Prerequisites	158
Configuring the T101 Protocol Stack	158
EXAMPLE	160
Configuring the T104 Protocol Stack	160
EXAMPLE	163
Configuration Example	164
Configuring the DNP3 Protocol Stacks	165
Configuring DNP3 Serial	165
EXAMPLE	167
Configuring DNP3 IP	167
EXAMPLE	169
Starting and Stopping the Protocol Translation Engine	169
EXAMPLE	170
Verifying Configuration	170
Debug Commands	171

CHAPTER 14

Raw Socket Transport	173
Information About Raw Socket Transport	173
TCP Transport	174
UDP Transport	174
Serial Data Processing	175
VRF-Aware Raw Socket	175
Prerequisites	176
Guidelines and Limitations	176
Default Settings	176
Configuring Raw Socket Transport	176
Enabling Raw Socket Transport on the Serial Interface	176

Configuring Common Raw Socket Line Options	177
Configuring Raw Socket TCP	178
Configuring the Raw Socket TCP Server	178
Configuring the Raw Socket TCP Client	180
Configuring a Raw Socket UDP Peer-to-Peer Connection	181
Verifying Configuration	182
Configuration Example	183
Raw Socket TCP	183
Raw Socket UDP	184
Raw Socket VRF	185
Show Line Details for Configuring Raw-TCP/UDP	186
Raw-Socket Show and Debug Commands	187

CHAPTER 15
Configuring Security for VPNs with IPsec 189

Information About Configuring Security for VPNs with IPsec	189
Supported Standards	189
Supported Encapsulation	191
IPsec Functionality Overview	191
IKEv1 Transform Sets	192
IKEv2 Transform Sets	192
How to Configure IPsec VPNs	192
Creating Crypto Access Lists	192
Configuring Transform Sets for IKEv1 and IKEv2 Proposals	193
Configuring Transform Sets for IKEv1	194
Configuring Transform Sets for IKEv2	195
Creating Crypto Map Sets	197
Creating Static Crypto Maps	197
Creating Dynamic Crypto Maps	200
Creating Crypto Map Entries to Establish Manual SAs	203
Applying Crypto Map Sets to Interfaces	205

CHAPTER 16
Configuring Resilient Ethernet Protocol (REP) 207

CHAPTER 17
System Messages 209

Information About Process Management	209
How to Find Error Message Details	209

CHAPTER 18

Environmental Monitoring 215

Environmental Monitoring	215
Environmental Monitoring and Reporting Functions	215
Environmental Monitoring Functions	216
Environmental Reporting Functions	217
Additional References	217
Technical Assistance	218

CHAPTER 19

IOx Application Hosting 219

Application Hosting	219
Information About Application Hosting	219
Need for Application Hosting	219
IOx Overview	220
Cisco Application Hosting Overview	220
IOXMAN	220
Application Hosting on the IR8340 Router	221
Application Hosting on Layer 2 and Layer 3 Interfaces	221
VirtualPortGroup	222
vNIC	222
How to Configure Application Hosting	223
Enabling IOx	223
Configuring Application Hosting to Layer 2 Interfaces	224
Configuring a VirtualPortGroup to a Layer 3 Data Port	225
Configuring Docker Run Time Options	227
Installing and Uninstalling Apps	228
Overriding the App Resource Configuration	229
IOx Configuration with ERSPAN	230
Verifying the Application Hosting Configuration	231
Configuration Examples for Application Hosting	233
Example: Enabling IOx	233
Example: Configuring a VirtualPortGroup to a Layer 3 Data Port	233

Example: Installing and Uninstalling Apps	233
Example: Overriding the App Resource Configuration	234
Signed Application Support	234
Cisco Cyber Vision	234

CHAPTER 20

ROM Monitor Overview 235

ROM Monitor Overview	235
Access ROM Monitor Mode	236
Checking the Current ROMMON Version	236
Commonly Used ROM Monitor Commands	237
Examples	238
Changing the ROM Monitor Prompt	238
Displaying the Configuration Register Setting	238
Environment Variable Settings	239
Frequently Used Environmental Variables	239
Displaying Environment Variable Settings	239
Entering Environment Variable Settings	240
Saving Environment Variable Settings	240
Exiting ROM Monitor Mode	240
Configuration Example	241
Upgrading the ROMmon for a Router	241

CHAPTER 21

Process Health Monitoring 243

Monitoring Control Plane Resources	243
Avoiding Problems Through Regular Monitoring	243
Cisco IOS Process Resources	243
Overall Control Plane Resources	253
Monitoring Hardware Using Alarms	255
Router Design and Monitoring Hardware	255
BootFlash Disk Monitoring	255
Approaches for Monitoring Hardware Alarms	255
Viewing the Console or Syslog for Alarm Messages	255
Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP	256

CHAPTER 22**Troubleshooting 257**

Troubleshooting 257

Understanding Diagnostic Mode 257

Before Contacting Cisco or Your Reseller 258

show interfaces Troubleshooting Command 258

Software Upgrade Methods 258

Change the Configuration Register 259

Configuring the Configuration Register for Autoboot 260

Reset the Router 261

Recovering a Lost Password 262

Reset the Configuration Register Value 262

Configuring a Console Port Transport Map 263

Viewing Console Port, SSH, and Telnet Handling Configurations 265

Using the factory reset Commands 266



CHAPTER 1

Overview

- [Introduction, on page 1](#)
- [Accessing the CLI Using a Router Console, on page 2](#)
- [Initial Bootup Security, on page 6](#)
- [Accessing the CLI from a Remote Console , on page 8](#)
- [CLI Session Management, on page 11](#)
- [Communications, services, and additional information, on page 12](#)

Introduction

The Cisco Catalyst IR8340 Rugged Series Router is Cisco's first industrial-grade fully integrated routing and switching platform. IR8340 is designed to provide outstanding flexibility and adaptability to address the latest needs of the network evolution.



Note The terms *IR8340* and *router* are used throughout this document in text and CLI examples to refer to the Cisco Catalyst IR8340 Rugged 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 IR8340 Router features 2 Pluggable Interface Module (PIM) slots, 2 single-wide IRM-NIM slots, 1 timing module slot, plus 12 onboard LAN ports and 2 WAN ports, and supports the following:

- 150W/250W PSU, Low Voltage DC and High Voltage AC/DC options
- Timing and SyncE support—IRIG-B (Analog & Digital), GNSS, and PTP



Note For more information about timing related configuration, see *Timing and Synchronization Configuration Guide, Cisco IOS XE 17 (Cisco Catalyst IR8340 Rugged Series Router)*.

- LTE PIM modules
- Network Interface Modules (NIMs)
- mSATA module
- 2 x 1G Combo WAN ports
- 4 x 1G Copper LAN Ports
- 4 x 1G Combo LAN ports
- 4 x 1G SFP LAN Ports
- PoE/PoE+/UPoE (up to 120w) support on LAN port 1-4
- 2 x IN and 1 x OUT Alarm ports (RJ45)

Accessing the CLI Using a Router Console

Cisco IR8340 routers have an RJ45 RS232 serial console port located on the router front panel. The default baud rate is 9600. You can use an RJ45 Roll Over 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 17.7.1.
*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:IR8340-K9,SN:FDO2523J7GF]
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

*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 9rDzH3rLqj1Fhek$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 successfully
*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 9rDzH3rLqjlFhek$G9UDZE7moWqsKJEZfJAH2yO.SPbKZeKJsEe./CPEz1.
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

When the device is first booted after factory reset or fresh from the factory, by default the following takes place:

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

### Examples

From a freshly booted device, below configurations for HTTPS and SSH are enabled.

```

ip http server
ip http authentication local
ip http secure-server
.
.

line vty 0 4
login
transport input ssh
line vty 5 14
login
transport input ssh

```

To enable Telnet, use the **line vty** command.

```

R1>enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

```

```
R1(config)#line vty 0
R1(config-line)#password Pass123
R1(config-line)#login
R1(config-line)#logging synchronous
R1(config-line)#exec-timeout 40
R1(config-line)#motd-banner
R1(config-line)#exit
R1(config)#
R1(config)#enable password Password
R1(config)#exit
```

To test the Telnet connectivity, from a client PC, type **telnet 192.168.10.1** and press **Enter**, then enter the telnet password. Execute the **enable** command and press **Enter**, then type the router password.

```
Packet Tracer PC Command Line 1.0
PC>telnet 192.168.10.1
Trying 192.168.10.1 ...Open
User Access Verification
Password:
R1>enable
Password:
R1#
```

Now you are remotely connected to router R1 and you can execute all router commands through Telnet command line interface.

## Accessing the CLI from a Remote Console

The remote console of the IR8340 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 IR8340 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                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                    | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 2</b> | <b>hostname <i>hostname</i></b><br><br><b>Example:</b><br>Router(config)# <b>hostname <i>your_hostname</i></b>                           | Configures a hostname and IP domain name for your device.<br><br><b>Note</b><br>Follow this procedure only if you are configuring the device as an SSH server.                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <b>ip domain-name <i>domain_name</i></b><br><br><b>Example:</b><br>Router(config)# <b>ip domain-name <i>your_domain_name</i></b>         | Configures a host domain for your device.                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 4</b> | <b>crypto key generate rsa modulus <i>size</i></b><br><br><b>Example:</b><br>Router(config)# <b>crypto key generate rsa modulus 2048</b> | 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.<br><br>We recommend that a minimum modulus size of 2048 bits.<br><br>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.<br><br><b>Note</b> |

|               | Command or Action                                               | Purpose                                                                        |
|---------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------|
|               |                                                                 | Follow this procedure only if you are configuring the device as an SSH server. |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b> | 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

- 
- |               |                                                                                                                                                                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b><code>configure terminal</code></b><br>Enters global configuration mode                                                                                                                                                                                                                       |
| <b>Step 2</b> | <b><code>line console 0</code></b>                                                                                                                                                                                                                                                               |
| <b>Step 3</b> | <b><code>session-timeout <i>minutes</i></code></b><br><br>The value of <i>minutes</i> 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 <i>minutes</i> to disable session timeout. |
| <b>Step 4</b> | <b><code>show line console 0</code></b><br>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

- 
- |               |                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>Router# configure terminal</b><br>Enters global configuration mode.                                                                               |
| <b>Step 2</b> | Enter the line upon which you want to be able to use the <b>lock</b> command.<br><b>Router(config)# line console 0</b>                               |
| <b>Step 3</b> | <b>Router(config)# lockable</b><br>Enables the line to be locked.                                                                                    |
| <b>Step 4</b> | <b>Router(config)# exit</b>                                                                                                                          |
| <b>Step 5</b> | <b>Router# lock</b><br>The system prompts you for a password, which you must enter twice.<br><br>Password: <password><br>Again: <password><br>Locked |
- 

## Communications, services, and additional information

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

## Cisco Bug Search Tool

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

## Documentation feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.



## CHAPTER 2

# Using Cisco IOS XE Software

- [Understanding Command Modes, on page 13](#)
- [Keyboard Shortcuts, on page 15](#)
- [Using the no and default Forms of Commands, on page 15](#)
- [Using the History Buffer to Recall Commands, on page 16](#)
- [Managing Configuration Files, on page 16](#)
- [Saving Configuration Changes, on page 16](#)
- [Filtering Output from the show and more Commands, on page 17](#)
- [Finding Support Information for Platforms and Cisco Software Images, on page 18](#)

## 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 <b>logout</b> command.                                                                                                                                                                                                                                                                                                                                                            |
| Privileged EXEC         | From user EXEC mode, use the <b>enable</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Router#            | To return to user EXEC mode, use the <b>disable</b> command.                                                                                                                                                                                                                                                                                                                              |
| Global configuration    | From privileged EXEC mode, use the <b>configure terminal</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Router(config)#    | To return to privileged EXEC mode from global configuration mode, use the <b>exit</b> or <b>end</b> command.                                                                                                                                                                                                                                                                              |
| Interface configuration | From global configuration mode, specify an interface using an <b>interface</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Router(config-if)# | To return to global configuration mode, use the <b>exit</b> command.<br><br>To return to privileged EXEC mode, use the <b>end</b> command.                                                                                                                                                                                                                                                |
| Diagnostic              | <p>The router boots up or accesses diagnostic mode in the following scenarios:</p> <ul style="list-style-type: none"> <li>• In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload.</li> <li>• A user-configured access policy is configured using the <b>transport-map</b> command that directs a user into diagnostic mode.</li> <li>• A break signal (<b>Ctrl-C</b>, <b>Ctrl-Shift-6</b>, or the <b>send break</b> command) is entered and the router is configured to go to diagnostic mode when the break signal is received.</li> </ul> | Router(diag)#      | <p>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.</p> <p>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.</p> |

| Command Mode | Access Method                                                                                                                                      | Prompt   | Exit Method                                                                                                                 |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------|----------|-----------------------------------------------------------------------------------------------------------------------------|
| ROM monitor  | From privileged EXEC mode, use the <b>reload</b> EXEC command. Press the <b>Break</b> 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                                               |
|---------------------------------------------|-------------------------------------------------------|
| <b>Ctrl-B</b> or the <b>Left Arrow</b> key  | Move the cursor back one character.                   |
| <b>Ctrl-F</b> or the <b>Right Arrow</b> key | Move the cursor forward one character.                |
| <b>Ctrl-A</b>                               | Move the cursor to the beginning of the command line. |
| <b>Ctrl-E</b>                               | Move the cursor to the end of the command line.       |
| <b>Esc B</b>                                | Move the cursor back one word.                        |
| <b>Esc F</b>                                | 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                                                                                                                                        |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ctrl-P</b> or the <b>Up Arrow</b> key <sup>1</sup>   | Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| <b>Ctrl-N</b> or the <b>Down Arrow</b> key <sup>1</sup> | Returns to more recent commands in the history buffer after recalling commands with <b>Ctrl-P</b> or the <b>Up Arrow</b> key.                  |
| Router# <b>show history</b>                             | While in EXEC mode, lists the last few commands you entered.                                                                                   |

<sup>1</sup> 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]?
```

```

Building configuration...
[OK]
Router#
*Sep 8 05:41:03.450: %SYS-6-PRIVCFG_ENCRYPT_SUCCESS: Successfully encrypted private config
file
Router#

```



**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
Cellular0/4/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/4/1 is up (spoofing), line protocol is up (spoofing)
0 unknown protocol drops
Cellular0/5/0 is up, line protocol is up
0 unknown protocol drops
Cellular0/5/1 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                                                                                                                                                       |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>help</code>                                 | Provides a brief description of the help system in any command mode.                                                                                          |
| <code>abbreviated-command-entry?</code>           | Provides a list of commands that begin with a particular character string.<br><br><b>Note</b><br>There is no space between the command and the question mark. |
| <code>abbreviated-command-entry&lt;Tab&gt;</code> | Completes a partial command name.                                                                                                                             |
| <code>?</code>                                    | Lists all the commands that are available for a particular command mode.                                                                                      |

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

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Comment                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router(config-if)# ?<br>Interface configuration commands:<br>.<br>.<br>.<br>ip<br>Protocol<br>keepalive<br>lan-name<br>llc2<br>load-interval<br>calculation<br>locaddr-priority<br>logging<br>interface<br>loopback<br>loopback on an<br>mac-address<br>MAC address<br>mls<br>commands<br>mpoa<br>configuration commands<br>mtu<br>(MTU)<br>netbios<br>access list<br>no<br>its defaults<br>nrzi-encoding<br>encoding<br>ntp<br>.<br>.<br>.<br>Router(config-if)# | Enter ? to display a list of all the interface configuration commands available for the interface. This example shows only some of the available interface configuration commands. |

| Command | Comment                                                                                                                                                                                                                                                                           |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p>Enter the command that you want to configure for the interface. This example uses the <b>ip</b> command.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. This example shows only some of the available interface IP configuration commands.</p> |

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Comment |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| <pre> Router(config-if)# ip ? Interface IP configuration subcommands: access-group Specify access control for packets address Set the IP address of an interface admission Apply Network Admission Control auth-proxy Apply authentication proxy authentication authentication subcommands bandwidth-percent Set EIGRP bandwidth limit bgp BGP interface commands broadcast-address Set the broadcast address of an interface cef Cisco Express Forwarding interface commands cgmp Enable/disable CGMP clear-dont-fragment Enable clear dont fragment (Currently Only SDWAN Tunnel Interface) dampening-change Percent interface metric must change to cause update dampening-interval Time in seconds to check interface metrics ddns Configure dynamic DNS dhcp Configure DHCP parameters for this interface directed-broadcast Enable forwarding of directed broadcasts dlep DLEP interface commands dns Configure DNS server flow NetFlow related commands flowspec FlowSpec configuration header-compression IPHC options hello-interval Configures EIGRP-IPv4 hello interval helper-address Specify a destination address for UDP broadcasts hold-time Configures EIGRP-IPv4 hold time igmp IGMP interface commands information-reply Enable sending ICMP Information Reply messages irdp ICMP Router Discovery Protocol load-sharing Style of load sharing local-proxy-arp Enable local-proxy ARP mask-reply Enable sending ICMP Mask Reply messages mfib Interface Specific MFIB Control mrm Configure IP Multicast Routing Monitor tester mroute-cache Enable switching cache for incoming multicast packets mtu Set IP Maximum Transmission Unit multicast IP multicast interface commands mux Enable IP multiplexing for outgoing packets nat NAT interface commands nbar Network-Based Application Recognition network-broadcast Accept and respond to network-prefix-directed broadcasts next-hop-self Configures EIGRP-IPv4 next-hop-self ospf OSPF interface commands pim PIM interface commands policy Enable policy routing portbundle IP Portbundle configuration </pre> |         |

| Command                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Comment                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| probe Enable HP Probe support<br>proxy-arp Enable proxy ARP<br>rarp-server Enable RARP server for static arp entries<br>reassembly Reassembly<br>redirects Enable sending ICMP Redirect messages<br>rgmp Enable/disable RGMP<br>rip Router Information Protocol<br>route-cache Enable fast-switching cache for outgoing packets<br>router IP router interface commands<br>rsvp RSVP Interface Commands<br>rtp RTP parameters<br>sap Session Advertisement Protocol interface commands<br>sdr Session Directory Protocol interface commands<br>security DDN IP Security Option<br>service IP service<br>split-horizon Perform split horizon<br>sticky-arp Allow the creation of sticky ARP entries<br>subscriber IP session configuration options<br>summary-address Perform address summarization<br>tcp TCP interface commands<br>topology-accounting Enable accounting for IP on all topologies of<br><br>Router(config-if)# <b>ip</b> |                                                                                                                                                                                                                                                                                                                                                                   |
| Router(config-if)# <b>ip address ?</b><br>A.B.C.D IP address<br>dhcp IP Address negotiated via DHCP<br>pool IP Address autoconfigured from a local DHCP pool<br>Router(config-if)# <b>ip address</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <p>Enter the command that you want to configure for the interface. This example uses the <b>ip address</b> command.</p> <p>Enter <b>?</b> to display what you must enter next on the command line.</p> <p>A carriage return (&lt;cr&gt;) is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.</p>                |
| Router(config-if)# <b>ip address 172.16.0.1 ?</b><br>A.B.C.D                      IP subnet mask<br>Router(config-if)# <b>ip address 172.16.0.1</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <p>Enter the keyword or argument that you want to use. This example uses the 172.16.0.1 IP address.</p> <p>Enter <b>?</b> to display what you must enter next on the command line. In this example, you must enter an IP subnet mask.</p> <p>&lt;cr&gt; is not displayed. Therefore, you must enter additional keywords or arguments to complete the command.</p> |

| Command                                                                                                                                                                                               | Comment                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?     secondary          Make this IP address a secondary address &lt;cr&gt; Router(config-if)# ip address 172.16.0.1 255.255.255.0</pre> | <p>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</p> <p>Enter ? to display what you must enter next on the command line. In this example, you can enter the <b>secondary</b> keyword, or you can press <b>Enter</b>.</p> <p>&lt;cr&gt; is displayed. Press <b>Enter</b> to complete the command, or enter another keyword.</p> |
| <pre>Router(config-if)# ip address 172.16.0.1 255.255.255.0 Router(config-if)#</pre>                                                                                                                  | <p>Press <b>Enter</b> to complete the command.</p>                                                                                                                                                                                                                                                                                                             |

## Using Software Advisor

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

## Using Software Release Notes

See the release notes for information about the following:

- 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 3

# Basic Router Configuration

This chapter contains the following sections:

- [IR8340 Interface Naming, on page 25](#)
- [Basic Configuration, on page 26](#)
- [Configuring Global Parameters, on page 31](#)
- [Configuring the Gigabit Ethernet Interface, on page 32](#)
- [Support for sub-interface on GigabitEthernet0/0/0, on page 33](#)
- [Configuring a Loopback Interface, on page 33](#)
- [Configuring CPU Allocation, on page 34](#)
- [Enabling Cisco Discovery Protocol, on page 35](#)
- [Configuring Command-Line Access, on page 35](#)
- [Configuring Static Routes, on page 37](#)
- [Configuring Dynamic Routes, on page 39](#)
- [Modular QoS \(MQC\), on page 40](#)

## IR8340 Interface Naming

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

| Hardware Interface         | Naming Convention    |
|----------------------------|----------------------|
| Gigabit Ethernet WAN ports | GigabitEthernet0/0/0 |
|                            | GigabitEthernet0/0/1 |

| Hardware Interface              | Naming Convention                                                                                                                                                                                                                                                                              |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Gigabit Ethernet LAN ports      | GigabitEthernet0/1/0<br>GigabitEthernet0/1/1<br>GigabitEthernet0/1/2<br>GigabitEthernet0/1/3<br>GigabitEthernet0/1/4<br>GigabitEthernet0/1/5<br>GigabitEthernet0/1/6<br>GigabitEthernet0/1/7<br>GigabitEthernet0/1/8<br>GigabitEthernet0/1/9<br>GigabitEthernet0/1/10<br>GigabitEthernet0/1/11 |
| NIM Interface                   | 0/2/0<br>0/2/1<br>0/3/0<br>0/3/1                                                                                                                                                                                                                                                               |
| Cellular Interface              | cellular 0/4/0<br>cellular 0/4/1<br>cellular 0/5/0<br>cellular 0/5/1                                                                                                                                                                                                                           |
| mSATA SSD                       | msata                                                                                                                                                                                                                                                                                          |
| GPIO (External Alarm Interface) | alarm contact 1-2                                                                                                                                                                                                                                                                              |

## 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:

```
IR8340#show running-config
Building configuration...

Current configuration : 6937 bytes
!
! Last configuration change at 17:35:35 UTC Wed Mar 23 2022
!
version 17.8
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
platform punt-keepalive disable-kernel-core
!
hostname Sumatra-DUT
!
boot-start-marker
boot system flash
0081684787552360_ir8340-universalk9.BLD_V178_THROTTLE_LATEST_20220321_143500_V17_8_0_65.SSA.bin
boot-end-marker
!
!
! card type command needed for slot/bay 0/3
no aaa new-model
!
!
!
!
!
!
!
!
!
!
login on-success log
!
!
!
!
!
!
subscriber templating
!
!
!
!
vtp mode transparent
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
!
crypto pki trustpoint TP-self-signed-829458546
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-829458546
 revocation-check none
 rsakeypair TP-self-signed-829458546
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-829458546
```

```

certificate self-signed 01
3082032E 30820216 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 38323934 35383534 36301E17 0D323230 33323331 37333433
395A170D 33323033 32323137 33343339 5A303031 2E302C06 03550403 1325494F
532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3832 39343538
35343630 82012230 0D06092A 864886F7 0D010101 05000382 010F0030 82010A02
82010100 90B8DF91 C27E2942 0C342B4E 5C7A03C5 91E9ACE7 C29E8D1B 291B8799
3C468901 6B4DA7E9 E4480CC0 B4C2E1D9 918BDBB9 26EB7EE4 E3D7F76B 42FD0642
D29E33DA 01ECAE68 2A7254DE 32163A82 959C75B7 DAA84B34 670B7CA3 F94B0803
A9B11490 A350030D 5DD8178F 1579E30B 8D0B079A 090917F3 60031B68 F961A0CE
9E958239 973E6B08 3D293F10 38136F15 83D8C801 A58D71E4 3CC128AE 8B9BF214
AA4B09E2 CB9841E3 0F455D66 504F89E9 F6B70AC7 1B2C3C48 5ED5679C 121A5415
198D7D0D 0AE444E1 76309174 67FF66E6 BBAFA506 EE10C77D EDD89004 BE72EC05
F960AAC0 F7DD0A3E 7769C277 3529B0CC 06788C4C B0A82D51 F8A74DAB 997D6716
3F0F694B 02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F
0603551D 23041830 16801439 96B67C33 D166686C 2C7A99C0 698D085E B69B0C30
1D060355 1D0E0416 04143996 B67C33D1 66686C2C 7A99C069 8D085EB6 9B0C300D
06092A86 4886F70D 01010505 00038201 01008D8D 7BED46B9 4DDF60D3 01BE178A
D4B97142 9BF6991E 70693302 878693DE 5C39373B FE6D2D77 3B353F2C 21707C5F
67C99A51 E07D5FF6 B59FCDF1 EC6751B0 8DB7ED72 FAD9AED5 7D7F7895 9DA6FAD5
72304A73 869F4013 1559F607 7F8303E2 8E8F1011 525BC32B A32EF28A 7EC811C2
45268BC9 225B65AB 94998717 0BFC0F4F C772233D 7B6635DB AA554FB4 67EC7F7B
258BDD81 855B64A5 6236CE38 58B795D7 FD5096BE 8DA304CF 987450BE 4AD62994
CCC2D3FB 540A8BA5 A8CE6109 4DAB37C4 A692F2C9 02B653F8 7B539BC1 5B338E26
A71F8C43 192521BD F10401D8 0E23D095 1C943214 A01B9E48 40299F2C 35183755
26956737 8CF47405 E7757043 80AA8C93 8B41
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
5FBODA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
80DDCD16 D6BACECA EEB7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
D697DF7F 28
quit
!
!
no license feature hseck9
license udi pid IR8340-K9 sn FDO2523J7GF
memory free low-watermark processor 63132
!
diagnostic bootup level minimal

```

Cisco Catalyst IR8340 Rugged Series Router Software Configuration Guide, Cisco IOS XE Release 17.7.x

```
!
interface GigabitEthernet0/1/8
!
interface GigabitEthernet0/1/9
!
interface GigabitEthernet0/1/10
!
interface GigabitEthernet0/1/11
!
interface Serial0/2/0
!
interface Serial0/2/1
!
interface Serial0/2/2
!
interface Serial0/2/3
!
interface Serial0/2/4
!
interface Serial0/2/5
!
interface Serial0/2/6
!
interface Serial0/2/7
!
interface Cellular0/4/0
no ip address
shutdown
!
interface Cellular0/4/1
no ip address
shutdown
!
interface Cellular0/5/0
no ip address
shutdown
!
interface Cellular0/5/1
no ip address
shutdown
!
interface Vlan1
no ip address
!
ip http server
ip http authentication local
ip http secure-server
ip forward-protocol nd
!
!
!
!
!
control-plane
!
!
!
!
!
line con 0
stopbits 1
line aux 0
```

```

line vty 0 4
 login
 transport input ssh
line vty 5 14
 login
 transport input ssh
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "CiscoTAC-1"
 active
 destination transport-method http
!
!
!
!
!
!
end

```

## Configuring Global Parameters

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

### Procedure

|               | Command or Action                                                                                                                               | Purpose                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>Router&gt; enable Router# configure terminal Router(config)#</pre>                         | Enters global configuration mode when using the console port.<br><br>Use the following to connect to the router with a remote terminal:<br><br><pre>telnet router-name or address Login: login-id Password: ***** Router&gt; enable</pre> |
| <b>Step 2</b> | <b>hostname <i>name</i></b><br><b>Example:</b><br><pre>Router(config)# hostname Router</pre>                                                    | Specifies the name for the router.                                                                                                                                                                                                        |
| <b>Step 3</b> | <b>enable secret <i>password</i> or enable password <i>password</i></b><br><b>Example:</b><br><pre>Router(config)# enable secret password</pre> | Specifies a password to prevent unauthorized access to the router.                                                                                                                                                                        |

# Configuring the Gigabit Ethernet Interface

The router features two Gigabit Ethernet (GE) ports that can be used to enable WAN uplink connectivity:

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



**Note** These ports are combo mode. Either copper or SFP can be used distinctly, but not at the same time for each interface.

To configure the Gigabit Ethernet interface, follow these steps:

## Procedure

|               | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                                       |                                                                                                                                                                                                                                                                                                     |
| <b>Step 2</b> | <b>ipv6 unicast-routing</b><br><br><b>Example:</b><br>Router(config)# <b>ipv6 unicast-routing</b>                               | Enables forwarding of IPv6 unicast data packets.                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>interface GigabitEthernet slot/bay/port</b><br><br><b>Example:</b><br>Router(config)# <b>interface GigabitEthernet 0/0/0</b> | Enters the configuration mode for an interface on the router.                                                                                                                                                                                                                                       |
| <b>Step 4</b> | <b>ip address ip-address mask</b><br><br><b>Example:</b><br>Router(config-if)# <b>ip address 192.168.12.2 255.255.255.0</b>     | Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address.                                                                                                                                                                              |
| <b>Step 5</b> | <b>ipv6 address ipv6-address/prefix</b><br><br><b>Example:</b><br>Router(config-if)# <b>ipv6 address 2001.db8::ffff:1/128</b>   | 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 <a href="#">IPv6 Addressing and Basic Connectivity Configuration Guide</a> . |
| <b>Step 6</b> | <b>no shutdown</b><br><br><b>Example:</b><br>Router(config-if)# <b>no shutdown</b>                                              | Enables the interface and changes its state from administratively down to administratively up.                                                                                                                                                                                                      |

|               | Command or Action                                                     | Purpose                                                                                 |
|---------------|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| <b>Step 7</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-if) # <b>exit</b> | 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                                                                                                                                                                                 |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                                                        |                                                                                                                                                                                         |
| <b>Step 2</b> | <b>interface</b> <i>type number</i><br><br><b>Example:</b><br>Router(config) # <b>interface</b> Loopback 0                                       | Enters configuration mode on the loopback interface.                                                                                                                                    |
| <b>Step 3</b> | (Option 1) <b>ip address</b> <i>ip-address mask</i><br><br><b>Example:</b><br>Router(config-if) # <b>ip address</b> 192.0.2.0 255.255.0.0        | Sets the IP address and subnet mask on the loopback interface. (If you are configuring an IPv6 address, use the <b>ipv6 address</b> <i>ipv6-address/prefix</i> command described below. |
| <b>Step 4</b> | (Option 2) <b>ipv6 address</b> <i>ipv6-address/prefix</i><br><br><b>Example:</b><br>Router(config-if) # <b>ipv6 address</b> 2001:db8::ffff:1/128 | Sets the IPv6 address and prefix on the loopback interface.                                                                                                                             |

|               | Command or Action                                                        | Purpose                                                                                       |
|---------------|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| <b>Step 5</b> | <b>exit</b><br><br><b>Example:</b><br><br>Router(config-if)# <b>exit</b> | 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
```

# Configuring CPU Allocation

You can change allocation of the available 8 cores of the IR8340 router to different functions in a flexible way. The core allocation is based on the customer configuration of the different services.

From Cisco IOS XE Release 17.9 onwards, you can use the **platform resource {control-plane-heavy|data-plane-heavy|service-plane-heavy}** command to adjust the cores across control plane, service plane, and data plane. However, you have to save the configuration and reboot the device for the configured profile to take effect.

```
Router#configure terminal
Router#platform resource ?
 control-plane-heavy Use Control Plane Heavy template
 data-plane-heavy Use Data Plane Heavy template
 service-plane-heavy Use Service Plane Heavy template
```

The following show command output shows the default CPU cores allocation:

```
Router#show platform software cpu alloc
CPU alloc information:
Control plane cpu alloc: 0
Data plane cpu alloc: 4-7
Service plane cpu alloc: 1-3
Slow control plane cpu alloc: 1-3
Template used: default-service_plane_heavy
```

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

```
Router#show platform software cpu alloc
CPU alloc information:
Control plane cpu alloc: 0
Data plane cpu alloc: 4-7
Service plane cpu alloc: 1-3
Slow control plane cpu alloc: 1-3
Template used: CLI-service_plane_heavy
```

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

```
Router#show platform software cpu alloc
CPU alloc information:
Control plane cpu alloc: 0
Data plane cpu alloc: 4-7
Service plane cpu alloc: 2-3
Slow control plane cpu alloc: 1-3
Template used: CLI-control_plane_heavy
```

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

```
Router#show platform software cpu alloc
CPU alloc information:
Control plane cpu alloc: 0
Data plane cpu alloc: 2-7
Service plane cpu alloc: 1
Slow control plane cpu alloc: 1-2
Template used: CLI-data_plane_heavy
```

## 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                                                                                                                                                                                                                                                                                                                |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>line</b> [aux   console   tty   vty] <i>line-number</i><br><b>Example:</b><br>Router(config)# <b>line console 0</b>                            | Enters line configuration mode, and specifies the type of line.<br><br>The example provided here specifies a console terminal for access.                                                                                                                                                                              |
| <b>Step 2</b> | <b>password</b> <i>password</i><br><b>Example:</b><br>Router(config-line)# <b>password userpass</b>                                               | Specifies a unique password for the console terminal line.                                                                                                                                                                                                                                                             |
| <b>Step 3</b> | <b>login</b><br><b>Example:</b><br>Router(config-line)# <b>login</b>                                                                              | Enables password checking at terminal session login.                                                                                                                                                                                                                                                                   |
| <b>Step 4</b> | <b>exec-timeout</b> <i>minutes</i> [ <i>seconds</i> ]<br><b>Example:</b><br>Router(config-line)# <b>exec-timeout 5 30</b><br>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.<br><br>The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of <b>0 0</b> specifies never to time out. |
| <b>Step 5</b> | <b>exit</b><br><b>Example:</b><br>Router(config-line)# <b>exit</b>                                                                                | Exits line configuration mode to re-enter global configuration mode.                                                                                                                                                                                                                                                   |
| <b>Step 6</b> | <b>line</b> [aux   console   tty   vty] <i>line-number</i><br><b>Example:</b><br>Router(config)# <b>line vty 0 4</b><br>Router(config-line)#      | Specifies a virtual terminal for remote console access.                                                                                                                                                                                                                                                                |
| <b>Step 7</b> | <b>end</b><br><b>Example:</b><br>Router(config-line)# <b>end</b>                                                                                  | 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                                                                                                                                                                                                                                                                                                                                                    |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | (Option 1) <b>ip route</b> <i>prefix mask {ip-address   interface-type interface-number [ip-address]}</i><br><br><b>Example:</b><br><br>Router(config)# <b>ip route</b> 192.10.2.3 255.255.0.0 10.10.10.2     | Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the <b>ipv6 route</b> command described below.)                                                                                                                                                                                                                  |
| <b>Step 2</b> | (Option 2) <b>ipv6 route</b> <i>prefix/mask {ipv6-address   interface-type interface-number [ipv6-address]}</i><br><br><b>Example:</b><br><br>Router(config)# <b>ipv6 route</b> 2001:db8:2::/64 2001:db8:3::0 | Specifies a static route for the IP packets. See additional information for IPv6 here: <a href="https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ipv6b-xe-16-10-book/read-me-first.html">https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ipv6b-xe-16-10-book/read-me-first.html</a> |
| <b>Step 3</b> | (Option 3) <b>ip route vrf</b> <i>vrf-name ip-address</i>                                                                                                                                                     | Configure IP router vrf.                                                                                                                                                                                                                                                                                                                                   |

|               | Command or Action                                                   | Purpose                                                          |
|---------------|---------------------------------------------------------------------|------------------------------------------------------------------|
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br><br>Router(config)# <b>end</b> | 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 layer 3 adjacent device.

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, GigabitEthernet0/0/0
```

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-17/series.html>

## Configuring Routing Information Protocol

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

### Procedure

|               | Command or Action                                                                                                                                            | Purpose                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>router rip</b><br><br><b>Example:</b><br><br>Router(config)# <b>router rip</b>                                                                            | Enters router configuration mode, and enables RIP on the router.                                                                                                   |
| <b>Step 2</b> | <b>version {1   2}</b><br><br><b>Example:</b><br><br>Router(config-router)# <b>version 2</b>                                                                 | Specifies use of RIP version 1 or 2.                                                                                                                               |
| <b>Step 3</b> | <b>network ip-address</b><br><br><b>Example:</b><br><br>Router(config-router)# <b>network 192.168.1.1</b><br>Router(config-router)# <b>network 10.10.7.1</b> | Specifies a list of networks on which RIP is to be applied, using the address of the network of each directly connected network.                                   |
| <b>Step 4</b> | <b>no auto-summary</b><br><br><b>Example:</b><br><br>Router(config-router)# <b>no auto-summary</b>                                                           | Disables automatic summarization of subnet routes into network-level routes. This allows subprefix routing information to pass across classful network boundaries. |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b><br><br>Router(config-router)# <b>end</b>                                                                                   | 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/xr-16-10/ire-xr-16-10-book/ire-enhanced-igrp.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/xr-16-10/ire-xr-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 4

# Configuring Secure Shell

This section contains the following topics:

- [Information About Secure Shell](#) , on page 41
- [How to Configure Secure Shell](#), on page 43
- [Information about Secure Copy](#), on page 47
- [Additional References](#), on page 49

## 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 IR8340 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 IR8340 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 IR8340 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                                                                                                                                                        |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                            | Enters global configuration mode.                                                                                                                              |
| <b>Step 2</b> | <b>hostname <i>hostname</i></b><br><br><b>Example:</b><br>Router(config)# <b>hostname <i>your_hostname</i></b>                   | Configures a hostname and IP domain name for your device.<br><br><b>Note</b><br>Follow this procedure only if you are configuring the device as an SSH server. |
| <b>Step 3</b> | <b>ip domain-name <i>domain_name</i></b><br><br><b>Example:</b><br>Router(config)# <b>ip domain-name <i>your_domain_name</i></b> | Configures a host domain for your device.                                                                                                                      |

|               | Command or Action                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | <b>crypto key generate rsa modulus <i>size</i></b><br><b>Example:</b><br><pre>Router(config)# crypto key generate rsa modulus 2048</pre> | <p>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.</p> <p>We recommend that a minimum modulus size of 2048 bits.</p> <p>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.</p> <p><b>Note</b><br/>Follow this procedure only if you are configuring the device as an SSH server.</p> |
| <b>Step 5</b> | <b>end</b><br><b>Example:</b><br><pre>Router(config)# end</pre>                                                                          | 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                                                                                                                                                                                                                                                                                              |
|---------------|---------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>IR8340# configure terminal</pre>       | Enters global configuration mode.                                                                                                                                                                                                                                                                    |
| <b>Step 2</b> | <b>ip ssh version [2]</b><br><b>Example:</b><br><pre>IR8340(config)# ip ssh version 2</pre> | <p>(Optional) Configures the device to run SSH Version 2.</p> <p>If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.</p> |

|               | Command or Action                                                                                                                                                                                                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <p><b>ip ssh {timeout <i>seconds</i>   authentication-retries <i>number</i>}</b></p> <p><b>Example:</b></p> <pre>IR8340(config)# ip ssh timeout 90 ip ssh authentication-retries 2</pre>                                                                                                                                    | <p>Configures the SSH control parameters:</p> <ul style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.</li> </ul> <p>Repeat this step when configuring both parameters.</p> |
| <b>Step 4</b> | <p>Use one or both of the following:</p> <ul style="list-style-type: none"> <li><b>line vty <i>line_number</i> [<i>ending line number</i>]</b></li> <li><b>transport input ssh</b></li> </ul> <p><b>Example:</b></p> <pre>IR8340(config)# line vty 1 10</pre> <p>or</p> <pre>IR8340(config-line)# transport input ssh</pre> | <p>(Optional) Configures the virtual terminal line settings.</p> <ul style="list-style-type: none"> <li>Enters line configuration mode to configure the virtual terminal line settings. For the <i>line_number</i> and <i>ending_line_number</i> arguments, the range is from 0 to 15.</li> <li>Specifies that the device prevents non-SSH Telnet connections, limiting the device to only SSH connections.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 5</b> | <p><b>end</b></p> <p><b>Example:</b></p> <pre>IR8340(config-line)# end</pre>                                                                                                                                                                                                                                                | <p>Exits line configuration mode and returns to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## 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                                                                                                                                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br><code>IR8340# configure terminal</code>                                                 | Enters global configuration mode.                                                                                                                  |
| <b>Step 2</b> | <b>aaa new-model</b><br><br><b>Example:</b><br><code>IR8340(config)# aaa new-model</code>                                                   | Enables AAA                                                                                                                                        |
| <b>Step 3</b> | <b>aaa authentication login default local</b><br><br><b>Example:</b><br><code>IR8340(config)# aaa authentication login default local</code> | Sets the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports. |
| <b>Step 4</b> | <b>line vty line-number</b><br><br><b>Example:</b><br><code>IR8340(config)# line vty 0 4</code><br><code>IR8340(config-line)#</code>        |                                                                                                                                                    |

|               | Command or Action                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b> | <b>aaa authorization exec default local</b><br><b>Example:</b><br><pre>IR8340(config-line)# aaa authorization exec default local</pre>                                                                            | Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 6</b> | <b>aaa authorization network local</b><br><b>Example:</b><br><pre>IR8340(config-line)# aaa authorization network local</pre>                                                                                      | Configures user AAA authorization for all network-related service requests.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 7</b> | <b>username <i>name</i> privilege <i>level</i> password <i>encryption-type</i> <i>password</i></b><br><b>Example:</b><br><pre>IR8340(config-line)# username your_user_name privilege 1 password 7 secret567</pre> | <p>Enters the local database, and establishes a username-based authentication system.</p> <p>Repeat this command for each user.</p> <ol style="list-style-type: none"> <li>For <i>name</i>, specify the user ID as one word. Spaces and quotation marks are not allowed.</li> <li>(Optional) For <i>level</i>, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.</li> <li>For <i>encryption-type</i>, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.</li> <li>For <i>password</i>, specify the password the user must enter to gain access to the switch. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the username command.</li> </ol> |
| <b>Step 8</b> | <b>end</b><br><b>Example:</b><br><pre>IR8340(config-line)# end</pre>                                                                                                                                              | 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 IR8340 for Secure Copy (SCP) server-side functionality, perform the following steps.

### Procedure

|               | Command or Action                                                            | Purpose                                                                                                            |
|---------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Device> enable                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Device# configure terminal   | Enters global configuration mode.                                                                                  |
| <b>Step 3</b> | <b>aaa new-model</b><br><b>Example:</b><br>Device(config)# aaa new-model     | Sets AAA authentication at login.                                                                                  |
| <b>Step 4</b> | <b>aaa authentication login {default   list-name} method1 [ method2... ]</b> | Enables the AAA access control system.                                                                             |

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

**Example**

```
scp://your_username@remotehost:/some/remote/directory/file flash:
```

## 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: <a href="https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf">https://www.cisco.com/en/US/docs/ios-xml/ios/san/configuration/xe-3se/3850/san-xe-3se-3850-book.pdf</a> |

| Related Topic                                              | Document Title                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuring RADIUS, TACACS+, Secure Shell, 802.1X and AAA. | Secure Shell Configuration Guide, Cisco IOS XE Gibraltar 16.11.x:<br><a href="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">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</a> |



## CHAPTER 5

# Installing the Software

---

This chapter contains the following sections:

- [Installing the Software, on page 51](#)
- [Installing the Cisco IOS XE Release, on page 52](#)
- [ROMMON Images, on page 53](#)
- [File Systems, on page 53](#)
- [Option to Enable or Disable USB Access, on page 54](#)
- [Autogenerated File Directories and Files, on page 55](#)
- [Flash Storage, on page 56](#)
- [Related Documentation, on page 56](#)

## 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.

The IR8340 uses Enhanced Smart Licensing, which is discussed in detail in [Smart Licensing Using Policy \(SLP\), on page 65](#).

## 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 IR8340. 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 IR8340 router:

- Network-Essentials
- Network-Advantage
- HSEC license



---

**Note** Details of the Network-Essentials and Network-Advantage contents can be found in the IR8340 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
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

Router#show running-config | i license
no license feature hseck9
license udi pid IR8340-K9 sn FDO2523J6N1
license boot level network-advantage
Router#

Router#reload
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
Proceed with reload? [confirm]
Sep 8 10:28:36.135: %PMAN-5-EXITACTION: R0/0: pvp: Process manager is exiting: process exit
with reload chassis code

Initializing Hardware ...
Disable swap drive feature. Skip swap drive checking !!

System Bootstrap, Version v0.33, DEVELOPMENT SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.
Compiled Mon Jul 12 22:57:23 2021 by gilchen

Current image running : Boot ROM1

Last reset cause (0x00000002): LocalSoft
IR8340-K9 platform with 8388608 Kbytes of main memory

.....
```

## 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 IR8340 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.                            |
| null:       | Directory or Filename                                                        |
| nvrn:       | Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM. |
| sdcard:     | SD card file system.                                                         |
| system:     | System memory file system, which includes the running configuration.         |
| tar:        | Archive file system.                                                         |
| tmpsys:     | Temporary system files file system.                                          |
| usb:        | USB file system.                                                             |
| webui:      | Web UI file system.                                                          |

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

## Option to Enable or Disable USB Access

USB flash drives offer inexpensive and easy storage space for the routers to store the images, configuration files and other files.



**Note** The IR8340 does not support ext3, ext4, and above for USB flash drives.

The IR8340 supports hot plug/unplug of USB flash drives. To access the USB flash drive, insert the device into router's USB interface.

While hot plug/unplug of a USB flash drive is supported, the functionality comes with security vulnerabilities. To prevent users from copying sensitive information to the USB flash drive, USB enable/disable functionality has been added.

By default, the USB flash drive is enabled. If you want to disable USB, use the following disable command:

```
Router#config terminal
Router(config)#platform usb disable
Router(config)#end
```

Once the USB flash drive has been disabled, the file system is not shown on the device and syslog messages will not be displayed when the USB is inserted. You will not be able to access the contents of the USB.

The USB is enabled by issuing a 'no' with the disable command:

```
Router#config terminal
Router(config)#no platform usb disable
Router(config)#end
```

The USB status can be displayed using the following command:

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

## 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.<br><br>These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router.                                                                                                 |
| core directory      | The storage area for .core files.<br><br>If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.                                                                                                                                        |
| managed directory   | This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router.                                                                                                                                                                                                                                                  |
| tracelogs directory | The storage area for trace files.<br><br>Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure.<br><br>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 [Smart Licensing Using Policy \(SLP\)](#), on page 65.

For further information on obtaining and installing feature licenses, see [Configuring the Cisco IOS Software Activation Feature](#).



## CHAPTER 6

# Software Maintenance Upgrade (SMU)

- [Software Maintenance Upgrade \(SMU\), on page 57](#)
- [SMU Workflow and Basic Requirements, on page 58](#)
- [SMU Example, on page 58](#)
- [Installing a Patch Image, on page 58](#)
- [Uninstalling the Patch Image, on page 60](#)

## 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 `ir8340-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
sdcard:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bininstall_add: START
Wed Aug 11 17:05:59 UTC 2021
Copying sdcard:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin to
```

```
bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
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 Wed Aug 11 17:06:22 UTC 2021
```

```
Router#
```

### Step 3 Activate the patch image.

```
Router# install activate file
bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bininstall_activate:
 START Thu Aug 6 11:53:59 PDT 2020
install_activate: START Wed Aug 11 17:06:35 UTC 2021
```

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

```
Building configuration...
[OK]Modified configuration has been saved
install_activate: Activating SMU
```

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

### Step 4 Commit the installation.

```
Router# install commitinstall_commit: START Wed Aug 11 17:12:40 UTC 2021
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
/bootflash/ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin Wed Aug 11
17:13:24 UTC 2021
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

SMU C bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
```

```
IMG C 17.07.01.0.139972
```

```

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
```

```

SMU C bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
```

```
IMG C 17.07.01.0.139972
```

```

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 scripts 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/ir8300-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

SMU C bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
IMG C 17.07.01.0.139972

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.

## Uninstalling the Patch Image Using Deactivate, Commit, and Remove

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 bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
IMG C 17.07.01.0.139972

Auto abort timer: inactive

```

### Procedure

#### Step 1 Deactivate the patch.

```
Router# install deactivate file
bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
install_deactivate: START Wed Aug 11 17:14:35 UTC 2021

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

Building configuration...
[OK]Modified configuration has been saved
install_deactivate: Deactivating SMU

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

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 D bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
IMG C 17.07.01.0.139972

```

```
Auto abort timer: active on install_deactivate, time before rollback - 01:55:21

```

## Step 2 Commit the action.

```
Router# install commit
install_commit: START Wed Aug 11 17:21:23 UTC 2021
install_commit: Committing SMU
Executing pre scripts....
Executing pre scripts 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
/bootflash/ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin Wed Aug 11
17:21:53 UTC 2021
```

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 I bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin
IMG C 17.07.01.0.139972

Auto abort timer: inactive

```

## Step 3 Remove the patch.

```
Router# install remove file
bootflash:ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bininstall_remove:
START Wed Aug 11 17:22:03 UTC 2021
install_remove: Removing SMU
Executing pre scripts....
Executing pre scripts done.

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

SUCCESS: install_remove
/bootflash/ir8340-universalk9.2021-06-14_14.55_suraiyer.0.cold.SSA.smu.bin Wed Aug 11
17:22:20 UTC 2021
```

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 17.07.01.0.139972

```

```
Auto abort timer: inactive

```

---



## CHAPTER 7

# Smart Licensing Using Policy (SLP)

---

- [Smart Licensing Using Policy](#), on page 65

## Smart Licensing Using Policy

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





## CHAPTER 8

# Configuring Ethernet Switch Ports

- [Configuring VLANs, on page 67](#)
- [IEEE 802.1x Protocol, on page 71](#)
- [Spanning Tree Protocol Overview, on page 74](#)
- [MAC Table Manipulation, on page 83](#)
- [Assigning IP Addresses to Switch Virtual Interfaces, on page 86](#)
- [SVI Supported Features, on page 86](#)
- [IGMP Snooping for IPv4, on page 88](#)
- [MLD Snooping, on page 88](#)
- [Configuring UniDirectional Link Detection, on page 91](#)
- [Configuring the Switched Port Analyzer, on page 92](#)
- [EtherChannel Overview, on page 106](#)
- [Modular Quality of Service Command-Line Interface, on page 113](#)

## Configuring VLANs

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

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

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

### Access Ports

An access port belongs to and carries the traffic of only one VLAN (unless it is configured as a voice VLAN port). Traffic is received and sent in native formats with no VLAN tagging. Traffic arriving on an access port

is assumed to belong to the VLAN assigned to the port. If an access port receives a tagged packet (IEEE 802.1Q tagged), the packet is dropped, and the source address is not learned.

### Trunk Ports

A trunk port carries the traffic of multiple VLANs and by default is a member of all VLANs in the VLAN database. These trunk port types are supported:

- An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic. An IEEE 802.1Q trunk port is assigned a default port VLAN ID (PVID), and all untagged traffic travels on the port default PVID. All untagged traffic and tagged traffic with a NULL VLAN ID are assumed to belong to the port default PVID. A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Although by default, a trunk port is a member of every VLAN known to the VTP, you can limit VLAN membership by configuring an allowed list of VLANs for each trunk port. The list of allowed VLANs does not affect any other port but the associated trunk port. By default, all possible VLANs (VLAN ID 1 to 4094) are in the allowed list. A trunk port can become a member of a VLAN only if VTP knows of the VLAN and if the VLAN is in the enabled state. If VTP learns of a new, enabled VLAN and the VLAN is in the allowed list for a trunk port, the trunk port automatically becomes a member of that VLAN and traffic is forwarded to and from the trunk port for that VLAN. If VTP learns of a new, enabled VLAN that is not in the allowed list for a trunk port, the port does not become a member of the VLAN, and no traffic for the VLAN is forwarded to or from the port.

For more information on VLANs, see [VLAN Configuration Guide, Cisco IOS XE Gibraltar 16.10.x](#).

## Creating a VLAN

With VTP version 1 and 2, if the device is in VTP transparent mode, you can assign VLAN IDs greater than 1006, but they are not added to the VLAN database.

To configure the Vlan, perform these steps. You can configure the Vlan in access or trunk mode. The procedure is same for the both the modes.

### Procedure

|               | Command or Action                                                                     | Purpose                                                                                                                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b> | Enter global configuration mode.                                                                                                                                                                                               |
| <b>Step 2</b> | <b>vlan <i>vlan-id</i></b><br><br><b>Example:</b><br>Router(config)# <b>vlan 20</b>   | Enters a VLAN ID, and enters VLAN configuration mode. Enter a new VLAN ID to create a VLAN, or enter an existing VLAN ID to modify that VLAN.<br><br><b>Note</b><br>The available VLAN ID range for this command is 1 to 4094. |

|               | Command or Action                                                                                                       | Purpose                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>name</b> <i>vlan-name</i><br><b>Example:</b><br>Router(config-vlan) # <b>name test20</b>                             | (Optional) Enters a name for the VLAN. If no name is entered for the VLAN, the default is to append the <i>vlan-id</i> value with leading zeros to the word VLAN. For example, VLAN0004 is a default VLAN name for VLAN 4.        |
| <b>Step 4</b> | <b>exit</b><br><b>Example:</b><br>Router(config-vlan) # <b>exit</b>                                                     | Returns to configuration mode.                                                                                                                                                                                                    |
| <b>Step 5</b> | <b>interface</b> <i>interface-id</i><br><b>Example:</b><br>Router(config) # <b>interface gigabitethernet 0/1/0</b>      | Specifies the physical port to be configured, and enter interface configuration mode.                                                                                                                                             |
| <b>Step 6</b> | <b>switchport mode access</b><br><b>Example:</b><br>Router(config-if) # <b>switchport mode access</b>                   | Configures the interface as a VLAN access port.                                                                                                                                                                                   |
| <b>Step 7</b> | <b>switchport access vlan</b> <i>vlan id</i><br><b>Example:</b><br>Router(config-if) # <b>switchport access vlan 20</b> | Specifies the VLAN for which this access port will carry traffic. If you do not enter this command, the access port carries traffic on VLAN1 only; use this command to change the VLAN for which the access port carries traffic. |
| <b>Step 8</b> | <b>end</b><br><b>Example:</b><br>Router(config-if) # <b>end</b>                                                         | Returns to configuration mode.                                                                                                                                                                                                    |

## Configuring LAN Ports for Layer 2 Switching

This section describes how configure all three types of ethernet LAN ports for Layer 2 switching on the Cisco IR8340 routers. The configuration tasks in this section apply to LAN ports on the router.

### Layer 2 LAN Port Modes

The following table lists the Layer 2 LAN port modes and describes how they function on LAN ports.

**Table 8: Layer 2 LAN Port Modes**

| Mode                          | Function                                                                                                                                                                                                       |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>switchport mode access</b> | Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change. |

| Mode                                     | Function                                                                                                                                                                                                                                            |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>switchport mode dynamic desirable</b> | Makes the LAN port actively attempt to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to <b>trunk</b> , <b>desirable</b> , or <b>auto</b> mode. This is the default mode for all LAN ports. |
| <b>switchport mode dynamic auto</b>      | Makes the LAN port willing to convert the link to a trunk link. The LAN port becomes a trunk port if the neighboring LAN port is set to <b>trunk</b> or <b>desirable</b> mode.                                                                      |
| <b>switchport mode trunk</b>             | Puts the LAN port into permanent trunking mode and negotiates to convert the link into a trunk link. The LAN port becomes a trunk port even if the neighboring port does not agree to the change.                                                   |
| <b>switchport nonegotiate</b>            | Puts the LAN port into permanent trunking mode but prevents the port from generating DTP frames. You must configure the neighboring port manually as a trunk port to establish a trunk link.                                                        |



**Note** DTP is a point-to-point protocol. However, some internetworking devices might forward DTP frames improperly. To avoid this problem, ensure that LAN ports connected to devices that do not support DTP are configured with the **access** keyword if you do not intend to trunk across those links. To enable trunking to a device that does not support DTP, use the **nonegotiate** keyword to cause the LAN port to become a trunk but not generate DTP frames.

## Default Layer 2 LAN Interface Configuration

The following table shows the Layer 2 LAN port default configuration.

**Table 9: Layer 2 LAN Interface Default Configuration**

| Feature                                         | Default                                  |
|-------------------------------------------------|------------------------------------------|
| Interface mode:                                 |                                          |
| • Before entering the <b>switchport</b> command |                                          |
| • After entering the <b>switchport</b> command  | <b>switchport mode dynamic desirable</b> |
| Default access VLAN                             | VLAN 1                                   |
| Native VLAN (for 802.1Q trunks)                 | VLAN 1                                   |

## Configuring LAN Interfaces for Layer 2 Switching

These sections describe how to configure Layer 2 switching on the Cisco IR8340 routers:



**Note** Use the default **default interface** *interface -type slot/subslot/port* command to revert an interface to its default configuration.

## IEEE 802.1x Protocol

The IEEE 802.1x standard defines a client/server-based access control and authentication protocol that prevents clients from connecting to a LAN through publicly accessible ports unless they are authenticated. The authentication server authenticates each client connected to a port before making available any services offered by the router or the LAN.

Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic can pass through the port. For more information on IEEE 802.1x port-based authentication, see the [Configuring IEEE 802.1x Port-Based Authentication](#) chapter of the *Security Configuration Guide, Cisco IOS XE Gibraltar 16.10.x*.

## Configuring IEEE 802.1X Port-Based Authentication

IEEE 802.1X port-based authentication is configured on a device to prevent unauthorized devices (supplicants) from gaining access to the network. The device can combine the function of a router, switch, and access point, depending on the fixed configuration or installed modules. The switch functions are provided by either built-in switch ports or a plug-in module with switch ports. This feature supports both access ports and trunk ports. For more information on 802.1X port-based authentication, see the [Configuring IEEE 802.1X Port-Based Authentication Guide](#).

## Enabling AAA Authorization for VLAN Assignment

AAA authorization limits the services available to a user. When AAA authorization is enabled, the device uses information retrieved from the user's profile, which is in the local user database or on the security server, to configure the user's session. The user is granted access to a requested service only if the information in the user profile allows it.

### Procedure

|               | Command or Action                                             | Purpose                                                                                                          |
|---------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b> | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |

|               | Command or Action                                                                                                                                                 | Purpose                                                                                                                                                    |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br><code>Router# configure terminal</code>                                                                       | Enter global configuration mode.                                                                                                                           |
| <b>Step 3</b> | <b>aaa new-model</b><br><br><b>Example:</b><br><code>Router(config)# aaa new-model</code>                                                                         | Enables AAA.                                                                                                                                               |
| <b>Step 4</b> | <b>aaa authorization network radius if-authenticated</b><br><br><b>Example:</b><br><code>Router(config)# aaa authorization network radius if-authenticated</code> | Configures the device for user RADIUS authorization for all network-related service requests. RADIUS authorization succeeds if the user has authenticated. |
| <b>Step 5</b> | <b>aaa authorization exec radius if-authenticated</b><br><br><b>Example:</b><br><code>Router(config)# aaa authorization exec radius if-authenticated</code>       | Configures the device for user RADIUS authorization if the user has privileged EXEC access. RADIUS authorization succeeds if the user has authenticated.   |
| <b>Step 6</b> | <b>end</b><br><br><b>Example:</b><br><code>Router(config)# end</code>                                                                                             | Returns to privileged EXEC mode.                                                                                                                           |

## Enabling IEEE 802.1X Authentication and Authorization

Follow these steps to enable IEEE 802.1X authentication and authorization.

### Procedure

|               | Command or Action                                                                                                                                                              | Purpose                                                                                                                                                                             |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                                                                                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                                             |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br><code>Router# configure terminal</code>                                                                                    | Enter global configuration mode.                                                                                                                                                    |
| <b>Step 3</b> | <b>aaa authentication dot1x {default   listname} method1 [method2...]</b><br><br><b>Example:</b><br><code>Router(config)# aaa authentication dot1x default group radius</code> | Creates a series of authentication methods that are used to determine user privilege to access the privileged command level so that the device can communicate with the AAA server. |

|               | Command or Action                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 4</b> | <b>dot1x system-auth-control</b><br><b>Example:</b><br><pre>Router(config)# dot1x system-auth-control</pre>                                                            | Globally enables 802.1X port-based authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 5</b> | <b>identity profile default</b><br><b>Example:</b><br><pre>Router(config)# identity profile default</pre>                                                              | Creates an identity profile and enters dot1x profile configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 6</b> | <b>exit</b><br><b>Example:</b><br><pre>Router(config-identity-prof)# exit</pre>                                                                                        | Exits dot1x profile configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 7</b> | <b>interface type slot/port</b><br><b>Example:</b><br><pre>Router(config)# interface GigabitEthernet 0/1/0</pre>                                                       | Enters interface configuration mode and specifies the interface to be enabled for 802.1X authentication.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Step 8</b> | <b>access-session port-control {auto   force-authorized   force-unauthorized}</b><br><b>Example:</b><br><pre>Router(config-if)# access-session port-control auto</pre> | <p>Enables 802.1X port-based authentication on the interface.</p> <ul style="list-style-type: none"> <li>• <b>auto</b> —Enables IEEE 802.1X authentication and causes the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes from down to up or when an EAPOL-start frame is received. The Device requests the identity of the supplicant and begins relaying authentication messages between the supplicant and the authentication server. Each supplicant attempting to access the network is uniquely identified by the Device by using the supplicant MAC address.</li> <li>• <b>force-authorized</b> —Disables IEEE 802.1X authentication and causes the port to change to the authorized state without any authentication exchange required. The port sends and receives normal traffic without IEEE 802.1X-based authentication of the client. This is the default setting.</li> <li>• <b>force-unauthorized</b> —Causes the port to remain in the unauthorized state,</li> </ul> |

|                | Command or Action                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                  | ignoring all attempts by the supplicant to authenticate. The Device cannot provide authentication services to the supplicant through the port.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 9</b>  | <b>dot1x pae</b> [supplicant   authenticator   both]<br><br><b>Example:</b><br>Device(config-if)# <b>dot1x pae authenticator</b> | Sets the Port Access Entity (PAE) type. <ul style="list-style-type: none"> <li>• <b>supplicant</b> —The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.</li> <li>• <b>authenticator</b> —The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.</li> <li>• <b>both</b> —The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages.</li> </ul> |
| <b>Step 10</b> | <b>end</b><br><br><b>Example:</b><br>router(config)# <b>end</b>                                                                  | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 11</b> | <b>show dot1x</b><br><br><b>Example:</b><br>Router# <b>show dot1x</b>                                                            | Displays whether 802.1X authentication has been configured on the device.                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## Spanning Tree Protocol Overview

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

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

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

The device that has *all* of its ports as the designated role or as the backup role is the root device. The device that has at least *one* of its ports in the designated role is called the designated device.

Spanning tree forces redundant data paths into a standby (blocked) state. If a network segment in the spanning tree fails and a redundant path exists, the spanning-tree algorithm recalculates the spanning-tree topology and activates the standby path. Devices send and receive spanning-tree frames, called bridge protocol data units (BPDUs), at regular intervals. The device does not forward these frames but uses them to construct a loop-free path. BPDUs contain information about the sending device and its ports, including device and MAC addresses, device priority, port priority, and path cost. Spanning tree uses this information to elect the root device and root port for the switched network and the root port and designated port for each switched segment.

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



**Note** By default, the device sends keepalive messages (to ensure the connection is up) only on interfaces that do not have small form-factor pluggable (SFP) modules. You can change the default for an interface by entering the **[no] keepalive** interface configuration command with no keywords.

IR8340 uses STP (the IEEE 802.1D bridge protocol) on all VLANs. By default, a single instance of STP runs on each configured VLAN (provided you do not manually disable STP). You can enable and disable STP on a per-VLAN basis.

For more information on STP, see the **Configuring Spanning Tree Protocol** chapter of the Layer 2 Configuration Guide.

## Default STP Configuration

The following table shows the default STP configuration.

**Table 10: STP Default Configuration**

| Feature                                                                                                       | Default Value                |
|---------------------------------------------------------------------------------------------------------------|------------------------------|
| Disable state                                                                                                 | STP disabled for all VLANs   |
| Bridge priority                                                                                               | 32768                        |
| STP port priority (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)     | 128                          |
| STP port cost (configurable on a per-port basis—used on LAN ports configured as Layer 2 access ports)         | Gigabit Ethernet: 4          |
| STP VLAN port priority (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports) | 128                          |
| STP VLAN port cost (configurable on a per-VLAN basis—used on LAN ports configured as Layer 2 trunk ports)     | Gigabit Ethernet: 1000000000 |

| Feature            | Default Value |
|--------------------|---------------|
| Hello time         | 2 seconds     |
| Forward delay time | 15 seconds    |
| Maximum aging time | 20 seconds    |
| Mode               | PVST          |

## Enabling STP



**Note** STP is disabled by default on all VLANs.

You can enable STP on a per-VLAN basis. The Cisco SM-X-16G4M2X or SM-X-40G8M2X Layer 2 Gigabit EtherSwitch Service Module maintain a separate instance of STP for each VLAN (except on VLANs on which you disable STP).

If you want to enable a mode that is different from the default mode, this procedure is required.

### Procedure

|               | Command or Action                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                 |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                    | Enter global configuration mode.                                                                                                                                                                                                                                                                        |
| <b>Step 2</b> | <b>spanning-tree mode {pvst   mst   rapid-pvst}</b>                                                                                      | Configures a spanning-tree mode.<br><br>All stack members run the same version of spanning tree.<br><br><ul style="list-style-type: none"> <li>• Select <b>pvst</b> to enable PVST+.</li> <li>• Select <b>mst</b> to enable MSTP.</li> <li>• Select <b>rapid-pvst</b> to enable rapid PVST+.</li> </ul> |
| <b>Step 3</b> | <b>interface interface-id</b>                                                                                                            | Specifies an interface to configure, and enters interface configuration mode. Valid interfaces include physical ports, VLANs, and port channels. The VLAN ID range is 1 to 4094. The port-channel range is 1 to 48.                                                                                     |
| <b>Step 4</b> | <b>spanning-tree link-type point-to-point</b><br><br><b>Example:</b><br>Device(config-if)# <b>spanning-tree link-type point-to-point</b> | Specifies that the link type for this port is point-to-point.<br><br>If you connect this port (local port) to a remote port through a point-to-point link and the local port becomes a designated port, the negotiates                                                                                  |

|               | Command or Action                                                                                                             | Purpose                                                                                                                                                                                                                                                            |
|---------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                               | with the remote port and rapidly changes the local port to the forwarding state.                                                                                                                                                                                   |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                               | Returns to privileged EXEC mode.                                                                                                                                                                                                                                   |
| <b>Step 6</b> | <b>clear spanning-tree detected-protocols</b><br><br><b>Example:</b><br>Router# <b>clear spanning-tree detected-protocols</b> | If any port on the device is connected to a port on a legacy IEEE 802.1D device, this command restarts the protocol migration process on the entire device.<br><br>This step is optional if the designated device detects that this device is running rapid PVST+. |
| <b>Step 7</b> | <b>show spanning-tree vlan <i>vlan_ID</i></b>                                                                                 | Verifies that STP is enabled.                                                                                                                                                                                                                                      |

### What to do next



#### Caution

Do not disable spanning tree on a VLAN unless all switches and bridges in the VLAN have spanning tree disabled. You cannot disable spanning tree on some switches and bridges in a VLAN and leave it enabled on other switches and bridges in the VLAN. This action can have unexpected results because switches and bridges with spanning tree enabled will have incomplete information regarding the physical topology of the network.



#### Caution

We do not recommend disabling spanning tree, even in a topology that is free of physical loops. Spanning tree serves as a safeguard against misconfigurations and cabling errors. Do not disable spanning tree in a VLAN without ensuring that there are no physical loops present in the VLAN.

This example shows how to enable STP on VLAN 200:

```
Device# configure terminal
Device(config)# spanning-tree vlan 200
Device(config)# end
Device#
```



#### Note

STP is disabled by default.

This example shows how to verify the configuration:

```
Device# show spanning-tree vlan 200

G0:VLAN0200
Spanning tree enabled protocol ieee
Root ID Priority 32768
Address 00d0.00b8.14c8
This bridge is the root
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
```

```

Bridge ID Priority 32768
 Address 00d0.00b8.14c8
 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
 Aging Time 300
Interface Role Sts Cost Prio.Nbr Status

Gi1/4 Desg FWD 200000 128.196 P2p
Gi1/5 Back BLK 200000 128.197 P2p
Device#

```

You must have at least one interface that is active in VLAN 200 to create a VLAN 200 spanning tree. In this example, two interfaces are active in VLAN 200.

## Configuring Optional STP Features

This section describes how to configure the following optional STP features:

### Enabling PortFast



**Caution** Use PortFast *only* when connecting a single end station to a Layer 2 access port. Otherwise, you might create a network loop.

To enable PortFast on a Layer 2 access port, perform this task:

#### Procedure

|               | Command or Action                                        | Purpose                                                                                |
|---------------|----------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface</b> {type slot/port}        | Selects a port to configure.                                                           |
| <b>Step 2</b> | Router(config-if)# <b>spanning-tree portfast</b>         | Enables PortFast on a Layer 2 access port connected to a single workstation or server. |
| <b>Step 3</b> | Router(config-if)# <b>spanning-tree portfast default</b> | Enables PortFast.                                                                      |
| <b>Step 4</b> | Router(config-if)# <b>end</b>                            | Exits configuration mode.                                                              |
| <b>Step 5</b> | Router# <b>show running interface</b> {type slot/port}   | Verifies the configuration.                                                            |

### Configuring PortFast BPDU Filtering

These sections describe how to configure PortFast BPDU filtering.

To enable PortFast BPDU filtering globally, perform this task:

## Procedure

|               | Command or Action                                                                                                                           | Purpose                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>Step 1</b> | <b>spanning-tree portfast bpdufilter default</b><br><br><b>Example:</b><br>Router(config)# <b>spanning-tree portfast bpdufilter default</b> | Enables BPDU filtering globally on the router. |
| <b>Step 2</b> | <b>show spanning-tree summary totals</b><br><br><b>Example:</b><br>Router(config)# <b>show spanning-tree summary totals</b>                 | Verifies the configuration.                    |

## Enabling PortFast BPDU Filtering

BPDU filtering is set to default on each port. This example shows how to enable PortFast BPDU filtering on the port and verify the configuration in PVST+ mode:

```
Router(config)# spanning-tree portfast bpdufilter default
```

```
Router(config)# ^Z
```

```
Router# show spanning-tree summary totals
```

```
Switch is in pvst mode
Root bridge for: G0:VLAN0013, G0:VLAN0020, G1:VLAN0020
EtherChannel misconfig guard is enabled
Extended system ID is enabled
Portfast Default is disabled
PortFast BPDU Guard Default is disabled
Portfast BPDU Filter Default is disabled
Loopguard Default is disabled
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is short
Name Blocking Listening Learning Forwarding STP Active

3 vlans 0 0 0 3 3
```

To enable PortFast BPDU filtering on a nontrunking port, perform this task:

## Procedure

|               | Command or Action                                                                                                          | Purpose                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| <b>Step 1</b> | <b>interface <i>interface-id</i></b><br><br><b>Example:</b><br>Router(config)# <b>interface gigabitethernet 0/1/0</b>      | Selects the interface to configure. |
| <b>Step 2</b> | <b>spanning-tree bpdufilter enable</b><br><br><b>Example:</b><br>Router(config-if)# <b>spanning-tree bpdufilter enable</b> | Enables BPDU filtering.             |

|               | Command or Action                                                                                                                                   | Purpose                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <b>Step 3</b> | <b>show spanning-tree interface <i>interface-id</i></b><br><br><b>Example:</b><br>Router# <b>show spanning-tree interface gigabitethernet 0/1/0</b> | Verifies the configuration. |

### What to do next

This example shows how to enable PortFast BPDU filtering on a nontrunking port:

```
Router(config)# interface gigabitethernet 0/1/0
Router(config-if)# spanning-tree bpdufilter enable

Router(config-if)# ^Z
Router# show spanning-tree interface gigabitethernet 0/1/0
Vlan Role Sts Cost Prio.Nbr Status

VLAN0010 Desg FWD 1000 160.196 Edge P2p
Router# show spanning-tree interface gigabitethernet 0/1/0 detail

Port 196 (gigabitethernet 0/1/0) of VLAN0010 is forwarding
 Port path cost 1000, Port priority 160, Port Identifier 160.196.
 Designated root has priority 32768, address 00d0.00b8.140a
 Designated bridge has priority 32768, address 00d0.00b8.140a
 Designated port id is 160.196, designated path cost 0
 Timers:message age 0, forward delay 0, hold 0
 Number of transitions to forwarding state:1
 The port is in the portfast mode by portfast trunk configuration
 Link type is point-to-point by default
 Bpdu filter is enabled
 BPDU:sent 0, received 0
Router#
```

## Enabling BPDU Guard

To enable BPDU Guard globally, perform this task:

### Procedure

|               | Command or Action                                                                                                                            | Purpose                                                           |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| <b>Step 1</b> | <b>spanning-tree portfast bpduguard default</b><br><br><b>Example:</b><br>Router(config)# <b>no spanning-tree portfast bpduguard default</b> | Enables BPDU Guard globally.<br><br>Disables BPDU Guard globally. |
| <b>Step 2</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                                              | Exits configuration mode.                                         |
| <b>Step 3</b> | <b>show spanning-tree summary totals</b><br><br><b>Example:</b><br>Router# <b>show spanning-tree summary totals</b>                          | Verifies the configuration.                                       |

### What to do next

This example shows how to enable BPDU Guard:

```
Router# configure terminal
Router(config)# spanning-tree portfast bpduguard
Router(config)# end
Router#
```

This example shows how to verify the configuration:

```
Router# show spanning-tree summary totals
 default
Root bridge for:VLAN0010
EtherChannel misconfiguration guard is enabled
Extended system ID is disabled
Portfast is enabled by default
PortFast BPDU Guard is disabled by default
Portfast BPDU Filter is enabled by default
Loopguard is disabled by default
UplinkFast is disabled
BackboneFast is disabled
Pathcost method used is long
Name Blocking Listening Learning Forwarding STP Active

2 vlans 0 0 0 3 3
Router#
```

## Enabling UplinkFast

UplinkFast increases the bridge priority to 49152 and adds 3000 to the STP port cost of all Layer 2 LAN interfaces on the device, decreasing the probability that the router will become the root bridge. The *max\_update\_rate* value represents the number of multicast packets transmitted per second (the default is 150 packets per second). UplinkFast cannot be enabled on VLANs that have been configured for bridge priority. To enable UplinkFast on a VLAN with bridge priority configured, restore the bridge priority on the VLAN to the default value by entering a **no spanning-tree vlan *vlan\_ID* priority** command in global configuration mode.



**Note** When you enable UplinkFast, it affects all VLANs on the device. You cannot configure UplinkFast on an individual VLAN.

To enable UplinkFast, perform this task:

### Procedure

|               | Command or Action                                                                                    | Purpose                      |
|---------------|------------------------------------------------------------------------------------------------------|------------------------------|
| <b>Step 1</b> | Router(config)# <b>spanning-tree uplinkfast</b><br>[ <b>max-update-rate</b> <i>max_update_rate</i> ] | Enables UplinkFast.          |
| <b>Step 2</b> | Router(config)# <b>no spanning-tree uplinkfast</b><br><b>max-update-rate</b>                         | Reverts to the default rate. |
| <b>Step 3</b> | Router(config)# <b>no spanning-tree uplinkfast</b>                                                   | Disables UplinkFast.         |
| <b>Step 4</b> | Router(config)# <b>end</b>                                                                           | Exits configuration mode.    |

|               | Command or Action                                     | Purpose                              |
|---------------|-------------------------------------------------------|--------------------------------------|
| <b>Step 5</b> | Router# <b>show spanning-tree vlan <i>vlan_ID</i></b> | Verifies that UplinkFast is enabled. |

### What to do next

This example shows how to enable UplinkFast with an update rate of 400 packets per second:

```
Router# configure terminal
Router(config)# spanning-tree uplinkfast max-update-rate 400
Router(config)# exit
Router#
```

This example shows how to verify that UplinkFast is enabled:

```
Router# show spanning-tree uplinkfast

UplinkFast is enabled
Router#
```

## Enabling BackboneFast



**Note** BackboneFast operates correctly only when enabled on all network devices in the network. BackboneFast is not supported on Token Ring VLANs. This feature is supported for use with third-party network devices.

To enable BackboneFast, perform this task:

### Procedure

|               | Command or Action                                     | Purpose                                |
|---------------|-------------------------------------------------------|----------------------------------------|
| <b>Step 1</b> | Router(config)# <b>spanning-tree backbonefast</b>     | Enables backbonefast.                  |
| <b>Step 2</b> | Router(config)# <b>no spanning-tree backbonefast</b>  | Disables BackboneFast.                 |
| <b>Step 3</b> | Router(config)# <b>end</b>                            | Exits configuration mode.              |
| <b>Step 4</b> | Router# <b>show spanning-tree vlan <i>vlan_ID</i></b> | Verifies that BackboneFast is enabled. |

### What to do next

This example shows how to enable BackboneFast:

```
Router# configure terminal
Router(config)# spanning-tree backbonefast
Router(config)# end
Router#
```

This example shows how to verify that BackboneFast is enabled:

```
Router# show spanning-tree backbonefast

BackboneFast is enabled
BackboneFast statistics

```

```

Number of transition via backboneFast (all VLANs) : 0
Number of inferior BPDUs received (all VLANs) : 0
Number of RLQ request PDUs received (all VLANs) : 0
Number of RLQ response PDUs received (all VLANs) : 0
Number of RLQ request PDUs sent (all VLANs) : 0
Number of RLQ response PDUs sent (all VLANs) : 0
Router#

```

## MAC Table Manipulation

This section includes the following:

### Creating a Static Entry in the MAC Address Table

Perform the following task to create a static entry in the MAC address table.

#### Procedure

|               | Command or Action                                                                                                                                                                                                           | Purpose                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                                                               | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                                       | Enter global configuration mode.                                        |
| <b>Step 3</b> | <b>mac address-table static mac-address vlan<br/>vlan-id interface Interface-id</b><br><br><b>Example:</b><br>Router(config)# <b>mac address-table static<br/>00ff.ff0d.2dc0 vlan 1 interface<br/>gigabitethernet 0/1/0</b> | Creates a static entry in the MAC address table.                        |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                                                                                                                             | Returns to privileged EXEC mode.                                        |
| <b>Step 5</b> | <b>show mac address-table</b><br><br><b>Example:</b><br>Router# <b>show mac address-table</b>                                                                                                                               | Verifies the MAC address table.                                         |

### MAC Address-Based Traffic Blocking

Perform the following task to block all traffic to or from a MAC address in a specified VLAN.

## Procedure

|               | Command or Action                                                                                                                                                    | Purpose                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><code>Router&gt; enable</code>                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><code>Router# configure terminal</code>                                                                              | Enter global configuration mode.                                                                                   |
| <b>Step 3</b> | <b>mac address-table static mac-address vlan vlan-id drop</b><br><b>Example:</b><br><code>Router(config)# mac address-table static 00ff.ff0d.2dc0 vlan 1 drop</code> | Creates a static entry with drop action in the MAC address table.                                                  |
| <b>Step 4</b> | <b>end</b><br><b>Example:</b><br><code>router(config)# end</code>                                                                                                    | Returns to privileged EXEC mode.                                                                                   |
| <b>Step 5</b> | <b>show mac address-table</b><br><b>Example:</b><br><code>Router# show mac address-table</code>                                                                      | Verifies the MAC address table.                                                                                    |

## Configuring and Verifying the Aging Timer

Perform this task to configure the aging timer.

## Procedure

|               | Command or Action                                                                                                            | Purpose                                                                                                                                                                                      |
|---------------|------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><code>Router&gt; enable</code>                                                           | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                           |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><code>Router# configure terminal</code>                                      | Enter global configuration mode.                                                                                                                                                             |
| <b>Step 3</b> | <b>mac address-table aging-time time</b><br><b>Example:</b><br><code>Router(config)# mac address-table aging-time 600</code> | Configures the MAC address aging timer age in seconds. <ul style="list-style-type: none"> <li>• The accept value is either 0 or 10-1000000 seconds. Default value is 300 seconds.</li> </ul> |

|               | Command or Action                                                                                                   | Purpose                                                                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Or<br>Router(config)# <b>mac address-table aging-time 0</b>                                                         | <ul style="list-style-type: none"> <li>The maximum aging timer supported by switch chipset is 634 seconds. If configure greater than 634 seconds, MAC address will age out after 634 seconds.</li> <li>The value 0 means dynamic MAC entries will never age out.</li> </ul> |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br>router(config)# <b>end</b>                                                     | Returns to privileged EXEC mode.                                                                                                                                                                                                                                            |
| <b>Step 5</b> | <b>show mac address-table aging-time</b><br><br><b>Example:</b><br>Router# <b>show mac address-table aging-time</b> | Verifies the MAC address table.                                                                                                                                                                                                                                             |

## MAC Learning on a Vlan

To disable or enable MAC learning on specified vlan, perform these steps.

### Procedure

|               | Command or Action                                                                                                                                                                 | Purpose                                                                                                          |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                             | Enter global configuration mode.                                                                                 |
| <b>Step 3</b> | <b>mac address-table learning vlan <i>vlan-id</i></b><br><b>interface <i>Interface-id</i></b><br><br><b>Example:</b><br>Router(config)# <b>mac address-table learning vlan 10</b> | Creates a static entry in the MAC address table.                                                                 |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br>router(config)# <b>end</b>                                                                                                                   | Returns to privileged EXEC mode.                                                                                 |

## Assigning IP Addresses to Switch Virtual Interfaces

To configure IP routing, you need to assign IP addresses to Layer 3 network interfaces. This enables communication with the hosts on those interfaces that use IP. IP routing is disabled by default, and no IP addresses are assigned to Switch Virtual Interfaces (SVIs).

An IP address identifies a destination for IP packets. Some IP addresses are reserved for special uses and cannot be used for host, subnet, or network addresses. RFC 1166, "Internet Numbers," contains the official description of these IP addresses.

An interface can have one primary IP address. A subnet mask identifies the bits that denote the network number in an IP address.

Beginning in privileged EXEC mode, follow these steps to assign an IP address and a network mask to an SVI.

### Procedure

|               | Command or Action                                                                                                                                            | Purpose                                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                                                                    | Enter global configuration mode.                                               |
| <b>Step 2</b> | <b>interface vlan</b> <i>vlan-id</i>                                                                                                                         | Enter interface configuration mode, and specify the Layer 3 VLAN to configure. |
| <b>Step 3</b> | <b>ip address</b> <i>ip-address subnet-mask</i>                                                                                                              | Configure the IP address and IP subnet mask.                                   |
| <b>Step 4</b> | <b>end</b>                                                                                                                                                   | Returns to privileged EXEC mode.                                               |
| <b>Step 5</b> | <b>show interfaces</b> [ <i>interface-id</i> ] <b>show ip interface</b> [ <i>interface-id</i> ] <b>show running-config interface</b> [ <i>interface-id</i> ] | Verify your entries.                                                           |
| <b>Step 6</b> | <b>copy running-config startup-config</b>                                                                                                                    | (Optional) Save your entries in the configuration file.                        |

## SVI Supported Features

The following table provided the supported features on the SVI.

Table 11: SVI Supported Features

| Technology | Feature                            | Use Case                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing    | Routing Protocol                   | Interconnects Layer 3 networks using protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol, and Enhanced Interior Gateway Routing Protocol (EIGRP) configured under SVI.<br><br>For more information on routing protocol, see the <a href="#">IP Routing: Protocol-Independent Configuration Guide</a> .                                                                                                                                                                                                               |
|            | Hot Standby Router Protocol (HSRP) | Supports redundancy and high availability with a secondary device connected to the LAN with SVI, using HSRP.<br><br>For more information on HSRP, see the <a href="#">First Hop Redundancy Protocols Configuration Guide</a> .                                                                                                                                                                                                                                                                                                                                  |
|            | DHCP                               | Cisco devices running Cisco software include Dynamic Host Configuration Protocol (DHCP) server and the relay agent software. The Cisco IOS DHCP server is a full DHCP server implementation that assigns and manages IP addresses from specified address pools within the device to DHCP clients. The DHCP server can be configured to assign additional parameters such as the IP address of the Domain Name System (DNS) server and the default device.<br><br>For more information on HSRP, see the, <a href="#">IP Addressing: DHCP Configuration Guide</a> |
|            | Multicast (IPv4)                   | Provides multicast support for clients connected to the switch ports.<br><br>For more information on HSRP, see the, <a href="#">IP Multicast: PIM Configuration Guide</a>                                                                                                                                                                                                                                                                                                                                                                                       |
|            | VRF                                | Associates a VRF instance with an SVI to map VLANs to different logical or physical VPN WAN connections.<br><br>For more information on VRF protocol, see the <a href="#">IP Routing: Protocol-Independent Configuration Guide</a> .                                                                                                                                                                                                                                                                                                                            |
| Security   | ACL                                | Provides packet filtering to control network traffic and restrict the access of users and devices to the network<br><br>For more information on ACL protocol, see the <a href="#">Security Configuration Guide: Access Control Lists</a> .                                                                                                                                                                                                                                                                                                                      |
|            | NAT                                | Provides NAT under SVI.<br><br>For more information on NAT, see the <a href="#">IP Addressing: NAT Configuration Guide</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Techology | Feature                                               | Use Case                                                                                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Qos       | Classification with standard and extended access list | Provides QoS classification with standard and extended access lists.<br><br>For more information on QoS, see the <a href="#">Security Configuration Guide: Access Control Lists</a> .                                                                                                |
|           | Class-based marking                                   | Provides QoS marking based on user-defined traffic class with DSCP and IP precedence values.<br><br>For more information on QoS Marking, see the <a href="#">QoS: Classification Configuration Guide</a> .                                                                           |
|           | Policing                                              | Limits the input or output transmission rate on SVI and specifies traffic handling policies when the traffic either conforms to or exceeds the specified rate limits.<br><br>For more information on Policing, see the <a href="#">QoS: Policing and Shaping Configuration Guide</a> |
| Bridging  | EVC under SVI                                         | Supports a default encapsulation EFP under SVI, to have VLAN/BD integrated.                                                                                                                                                                                                          |
|           | EVC with MAC ACL under SVI                            | For more information on EVC, see <i>Layer 2 Configuration Guide, Cisco IOS XE Gibraltar 16.11</i> .                                                                                                                                                                                  |

## IGMP Snooping for IPv4

IGMP snooping allows switches to examine IGMP packets and make forwarding decisions based on their content. You can configure the switch to use IGMP snooping in subnets that receive IGMP queries from either IGMP or the IGMP snooping querier. IGMP snooping constrains IPv4 multicast traffic at Layer 2 by configuring Layer 2 LAN ports dynamically to forward IPv4 multicast traffic only to those ports that want to receive it.

Layer 2 switches can use IGMP snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. As the name implies, IGMP snooping requires the LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients. For more information on this feature, see [https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600\\_15\\_0s\\_book/snooigmp.html](https://www.cisco.com/c/en/us/td/docs/routers/7600/ios/15S/configuration/guide/7600_15_0s_book/snooigmp.html).

## MLD Snooping

In IP Version 4 (IPv4), Layer 2 switches can use Internet Group Management Protocol (IGMP) snooping to limit the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded to only those interfaces associated with IP multicast devices. In IPv6, MLD snooping performs a similar function. With MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that

want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets.

MLD is a protocol used by IPv6 multicast routers to discover the presence of multicast listeners (nodes wishing to receive IPv6 multicast packets) on the links that are directly attached to the routers and to discover which multicast packets are of interest to neighboring nodes. MLD is derived from IGMP; MLD Version 1 (MLDv1) is equivalent to IGMPv2, and MLD Version 2 (MLDv2) is equivalent to IGMPv3. MLD is a subprotocol of Internet Control Message Protocol Version 6 (ICMPv6), and MLD messages are a subset of ICMPv6 messages, identified in IPv6 packets by a preceding Next Header value of 58.

## MLD Snooping Configuration Guidelines

When configuring MLD snooping, consider these guidelines:

- You can configure MLD snooping characteristics at any time, but you must globally enable MLD snooping by using the **ipv6 mld snooping** global configuration command for the configuration to take effect.
- MLD snooping and IGMP snooping act independently of each other. You can enable both features at the same time on the switch.

## Default MLD Snooping Configuration

*Table 12: Default MLD Snooping Configuration*

| Feature                          | Default Setting                                                                                                                                      |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| MLD snooping (Global)            | Disabled.                                                                                                                                            |
| MLD snooping (per VLAN)          | Enabled. MLD snooping must be globally enabled for VLAN MLD snooping to take place.                                                                  |
| IPv6 Multicast addresses         | None configured.                                                                                                                                     |
| IPv6 Multicast router ports      | None configured.                                                                                                                                     |
| MLD snooping Immediate Leave     | Disabled.                                                                                                                                            |
| MLD snooping robustness variable | Global: 2; Per VLAN: 0.<br><br><b>Note</b><br>The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count. |
| <b>Note</b>                      | The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.                                               |
| Last listener query count        | Global: 2; Per VLAN: 0.<br><br><b>Note</b><br>The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count. |

| Feature                      | Default Setting                                                                                                                                                   |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Note</b>                  | The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global count.                                                            |
| Last listener query interval | Global: 1000 (1 second); VLAN: 0.<br><br><b>Note</b><br>The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global interval. |
| <b>Note</b>                  | The VLAN value overrides the global setting. When the VLAN value is 0, the VLAN uses the global interval.                                                         |
| TCN query solicit            | Disabled.                                                                                                                                                         |
| TCN query count              | 2                                                                                                                                                                 |
| MLD listener suppression     |                                                                                                                                                                   |

## Enabling or Disabling MLD Snooping on a VLAN

To enable MLD snooping on a VLAN, perform this procedure:

### Procedure

|               | Command or Action                                                                                                      | Purpose                                                                                                                                                                         |
|---------------|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                          | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                                         |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                  | Enter global configuration mode.                                                                                                                                                |
| <b>Step 3</b> | <b>ipv6 mld snooping</b><br><br><b>Example:</b><br>Router(config)# <b>ipv6 mld snooping</b>                            | Enables MLD snooping on the switch.                                                                                                                                             |
| <b>Step 4</b> | <b>ipv6 mld snooping vlan <i>vlan-id</i></b><br><br><b>Example:</b><br>Device(config)# <b>ipv6 mld snooping vlan 1</b> | Enables MLD snooping on the VLAN. The VLAN ID range is 1 to 1001 and 1006 to 4094.<br><br><b>Note</b><br>MLD snooping must be globally enabled for VLAN snooping to be enabled. |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b>                                                                                      | Returns to privileged EXEC mode.                                                                                                                                                |

|  | Command or Action          | Purpose |
|--|----------------------------|---------|
|  | Router(config)# <b>end</b> |         |

## Configuring UniDirectional Link Detection

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it disables the affected port and alerts you. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

### Enabling UDLD Globally

Follow these steps to enable UDLD in the aggressive or normal mode and to set the configurable message timer on all fiber-optic ports on the device.

#### Procedure

|               | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 2</b> | <b>udld {aggressive   enable   message time message-timer-interval}</b><br><br><b>Example:</b><br>Router(config)# <b>udld enable message time 10</b> | Specifies the UDLD mode of operation: <ul style="list-style-type: none"> <li>• <b>aggressive</b> —Enables UDLD in aggressive mode on all fiber-optic ports.</li> <li>• <b>enable</b> —Enables UDLD in normal mode on all fiber-optic ports on the . UDLD is disabled by default.<br/><br/>An individual interface configuration overrides the setting of the <b>udld enable</b> global configuration command.</li> <li>• <b>message time message-timer-interval</b> —Configures the period of time between UDLD probe messages on ports that are in the advertisement phase and are detected to be bidirectional. The range is from 1 to 90 seconds; the default value is 15.</li> </ul> <p><b>Note</b><br/>This command affects fiber-optic ports only. Use the <b>udld</b> interface configuration command to enable UDLD on other port types.</p> |

|               | Command or Action                                               | Purpose                                                  |
|---------------|-----------------------------------------------------------------|----------------------------------------------------------|
|               |                                                                 | Use the <b>no</b> form of this command, to disable UDLD. |
| <b>Step 3</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b> | Returns to privileged EXEC mode.                         |

## Enabling UDLD on an Interface

Follow these steps either to enable UDLD in the aggressive or normal mode or to disable UDLD on a port.

### Procedure

|               | Command or Action                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                           | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 2</b> | <b>interface <i>interface-id</i></b><br><br><b>Example:</b><br>Router(config)# <b>interface gigabitethernet</b><br><b>0/1/0</b> | Specifies the port to be enabled for UDLD, and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                 |
| <b>Step 3</b> | <b>udld port [aggressive]</b><br><br><b>Example:</b><br>Router(config-if)# <b>udld port aggressive</b>                          | UDLD is disabled by default. <ul style="list-style-type: none"> <li>• <b>udld port</b> —Enables UDLD in normal mode on the specified port.</li> <li>• <b>udld port aggressive</b> —(Optional) Enables UDLD in aggressive mode on the specified port.</li> </ul> <p><b>Note</b><br/>Use the <b>no udld port</b> interface configuration command to disable UDLD on a specified fiber-optic port.</p> |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br>Router(config-if)# <b>end</b>                                                              | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring the Switched Port Analyzer

This section describes how to configure a Switched Port Analyzer (SPAN) session.

- IR8340 can support 66 SPAN sessions in all ports. However, only eight of them can be used as source sessions which includes local SPAN sessions and remote SPAN source sessions. The remaining sessions can be used as remote SPAN destination sessions.
- The session ID range is from 1 to 66.



**Note** Tx, Rx, or both Tx and Rx monitoring is supported.

## SPAN and RSPAN

You can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the device or on another device that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports or VLANs. You must dedicate the destination port for SPAN use. Destination ports do not receive or forward traffic by default. It can receive or forward traffic when ingress-forwarding is enabled on the destination ports.

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

You can use the SPAN or RSPAN destination port to inject traffic from a network security device. For example, if you connect a Cisco Intrusion Detection System (IDS) sensor appliance to a destination port, the IDS device can send TCP reset packets to close down the TCP session of a suspected attacker.

## Creating a Local SPAN Session

Follow these steps to create a SPAN session and specify the source (monitored) ports or VLANs and the destination (monitoring) ports.

### Procedure

|               | Command or Action                                                                                                  | Purpose                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><code>Router&gt; enable</code>                                                 | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                            |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><code>Router# configure terminal</code>                            | Enter global configuration mode.                                                                                                                                 |
| <b>Step 3</b> | <b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }<br><b>Example:</b> | Removes any existing SPAN configuration for the session.<br><ul style="list-style-type: none"> <li>• For <i>session_number</i>, the range is 1 to 66.</li> </ul> |

|               | Command or Action                                                                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <code>Router(config)# no monitor session all</code>                                                                                                                                                                                                                                            | <ul style="list-style-type: none"> <li>• <b>all</b> —Removes all SPAN sessions.</li> <li>• <b>local</b> —Removes all local sessions.</li> <li>• <b>remote</b> —Removes all remote SPAN sessions.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 4</b> | <p><b>monitor session</b> <i>session_number</i> <b>source</b> {<b>interface</b> <i>interface-id</i>   <b>vlan</b> <i>vlan-id</i>} [,   -] [<b>both</b>   <b>rx</b>   <b>tx</b>]</p> <p><b>Example:</b></p> <pre>Router(config)# monitor session 1 source interface gigabitethernet 0/1/0</pre> | <p>Specifies the SPAN session and the source port/Vlan (monitored port).</p> <ul style="list-style-type: none"> <li>• For <i>session_number</i> , the range is 1 to 66.</li> <li>• For <i>interface-id</i> , specify the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (<b>port-channel</b> <i>port-channel-number</i> ). Valid port-channel numbers are 1 to 32.</li> <li>• For <i>vlan-id</i> , specify the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).</li> </ul> <p><b>Note</b><br/>A single session can include multiple sources (ports or VLANs) defined in a series of commands, but you cannot combine source ports and source VLANs in one session.</p> <ul style="list-style-type: none"> <li>• (Optional) [,   -] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</li> <li>• (Optional) <b>both</b>   <b>rx</b>   <b>tx</b> —Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. <ul style="list-style-type: none"> <li>• <b>both</b> —Monitors both received and sent traffic.</li> <li>• <b>rx</b> —Monitors received traffic.</li> <li>• <b>tx</b> —Monitors sent traffic.</li> </ul> </li> </ul> <p><b>Note</b><br/>You can use the <b>monitor session</b> <i>session_number</i> <b>source</b> command multiple times to configure multiple source ports.</p> |

|               | Command or Action                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b> | <p><b>monitor session</b> <i>session_number</i> <b>destination</b> {<b>interface</b> <i>interface-id</i> [,   -] [<b>encapsulation</b> {<b>replicate</b>   <b>dot1q</b>}]}</p> <p><b>Example:</b></p> <pre>Router(config)# monitor session 1 destination interface gigabitethernet 0/1/0 encapsulation replicate</pre> | <p><b>Note</b></p> <p>For local SPAN, you must use the same session number for the source and destination interfaces.</p> <ul style="list-style-type: none"> <li>• For <i>session_number</i>, specify the session number entered in step 4.</li> <li>• (Optional) [,   -] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</li> </ul> <p>(Optional) <b>encapsulation replicate</b> specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).</p> <p>(Optional) <b>encapsulation dot1q</b> specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation.</p> <p><b>Note</b></p> <p>You can use <b>monitor session</b> <i>session_number</i> <b>destination</b> command multiple times to configure multiple destination ports.</p> |
| <b>Step 6</b> | <p><b>end</b></p> <p><b>Example:</b></p> <pre>Router(config)# end</pre>                                                                                                                                                                                                                                                | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 7</b> | <p><b>show running-config</b></p> <p><b>Example:</b></p> <pre>Router# show running-config</pre>                                                                                                                                                                                                                        | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 8</b> | <p><b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>Router# copy running-config startup-config</pre>                                                                                                                                                                                          | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Creating a Local SPAN with Incoming Traffic Allowed on Destination

Follow these steps to create a SPAN session, to specify the source ports or VLANs and the destination ports, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

## Procedure

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><pre>Router&gt; enable</pre>                                                                                                                                                                                                                                                                                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>Router# configure terminal</pre>                                                                                                                                                                                                                                                                                | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>no monitor session</b> <i>{session_number   all   local   remote}</i><br><b>Example:</b><br><pre>Router(config)# no monitor session all</pre>                                                                                                                                                                                                                     | Removes any existing SPAN configuration for the session. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, the range is 1 to 66.</li> <li>• <b>all</b> —Removes all SPAN sessions.</li> <li>• <b>local</b> —Removes all local sessions.</li> <li>• <b>remote</b> —Removes all remote SPAN sessions.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 4</b> | <b>monitor session</b> <i>session_number</i> <b>source</b> <i>{interface interface-id   vlan vlan-id}</i> [,   -] <i>[both   rx   tx]</i><br><b>Example:</b><br><pre>Router(config)# monitor session 2 source gigabitethernet 0/1/0 rx</pre>                                                                                                                         | Specifies the SPAN session and the source port (monitored port).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 5</b> | <b>monitor session</b> <i>session_number</i> <b>destination</b> <i>{interface interface-id [,   -] [encapsulation {replicate} [ingress {dot1q vlan vlan-id   untagged vlan vlan-id   vlan vlan-id}]}</i><br><b>Example:</b><br><pre>Router(config)# monitor session 2 destination interface gigabitethernet 0/1/0 encapsulation replicate ingress dot1q vlan 6</pre> | Specifies the SPAN session, the destination port, the packet encapsulation, and the ingress VLAN and encapsulation. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, specify the session number entered in Step 4.</li> <li>• For <i>interface-id</i>, specify the destination port. The destination interface must be a physical port or port-channel; it cannot be an EtherChannel, and it cannot be a VLAN.</li> <li>• (Optional) [,   -] —Specifies a series or range of interfaces. Enter a space before and after the comma or hyphen.</li> <li>• (Optional) <b>encapsulation replicate</b> specifies that the destination interface replicates the source interface encapsulation method. If not selected, the</li> </ul> |

|               | Command or Action                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                   | <p>default is to send packets in native form (untagged).</p> <ul style="list-style-type: none"> <li>• (Optional) <b>encapsulation dot1q</b> specifies that the destination interface accepts the source interface incoming packets with IEEE 802.1Q encapsulation.</li> <li>• <b>ingress</b> enables forwarding of incoming traffic on the destination port and to specify the encapsulation type: <ul style="list-style-type: none"> <li>• <b>dot1q vlan</b> vlan-id— Accepts incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.</li> <li>• <b>untagged vlan</b> vlan-id or <b>vlan</b> vlan-id— Accepts incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.</li> </ul> </li> </ul> |
| <b>Step 6</b> | <b>end</b><br><b>Example:</b><br>Router(config)# <b>end</b>                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 7</b> | <b>show running-config</b><br><b>Example:</b><br>Router# <b>show running-config</b>                               | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 8</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br>Router# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Specifying VLANs to Filter

Follow these steps to limit SPAN source traffic to specific VLANs.

### Procedure

|               | Command or Action                                         | Purpose                                                                                                                   |
|---------------|-----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Router> <b>enable</b> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |

|               | Command or Action                                                                                                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                                                                                                                 | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 3</b> | <b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }<br><br><b>Example:</b><br>Router(config)# <b>no monitor session all</b>                                                                                                                               | Removes any existing SPAN configuration for the session. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, the range is 1 to 66.</li> <li>• <b>all</b> —Removes all SPAN sessions.</li> <li>• <b>local</b> —Removes all local sessions.</li> <li>• <b>remote</b> —Removes all remote SPAN sessions.</li> </ul>                                                                                                                                                                        |
| <b>Step 4</b> | <b>monitor session</b> <i>session_number</i> <b>source</b> { <b>interface</b> <i>interface-id</i> }<br><br><b>Example:</b><br>Router(config)# <b>monitor session 2 source interface gigabitethernet 0/1/0 rx</b>                                                                                      | Specifies the characteristics of the source port (monitored port) and SPAN session. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, the range is 1 to 66.</li> <li>• For <i>interface-id</i>, specify the source port to monitor. The interface specified must already be configured as a trunk port.</li> </ul>                                                                                                                                                                    |
| <b>Step 5</b> | <b>monitor session</b> <i>session_number</i> <b>filter vlan</b> <i>vlan-id</i> [,   -]<br><br><b>Example:</b><br>Router(config)# <b>monitor session 2 filter vlan 1 - 5 , 9</b>                                                                                                                       | Limits the SPAN source traffic to specific VLANs. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, enter the session number specified in Step 4.</li> <li>• For <i>vlan-id</i>, the range is 1 to 4094.</li> <li>• (Optional) Use a comma (,) to specify a series of VLANs, or use a hyphen (-) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.</li> </ul>                                                         |
| <b>Step 6</b> | <b>monitor session</b> <i>session_number</i> <b>destination</b> { <b>interface</b> <i>interface-id</i> [,   -] [ <b>encapsulation</b> <b>replicate</b>   <b>encapsulation dot1q</b> ]}<br><br><b>Example:</b><br>Router(config)# <b>monitor session 2 destination interface gigabitethernet 0/1/0</b> | Specifies the SPAN session and the destination port (monitoring port). <ul style="list-style-type: none"> <li>• For <i>session_number</i>, specify the session number entered in Step 4.</li> <li>• For <i>interface-id</i>, specify the destination port. The destination interface must be a physical port or port-channel; it cannot be an EtherChannel, and it cannot be a VLAN.</li> <li>• (Optional) [,   -] Specifies a series or range of interfaces. Enter a space before and after</li> </ul> |

|               | Command or Action                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                       | <p>the comma; enter a space before and after the hyphen.</p> <ul style="list-style-type: none"> <li>• (Optional) <b>encapsulation replicate</b> specifies that the destination interface replicates the source interface encapsulation method. If not selected, the default is to send packets in native form (untagged).</li> <li>• (Optional) <b>encapsulation dot1q</b> IEEE 802.1Q is a standard protocol for interconnecting multiple switches and routers and for defining VLAN topologies. Applies a VLAN ID to the subinterface.</li> </ul> |
| <b>Step 7</b> | <b>end</b><br><br><b>Example:</b><br>Router(config) # <b>end</b>                                                      | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 8</b> | <b>show running-config</b><br><br><b>Example:</b><br>Router# <b>show running-config</b>                               | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 9</b> | <b>copy running-config startup-config</b><br><br><b>Example:</b><br>Router# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

## Verifying the SPAN Session

Use the **show monitor session** command to verify the sources and destinations configured for the SPAN session.

```
Router#show monitor session 1
```

```
Session 1

Session 1

Type : Local Session
Source Ports :
Both : Gi0/1/0
Destination Ports : Gi0/1/1
```

## Removing a SPAN Session

To remove sources or destinations from the SPAN session, use the **no monitor session** session command in global configuration mode as shown in the following example:

```
Router(config)#no monitor session 1
```

## Configuring a VLAN as an RSPAN VLAN

Follow these steps to create a new VLAN, then configure it to be the RSPAN VLAN for the RSPAN session.

### Procedure

|               | Command or Action                                                                                                 | Purpose                                                                                                                                                                                                                                                                                      |
|---------------|-------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Router> <b>enable</b>                                                         | Enables privileged EXEC mode.<br><ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>                                                                                                                                                                          |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                 | Enter global configuration mode.                                                                                                                                                                                                                                                             |
| <b>Step 3</b> | <b>vlan <i>vlan-id</i></b><br><b>Example:</b><br>Router(config)# <b>vlan 100</b>                                  | Enters a VLAN ID to create a VLAN, or enters the VLAN ID of an existing VLAN, and enters VLAN configuration mode. The range is 2 to 1001 and 1006 to 4094.<br><br>The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 through 1005 (reserved for Token Ring and FDDI VLANs). |
| <b>Step 4</b> | <b>remote-span</b><br><b>Example:</b><br>Router(config)# <b>remote-span</b>                                       | Configures the VLAN as an RSPAN VLAN.                                                                                                                                                                                                                                                        |
| <b>Step 5</b> | <b>end</b><br><b>Example:</b><br>Router(config)# <b>end</b>                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                             |
| <b>Step 6</b> | <b>show running-config</b><br><b>Example:</b><br>Router# <b>show running-config</b>                               | Verifies your entries.                                                                                                                                                                                                                                                                       |
| <b>Step 7</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br>Router# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                     |

### What to do next

You must create the RSPAN VLAN in all devices that will participate in RSPAN. If the RSPAN VLAN-ID is in the normal range (lower than 1005) and VTP is enabled in the network, you can create the RSPAN VLAN in one device, and VTP propagates it to the other devices in the VTP domain. For extended-range VLANs (greater than 1005), you must configure RSPAN VLAN on both source and destination devices and any intermediate devices.

Use VTP pruning to get an efficient flow of RSPAN traffic, or manually delete the RSPAN VLAN from all trunks that do not need to carry the RSPAN traffic.

To remove the remote SPAN characteristic from a VLAN and convert it back to a normal VLAN, use the **no remote-span** VLAN configuration command.

To remove a source port or VLAN from the SPAN session, use the **no monitor session** *session\_number* **source** {**interface** *interface-id* | **vlan** *vlan-id*} global configuration command. To remove the RSPAN VLAN from the session, use the **no monitor session** *session\_number* {**Source|destination**} **remote vlan** *vlan-id*.

## Creating an RSPAN Source Session

Follow these steps to create and start an RSPAN source session and to specify the monitored source and the destination RSPAN VLAN.

### Procedure

|               | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br><code>Router&gt; enable</code>                                                                                                                                     | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                                                                                                                              |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br><code>Router# configure terminal</code>                                                                                                                | Enter global configuration mode.                                                                                                                                                                                                                                     |
| <b>Step 3</b> | <b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }<br><br><b>Example:</b><br><code>Router(config)# no monitor session all</code>                              | Removes any existing SPAN configuration for the session.<br><br>• For <i>session_number</i> , the range is 1 to 66.<br>• <b>all</b> —Removes all SPAN sessions.<br>• <b>local</b> —Removes all local sessions.<br>• <b>remote</b> —Removes all remote SPAN sessions. |
| <b>Step 4</b> | <b>monitor session</b> <i>session_number</i> <b>source</b> { <b>interface</b> <i>interface-id</i>   <b>vlan</b> <i>vlan-id</i> } [,   -]<br>[ <b>both</b>   <b>rx</b>   <b>tx</b> ]<br><br><b>Example:</b> | Specifies the RSPAN session and the source port (monitored port).<br><br>• For <i>session_number</i> , the range is 1 to 66.<br>• Enter a source port or source VLAN for the RSPAN session:                                                                          |

|               | Command or Action                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <pre>Router(config)# monitor session 1 source interface gigabitethernet 0/1/0 tx</pre>                                                                                                            | <ul style="list-style-type: none"> <li>For interface-id , specifies the source port to monitor. Valid interfaces include physical interfaces and port-channel logical interfaces (<b>port-channel</b> port-channel-number ). Valid port-channel numbers are 1 to 32.</li> <li>For vlan-id , specifies the source VLAN to monitor. The range is 1 to 4094 (excluding the RSPAN VLAN).<br/>A single session can include multiple sources (ports or VLANs), defined in a series of commands, but you cannot combine source ports and source VLANs in one session.</li> <li>(Optional) [,   -] —Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</li> <li>(Optional) <b>both</b>   <b>rx</b>   <b>tx</b> —Specifies the direction of traffic to monitor. If you do not specify a traffic direction, the source interface sends both sent and received traffic. <ul style="list-style-type: none"> <li><b>both</b> —Monitors both received and sent traffic.</li> <li><b>rx</b> —Monitors received traffic.</li> <li><b>tx</b> —Monitors sent traffic.</li> </ul> </li> </ul> |
| <b>Step 5</b> | <p><b>monitor session</b> <i>session_number</i> <b>destination remote vlan</b> <i>vlan_id</i></p> <p><b>Example:</b></p> <pre>Router(config)# monitor session 1 destination remote vlan 100</pre> | <p>Specifies the RSPAN session, the destination RSPAN VLAN, and the destination-port group.</p> <ul style="list-style-type: none"> <li>For session_number , enter the number defined in Step 4.</li> <li>For vlan-id , specify the RSPAN VLAN in source session, which will transport mirrored traffic to destination session.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 6</b> | <p><b>end</b></p> <p><b>Example:</b></p> <pre>Router(config)# end</pre>                                                                                                                           | <p>Returns to privileged EXEC mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|               | Command or Action                                                                                                     | Purpose                                                  |
|---------------|-----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>Step 7</b> | <b>show running-config</b><br><br><b>Example:</b><br>Router# <b>show running-config</b>                               | Verifies your entries.                                   |
| <b>Step 8</b> | <b>copy running-config startup-config</b><br><br><b>Example:</b><br>Router# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file. |

## Specifying VLANs to Filter on RSPAN Source Session

Follow these steps to configure the RSPAN source session to limit RSPAN source traffic to specific VLANs.

### Procedure

|               | Command or Action                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                                                                                                                                               |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                 | Enter global configuration mode.                                                                                                                                                                                                                                                      |
| <b>Step 3</b> | <b>no monitor session</b> { <i>session_number</i>   <b>all</b>   <b>local</b>   <b>remote</b> }<br><br><b>Example:</b><br>Router(config)# <b>no monitor session 2</b>                                 | Removes any existing SPAN configuration for the session.<br><br>• For <i>session_number</i> , the range is 1 to 66.<br>• <b>all</b> —Removes all SPAN sessions.<br>• <b>local</b> —Removes all local sessions.<br>• <b>remote</b> —Removes all remote SPAN sessions.                  |
| <b>Step 4</b> | <b>monitor session</b> <i>session_number</i> <b>source interface</b> <i>interface-id</i><br><br><b>Example:</b><br>Router(config)# <b>monitor session 2 source interface gigabitethernet 0/1/0 rx</b> | Specifies the characteristics of the source port (monitored port) and SPAN session.<br><br>• For <i>session_number</i> , the range is 1 to 66.<br>• For <i>interface-id</i> , specify the source port to monitor. The interface specified must already be configured as a trunk port. |
| <b>Step 5</b> | <b>monitor session</b> <i>session_number</i> <b>filter vlan</b> <i>vlan-id</i> [,   -]                                                                                                                | Limits the SPAN source traffic to specific VLANs.                                                                                                                                                                                                                                     |

|               | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <b>Example:</b><br><pre>Router(config)# monitor session 2 filter vlan 1 - 5 , 9</pre>                                                                                    | <ul style="list-style-type: none"> <li>For session_number , enter the session number specified in step 4.</li> <li>For vlan-id , the range is 1 to 4094.</li> <li>(Optional) ,   - Use a comma ( , ) to specify a series of VLANs or use a hyphen ( - ) to specify a range of VLANs. Enter a space before and after the comma; enter a space before and after the hyphen.</li> </ul> |
| <b>Step 6</b> | <b>monitor session session_number destination remote vlan vlan-id</b><br><br><b>Example:</b><br><pre>Router(config)# monitor session 2 destination remote vlan 902</pre> | Specifies the RSPAN session and the destination remote VLAN (RSPAN VLAN). <ul style="list-style-type: none"> <li>For session_number , enter the session number specified in Step 4.</li> <li>For vlan-id , specify the RSPAN VLAN to carry the monitored traffic to the destination port.</li> </ul>                                                                                 |
| <b>Step 7</b> | <b>end</b><br><br><b>Example:</b><br><pre>Router(config)# end</pre>                                                                                                      | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 8</b> | <b>show running-config</b><br><br><b>Example:</b><br><pre>Router# show running-config</pre>                                                                              | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 9</b> | <b>copy running-config startup-config</b><br><br><b>Example:</b><br><pre>Router# copy running-config startup-config</pre>                                                | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                             |

## Creating an RSPAN Destination Session and Configuring Incoming Traffic

Follow these steps to create an RSPAN destination session, to specify the source RSPAN VLAN and the destination port, and to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance).

### Procedure

|               | Command or Action                                                    | Purpose                                                                                                          |
|---------------|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br><pre>Router&gt; enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |

|               | Command or Action                                                                                                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                                                                                                  | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 3</b> | <b>no monitor session {session_number   all   local   remote}</b><br><b>Example:</b><br>Router(config)# <b>no monitor session 2</b>                                                                                                                                                | Removes any existing SPAN configuration for the session. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, the range is 1 to 66.</li> <li>• <b>all</b> —Removes all SPAN sessions.</li> <li>• <b>local</b> —Removes all local sessions.</li> <li>• <b>remote</b> —Removes all remote SPAN sessions.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 4</b> | <b>monitor session session_number source remote vlan vlan-id</b><br><b>Example:</b><br>Router(config)# <b>monitor session 2 source remote vlan 901</b>                                                                                                                             | Specifies the RSPAN session and the source RSPAN VLAN. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, the range is 1 to 66.</li> <li>• For <i>vlan-id</i>, specify the RSPAN VLAN in destination session, which will receive mirrored traffic from the source session.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 5</b> | <b>monitor session session_number destination {interface interface-id [,   -] [ingress {dot1q vlan vlan-id   untagged vlan vlan-id   vlan vlan-id}]}</b><br><b>Example:</b><br>Router(config)# <b>monitor session 2 destination interface gigabitethernet 0/1/0 ingress vlan 6</b> | Specifies the SPAN session, the destination port, the packet encapsulation, and the incoming VLAN and encapsulation. <ul style="list-style-type: none"> <li>• For <i>session_number</i>, enter the number defined in Step 5.</li> </ul> <p>In an RSPAN destination session, you must use the same session number for the source RSPAN VLAN and the destination port.</p> <ul style="list-style-type: none"> <li>• For <i>interface-id</i>, specify the destination interface. The destination interface must be a physical interface.</li> <li>• Though visible in the command-line help string, <b>encapsulation replicate</b> is not supported for RSPAN. The original VLAN ID is overwritten by the RSPAN VLAN ID, and all packets appear on the destination port as untagged.</li> <li>• (Optional) [,   -] Specifies a series or range of interfaces. Enter a space before and after the comma; enter a space before and after the hyphen.</li> </ul> |

|               | Command or Action                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                   | <ul style="list-style-type: none"> <li>Enter <b>ingress</b> with additional keywords to enable forwarding of incoming traffic on the destination port and to specify the encapsulation type: <ul style="list-style-type: none"> <li><b>dot1q vlan</b> vlan-id— Forwards incoming packets with IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN.</li> <li><b>untagged vlan</b> vlan-id or <b>vlan</b> vlan-id— Forwards incoming packets with untagged encapsulation type with the specified VLAN as the default VLAN.</li> </ul> </li> </ul> |
| <b>Step 6</b> | <b>end</b><br><b>Example:</b><br>Router(config)# <b>end</b>                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 7</b> | <b>show running-config</b><br><b>Example:</b><br>Router# <b>show running-config</b>                               | Verifies your entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 8</b> | <b>copy running-config startup-config</b><br><b>Example:</b><br>Router# <b>copy running-config startup-config</b> | (Optional) Saves your entries in the configuration file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

## EtherChannel Overview

EtherChannel provides fault-tolerant high-speed links between switches, routers, and servers. You can use the EtherChannel to increase the bandwidth between the wiring closets and the data center, and you can deploy it anywhere in the network where bottlenecks are likely to occur. EtherChannel provides automatic recovery for the loss of a link by redistributing the load across the remaining links. If a link fails, EtherChannel redirects traffic from the failed link to the remaining links in the channel without intervention.

An EtherChannel consists of individual Ethernet links bundled into a single logical link

The EtherChannel provides full-duplex bandwidth up to 4 Gb/s (Gigabit EtherChannel) between your switch and another switch or host.

Each EtherChannel can consist of up to four compatibly configured Ethernet ports.

## Channel Groups and Port-Channel Interfaces

An EtherChannel comprises a channel group and a port-channel interface. The channel group binds physical ports to the port-channel interface. Configuration changes applied to the port-channel interface apply to all the physical ports bound together in the channel group. The channel-group command binds the physical port and the port-channel interface together. Each EtherChannel has a port-channel logical interface numbered from 1 to 32. This port-channel interface number corresponds to the one specified with the channel-group interface configuration command.

## Port Aggregation Protocol

The Port Aggregation Protocol (PAgP) is a Cisco-proprietary protocol that can be run only on Cisco devices and on those devices licensed by vendors to support PAgP. PAgP facilitates the automatic creation of EtherChannels by exchanging PAgP packets between Ethernet ports.

By using PAgP, the device learns the identity of partners capable of supporting PAgP and the capabilities of each port. It then dynamically groups similarly configured ports (on a single device in the stack) into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, PAgP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, PAgP adds the group to the spanning tree as a single device port.

## Link Aggregation Control Protocol

The LACP is defined in IEEE 802.3ad and enables Cisco devices to manage Ethernet channels between devices that conform to the IEEE 802.3ad protocol. LACP facilitates the automatic creation of EtherChannels by exchanging LACP packets between Ethernet ports.

By using LACP, the switch learns the identity of partners capable of supporting LACP and the capabilities of each port. It then dynamically groups similarly configured ports into a single logical link (channel or aggregate port). Similarly configured ports are grouped based on hardware, administrative, and port parameter constraints. For example, LACP groups the ports with the same speed, duplex mode, native VLAN, VLAN range, and trunking status and type. After grouping the links into an EtherChannel, LACP adds the group to the spanning tree as a single device port.

## Configuring Layer 2 EtherChannels

Configure Layer 2 EtherChannels by assigning ports to a channel group with the **channel-group** command in interface configuration mode. This command automatically creates the port-channel logical interface.

Use the **show etherchannel swport xxx** command to view the EtherChannels.

### Procedure

|               | Command or Action                                                 | Purpose                                                                                                          |
|---------------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br><br>Router> <b>enable</b> | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |

|               | Command or Action                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                                                                                      | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 3</b> | <b>interface</b> [ <i>interface-id</i> ]<br><b>Example:</b><br>Router(config)# <b>interface gigabitethernet 0/1/0</b>                                                                                                                                                  | <p>Specifies a physical port, and enters interface configuration mode.</p> <p>Valid interfaces are physical ports.</p> <p>For a PAgP EtherChannel, you can configure up to four ports of the same type and speed for the same group.</p> <p>For a LACP EtherChannel, you can configure up to 8 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 4</b> | <b>switchport mode</b> { <i>access</i>   <i>trunk</i> }<br><b>Example:</b><br>Router(config-if)# <b>switchport mode access</b>                                                                                                                                         | Assigns all ports as static-access ports in the same VLAN, or configure them as trunks. If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 5</b> | <b>switchport access vlan</b> <i>vlan-id</i><br><b>Example:</b><br>Router(config-if)# <b>switchport access vlan 22</b>                                                                                                                                                 | (Optional) If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 6</b> | <b>channel-group</b> <i>channel-group-number</i> <b>mode</b> { <i>auto</i> [ <i>non-silent</i> ]   <i>desirable</i> [ <i>non-silent</i> ]   <i>on</i> }   { <i>active</i>   <i>passive</i> }<br><b>Example:</b><br>Router(config-if)# <b>channel-group 5 mode auto</b> | <p>Assigns the port to a channel group, and specifies the PAgP or the LACP mode.</p> <p>For <b>mode</b>, select one of these keywords:</p> <ul style="list-style-type: none"> <li>• <b>auto</b> — Enables PAgP only if a PAgP device is detected. It places the port into a passive negotiating state, in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation.</li> <li>• <b>desirable</b> — Unconditionally enables PAgP. It places the port into an active negotiating state, in which the port starts negotiations with other ports by sending PAgP packets.</li> <li>• <b>on</b> — Forces the port to channel without PAgP or LACP. In the <b>on</b> mode, an EtherChannel exists only when a port group in the <b>on</b> mode is connected to another port group in the <b>on</b> mode.</li> </ul> |

|               | Command or Action                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                  | <ul style="list-style-type: none"> <li>• <b>non-silent</b> — (Optional) If your device is connected to a partner that is PAgP-capable, configures the device port for nonsilent operation when the port is in the <b>auto</b> or <b>desirable</b> mode. If you do not specify <b>non-silent</b>, silent is assumed. The silent setting is for connections to file servers or packet analyzers. This setting allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission.</li> <li>• <b>active</b> — Enables LACP only if a LACP device is detected. It places the port into an active negotiating state in which the port starts negotiations with other ports by sending LACP packets.</li> <li>• <b>passive</b> — Enables LACP on the port and places it into a passive negotiating state in which the port responds to LACP packets that it receives, but does not start LACP packet negotiation.</li> </ul> |
| <b>Step 7</b> | <b>end</b><br><br><b>Example:</b><br>Router(config) # <b>end</b> | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## Configuring EtherChannel Load-Balancing

You can configure EtherChannel load-balancing to use one of several different forwarding methods. This task is optional.

### Procedure

|               | Command or Action                                                                                                                                                                                                        | Purpose                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                                    | Enter global configuration mode.                                                                                                                                                                                   |
| <b>Step 2</b> | <b>port-channel swport load-balance { dst-ip   dst-mac   dst-mixed-ip-port   dst-port   extended [ dst-ip   dst-mac   dst-port   ipv6-label   l3-protocol   src-ip   src-mac   src-port ]   src-dst-ip   src-dst-mac</b> | Configures an EtherChannel load-balancing method.<br><br>Select one of these load-distribution methods: <ul style="list-style-type: none"> <li>• <b>dst-ip</b> — Specifies destination-host IP address.</li> </ul> |

|               | Command or Action                                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <b>src-dst-mixed-ip-port src-dst-portsrc-ip   src-mac   src-mixed-ip-port   src-port }</b><br><br><b>Example:</b><br><pre>Router(config)# port-channel swport load-balance src-mac</pre> | <ul style="list-style-type: none"> <li>• <b>dst-mac</b> —Specifies the destination-host MAC address of the incoming packet.</li> <li>• <b>dst-mixed-ip-port</b> —Specifies the host IP address and TCP/UDP port.</li> <li>• <b>dst-port</b> —Specifies the destination TCP/UDP port.</li> <li>• <b>extended</b> —Specifies extended load balance methods--combinations of source and destination methods beyond those available with the standard command.</li> <li>• <b>ipv6-label</b> —Specifies the IPv6 flow label.</li> <li>• <b>l3-proto</b> —Specifies the Layer 3 protocol.</li> <li>• <b>src-dst-ip</b> —Specifies the source and destination host IP address.</li> <li>• <b>src-dst-mac</b> —Specifies the source and destination host MAC address.</li> <li>• <b>src-dst-mixed-ip-port</b> —Specifies the source and destination host IP address and TCP/UDP port.</li> <li>• <b>src-dst-port</b> —Specifies the source and destination TCP/UDP port.</li> <li>• <b>src-ip</b> —Specifies the source host IP address.</li> <li>• <b>src-mac</b> —Specifies the source MAC address of the incoming packet.</li> <li>• <b>src-mixed-ip-port</b> —Specifies the source host IP address and TCP/UDP port.</li> <li>• <b>src-port</b> —Specifies the source TCP/UDP port.</li> </ul> |
| <b>Step 3</b> | <b>end</b><br><br><b>Example:</b><br><pre>Router(config)# end</pre>                                                                                                                      | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

## Configuring the PAgP Learn Method and Priority

This task is optional.

## Procedure

|               | Command or Action                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                              | Enables privileged EXEC mode.<br><br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                      | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>interface</b> <i>[interface-id]</i><br><br><b>Example:</b><br>Router(config)# <b>interface</b> gigabitethernet 0/1/0    | Specifies the port for transmission, and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 4</b> | <b>pagp learn-method physical-port</b><br><br><b>Example:</b><br>Router(config-if)# <b>pagp learn-method physical port</b> | <p>Selects the PAgP learning method.</p> <p>By default, <b>aggregation-port learning</b> is selected, which means the device sends packets to the source by using any of the ports in the EtherChannel. With aggregate-port learning, it is not important on which physical port the packet arrives.</p> <p>Selects <b>physical-port</b> to connect with another device that <b>is</b> a physical learner.</p> <p>Make sure to configure the <b>port-channel load-balance</b> global configuration command to <b>src-mac</b> .</p> <p>The learning method must be configured the same at both ends of the link.</p> |
| <b>Step 5</b> | <b>pagp port-priority priority</b><br><br><b>Example:</b><br>Router(config-if)# <b>pagp port-priority 200</b>              | <p>Assigns a priority so that the selected port is chosen for packet transmission.</p> <p>For <i>priority</i>, the range is 0 to 255. The default is 128. The higher the priority, the more likely that the port will be used for PAgP transmission.</p>                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 6</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                            | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

## Configuring the LACP Port Channel Min-Links Feature

You can specify the minimum number of active ports that must be in the link-up state and bundled in an EtherChannel for the port channel interface to transition to the link-up state. Using EtherChannel min-links,

you can prevent low-bandwidth LACP EtherChannels from becoming active. Port channel min-links also cause LACP EtherChannels to become inactive if they have too few active member ports to supply the required minimum bandwidth.

To configure the minimum number of links that are required for a port channel. Perform the following tasks.

## Procedure

|               | Command or Action                                                                                                                     | Purpose                                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                         | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                                                                                                                                     |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                 | Enter global configuration mode.                                                                                                                                                                                                            |
| <b>Step 3</b> | <b>interface port-channel</b> [ <i>channel-number</i> ]<br><br><b>Example:</b><br>Router(config)# <b>interface port-channel</b><br>2  | Enters interface configuration mode for a port-channel.<br><br>For <i>channel-number</i> , the range is 1 to 63.                                                                                                                            |
| <b>Step 4</b> | <b>port-channel min-links</b> <i>min-links-number</i><br><br><b>Example:</b><br>Router(config-if)# <b>port-channel min-links</b><br>3 | Specifies the minimum number of member ports that must be in the link-up state and bundled in the EtherChannel for the port channel interface to transition to the link-up state.<br><br>For <i>min-links-number</i> , the range is 2 to 8. |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                                       | Returns to privileged EXEC mode.                                                                                                                                                                                                            |

## Configuring LACP Fast Rate Timer

You can change the LACP timer rate to modify the duration of the LACP timeout. Use the **lacp rate** command to set the rate at which LACP control packets are received by an LACP-supported interface. You can change the timeout rate from the default rate (30 seconds) to the fast rate (1 second). This command is supported only on LACP-enabled interfaces.

## Procedure

|               | Command or Action                                             | Purpose                                                                 |
|---------------|---------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b> | Enables privileged EXEC mode.<br><br>• Enter your password if prompted. |

|               | Command or Action                                                                                                                        | Purpose                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                    | Enter global configuration mode.                                                                                                                                                     |
| <b>Step 3</b> | <b>interface</b> <i>type slot/port</i><br><br><b>Example:</b><br>Router(config)# <b>interface</b> <b>gigabitEthernet</b><br><b>0/1/0</b> | Configures an interface and enters interface configuration mode.                                                                                                                     |
| <b>Step 4</b> | <b>lacp rate { normal   fast}</b><br><br><b>Example:</b><br>Router(config-if)# <b>lacp rate fast</b>                                     | Configures the rate at which LACP control packets are received by an LACP-supported interface.<br><br>To reset the timeout rate to its default, use the <b>no lacp rate</b> command. |
| <b>Step 5</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b>                                                                          | Returns to privileged EXEC mode.                                                                                                                                                     |
| <b>Step 6</b> | <b>show lacp internal</b><br><br><b>Example:</b><br>Router# <b>show lacp internal</b><br>Router# <b>show lacp counters</b>               | Verifies your configuration.                                                                                                                                                         |

## Modular Quality of Service Command-Line Interface

The MQC (Modular Quality of Service (QoS) Command-Line Interface (CLI)) enables you to set packet classification and marking based on a QoS group value. With the device, QoS features are enabled through the Modular QoS command-line interface (MQC). The MQC is a command-line interface (CLI) structure that allows you to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic. One of the main goals of MQC is to provide a platform-independent interface for configuring QoS across Cisco platforms. For more information on the Modular Quality of Service, see the [Quality of Service Configuration Guide, Cisco IOS XE Fuji 16.9.x](#).

**Note** QoS limitations on IR8340 platforms

1. Quality of Service (QoS) is supported for traffic moving between switch ports.
2. For inter-vlan routing between switch ports, QoS limitations are:
  - It is supported only when a policy is applied on the Switch Virtual Interface (SVI).
  - Only marking and policing actions based on Differentiated Services Code Point (DSCP) match are supported on SVI.
  - Queuing and shaping actions are not supported on SVI.
3. For traffic moving from LAN to WAN port, QoS limitations are:
  - It is supported only when a policy is applied on SVI.
  - Only marking and policing actions based on Differentiated Services Code Point (DSCP) match are supported on SVI.
  - Queuing and shaping actions are not supported on SVI.

## Creating a Traffic Class

To create a traffic class containing match criteria, use the **class-map** command to specify the traffic class name, and then use the following **match** commands in class-map configuration mode, as needed.

### Before you begin

All match commands specified in this configuration task are considered optional, but you must configure at least one match criterion for a class.

### Procedure

|               | Command or Action                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                   | Enter global configuration mode.                                                                                                                                                                                                                                                                                                |
| <b>Step 2</b> | <b>class-map</b> <i>class-map name</i> { <b>match-any</b> }<br><br><b>Example:</b><br>Router(config)# <b>class-map type ngs-w-qos test_1000</b><br>Router(config-cmap)# | Enters class map configuration mode. <ul style="list-style-type: none"> <li>• Creates a class map to be used for matching packets to the class whose name you specify.</li> <li>• <b>match-any:</b> Any one of the match criteria must be met for traffic entering the traffic class to be classified as part of it.</li> </ul> |

|               | Command or Action                                                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>match access-group</b> { <i>index number</i>   <i>name</i> }<br><b>Example:</b><br>Router(config-cmap) # <b>match access-group 100</b><br>Router(config-cmap) #       | The following parameters are available for this command: <ul style="list-style-type: none"> <li>• access-group</li> <li>• cos</li> <li>• dscp</li> <li>• group-object</li> <li>• ip</li> <li>• mpls</li> <li>• precedence</li> <li>• protocol</li> <li>• qos-group</li> <li>• vlan</li> <li>• wlan</li> </ul> (Optional) For this example, enter the access-group ID: <ul style="list-style-type: none"> <li>• Access list index (value from 1 to 2799)</li> <li>• Named access list</li> </ul> |
| <b>Step 4</b> | <b>match cos</b> <i>cos value</i><br><b>Example:</b><br>Router(config-cmap) # <b>match cos 2 3 4 5</b>                                                                   | (Optional) Matches IEEE 802.1Q or ISL class of service (user) priority values. <ul style="list-style-type: none"> <li>• Enters up to 4 CoS values separated by spaces (0 to 7).</li> </ul>                                                                                                                                                                                                                                                                                                      |
| <b>Step 5</b> | <b>match dscp</b> <i>dscp value</i><br><b>Example:</b><br>Router(config-cmap) # <b>match dscp af11 af12</b>                                                              | (Optional) Matches the DSCP values in IPv4 and IPv6 packets.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 6</b> | <b>match ip</b> { <b>dscp</b> <i>dscp value</i>   <b>precedence</b> <i>precedence value</i> }<br><b>Example:</b><br>Router(config-cmap) # <b>match ip dscp af11 af12</b> | (Optional) Matches IP values including the following: <ul style="list-style-type: none"> <li>• <b>dscp</b>—Matches IP DSCP (DiffServ codepoints).</li> <li>• <b>precedence</b>—Matches IP precedence (0 to 7).</li> </ul>                                                                                                                                                                                                                                                                       |
| <b>Step 7</b> | <b>match qos-group</b> <i>qos group value</i><br><b>Example:</b><br>Router(config-cmap) # <b>match qos-group 10</b>                                                      | (Optional) Matches QoS group value (from 0 to 31).                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|               | Command or Action                                                                                                     | Purpose                                        |
|---------------|-----------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| <b>Step 8</b> | <b>match vlan</b> <i>vlan value</i><br><br><b>Example:</b><br><code>Router(config-cmap)# <b>match vlan</b> 210</code> | (Optional) Matches a VLAN ID (from 1 to 4095). |
| <b>Step 9</b> | <b>end</b><br><br><b>Example:</b><br><code>Router(config)# <b>end</b></code>                                          | Saves the configuration changes.               |

**What to do next**

Configure the policy map.

## Creating a Traffic Policy

To create a traffic policy, use the **policy-map** global configuration command to specify the traffic policy name.

The traffic class is associated with the traffic policy when the **class** command is used. The **class** command must be entered after you enter the policy map configuration mode. After entering the **class** command, the device is automatically in policy map class configuration mode, which is where the QoS policies for the traffic policy are defined.

The following policy map class-actions are supported:

- bandwidth—Bandwidth configuration options.
- exit—Exits from the QoS class action configuration mode.
- no—Negates or sets default values for the command.
- police—Policer configuration options.
- priority—Strict scheduling priority configuration options for this class.
- queue-buffers—Queue buffer configuration options.
- queue-limit—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.
- service-policy—Configures the QoS service policy.
- set—Sets QoS values using the following options:
  - CoS values
  - DSCP values
  - Precedence values
  - QoS group values
- shape—Traffic-shaping configuration options.

**Before you begin**

You should have first created a class map.

**Procedure**

|               | Command or Action                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                  | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 2</b> | <b>policy-map type <i>policy-map name</i></b><br><br><b>Example:</b><br>Router(config)# <b>policy-map type ngs-w-qos</b><br><b>test_1000</b>                                                           | Enters policy map configuration mode.<br><br>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                                                                                                                                                                 |
| <b>Step 3</b> | <b>class { <i>class-name</i>   <b>class-default</b> }</b><br><br><b>Example:</b><br>Router(config-pmap)# <b>class test_1000</b>                                                                        | Specifies the name of the class whose policy you want to create or change.<br><br>You can also create a system default class for unclassified packets.                                                                                                                                                                                                                                    |
| <b>Step 4</b> | <b>bandwidth { <i>kb/s kb/s value</i>   <b>percent</b> <i>percentage</i>   <b>remaining</b> {<i>percent</i>   <i>ratio</i>} }</b><br><br><b>Example:</b><br>Router(config-pmap-c)# <b>bandwidth 50</b> | (Optional) Sets the bandwidth using one of the following:<br><ul style="list-style-type: none"><li>• <b>kb/s</b>—Kilobits per second, enter a value between 20000 and 10000000 for Kb/s.</li><li>• <b>percent</b>—Enter the percentage of the total bandwidth to be used for this policy map.</li><li>• <b>remaining</b>—Enter the percentage ratio of the remaining bandwidth.</li></ul> |
| <b>Step 5</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap-c)# <b>exit</b>                                                                                                                               | (Optional) Exits from QoS class action configuration mode.                                                                                                                                                                                                                                                                                                                                |
| <b>Step 6</b> | <b>no</b><br><br><b>Example:</b><br>Router(config-pmap-c)# <b>no</b>                                                                                                                                   | (Optional) Negates the command.                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 7</b> | <b>police { <i>target_bit_rate</i>   <b>cir</b>   <b>rate</b> }</b><br><br><b>Example:</b><br>Router(config-pmap-c)# <b>police 100000</b>                                                              | (Optional) Configures the policer:<br><ul style="list-style-type: none"><li>• <b>target_bit_rate</b>—Enter the bit rate per second, enter a value between 8000 and 10000000000.</li><li>• <b>cir</b>—Committed Information Rate</li></ul>                                                                                                                                                 |

|                | Command or Action                                                                                                                           | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                             | <ul style="list-style-type: none"> <li>• <b>rate</b>—Specify police rate, PCR for hierarchical policies or SCR for single-level ATM 4.0 policer policies.</li> </ul>                                                                                                                                                                                                                                                                  |
| <b>Step 8</b>  | <b>priority level</b> <i>level value</i><br><b>Example:</b><br><pre>Router(config-pmap-c) # priority level 1</pre>                          | (Optional) Sets the strict scheduling priority for this class. Command options include: <ul style="list-style-type: none"> <li>• <b>level</b>—Establishes a multi-level priority queue. Enter a value (1 or 2).</li> </ul>                                                                                                                                                                                                            |
| <b>Step 9</b>  | <b>queue-buffers ratio</b> <i>ratio limit</i><br><b>Example:</b><br><pre>Router(config-pmap-c) # queue-buffers ratio 10</pre>               | (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0 to 100).                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 10</b> | <b>queue-limit { packets   cos   dscp   percent }</b><br><b>Example:</b><br><pre>Router(config-pmap-c) # queue-limit cos 7 percent 50</pre> | (Optional) Specifies the queue maximum threshold for the tail drop: <ul style="list-style-type: none"> <li>• <b>packets</b>—Packets by default, enter a value between 1 to 2000000.</li> <li>• <b>cos</b>—Enter the parameters for each COS value.</li> <li>• <b>dscp</b>—Enter the parameters for each DSCP value.</li> <li>• <b>percent</b>—Enter the percentage for the threshold.</li> </ul>                                      |
| <b>Step 11</b> | <b>service-policy</b> <i>policy-map name</i><br><b>Example:</b><br><pre>Router(config-pmap-c) # service-policy test_2000</pre>              | (Optional) Configures the QoS service policy.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 12</b> | <b>set { cos   dscp   ip   precedence   qos-group   wlan }</b><br><b>Example:</b><br><pre>Router(config-pmap-c) # set cos 7</pre>           | (Optional) Sets the QoS values. Possible QoS configuration values include: <ul style="list-style-type: none"> <li>• <b>cos</b>—Sets the IEEE 802.1Q/ISL class of service/user priority.</li> <li>• <b>dscp</b>—Sets DSCP in IP(v4) and IPv6 packets.</li> <li>• <b>ip</b>—Sets IP specific values.</li> <li>• <b>precedence</b>—Sets precedence in IP(v4) and IPv6 packet.</li> <li>• <b>qos-group</b>—Sets the QoS Group.</li> </ul> |

|                | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 13</b> | <b>shape average</b> { <i>target_bit_rate</i>   <b>percent</b> }<br><b>Example:</b><br>Router(config-pmap-c) # <b>shape average percent 50</b> | (Optional) Sets the traffic shaping. Command parameters include: <ul style="list-style-type: none"> <li>• <i>target_bit_rate</i>—Target bit rate.</li> <li>• <b>percent</b>—Percentage of interface bandwidth for Committed Information Rate.</li> </ul> |
| <b>Step 14</b> | <b>end</b><br><b>Example:</b><br>Router(config) # <b>end</b>                                                                                   | Saves the configuration changes.                                                                                                                                                                                                                         |

**What to do next**

Configure the interface.

## Configuring Class-Based Packet Marking

This is an important procedure that explains how to configure the following class-based packet marking features on your device:

- CoS value
- DSCP value
- IP value
- Precedence value
- QoS group value
- WLAN value

**Before you begin**

You should have created a class map and a policy map before beginning this procedure.

**Procedure**

|               | Command or Action                                                                 | Purpose                               |
|---------------|-----------------------------------------------------------------------------------|---------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b> | Enter global configuration mode.      |
| <b>Step 2</b> | <b>policy-map type <i>policy-map name</i></b><br><b>Example:</b>                  | Enters policy map configuration mode. |

|               | Command or Action                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <pre>Router(config)# policy-map type ngs-w-qos policy1 Device(config-pmap)#</pre>                                         | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 3</b> | <p><b>class</b> <i>class name</i></p> <p><b>Example:</b></p> <pre>Router(config)# class class1 Device(config-pmap)#</pre> | <p>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.</p> <p>Command options for policy class map configuration mode include the following:</p> <ul style="list-style-type: none"> <li>• <b>bandwidth</b>—Bandwidth configuration options.</li> <li>• <b>exit</b>—Exits from the QoS class action configuration mode.</li> <li>• <b>no</b>—Negates or sets default values for the command.</li> <li>• <b>police</b>—Policer configuration options.</li> <li>• <b>priority</b>—Strict scheduling priority configuration options for this class.</li> <li>• <b>queue-buffers</b>—Queue buffer configuration options.</li> <li>• <b>queue-limit</b>—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.</li> <li>• <b>service-policy</b>—Configures the QoS service policy.</li> <li>• <b>set</b>—Sets QoS values using the following options: <ul style="list-style-type: none"> <li>• CoS values</li> <li>• DSCP values</li> <li>• Precedence values</li> <li>• QoS group values</li> <li>• WLAN values</li> </ul> </li> <li>• <b>shape</b>—Traffic-shaping configuration options.</li> </ul> <p><b>Note</b><br/>This procedure describes the available configurations using <b>set</b> command options. The other command options (<b>bandwidth</b>) are described in other sections of this guide.</p> |

|               | Command or Action                                                                                                                                                                                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                                                                                                                                                                                     | Although this task lists all of the possible <b>set</b> commands, only one <b>set</b> command is supported per class.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 4</b> | <p><b>set cos</b> {<i>cos value</i>   <b>cos table</b> <i>table-map name</i>   <b>dscp table</b> <i>table-map name</i>   <b>precedence table</b> <i>table-map name</i>   <b>qos-group table</b> <i>table-map name</i>   <b>wlan user-priority table</b> <i>table-map name</i>}</p> <p><b>Example:</b></p> <pre>Router(config-pmap)# set cos 5</pre> | <p>(Optional) Sets the specific IEEE 802.1Q Layer 2 CoS value of an outgoing packet. Values are from 0 to 7.</p> <p>You can also set the following values using the <b>set cos</b> command:</p> <ul style="list-style-type: none"> <li>• <b>cos table</b>—Sets the CoS value based on a table map.</li> <li>• <b>dscp table</b>—Sets the code point value based on a table map.</li> <li>• <b>precedence table</b>—Sets the code point value based on a table map.</li> <li>• <b>qos-group table</b>—Sets the CoS value from QoS group based on a table map.</li> <li>• <b>wlan user-priority table</b>—Sets the CoS value from the WLAN user priority based on a table map.</li> </ul>                                                                                             |
| <b>Step 5</b> | <p><b>set dscp</b> {<i>dscp value</i>   <b>default</b>   <b>dscp table</b> <i>table-map name</i>   <b>ef</b>   <b>precedence table</b> <i>table-map name</i>   <b>qos-group table</b> <i>table-map name</i>   <b>wlan user-priority table</b> <i>table-map name</i>}</p> <p><b>Example:</b></p> <pre>Router(config-pmap)# set dscp af11</pre>       | <p>(Optional) Sets the DSCP value.</p> <p>In addition to setting specific DSCP values, you can also set the following using the <b>set dscp</b> command:</p> <ul style="list-style-type: none"> <li>• <b>default</b>—Matches packets with default DSCP value (000000).</li> <li>• <b>dscp table</b>—Sets the packet DSCP value from DSCP based on a table map.</li> <li>• <b>ef</b>—Matches packets with EF DSCP value (101110).</li> <li>• <b>precedence table</b>—Sets the packet DSCP value from precedence based on a table map.</li> <li>• <b>qos-group table</b>—Sets the packet DSCP value from a QoS group based upon a table map.</li> <li>• <b>wlan user-priority table</b>—Sets the packet DSCP value based upon a WLAN user-priority based upon a table map.</li> </ul> |

|        | Command or Action                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 6 | <b>set ip {dscp   precedence}</b><br><b>Example:</b><br>Router(config-pmap)# <b>set ip dscp c3</b>                                                                 | <p>(Optional) Sets IP specific values. These values are either IP DSCP or IP precedence values.</p> <p>You can set the following values using the <b>set ip dscp</b> command:</p> <ul style="list-style-type: none"> <li>• <b>dscp value</b>—Sets a specific DSCP value.</li> <li>• <b>default</b>—Matches packets with default DSCP value (000000).</li> <li>• <b>dscp table</b>—Sets the packet DSCP value from DSCP based on a table map.</li> <li>• <b>ef</b>—Matches packets with EF DSCP value (101110).</li> <li>• <b>precedence table</b>—Sets the packet DSCP value from precedence based on a table map.</li> <li>• <b>qos-group table</b>—Sets the packet DSCP value from a QoS group based upon a table map.</li> <li>• <b>wlan user-priority table</b>—Sets the packet DSCP value based upon a WLAN user-priority based upon a table map.</li> </ul> <p>You can set the following values using the <b>set ip precedence</b> command:</p> <ul style="list-style-type: none"> <li>• <b>precedence value</b>—Sets the precedence value (from 0 to 7) .</li> <li>• <b>cos table</b>—Sets the packet precedence value from Layer 2 CoS based on a table map.</li> <li>• <b>dscp table</b>—Sets the packet precedence from DSCP value based on a table map.</li> <li>• <b>precedence table</b>—Sets the precedence value from precedence based on a table map</li> <li>• <b>qos-group table</b>—Sets the precedence value from a QoS group based upon a table map.</li> </ul> |
| Step 7 | <b>set precedence {precedence value   cos table table-map name   dscp table table-map name   precedence table table-map name   qos-group table table-map name}</b> | <p>(Optional) Sets precedence values in IPv4 and IPv6 packets.</p> <p>You can set the following values using the <b>set precedence</b> command:</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                | Command or Action                                                                                                                                                                                                                                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <b>Example:</b><br>Router(config-pmap) # <b>set precedence 5</b>                                                                                                                                                                                                                                                                          | <ul style="list-style-type: none"> <li>• <b>precedence value</b>—Sets the precedence value (from 0 to 7) .</li> <li>• <b>cos table</b>—Sets the packet precedence value from Layer 2 CoS on a table map.</li> <li>• <b>dscp table</b>—Sets the packet precedence from DSCP value on a table map.</li> <li>• <b>precedence table</b>—Sets the precedence value from precedence based on a table map.</li> <li>• <b>qos-group table</b>—Sets the precedence value from a QoS group based upon a table map.</li> </ul>                                                                                                                  |
| <b>Step 8</b>  | <b>set qos-group</b> { <i>qos-group value</i>   <b>dscp table</b> <i>table-map name</i>   <b>precedence table</b> <i>table-map name</i> }<br><br><b>Example:</b><br>Router(config-pmap) # <b>set qos-group 10</b>                                                                                                                         | (Optional) Sets QoS group values. You can set the following values using this command: <ul style="list-style-type: none"> <li>• <b>qos-group value</b>—A number from 1 to 31.</li> <li>• <b>dscp table</b>—Sets the code point value from DSCP based on a table map.</li> <li>• <b>precedence table</b>—Sets the code point value from precedence based on a table map.</li> </ul>                                                                                                                                                                                                                                                   |
| <b>Step 9</b>  | <b>set wlan user-priority table</b> { <i>wlan user-priority table value</i>   <b>cos table</b> <i>table-map name</i>   <b>dscp table</b> <i>table-map name</i>   <b>qos-group table</b> <i>table-map name</i>   <b>wlan table</b> <i>table-map name</i> }<br><br><b>Example:</b><br>Router(config-pmap) # <b>set wlan user-priority 1</b> | (Optional) Sets the WLAN user priority value. You can set the following values using this command: <ul style="list-style-type: none"> <li>• <b>wlan user-priority value</b>—A value between 0 to 7.</li> <li>• <b>cos table</b>—Sets the WLAN user priority value from CoS based on a table map.</li> <li>• <b>dscp table</b>—Sets the WLAN user priority value from DSCP based on a table map.</li> <li>• <b>qos-group table</b>—Sets the WLAN user priority value from QoS group based on a table map.</li> <li>• <b>wlan table</b>—Sets the WLAN user priority value from the WLAN user priority based on a table map.</li> </ul> |
| <b>Step 10</b> | <b>end</b><br><br><b>Example:</b>                                                                                                                                                                                                                                                                                                         | Saves the configuration changes.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                | Command or Action                                                                   | Purpose                                                                                                   |
|----------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
|                | Router(config)# <b>end</b>                                                          |                                                                                                           |
| <b>Step 11</b> | <b>show policy-map</b><br><b>Example:</b><br>Router(config)# <b>show policy-map</b> | (Optional) Displays policy configuration information for all classes configured for all service policies. |

**What to do next**

Attach the traffic policy to an interface using the **service-policy** command.

## Attaching a Traffic Policy to an Interface

After the traffic class and traffic policy are created, you must use the **service-policy** interface configuration command to attach a traffic policy to an interface, and to specify the direction in which the policy should be applied (either on packets coming into the interface or packets leaving the interface).

**Before you begin**

A traffic class and traffic policy must be created before attaching a traffic policy to an interface.

**Procedure**

|               | Command or Action                                                                                                                                | Purpose                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                | Enter global configuration mode.                                                                                                                                                                                   |
| <b>Step 2</b> | <b>interface type</b>                                                                                                                            |                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>service-policy {input policy-map   output policy-map}</b><br><b>Example:</b><br>Router(config-if)# <b>service-policy output policy_map_01</b> | Attaches a policy map to an input or output interface. This policy map is then used as the service policy for that interface.<br>In this example, the traffic policy evaluates all traffic leaving that interface. |
| <b>Step 4</b> | <b>end</b><br><b>Example:</b><br>Router(config)# <b>end</b>                                                                                      | Saves the configuration changes.                                                                                                                                                                                   |
| <b>Step 5</b> | <b>show policy map</b><br><b>Example:</b><br>Router(config)# <b>show policy map</b>                                                              | (Optional) Displays statistics for the policy on the specified interface.                                                                                                                                          |

### Example

### What to do next

Proceed to attach any other traffic policy to an interface, and to specify the direction in which the policy should be applied.

## Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions supported are remarking and policing.

### Before you begin

You should have already decided upon the classification, policing, and marking of your network traffic by policy maps prior to beginning this procedure.

### Procedure

|               | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                              | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 2</b> | <b>class-map</b> { <i>class-map name</i>   <b>match-any</b> }<br><br><b>Example:</b><br>Device(config)# <b>class-map ipclass1</b><br>Device(config-cmap)# <b>exit</b>                              | Enters class map configuration mode.<br><br><ul style="list-style-type: none"> <li>Creates a class map to be used for matching packets to the class whose name you specify.</li> <li>If you specify <b>match-any</b>, one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default.</li> </ul> |
| <b>Step 3</b> | <b>match access-group</b> { <i>access list index</i>   <i>access list name</i> }<br><br><b>Example:</b><br>Device(config-cmap)# <b>match access-group 1000</b><br>Device(config-cmap)# <b>exit</b> | The following parameters are available for this command: <ul style="list-style-type: none"> <li>access-group</li> <li>cos</li> <li>dscp</li> <li>group-object</li> <li>ip</li> </ul>                                                                                                                                                                                              |

|               | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>• mpls</li> <li>• precedence</li> <li>• protocol</li> <li>• qos-group</li> <li>• vlan</li> <li>• wlan</li> </ul> <p>(Optional) For this example, enter the access-group ID:</p> <ul style="list-style-type: none"> <li>• Access list index (value from 1 to 2799)</li> <li>• Named access list</li> </ul>                                                                                                                                                                                                                                                                                                 |
| <b>Step 4</b> | <b>policy-map</b> <i>policy-map name</i><br><b>Example:</b><br>Router(config)# <b>policy-map type</b> ngsw-qos <b>flowit</b><br>Device(config-pmap) #                                   | <p>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.</p> <p>By default, no policy maps are defined.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 5</b> | <b>class</b> { <i>class-map-name</i>   <b>class-default</b> }<br><b>Example:</b><br>Device(config-pmap) # <b>class ipclass1</b>                                                         | <p>Defines a traffic classification, and enter policy-map class configuration mode.</p> <p>By default, no policy map class-maps are defined.</p> <p>If a traffic class has already been defined by using the <b>class-map</b> global configuration command, specify its name for class-map-name in this command.</p> <p>A <b>class-default</b> traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied <b>match any</b> included in the <b>class-default</b> class, all packets that have not already matched the other traffic classes will match <b>class-default</b>.</p> |
| <b>Step 6</b> | <b>set</b> { <b>cos</b>   <b>dscp</b>   <b>ip</b>   <b>precedence</b>   <b>qos-group</b>   <b>wlan user-priority</b> }<br><b>Example:</b><br>Device(config-pmap-c) # <b>set dscp 45</b> | <p>(Optional) Sets the QoS values. Possible QoS configuration values include:</p> <ul style="list-style-type: none"> <li>• <b>cos</b>—Sets the IEEE 802.1Q/ISL class of service/user priority.</li> <li>• <b>dscp</b>—Sets DSCP in IP(v4) and IPv6 packets.</li> <li>• <b>ip</b>—Sets IP specific values.</li> </ul>                                                                                                                                                                                                                                                                                                                             |

|                | Command or Action                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                                                                       | <ul style="list-style-type: none"> <li>• <b>precedence</b>—Sets precedence in IP(v4) and IPv6 packet.</li> <li>• <b>qos-group</b>—Sets QoS group.</li> <li>• <b>wlan user-priority</b>—Sets WLAN user priority.</li> </ul> <p>In this example, the <b>set dscp</b> command classifies the IP traffic by setting a new DSCP value in the packet.</p>                                                                                                                              |
| <b>Step 7</b>  | <b>police</b> { <i>target_bit_rate</i>   <b>cir</b>   <b>rate</b> }<br><br><b>Example:</b><br>Device(config-pmap-c) # <b>police 100000 conform-action transmit exceed-action drop</b> | (Optional) Configures the policer: <ul style="list-style-type: none"> <li>• <b>target_bit_rate</b>—Specifies the bit rate per second, enter a value between 8000 and 10000000000.</li> <li>• <b>cir</b>—Committed Information Rate.</li> <li>• <b>rate</b>—Specifies the police rate PCR for hierarchical policies.</li> </ul> <p>In this example, the <b>police</b> command adds a policer to the class where any traffic beyond the 100000 set target bit rate is dropped.</p> |
| <b>Step 8</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap-c) # <b>exit</b>                                                                                                             | Returns to policy map configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 9</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config-pmap) # <b>exit</b>                                                                                                               | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 10</b> | <b>interface</b> [ <i>interface-id</i> ]<br><br><b>Example:</b><br>Router(config) # <b>interface gigabitethernet 0/1/0</b>                                                            | Specifies the port to attach to the policy map, and enters interface configuration mode.<br><br>Valid interfaces include physical ports.                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 11</b> | <b>service-policy input</b> [ <i>policy-map-name</i> ]<br><br><b>Example:</b><br>Device(config-if) # <b>service-policy input flowit</b>                                               | Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 12</b> | <b>end</b><br><br><b>Example:</b><br>Router(config-if) # <b>end</b>                                                                                                                   | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                | Command or Action                                                                                                                                            | Purpose                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <b>Step 13</b> | <b>show policy-map</b> [ <i>policy-map-name</i> [ <b>class</b> <i>class-map-name</i> ]]<br><br><b>Example:</b><br><br>Router(config)# <b>show policy-map</b> | (Optional) Verifies your entries.                        |
| <b>Step 14</b> | <b>copy running-config startup-config</b><br><br><b>Example:</b><br><br>Router(config)# <b>copy running-config startup-config</b>                            | (Optional) Saves your entries in the configuration file. |

### What to do next

If applicable to your QoS configuration, configure classification, policing, and marking of traffic on SVIs by using policy maps.



## CHAPTER 9

# Power over Ethernet

- [Power over Ethernet, on page 129](#)
- [Device Detection and Power Allocation, on page 130](#)
- [Configuring Power Over Ethernet, on page 130](#)
- [Configuring Universal PoE, on page 131](#)
- [PoE Debug Commands, on page 132](#)

## 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 Cisco IR8340 routers support standard Power over Ethernet (PoE), Power over Ethernet Plus (PoE+), Cisco Enhanced Power over Ethernet (EPoE), and Cisco Universal Power over Ethernet (UPoE) on all copper ports. The total PoE available power is 120 W to be shared by the four LAN ports.

The following features are supported:

- UPoE—Supported on LAN port 1 and 2 with a maximum of 60 watts of power on each port
- PoE+—Supported on all PoE ports (LAN port 1-4) with a maximum of 30 watts of power on each port
- PoE—Supported on all PoE ports (LAN port 1-4) with a maximum of 15 watts of power on each port
- Support both Cisco PD and IEEE802.3af/IEEE802.3 on all ports, with DC power disconnected.
- Per port power consumption measurement.
- Ability to specify max power consumption on every port.
- PoE power policing—Comprises the following two modes, which determines the action to take on the interface after a port shuts down because of an inline-power policing violation:
  - **Logging**—An error message is logged to the console and the interface restarts; the device powers up.
  - **Errdisable** (default)—In addition to logging an error message to the console, the interface is placed in an errdisable state so that the device attached to the port does not receive inline-power until you restart the port or configure an errdisable autorecovery mechanism.
- Static power allocation on ports.

- Load Shedding upon PSU removal or failure.

## 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.

## Configuring Power Over Ethernet

Each copper port on the router can auto detect one of following connected devices, and supply power to them properly:

- An IEEE 802.3af and IEEE 802.3at compliant power device
- Cisco EPOE and UPOE power device

To configure power over ethernet, use these commands:

### Procedure

|               | Command or Action                                                                                                       | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                   | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 2</b> | <b>interface interface-id</b><br><br><b>Example:</b><br>Router(config)# <b>interface gigabitethernet0/1/0</b>           | Specifies the physical port to be configured, and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 3</b> | <b>power inline [auto  max max-wattage] never</b><br><br><b>Example:</b><br>Router(config-if)# <b>power inline auto</b> | Configures the PoE mode on the port. The keywords have these meanings: <ul style="list-style-type: none"> <li>• Auto—Enables powered-device detection. If enough power is available, automatically allocates power to the PoE port after device detection. This is the default setting.</li> <li>• Max max-wattage—Limits the power allowed on the port. The range for PoE+ ports is 4000 to 30000 mW. The range for</li> </ul> |

|               | Command or Action                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                          | <p>Cisco UPOE ports is 4000 to 60000 mW. If no value is specified, the maximum is allowed.</p> <ul style="list-style-type: none"> <li>• Never—Disables device detection, and disable power to the port.</li> </ul> <p><b>Note</b><br/>If a port has a Cisco powered device connected to it, do not use the <b>power inline never</b> command to configure the port. A false link-up can occur, placing the port into the error-disabled state.</p> |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br><code>router(config-if)# end</code> | Returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                   |

### What to do next

Use the following commands to check the PoE port status:

```
Router#show power inline
Available:120.0(w) Used:70.0(w) Remaining:50.0(w)
Interface Admin Oper Power Device Class Max
 (Watts)

Gi0/1/0 auto on 30.0 Ieee PD 4 60.0
Gi0/1/1 auto on 30.0 Ieee PD 4 60.0
Gi0/1/2 auto on 3.7 IP Phone 7811 1 30.0
Gi0/1/3 auto on 6.3 IP Phone 7962 2 30.0

Totals: 4 on 70.0

Router#show power inline gigabitEthernet 0/1/0
Interface Admin Oper Power Device Class Max
 (Watts)

Gi0/1/0 auto on 60.0 IR8340-K9 4 60.0
Router#
```

## Configuring Universal PoE

Cisco UPOE can provide a maximum of 60Watts power over both signal and spare pairs of RJ45 cable. UPOE capable switch port can enable spare pair and supply power to it through CDP or LLDP negotiations with UPOE power device automatically.

If end-point power device is capable to consume power on both signal and spare pairs but without corresponding CDP/LLDP negotiation mechanism available, following configurations can be used to manually force four-pair on specific port.

## Procedure

|               | Command or Action                                                                                                              | Purpose                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                          | Enter global configuration mode.                                                       |
| <b>Step 2</b> | <b>interface <i>interface-id</i></b><br><br><b>Example:</b><br>Router(config)# <b>interface</b><br><b>gigabitethernet0/1/0</b> | Specifies the physical port to be configured, and enters interface configuration mode. |
| <b>Step 3</b> | <b>power inline four-pair forced</b><br><br><b>Example:</b><br>Router(config-if)# <b>power inline four-pair forced</b>         | Forces power enabling on both signal and spare pairs from a switch port.               |
| <b>Step 4</b> | <b>end</b><br><br><b>Example:</b><br>router(config-if)# <b>end</b>                                                             | Returns to privileged EXEC mode.                                                       |

## PoE Debug Commands

The following table shows the PoE debug commands:

| Command                         | Description                                  |
|---------------------------------|----------------------------------------------|
| <b>debug ilpower controller</b> | Display PoE controller debug messages.       |
| <b>debug ilpower event</b>      | Display PoE event debug messages.            |
| <b>debug ilpower port</b>       | Display PoE port management debug messages.  |
| <b>debug ilpower powerman</b>   | Display PoE power management debug messages. |
| <b>debug ilpower cdp</b>        | Display PoE CDP debug messages.              |
| <b>debug ilpower registries</b> | Display PoE registries debug messages.       |
| <b>debug ilpower scp</b>        | Display PoE scp debug messages.              |



## CHAPTER 10

# Configuring the T1/E1 Network Interface Module

The Cisco T1/E1 Network Interface Modules (NIM) are inserted into the NIM slot on the router to provide T1, fractional T1, E1, and fractional E1 support for data applications.

- [Information About T1/E1 Network Interface Module, on page 133](#)
- [Configuring T1/E1 Network Interface Module, on page 133](#)

## Information About T1/E1 Network Interface Module

The IR8340 router has two Network Interface Module (NIM) slots, 0/2 and 0/3. The T1/E1 Network Interface Module IRM-NIM-2T1E1 can be installed in these two slots. It is a 2-port channelized data module and supports 24/31 channel groups for T1/E1 per port. Each T1/E1 module has two ports, P0 and P1. Each port is linked to a controller in configuration as below:

- If the module is in slot 0/2, it has two controllers 0/2/0 and 0/2/1.
- If the Module is in slot 0/3, it has two controllers 0/3/0 and 0/3/1.

Use RJ-48 cables to connect the T1/E1 modules between two devices.

## Configuring T1/E1 Network Interface Module

### Configuring the Card Type

The T1/E1 network interface module will not be operational until a card type is configured.

#### Procedure

|               | Command or Action                                             | Purpose                                                                                                          |
|---------------|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b> | Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul> |

|               | Command or Action                                                                                       | Purpose                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                   | Enter global configuration mode.                                                                                              |
| <b>Step 3</b> | <b>card type {t1 e1} slot subslot</b><br><br><b>Example:</b><br>Router(config)# <b>card type t1 0 2</b> | Specifies card type as T1 or E1 for the network interface module. In this example, the T1/E1 module is connected on 0/2 slot. |

## Changing the Card Type

### Procedure

|               | Command or Action                                                                                             | Purpose                                                                                                                          |
|---------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                 | Enables privileged EXEC mode.<br><br>• Enter your password if prompted.                                                          |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                         | Enter global configuration mode.                                                                                                 |
| <b>Step 3</b> | <b>no card type {t1 e1} slot subslot</b><br><br><b>Example:</b><br>Router(config)# <b>no card type t1 0 2</b> | (Optional) Removes the previous configuration.                                                                                   |
| <b>Step 4</b> | <b>card type {t1 e1} slot subslot</b><br><br><b>Example:</b><br>Router(config)# <b>card type e1 0 2</b>       | Specifies T1 or E1 connectivity for the network interface module.                                                                |
| <b>Step 5</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config)# <b>exit</b>                                             | Exits the card configuration mode and returns to global configuration mode.                                                      |
| <b>Step 6</b> | <b>write</b><br><br><b>Example:</b><br>Router(config)# <b>write</b>                                           | Rebuilds the router configuration.                                                                                               |
| <b>Step 7</b> | <b>reload</b><br><br><b>Example:</b><br>Router(config)# <b>reload</b>                                         | Reloads router so that changes can take effect. After this command executes, the router goes into the ROM monitor (rommon) mode. |

|               | Command or Action                                                   | Purpose                                                                   |
|---------------|---------------------------------------------------------------------|---------------------------------------------------------------------------|
| <b>Step 8</b> | <b>boot</b><br><br><b>Example:</b><br>Router (rommon) # <b>boot</b> | Boots the router with the configuration for the newly selected card type. |

## Configuring the T1/E1 Network Interface Module for Data Support

### Procedure

|               | Command or Action                                                                                                                                                                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                                                   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                         |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                           | Enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <b>controller {t1 e1} slot/subslot/port</b><br><br><b>Example:</b><br>Router (config) # <b>controller t1 0/2/0</b>                                                                                              | Enters controller configuration mode for the network interface module. <ul style="list-style-type: none"> <li>Valid values for slot is 0, subslot is 2 or 3, and port is 0 or 1.</li> </ul>                                                                                                                                                                                                                              |
| <b>Step 4</b> | Do one of the following: <b>framing {sf esf}</b> or <b>framing {crc4 no-crc4}</b><br><br><b>Example:</b><br>Router (config-controller) # <b>framing esf</b><br>Router (config-controller) # <b>framing crc4</b> | In T1 configurations, specifies super frame ( <b>sf</b> ) or extended super frame ( <b>esf</b> ) as the frame type for data lines. Default is <b>esf</b> .<br><br>In E1 configurations, specifies cyclic redundancy check 4 ( <b>crc4</b> ) or <b>no-crc4</b> as the frame type for data lines. Default is <b>crc4</b> .                                                                                                 |
| <b>Step 5</b> | Do one of the following: <b>linecode {ami b8zs}</b> or <b>linecode {ami hdb3}</b><br><br><b>Example:</b><br>Router (config-controller) # <b>linecode b8zs</b>                                                   | In T1 configurations, specifies alternate mark inversion (AMI) or bipolar 8-zero substitution (b8zs) as the linecode. Default is <b>b8zs</b> .<br><br><b>Note</b><br>When using linecode AMI, we recommend that you select 56 kbps as the speed or make sure that the channel groups created do not contain all the timeslots. See step 11. This is to avoid exceeding the “15 zeroes” threshold specified by standards. |
| <b>Step 6</b> | <b>fdl {att ansi both}</b><br><br><b>Example:</b><br>Router (config-controller) # <b>fdl both</b>                                                                                                               | T1 only. Sets the facility data link (fdl) exchange standard for T1 interfaces using esf framing. You can select the ATT standard                                                                                                                                                                                                                                                                                        |

|               | Command or Action                                                                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                                                                                            | (ATT TR54016), the ANSI standard (ANSI T1.403), or both standards. Default is <b>ansi</b> . To disable fdl, enter the <b>no fdl</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 7</b> | <b>clock source</b> { <b>internal</b>   <b>line</b> [ <b>primary</b>   <b>secondary</b> ]   <b>network</b> }<br><br><b>Example:</b><br><pre>Router(config-controller)# clock source network</pre>                                                          | <p>Specifies the clock source. The options are as follows:</p> <ul style="list-style-type: none"> <li>• <b>internal</b>—Sets the controller framer as the clock master.</li> </ul> <p>The <b>clock source i nternal</b> command is only applicable with the <b>channel-group</b> command and the <b>pri-group</b> (for data) command.</p> <p><b>Note</b><br/>The <b>pri-group</b> command is supported on the NIM-xCE1T1-PRI for data without the keyword <b>voice-dsp</b> .</p> <ul style="list-style-type: none"> <li>• <b>line</b>—Specifies the phase-locked loop (PLL) on a port. When both a primary port and a secondary port are configured and the primary port fails, the PLL switches over to the secondary. When the PLL on the primary port becomes active again, the PLL automatically switches to the primary port.</li> <li>• <b>network</b>—Sets the controller to sync to the TDMSW clock for both TDM voice and data support. This configures the far end of the T1/E1 line as the clock line.</li> </ul> <p>Default is line.</p> |
| <b>Step 8</b> | <b>line-termination</b> { <b>75-ohm</b>   <b>120-ohm</b> }<br><br><b>Example:</b><br><pre>Router(config-controller)# line-termination 75-ohm</pre>                                                                                                         | <p>E1 only. Sets the line termination on an E1 controller.</p> <ul style="list-style-type: none"> <li>• <b>75-ohm</b> specifies 75-ohm unbalanced termination.</li> <li>• <b>120-ohm</b> specifies 120-ohm balanced termination.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 9</b> | <b>loopback</b> { <b>diagnostic</b>   <b>local</b> { <b>payload</b>   <b>line</b> }   <b>remote</b> { <b>iboc</b>   <b>esf</b> { <b>payload</b>   <b>line</b> }}}<br><br><b>Example:</b><br><pre>Router(config-controller)# loopback remote esf line</pre> | <p>Sets the loopback method for testing the interface. Options are:</p> <ul style="list-style-type: none"> <li>• <b>diagnostic</b> —Loops the transmit signal back to receive.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|                | Command or Action                                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                                                                                                   | <ul style="list-style-type: none"> <li>• <b>local</b> — Puts the interface into local loopback mode at the <b>payload</b> or <b>line</b> level.</li> <li>• <b>remote</b> — Puts the interface into remote loopback mode through an inband bit oriented code (iboc) or, for T1 only, <b>remote esf</b>, which uses fdl codes to set <b>payload</b> or <b>line</b> levels.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 10</b> | <p>Do one of the following: <b>cablelength long</b> <i>db-loss-value</i> or <b>cablelength short</b> <i>length</i></p> <p><b>Example:</b></p> <pre>Router(config-controller)# cablelength short 110</pre>         | <p>T1 only. The <b>cablelength long</b> command attenuates the pulse from the transmitter using pulse equalization and line build-out. This command applies to cables longer than 660 feet. Loss values are:</p> <ul style="list-style-type: none"> <li>• 0db</li> <li>• -7.5db</li> <li>• -15db</li> <li>• -22.5db</li> </ul> <p>Default attenuation is 0db.</p> <p>The <b>cablelength short</b> command sets transmission attenuation for cable lengths of 660 feet or less. When you use the <b>cablelength short</b> command, specify the length as follows:</p> <ul style="list-style-type: none"> <li>• <b>110</b> for cable lengths from 0 to 110 feet</li> <li>• <b>220</b> for cable lengths from 111 to 220 feet</li> <li>• <b>330</b> for cable lengths from 221 to 330 feet</li> <li>• <b>440</b> for cable lengths from 331 to 440 feet</li> <li>• <b>550</b> for cable lengths from 441 to 550 feet</li> <li>• <b>660</b> for cable lengths from 551 to 660 feet</li> </ul> <p>There is no default cable length.</p> |
| <b>Step 11</b> | <p><b>channel group</b> <i>channel-group-number</i> {<i>timeslots range</i> [<i>speed kbps</i>]   <b>unframed</b>}</p> <p><b>Example:</b></p> <pre>Router(config-controller)# channel group 1 timeslots 1-4</pre> | <p>Configures the serial WAN on a T1 or E1 interface by specifying channels and their timeslots.</p> <p>For T1, values are as follows:</p> <ul style="list-style-type: none"> <li>• <b>channel-group-number</b> is from 0 to 23.</li> <li>• <b>timeslots</b> range is from 1 to 24.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                | Command or Action                                                                                                                             | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                               | <ul style="list-style-type: none"> <li>• Default value of <b>speed</b> for T1 is 64 kbps. Configuration of <b>speed</b> is optional.</li> </ul> <p>For E1, values are as follows:</p> <ul style="list-style-type: none"> <li>• channel-group-number is from 0 to 30.</li> <li>• <b>timeslots</b> range is from 1 to 31.</li> <li>• Default value of <b>speed</b> for E1 is 64 kbps. Configuration of <b>speed</b> is optional.</li> <li>• <b>unframed</b> (E1 only) specifies that all 31 timeslots are to be used for data and that none are to be used for framing signals.</li> </ul> |
| <b>Step 12</b> | <b>national reserve</b> <i>N sa4 sa5 sa6 sa7 sa8</i><br><b>Example:</b><br><pre>Router(config-controller)# national reserve 0 1 1 1 1 0</pre> | E1 only. Sets the six required national bits in E1 in the G.751 frame. Default is 1 1 1 1 1 1.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 13</b> | <b>crc-threshold</b> <i>value</i><br><b>Example:</b><br><pre>Router(config-controller)# crc-threshold 500</pre>                               | T1 only. Defines a severely errored second by specifying the number of CRC errors that must occur in one second to reach the severely errored second state. Default is 320.                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 14</b> | <b>yellow {generation detection}</b><br><b>Example:</b><br><pre>Router(config-controller)# no yellow detection</pre>                          | <p>Enables generation and detection of yellow alarms. Default condition is that <b>generation</b> and <b>detection</b> of yellow alarms are enabled.</p> <p>Use the <b>no</b> form of the command to disable yellow alarm detection.</p>                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 15</b> | <b>bert pattern</b> <i>pattern interval time</i><br><b>Example:</b><br><pre>Router(config-controller)# bert pattern 2^11 interval 1440</pre>  | <p>(Optional) Activates the BERT with the chosen test pattern for a specified duration. Configure BERT patterns on the T1/E1 network interface modules as follows:</p> <ul style="list-style-type: none"> <li>• When the linecode is AMI, use patterns 2^11, 2^15, or 2^20-QRSS.</li> <li>• When the linecode is b8zs or hdb3, use patterns 2^11, 2^15, 2^20-QRSS, or 2^20-O.153.</li> <li>• The <b>interval</b> time is from 1 to 14,400 minutes.</li> </ul>                                                                                                                            |

## Example of T1/E1 Network Interface Module Configuration

The following example shows the configuration of the router with the T1/E1 NIM installed and configured for data.

```
card type t1 0 2
controller T1 0/2/0
framing esf
linecode b8zs
cablelength long 0db
channel-group 0 timeslots 1
channel-group 1 timeslots 2
channel-group 2 timeslots 3
interface Serial0/2/0:0
 ip address 1.1.1.1 255.255.255.0
!
interface Serial0/2/0:1
 ip address 2.2.2.1 255.255.255.0
!
interface Serial0/2/0:2
 ip address 3.3.3.1 255.255.255.0
```





## CHAPTER 11

# Configuring the Serial Network Interface Module

- [About the Asynchronous/Synchronous Serial Network Interface Module, on page 141](#)
- [Configuring the Serial Interface to Sync or Async Mode, on page 141](#)
- [Configuring Synchronous Serial Ports, on page 142](#)
- [Configuring Asynchronous Serial Ports, on page 149](#)

## About the Asynchronous/Synchronous Serial Network Interface Module

The 8-port Asynchronous/Synchronous Network Interface Module (NIM) IRM-NIM-RS232 provides asynchronous/synchronous serial connections supporting EIA-RS232 for the Cisco IR8340 Router.

The IR8340 router has two NIM slots, 0/2 and 0/3. The serial NIMs can be installed in these two slots.

Each RS-232 Serial Module has 8 serial interfaces. The interface numbers are:

- serial 0/2/0 - serial 0/2/7—If the serial module is in slot 0/2.
- serial 0/3/0 - serial 0/3/7—If the serial module is in slot 0/3.

The following features are supported:

- Supports DCE and DTE.
- Each serial port can be configured as either Asynchronous or Synchronous mode.
- A maximum speed of 256 kbps is supported for RS232 Synchronous port.
- A maximum speed of 230.4 kbps is supported for Asynchronous port.

## Configuring the Serial Interface to Sync or Async Mode

By using the Physical Layer mode option, you can configure the serial interface to Synchronous or Asynchronous mode as needed. By default it will be in Synchronous mode. Use the following commands to configure the serial interface:

```
interface serial slot/subslot/port
```

**physical-layer {async|sync}**

```

Router(config)#interface Serial0/3/0
Router(config-if)#physical-layer ?
 async Configure asynchronous physical layer on serial interface
 sync Configure synchronous physical layer on serial interface

Router(config-if)#

```

## Configuring Synchronous Serial Ports

After the serial port mode is configured as synchronous mode, connect the DCE type serial cable to one side and DTE cable on the other side. The serial link will come up.

## Checking DCE and DTE Cable Type

After the serial port mode is configured as Sync, connect the DCE type serial cable to one side and DTE cable on the other side. The serial link will come up. Use the following command to check cable type:

```

Router1#show controllers Serial 0/3/0

Serial0/3/0 - (IRM-NIM-RS232) is administratively down
Encapsulation : HDLC
Cable type: RS-232 DCE
mtu 1500, max_buffer_size 1524, max_pak_size 1656 enc 132
loopback: Off, crc: 16, invert_data: Off
nrzi: Off, idle char: Flag
dce_terminal_timing_enable: Off ignore_dtr: Off
tx_clockrate: 64000bps, rx_clockrate: 64000bps, serial_clock_index: 0
serial_restartdelay:60000, serial_restartdelay_def:60000

 RTS up, CTS down, DTR up, DCD down, DSR down

Router1#

Router2#show controllers Serial 0/3/1

Serial0/3/1 - (IRM-NIM-RS232) is administratively down
Encapsulation : HDLC
Cable type: RS-232 DTE
mtu 1500, max_buffer_size 1524, max_pak_size 1656 enc 132
loopback: Off, crc: 16, invert_data: Off
nrzi: Off, idle char: Flag
tx_invert_clk: Off, ignore_dcd: Off
tx_clockrate: 31998bps, rx_clockrate: 31998bps, rx_clock_threshold: 0
serial_restartdelay:60000, serial_restartdelay_def:60000

 RTS down, CTS down, DTR down, DCD down, DSR down

Router2#

```

The **show interfaces serial0/3/0 controller** command can also be used to check the cable type.

## Specifying Synchronous Serial Encapsulation

The synchronous serial interfaces support the following serial encapsulation methods:

- Frame-Relay

- PPP (chap and pap)
- HDLC (default)

Use the following command to configure synchronous serial encapsulation. To remove the configuration, use the no form of the command.

**[no] encapsulation {frame-relay|ppp|hdlc}**

## DCE and DTE Configuration for HDLC Encapsulation

The following examples show the basic DCE and DTE configuration for HDLC encapsulation.

```
U1 configuration (DCE Side)
=====
U1#show running-config interface Serial0/3/1
Building configuration...
Current configuration : 99 bytes
!
interface Serial0/3/1
ip address 31.31.31.1 255.255.255.0
no keepalive
clock rate 256000
end

U1#show interfaces Serial0/3/1
Serial0/3/1 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 31.31.31.1/24
MTU 1500 bytes, BW 256 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 2/255
Encapsulation HDLC, loopback not set
Keepalive not set
Last input 00:00:31, output 00:00:09, output hang never

U1#ping 31.31.31.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 31.31.31.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

U2 configuration (DTE Side)
=====
U2#show running-config interface Serial0/3/1
Building configuration...
Current configuration : 80 bytes
!
interface Serial0/3/1
ip address 31.31.31.2 255.255.255.0
no keepalive
end

U2#show interfaces Serial0/3/1
Serial0/3/1 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 31.31.31.2/24
MTU 1500 bytes, BW 2000 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation HDLC, loopback not set
Keepalive not set
Last input 00:00:33, output 00:00:10, output hang never

U2#ping 31.31.31.1
```

```
*Jan 26 15:29:49.206 IST: %LINK-3-UPDOWN: Interface Serial0/3/6, changed state to down
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 31.31.31.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 7/8/9 ms
```

## DCE and DTE Configuration for PPP (CHAP) Encapsulation

The following examples show the basic DCE and DTE configuration for PPP (CHAP) encapsulation.

```
U1 configuration (DCE side)
=====
U1#show running-config interface Serial0/3/2
Building configuration...
Current configuration : 118 bytes
!
interface Serial0/3/2
ip address 32.32.32.1 255.255.255.0
encapsulation ppp
no keepalive
clock rate 256000
end
U1#show interfaces Serial0/3/2
Serial0/3/2 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 32.32.32.1/24
MTU 1500 bytes, BW 256 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set
Keepalive not set
Last input 00:00:13, output 00:00:13, output hang never

===configuration for ppp-chap authentication=====
U1(config)#username u1 secret userpassword
U1#show running-config interface Serial0/3/1
Building configuration...
Current configuration : 143 bytes
!
interface Serial0/3/1
ip address 31.31.31.2 255.255.255.0
encapsulation ppp
no keepalive
ppp authentication chap
clock rate 256000
end

U1#ping 32.32.32.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 32.32.32.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

U2 configuration (DTE Side)
=====
U2#show running-config interface Serial0/3/2
Building configuration...
Current configuration : 99 bytes
!
interface Serial0/3/2
ip address 32.32.32.2 255.255.255.0
encapsulation ppp
no keepalive
end
```

```

U2#show interfaces Serial0/3/2
Serial0/3/2 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 32.32.32.2/24
MTU 1500 bytes, BW 2000 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set
Keepalive not set
Last input 00:00:08, output 00:00:15, output hang never

===configuration for ppp-chap authentication=====
U2(config)#username U1 secret userpassword
U2#show running-config interface Serial0/3/1
Building configuration...
Current configuration : 124 bytes
!
interface Serial0/3/1
ip address 31.31.31.2 255.255.255.0
encapsulation ppp
no keepalive
ppp authentication chap
end

U2#ping 32.32.32.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 32.32.32.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms

```

## DCE and DTE Configuration for PPP (PAP) Encapsulation

The following examples show the basic DCE and DTE configuration for PPP (PAP) encapsulation.

```

U1 configuration (DCE side)
=====
U1#show running-config interface Serial0/3/2
Building configuration...
Current configuration : 118 bytes
!
interface Serial0/3/2
ip address 32.32.32.1 255.255.255.0
encapsulation ppp
no keepalive
clock rate 256000
end
U1#show interfaces Serial0/3/2
Serial0/3/2 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 32.32.32.1/24
MTU 1500 bytes, BW 256 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set
Keepalive not set
Last input 00:00:13, output 00:00:13, output hang never

===configuration for ppp-pap authentication=====
U1(config)#username u1 secret userpassword
U1#show running-config interface Serial0/3/1
Building configuration...
Current configuration : 181 bytes
!

```

```

interface Serial0/3/1
ip address 31.31.31.1 255.255.255.0
encapsulation ppp
ppp authentication pap
ppp pap sent-username Sumatra-1 password 0 userpassword
clock rate 256000
end
U1#

U1#ping 32.32.32.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 32.32.32.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms

U2 configuration (DTE Side)
=====
U2#show running-config interface Serial0/3/2
Building configuration...
Current configuration : 99 bytes
!
interface Serial0/3/2
ip address 32.32.32.2 255.255.255.0
encapsulation ppp
no keepalive
end

U2#show interfaces Serial0/3/2
Serial0/3/2 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 32.32.32.2/24
MTU 1500 bytes, BW 2000 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation PPP, LCP Open
Open: IPCP, CDPCP, loopback not set
Keepalive not set
Last input 00:00:08, output 00:00:15, output hang never

===configuration for ppp-pap authentication=====
U2(config)#username U1 secret userpassword
U2#show running-config interface Serial0/3/1
Building configuration...
Current configuration : 176 bytes
!
interface Serial0/3/1
ip address 31.31.31.2 255.255.255.0
encapsulation ppp
no keepalive
ppp authentication pap
ppp pap sent-username Sumatra-2 password 0 userpassword
end
U2

U2#ping 32.32.32.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 32.32.32.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms

```

## DCE and DTE Configuration for Frame Relay Encapsulation

The following examples show the basic DCE and DTE configuration for Frame Relay encapsulation.

```
U1 configuration (DCE side)
=====
U1#show running-config interface Serial0/3/3
Building configuration...
Current configuration : 158 bytes
!
interface Serial0/3/3
ip address 33.33.33.1 255.255.255.0
encapsulation frame-relay
no keepalive
clock rate 256000
frame-relay interface-dlci 100
end
U1#show interfaces Serial0/3/3
Serial0/3/3 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 33.33.33.1/24
MTU 1500 bytes, BW 256 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, loopback not set
Keepalive not set
FR SVC disabled, LAPF state down
Broadcast queue 0/64, broadcasts sent/dropped 1/0, interface broadcasts 0
Last input 00:00:16, output 00:00:16, output hang never

U1#ping 33.33.33.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 33.33.33.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/9 ms

U2 configuration (DTE Side)
=====
U2#show running-config interface Serial0/3/3
Building configuration...
Current configuration : 139 bytes
!
interface Serial0/3/3
ip address 33.33.33.2 255.255.255.0
encapsulation frame-relay
no keepalive
frame-relay interface-dlci 100
end
U2#show interfaces Serial0/3/3
Serial0/3/3 is up, line protocol is up
Hardware is IRM-NIM-RS232
Internet address is 33.33.33.2/24
MTU 1500 bytes, BW 2000 Kbit/sec, DLY 20000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation FRAME-RELAY, loopback not set
Keepalive not set
FR SVC disabled, LAPF state down
Broadcast queue 0/64, broadcasts sent/dropped 1/0, interface broadcasts 0
Last input 00:05:05, output 00:05:05, output hang never

U2#ping 33.33.33.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 33.33.33.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/8 ms
```

## Serial Synchronous Show and Debug Commands

This section provides show and debug commands of the serial synchronous interfaces.

1. Connect to the NIM console using Telnet or Secure Shell (SSH) and open a session to the device using the **hw-module session slot/subslot** command in privileged EXEC mode.

To exit the session, press **Ctrl-a** and **Ctrl-q** from your keyboard.

2. **show platform hardware subslot slot-number module device ge-stats**
3. **show platform hardware subslot slot-number module host-if status**
4. **show platform hardware subslot slot-number module host-if statistics**
5. **show platform hardware subslot slot-number module device ?**
  - help: the current information
  - scc-info: module serial information
  - scc-stats: module serial stats
  - scc-stats-p<x>: module serial port stats
  - ge-info: module ge information
  - ge-stats: module ge stats
  - fpga: module fpga information
  - fpga-p<x>: module fpga port information
  - fc-p<x>: module port flow control information
  - mempool: module mempool information
6. **debug hw-module subslot slot-number ?**
  - commands: Control plane configuration and commands
  - errors: Error handling and race conditions
  - events: Control plane event notifications
  - ha: SPA Specific HA
  - interrupts: Interrupt handling
  - obfl: SPA Specific OBFL (on-board failure logging)
  - oir: SPA OIR information
  - periodic: Periodic processing (for example, plugin\_one\_sec)
7. **show monitor event-trace spa all**
8. Use **show diag subslot slot-number eeprom detail** to check NIM eeprom contents

# Configuring Asynchronous Serial Ports

Configure the serial interface to Asynchronous mode by using these commands:

```
Router(config)#interface Serial0/3/0
Router(config-if)#physical-layer async
```

## Specifying Asynchronous Serial Encapsulation

The asynchronous serial interfaces support the following serial encapsulation methods:

- Block Serial tunneling (BSTUN)
- Raw socket TCP (Raw-TCP)
- Raw socket UDP (Raw-UDP)
- SCADA

Use the following command to configure asynchronous serial encapsulation. To remove the configuration, use the no form of the command.

**[no] encapsulation {bstun|raw-tcp|raw-udp|scada}**

### Example

```
Router(config)#interface Serial0/3/0
Router(config-if)#physical-layer async
Router(config-if)#encapsulation raw-tcp
Router(config-if)#end
Router#show running-config interface Serial0/3/0
Building configuration...

Current configuration : 89 bytes
!
interface Serial0/3/0
 physical-layer async
 no ip address
 encapsulation raw-tcp
end

Router#
```

Encapsulation methods are set according to the type of protocol or application you configure in the Cisco IOS software.





## CHAPTER 12

# Cellular Pluggable Interface Module Configuration Guide

---

- [Cellular Pluggable Interface Module Configuration Guide, on page 151](#)
- [Support for the P-5GS6-GL Pluggable Module on the ESR6300, on page 151](#)
- [Galileo Support on the LTE Pluggable Modules, on page 151](#)

## Cellular Pluggable Interface Module Configuration Guide

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



### Important

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

---

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

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

## Galileo Support on the LTE Pluggable Modules

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



### Note

Only ONE constellation can be enabled at a time.

---

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

## Configuration Commands

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

Example:

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




---

**Note** The default setting is gps mode.

---

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

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

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

## Show Commands

The following example shows the current GNSS constellation as Galileo:

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

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

More information is available in the [Cellular Pluggable Interface Module Configuration Guide](#).



## CHAPTER 13

# Information About SCADA

---

- [SCADA Overview, on page 153](#)
- [Role of the IR8340, on page 153](#)
- [Key Terms, on page 154](#)
- [Protocol Translation Application, on page 154](#)
- [Prerequisites, on page 155](#)
- [Guidelines and Limitations, on page 156](#)
- [Default Settings, on page 156](#)
- [Configuring Protocol Translation, on page 156](#)
- [Configuring the T101 Protocol Stack, on page 158](#)
- [Configuring the T104 Protocol Stack, on page 160](#)
- [Configuration Example, on page 164](#)
- [Configuring the DNP3 Protocol Stacks, on page 165](#)
- [Starting and Stopping the Protocol Translation Engine, on page 169](#)
- [Verifying Configuration, on page 170](#)
- [Debug Commands, on page 171](#)

## SCADA Overview

SCADA refers to a control and management system employed in industries such as water management, electric power, and manufacturing. A SCADA system collects data from various types of equipment within the system and forwards that information back to a Control Center for analysis. Generally, individuals located at the Control Center monitor the activity on the SCADA system and intervene when necessary.

The Remote Terminal Unit (RTU) acts as the primary control system within a SCADA system. RTUs are configured to control specific functions within the SCADA system, which can be modified as necessary through a user interface.

Change the serial interface mode as async and then configure the interface.

## Role of the IR8340

In the network, the Control Center always serves as the master in the network when communicating with the IR8340. The IR8340 serves as a proxy master station for the Control Center when it communicates with the RTU.

The IR8340 provides protocol translation to serve as a SCADA gateway to do the following:

- Receive data from RTUs and relay configuration commands from the Control Center to RTUs.
- Receive configuration commands from the Control Center and relay RTU data to the Control Center.
- Terminate incoming requests from the Control Center, when an RTU is offline.

The IR8340 performs Protocol Translation for the following protocols:

- IEC 60870 T101 to/from IEC 60870 T104
- DNP3 serial to DNP3 IP

## Key Terms

The following terms are relevant when you configure the T101 and T104 protocol stacks on the IR8340:

- **Channel**—A channel is configured on each IR8340 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single T101 (RTU) or T104 (Control Center) protocol stack.
- **Link Address**—Refers to the device or station address.
- **Link Mode (Balanced and Unbalanced)**—Refers to the modes of data transfer.
  - An Unbalanced setting refers to a data transfer initiated from the master.
  - A Balanced setting can refer to either a master or slave initiated data transfer.
- **Sector**—Refers to a single RTU within a remote site.
- **Sessions**—Represents a single connection to a remote site.

The following terms are relevant when you configure the DNP3 protocol stacks on the on the IR8340:

- **Channel**—A channel is configured on the IR8340 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single DNP3 serial (RTU) or DNP3 IP (Control Center) protocol stack.
- **Link Address**—Refers to the device or station address.
- **Sessions**—Represents a single connection to a remote site.

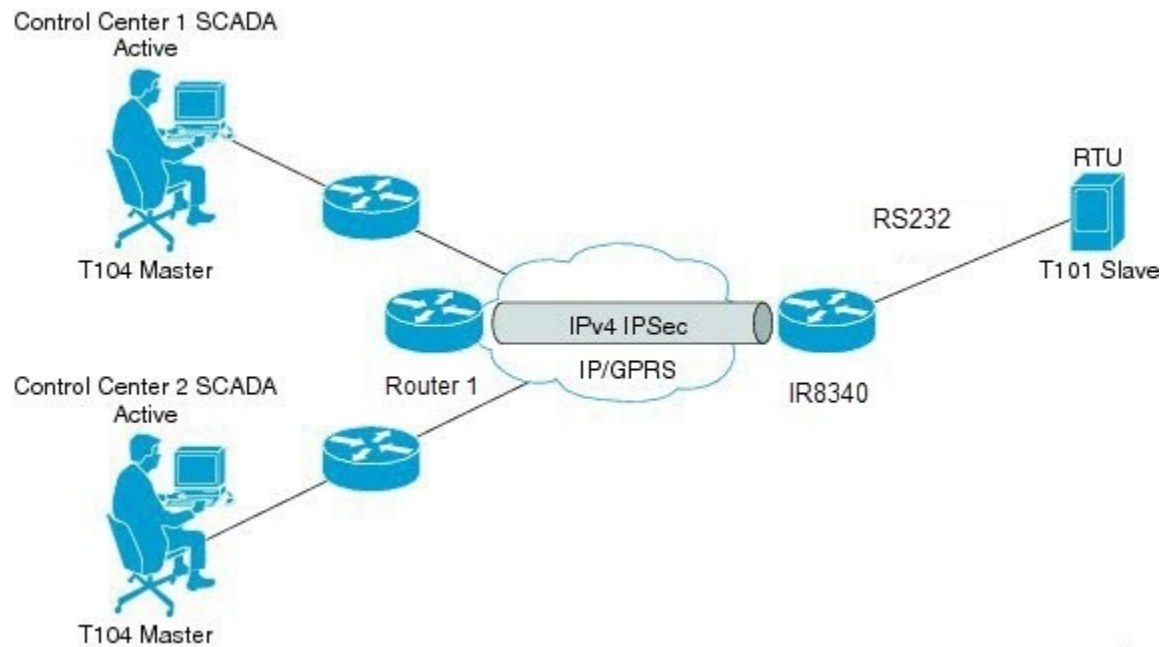
## Protocol Translation Application

In the following figure, IR8340 (installed within a secondary substation of the Utility Network) employs Protocol Translation to provide secure, end-to-end connectivity between Control Centers and RTUs within a SCADA System.

The IR8340 connects to the RTU (slave) through a RS232 connection. To protect the traffic when forwarded over public infrastructures (for example, cellular), the IR8340 forwards SCADA data from the RTU to the Control Center in the SCADA system through an IPSec tunnel (FlexVPN site-to-site or hub and spoke). The IPSec tunnel protects all traffic between the IR8340 and the Head-end aggregation router. SCADA traffic can

be inspected through an IPS device positioned in the path of the SCADA traffic before it is forwarded to the proper Control Center.

**Figure 1: Routers Within a SCADA System**



## Prerequisites

RTUs must be configured and operating in the network.

For each RTU that connects to the IR8340, you will need the following information for T101/T104:

- Channel information
  - Channel name
  - Connection type: serial
  - Link transmission procedure setting: unbalanced or balanced
  - Address field of the link (number expressed in octets)
- Session information
  - Session name
  - Size of common address of Application Service Data Unit (ASDU) (number expressed in octets)
  - Cause of transmission (COT) size (number expressed in octets)
  - Information object address (IOA) size (number expressed in octets)
- Sector information
  - Sector name

- ASDU address, (number expressed in octets)

For each RTU that connects to the IR8340, you will need the following information for DNP3:

- Channel information
  - Channel name
  - Connection type: serial
  - Link address
- Session information
  - Session name

## Guidelines and Limitations

- Each channel supports only one session.
- Each sessions supports only one sector.
- The object types 8, 17, 18, 19, 20, 38, 39, and 40 are not supported for IEC protocol translation.

## Default Settings

| T101/T104 Parameters | Default |
|----------------------|---------|
| Role for T101        | Slave   |
| Role for T104        | Master  |

| DNP3 Parameters                    | Default     |
|------------------------------------|-------------|
| Unsolicited Response (DNP3-serial) | Not Enabled |
| Send Unsolicited Message (DNP3-IP) | Enabled     |

## Configuring Protocol Translation

Before making any configuration changes to a IR8340 operating with Protocol Translation, please review the section on [Starting and Stopping the Protocol Translation Engine, on page 169](#).

## Enabling the IR8340 Serial Port and SCADA Encapsulation

Before you can enable and configure Protocol Translation on the IR8340, you must first enable the serial port on the IR8340 and enable SCADA encapsulation on that port.

### Before you begin

Determine availability of serial port on the IR8340.

### Procedure

|               | Command or Action                                  | Purpose                                                                                                                                                              |
|---------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                          | Enters the global configuration mode.                                                                                                                                |
| <b>Step 2</b> | <b>interface serial</b> <i>slot/port/interface</i> | Enters the interface command mode for the serial slot/port/interface.<br><br><i>slot</i> –value of 0<br><i>port</i> –value of 2 or 3<br><i>interface</i> –value of 0 |
| <b>Step 3</b> | <b>physical-layer async</b>                        | Configure the serial interface to Asynchronous mode.                                                                                                                 |
| <b>Step 4</b> | <b>no shutdown</b>                                 | Brings up the port, administratively.                                                                                                                                |
| <b>Step 5</b> | <b>encapsulation scada</b>                         | Enables encapsulation on the serial port for protocol translation and other SCADA protocols.                                                                         |

### EXAMPLE

This example shows how to enable serial port 0/2/0 and how to enable encapsulation on that interface to support SCADA protocols.

```
router# configure terminal
router(config)# interface serial 0/2/0
router(config-if)# physical-layer async
router(config-if)# no shutdown
router(config-if)# encapsulation scada
```

## Configuring T101 and T104 Protocol Stacks

You can configure T101 and T104 protocol stacks, which allow end-to-end communication between Control Centers (T104) and RTUs (T101) within a SCADA system.

- [Configuring the T101 Protocol Stack, on page 158](#)
- [Configuring the T104 Protocol Stack, on page 160](#)
- [Starting and Stopping the Protocol Translation Engine, on page 169](#)

## Prerequisites

Ensure that you have gathered all the required configuration information.

Enable the serial port and SCADA encapsulation.

## Configuring the T101 Protocol Stack

Configure the channel, session, and sector parameters for the T101 protocol stack.

### Before you begin

Ensure that you have gathered all the required configuration information. (See [Prerequisites](#), on page 155.)

Enable the serial port and SCADA encapsulation. (See [Enabling the IR8340 Serial Port and SCADA Encapsulation](#), on page 157.)

### Procedure

|               | Command or Action                                               | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                       | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 2</b> | <b>scada-gw protocol t101</b>                                   | Enters the configuration mode for the T101 protocol.                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <b>channel</b> <i>channel_name</i>                              | <p>Enters the channel configuration mode for the T101 protocol.</p> <p><i>channel_name</i> –Identifies the channel on which the serial port of the IR8340 communicates to the RTU.</p> <p><b>Note</b><br/>When the entered channel name does not already exist, the router creates a new channel.</p> <p>Entering the <b>no</b> form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</p> |
| <b>Step 4</b> | <b>role master</b>                                              | Assigns the master role to the T101 protocol channel (default).                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Step 5</b> | <b>link-mode</b> { <b>balanced</b>   <b>unbalanced</b> }        | <p>Configures the link-mode as either balanced or unbalanced.</p> <p>unbalanced—Refers to a data transfer initiated from the master.</p> <p>balanced—Refers to either a master or slave data transfer.</p>                                                                                                                                                                                                                                                   |
| <b>Step 6</b> | <b>link-addr-size</b> { <b>none</b>   <b>one</b>   <b>two</b> } | Defines the link address size in octets.                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                | Command or Action                                                    | Purpose                                                                                                                                                                                                         |
|----------------|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 7</b>  | <b>bind-to-interface serial</b> <i>slot/port/interface</i>           | Defines the IR8340 serial interface on which the system sends its T101 protocol traffic.<br><br><i>slot</i> –Value of 0<br><i>port</i> –Value of 2<br><i>interface</i> –Value of 0                              |
| <b>Step 8</b>  | <b>exit</b>                                                          | Ends configuration of the channel and exits the channel configuration mode. Saves all settings.                                                                                                                 |
| <b>Step 9</b>  | <b>session</b> <i>session_name</i>                                   | Enters the session configuration mode and assigns a name to the session.                                                                                                                                        |
| <b>Step 10</b> | <b>attach-to-channel</b> <i>channel_name</i>                         | Attaches the session to the channel.<br><br>Enter the same channel name that you entered in Step 3 .<br><br><i>channel_name</i> –Identifies the channel.                                                        |
| <b>Step 11</b> | <b>common-addr-size</b> { <b>one</b>   <b>two</b>   <b>three</b> }   | Defines the common address size in octets.                                                                                                                                                                      |
| <b>Step 12</b> | <b>cot size</b> { <b>one</b>   <b>two</b>   <b>three</b> }           | Defines the cause of transmission such as spontaneous or cyclic data schemes in octets.                                                                                                                         |
| <b>Step 13</b> | <b>info-obj-addr-size</b> { <b>one</b>   <b>two</b>   <b>three</b> } | Defines the information object element address size in octets.                                                                                                                                                  |
| <b>Step 14</b> | <b>link-addr-size</b> { <b>one</b>   <b>two</b>   <b>three</b> }     | Defines the link address size in octets.                                                                                                                                                                        |
| <b>Step 15</b> | <b>link-addr</b> <i>link_address</i>                                 | Refers to the link address of the RTU.<br><br><b>Note</b><br>The link address entered here must match the value set on the RTU to which the serial port connects.<br><br><i>link_address</i> –Range of 0-65535. |
| <b>Step 16</b> | <b>exit</b>                                                          | Exits the session configuration mode.                                                                                                                                                                           |
| <b>Step 17</b> | <b>sector</b> <i>sector_name</i>                                     | Enters the sector configuration mode and assigns a name to the sector for the RTU.<br><br><i>sector_name</i> –Identifies the sector.                                                                            |
| <b>Step 18</b> | <b>attach-to-session</b> <i>session_name</i>                         | Attaches the RTU sector to the session.<br><br>Enter the same session name that you entered in Step 9 .<br><br><i>session_name</i> - Identifies the session.                                                    |

## EXAMPLE

|                | Command or Action                    | Purpose                                          |
|----------------|--------------------------------------|--------------------------------------------------|
| <b>Step 19</b> | <b>asdu-addr</b> <i>asdu_address</i> | Refers to the ASDU structure address of the RTU. |
| <b>Step 20</b> | <b>exit</b>                          | Exits the sector configuration mode.             |
| <b>Step 21</b> | <b>exit</b>                          | Exits the protocol configuration mode.           |

## EXAMPLE

This example shows how to configure the parameters for the T101 protocol stack.

```

router# configure terminal
router(config)# scada-gw protocol t101
router(config-t101)# channel rtu_channel
router(config-t101-channel)# role master
router(config-t101-channel)# link-mode unbalanced
router(config-t101-channel)# link-addr-size one
router(config-t101-channel)# bind-to-interface serial 0/2/0
router(config-t101-channel)# exit
router(config-t101)# session rtu_session
router(config-t101-session)# attach-to-channel rtu_channel
router(config-t101-session)# common-addr-size two
router(config-t101-session)# cot-size one
router(config-t101-session)# info-obj-addr-size two
router(config-t101-session)# link-addr 3
router(config-t101-session)# exit
router(config-t101)# sector rtu_sector
router(config-t101-sector)# attach-to-session rtu_session
router(config-t101-sector)# asdu-addr 3
router(config-t101-sector)# exit
router(config-t101)# exit
router(config)#

```

## Configuring the T104 Protocol Stack

Follow the steps below for each Control Center that you want to connect to over a T104 protocol.

### Before you begin

Ensure that you have gathered all the required configuration information. (See [Prerequisites](#), on page 155.)

Enable the serial port and SCADA encapsulation. (See [Enabling the IR8340 Serial Port and SCADA Encapsulation](#), on page 157.)

### Procedure

|               | Command or Action             | Purpose                                              |
|---------------|-------------------------------|------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>     | Enters configuration mode.                           |
| <b>Step 2</b> | <b>scada-gw protocol t104</b> | Enters the configuration mode for the T104 protocol. |

|               | Command or Action                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>channel</b> <i>channel_name</i> | <p>Enters the channel configuration mode for the T104 protocol.</p> <p><i>channel_name</i> –Identifies the channel on which the router communicates with the Control Center.</p> <p><b>Note</b><br/>When the entered channel name does not already exist, the router creates a new channel.</p> <p>Entering the <b>no</b> form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</p> |
| <b>Step 4</b> | <b>k-value</b> <i>value</i>        | <p>Sets the maximum number of outstanding Application Protocol Data Units (APDUs) for the channel.</p> <p><b>Note</b><br/>An APDU incorporates the ASDU and a control header.</p> <p><i>value</i> –Range of values from 1 to 32767. Default value is 12 APDUs.</p>                                                                                                                                                                                     |
| <b>Step 5</b> | <b>w-value</b> <i>value</i>        | <p>Sets the maximum number of APDUs for the channel.</p> <p><i>value</i> –Range of values from 1 to 32767. Default value is 8 APDUs.</p>                                                                                                                                                                                                                                                                                                               |
| <b>Step 6</b> | <b>t0-timeout</b> <i>value</i>     | Defines the t0-timeout value for connection establishment of the T104 channel.                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 7</b> | <b>t1-timeout</b> <i>value</i>     | Defines the t1-timeout value for send or test APDUs on the T104 channel.                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Step 8</b> | <b>t2-timeout</b> <i>value</i>     | <p>Defines the t2-timeout value for acknowledgements when the router receives no data message.</p> <p><b>Note</b><br/>The t2 value must always be set to a lower value than the t1 value on the T104 channel.</p>                                                                                                                                                                                                                                      |
| <b>Step 9</b> | <b>t3-timeout</b> <i>value</i>     | <p>Defines the t3-timeout value for sending s-frames in case of a long idle state on the T104 channel.</p> <p><b>Note</b><br/>The t3 value must always be set to a higher value than the t1 value on the T104 channel.</p>                                                                                                                                                                                                                             |

|                | Command or Action                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 10</b> | <b>tcp-connection</b> {0 1} <b>local-port</b> { <i>port_number</i>   <b>default</b> } <b>remote-ip</b> { <i>A.B.C.D</i>   <i>A.B.C.D/LEN</i>   <b>any</b> } [ <b>vrf</b> <i>WORD</i> ] | In a configuration where there are redundant Control Centers, sets the connection value for the secondary Control Center as defined on the primary Control Center.<br><br><i>port-number</i> —value between 2000 and 65535.<br>default—value of 2404.<br><i>A.B.C.D</i> —single host.<br><i>A.B.C.D/nn</i> —subnet <i>A.B.C.D/LEN</i> .<br>any—any remote hosts 0.0.0.0/0.<br>WORD—VRF name. |
| <b>Step 11</b> | <b>exit</b>                                                                                                                                                                            | Exits the channel configuration mode.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 12</b> | <b>session</b> <i>session_name</i>                                                                                                                                                     | Enters the session configuration mode and assigns a name to the session.<br><br><i>session_name</i> —Use the same name that you assigned to the channel in Step 3.                                                                                                                                                                                                                           |
| <b>Step 13</b> | <b>attach-to-channel</b> <i>channel_name</i>                                                                                                                                           | Defines the name of the channel that transports the session traffic.                                                                                                                                                                                                                                                                                                                         |
| <b>Step 14</b> | <b>cot size</b> { <b>one</b>   <b>two</b>   <b>three</b> }                                                                                                                             | Defines the cause of transmission (cot), such as spontaneous or cyclic data schemes in octets.                                                                                                                                                                                                                                                                                               |
| <b>Step 15</b> | <b>exit</b>                                                                                                                                                                            | Exits the session configuration mode.                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 16</b> | <b>sector</b> <i>sector_name</i>                                                                                                                                                       | Enters the sector configuration mode and assigns a name to the sector for the Control Center.                                                                                                                                                                                                                                                                                                |
| <b>Step 17</b> | <b>attach-to-session</b> <i>session_name</i>                                                                                                                                           | Attaches the Control Center sector to the channel.<br><br><i>session_name</i> —Use the same name that you assigned to the channel in Step 3.                                                                                                                                                                                                                                                 |
| <b>Step 18</b> | <b>asdu-addr</b> <i>asdu_address</i>                                                                                                                                                   | Refers to the ASDU structure address. Value entered here must match the ASDU value on the RTU.<br><br><i>asdu_address</i> — <i>asdu_address</i> —Value of 1 or 2.                                                                                                                                                                                                                            |
| <b>Step 19</b> | <b>map-to-sector</b> <i>sector_name</i>                                                                                                                                                | Maps the Control Center (T104) sector to the RTU (T101) sector.                                                                                                                                                                                                                                                                                                                              |
| <b>Step 20</b> | Return to Step 1.                                                                                                                                                                      | Repeat all steps in this section for each Control Center active in the network.                                                                                                                                                                                                                                                                                                              |

## EXAMPLE

This example shows how to configure the parameters for the T104 protocol stack on *Control Center 1* and *Control Center 2*, both of which are configured as *masters*, and how to map the T104 sector to the T101 sector.

To configure Control Center 1 (*cc\_master1*), enter the following commands.

```
router# configure terminal
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master1
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2050 remote-ip 209.165.200.225
router(config-t104-channel)# tcp-connection 1 local-port 2051 remote-ip 209.165.201.25
router(config-t104-channel)# exit
router(config-t104)# session cc_master1
router(config-t104-session)# attach-to-channel cc_master1
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master1-sector
router(config-t104-sector)# attach-to-session cc_master1
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104)# exit
router(config)#
```

To configure Control Center 2 (*cc\_master2*), enter the following commands.

```
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master2
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2060 remote-ip 209.165.201.237
router(config-t104-channel)# tcp-connection 1 local-port 2061 remote-ip 209.165.200.27
router(config-t104-channel)# exit
router(config-t104)# session
cc_master2
router(config-t104-session)# attach-to-channel cc_master2
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master2-sector
router(config-t104-sector)# attach-to-session cc_master2
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104-sector)# exit
router(config-t104)# exit
router(config)#
```

## Configuration Example

The following example shows how to configure the serial port interface for T101 connection, configure T101 and T104 protocol stacks, and starts the Protocol Translation Engine on the IR8340.

```
router# configure terminal
router(config)# interface serial 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
router (config-if)# exit
router(config)# scada-gw protocol t101
router(config-t101)# channel rtu_channel
router(config-t101-channel)# role master
router(config-t101-channel)# link-mode unbalanced
router(config-t101-channel)# link-addr-size one
router(config-t101-channel)# bind-to-interface serial 0/2/0
router(config-t101-channel)# exit
router(config-t101)# session rtu_session
router(config-t101-session)# attach-to-channel rtu_channel
router(config-t101-session)# common-addr-size two
router(config-t101-session)# cot-size one
router(config-t101-session)# info-obj-addr-size two
router(config-t101-session)# link-addr 3
router(config-t101-session)# exit
router(config-t101)# sector rtu_sector
router(config-t101-sector)# attach-to-session rtu_session
router(config-t101-sector)# asdu-addr 3
router(config-t101-sector)# exit
router(config-t101)# exit
router(config)# scada-gw protocol t104
router(config-t104)# channel cc_master1
router(config-t104-channel)# k-value 12
router(config-t104-channel)# w-value 8
router(config-t104-channel)# t0-timeout 30
router(config-t104-channel)# t1-timeout 15
router(config-t104-channel)# t2-timeout 10
router(config-t104-channel)# t3-timeout 30
router(config-t104-channel)# tcp-connection 0 local-port 2050 remote-ip any
router(config-t104-channel)# tcp-connection 1 local-port 2051 remote-ip any
router(config-t104-channel)# exit
router(config-t104)# session cc_master1
router(config-t104-session)# attach-to-channel cc_master1
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master1-sector
router(config-t104-sector)# attach-to-session cc_master1
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104-sector)# exit

router(config-t104)# session cc_master2
router(config-t104-session)# attach-to-channel cc_master2
router(config-t104-session)# cot-size two
router(config-t104-session)# exit
router(config-t104)# sector cc_master2-sector
router(config-t104-sector)# attach-to-session cc_master2
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
router(config-t104-sector)# exit
```

```
router(config-t104)# exit
router(config)# scada-gw enable
```

This example configures end-to-end communication between Control Centers and RTUs within a SCADA system using the DNP3 protocol stacks and starts the Protocol Translation Engine on the IR8340:

```
router# configure terminal
router(config)# interface serial 0/2/0
router (config-if)# no shutdown
router (config-if)# encapsulation scada
router (config-if)# exit
router(config)# scada-gw protocol dnp3-serial
router(config-dnp3s)# channel rtu_channel
router(config-dnp3s-channel)# bind-to-interface serial 0/2/0
router(config-dnp3s-channel)# link-addr source 3
router(config-dnp3s-channel)# unsolicited-response enable
router(config-dnp3s-channel)# exit
router(config-dnp3s)# session rtu_session
router(config-dnp3s-session)# attach-to-channel rtu_channel
router(config-dnp3s-session)# link-addr dest 3
router(config-dnp3s-session)# exit
router(config-dnp3s)# exit
router(config)# scada-gw protocol dnp3-ip
router(config-dnp3n)# channel cc_channel
router(config-dnp3n-channel)# link-addr dest 3
router(config-dnp3n-channel)# tcp-connection local-port default remote-ip any
router(config-dnp3n-channel)# exit
router(config-dnp3n)# session cc_session
router(config-dnp3n-session)# attach-to-channel cc_channel
router(config-dnp3n-session)# link-addr source 3
router(config-dnp3n-session)# map-to-session rtu_session
router(config-dnp3n)# exit
router(config)# exit
router(config)# scada-gw enable
```



**Note** IOA addresses obtained from T101 side are sent to T104 side without any modification by the SCADA Gateway

## Configuring the DNP3 Protocol Stacks

You can configure the DNP3 serial and DNP3 IP protocol stacks, which allow end-to-end communication between Control Centers and RTUs within a SCADA system.

### Configuring DNP3 Serial

Configure the channel and session parameters for the DNP serial communication with an RTU.

#### Procedure

|               | Command or Action         | Purpose                           |
|---------------|---------------------------|-----------------------------------|
| <b>Step 1</b> | <b>configure terminal</b> | Enters global configuration mode. |

|                | Command or Action                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b>  | <b>scada-gw protocol dnp3-serial</b>             | Enters configuration mode for the DNP3 serial protocol.                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 3</b>  | <b>channel</b> <i>channel_name</i>               | <p>Enters channel configuration mode for the DNP3 serial protocol.</p> <p><i>channel_name</i> –Identifies the channel on which the router serial port communicates to the RTU.</p> <p>Note: When the entered channel name does not already exist, the router creates a new channel</p> <p>Entering the <b>no</b> form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</p> |
| <b>Step 4</b>  | <b>bind-to-interface serial 0/2/0</b>            | Defines the router async interface on which the system sends its DNP3 protocol traffic.                                                                                                                                                                                                                                                                                                                                                       |
| <b>Step 5</b>  | <b>link-addr source</b> <i>source_address</i>    | <p>Refers to the link address of the master.</p> <p><i>source_address</i> –Range of values from 1 to 65535.</p>                                                                                                                                                                                                                                                                                                                               |
| <b>Step 6</b>  | <b>unsolicited-response enable</b>               | <p>(Optional) Allows unsolicited responses.</p> <p>Entering the <b>no</b> form of this command disables unsolicited responses.</p> <p>The default is disabled.</p>                                                                                                                                                                                                                                                                            |
| <b>Step 7</b>  | <b>exit</b>                                      | Ends configuration of the channel and exits channel configuration mode. Saves all settings.                                                                                                                                                                                                                                                                                                                                                   |
| <b>Step 8</b>  | <b>session</b> <i>session_name</i>               | <p>Enters session configuration mode and assigns a name to the session.</p> <p>Note: When the entered session name does not already exist, the router creates a new session.</p> <p>Entering the <b>no</b> form of this command deletes an existing session.</p>                                                                                                                                                                              |
| <b>Step 9</b>  | <b>attach-to-channel</b> <i>channel_name</i>     | <p>Attaches the session to the channel.</p> <p>Note: Enter the same channel name that you entered in Step 3 above</p> <p><i>channel_name</i> –Identifies the channel.</p>                                                                                                                                                                                                                                                                     |
| <b>Step 10</b> | <b>link-addr dest</b> <i>destination_address</i> | <p>Refers to the link address of the slave.</p> <p><i>destination_address</i> –Range of values from 1 to 65535.</p>                                                                                                                                                                                                                                                                                                                           |

|                | Command or Action | Purpose                            |
|----------------|-------------------|------------------------------------|
| <b>Step 11</b> | <b>exit</b>       | Exits session configuration mode.  |
| <b>Step 12</b> | <b>exit</b>       | Exits protocol configuration mode. |

## EXAMPLE

This example shows how to configure the parameters for the DNP3-serial protocol stack:

```

router# configure terminal
router(config)# scada-gw protocol dnp3-serial
router(config-dnp3s)# channel rtu_channel
router(config-dnp3s-channel)# bind-to-interface serial 0/2/0
router(config-dnp3s-channel)# link-addr source 3
router(config-dnp3s-channel)# unsolicited-response enable
router(config-dnp3s-channel)# exit
router(config-dnp3s)# session rtu_session
router(config-dnp3s-session)# attach-to-channel rtu_channel
router(config-dnp3s-session)# link-addr dest 3
router(config-dnp3s-session)# exit
router(config-dnp3s)# exit
router(config)#

```

## Configuring DNP3 IP

Follow the steps below for the Control Center that you want to connect to over DNP3 IP. For redundancy, you can create multiple connections that share the same session configuration under the same session.

### Procedure

|               | Command or Action                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                        | Enters configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 2</b> | <b>scada-gw protocol dnp3-ip</b>                 | Enters configuration mode for the DNP-IP protocol.                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 3</b> | <b>channel <i>channel_name</i></b>               | <p>Enters channel configuration mode for the DNP-IP protocol.</p> <p><i>channel_name</i> –Identifies the channel on which the router communicates with the Control Center.</p> <p>Note: When the entered channel name does not already exist, the router creates a new channel.</p> <p>Entering the <b>no</b> form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</p> |
| <b>Step 4</b> | <b>link-addr dest <i>destination_address</i></b> | Refers to the link address of the master.                                                                                                                                                                                                                                                                                                                                                                                                  |

|                | Command or Action                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                   | <i>destination_address</i> –Range of values from 1 to 65535.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 5</b>  | <b>send-unsolicited-msg enable</b>                                                                                                | (Optional) Allow unsolicited messages.<br>The default is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 6</b>  | <b>tcp-connection local-port</b> [default   <i>local_port</i> ] <b>remote-ip</b> [any   <i>remote_ip</i>   <i>remote_subnet</i> ] | Configures the local port number and remote IP address for the TCP connection: <ul style="list-style-type: none"> <li>• <b>default</b>–20000.</li> <li>• <i>local_port</i> –Range of values from 2000 to 65535.</li> <li>• <b>any</b>–Any remote hosts 0.0.0.0/0</li> <li>• <i>remote_ip</i> –Single host: A.B.C.D</li> <li>• <i>remote_subnet</i> –Subnet: A.B.C.D/LEN</li> </ul> <p>If <i>remote_subnet</i> is specified, when two channels have the same local ports, the remote subnets cannot overlap each other.</p> <p>Note: Every &lt;local-port, remote-ip&gt; must be unique per channel. If <i>remote_subnet</i> is specified, when two channels have the same local ports, the remote subnets cannot overlap each other.</p> |
| <b>Step 7</b>  | <b>exit</b>                                                                                                                       | Exits channel configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 8</b>  | <b>session</b> <i>session_name</i>                                                                                                | Enters session configuration mode and assigns a name to the session.<br><br>Note: When the entered session name does not already exist, the router creates a new session.<br><br>Entering the <b>no</b> form of this command deletes an existing session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 9</b>  | <b>attach-to-channel</b> <i>channel_name</i>                                                                                      | Attaches the session to the channel.<br><br>Enter the same channel name that you entered in Step 3.<br><br><i>channel_name</i> –Identifies the channel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 10</b> | <b>link-addr source</b> <i>source_address</i>                                                                                     | Refers to the link address of the slave.<br><br><i>source_address</i> –Value of 1-65535.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 11</b> | <b>map-to-session</b> <i>session_name</i>                                                                                         | Maps the dnp3-ip session to an existing dnp3-serial session.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                | Command or Action | Purpose                                                                  |
|----------------|-------------------|--------------------------------------------------------------------------|
|                |                   | Note: One dnp3-ip session can be mapped to only one dnp3-serial session. |
| <b>Step 12</b> | <b>exit</b>       | Exits session configuration mode.                                        |
| <b>Step 13</b> | <b>exit</b>       | Exits protocol configuration mode.                                       |

## EXAMPLE

This example shows how to configure the DNP3 IP parameters:

```

router# configure terminal
router(config)# scada-gw protocol dnp3-ip
router(config-dnp3n)# channel cc_channel
router(config-dnp3n-channel)# link-addr dest 3
router(config-dnp3n-channel)# tcp-connection local-port default remote-ip any
router(config-dnp3n-channel)# exit
router(config-dnp3n)# session cc_session
router(config-dnp3n-session)# attach-to-channel cc_channel
router(config-dnp3n-session)# link-addr source 4
router(config-dnp3n-session)# map-to-session rtu_session
router(config-dnp3n)# exit
router(config)# exit

```

## Starting and Stopping the Protocol Translation Engine

You must start the Protocol Translation Engine to use Protocol Translation on the IR8340.

**Starting**—After enabling SCADA encapsulation on the IR8340 serial port and configuring the T101 and T104 protocols on the IR8340, you can start the Protocol Translation Engine.

**Stopping**—Before you can make any configuration changes to Protocol Translation on the IR8340 with an active Protocol Translation Engine, you must stop the engine.

### Before you begin

Before **starting** the Protocol Translation Engine on the router for the **first time**, make sure you complete the following items:

[Enabling the IR8340 Serial Port and SCADA Encapsulation, on page 157](#)

[Configuring T101 and T104 Protocol Stacks, on page 157](#)

### Procedure

|               | Command or Action           | Purpose                                                                                                                 |
|---------------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>   | Enters global configuration mode.                                                                                       |
| <b>Step 2</b> | <b>[no] scada-gw enable</b> | Starts ( <b>scada-gw enable</b> ) or stops ( <b>no scada-gw enable</b> ) the Protocol Translation Engine on the IR8340. |

## EXAMPLE

To start the protocol translation engine on the router, enter the following commands:

```
router# configure terminal
router(config)# scada-gw enable
```

To stop the protocol translation engine on the router, enter the following commands:

```
router# configure terminal
router(config)# no
scada-gw enable
```

## Verifying Configuration

| Command                      | Purpose                                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>show running-config</b>   | Shows the configuration of the router including active features and their settings.                               |
| <b>show scada database</b>   | Displays details on the SCADA database.                                                                           |
| <b>show scada statistics</b> | Shows statistics for the SCADA gateway, including the number of messages sent and received, timeouts, and errors. |
| <b>show scada tcp</b>        | Displays TCP connections associated with the SCADA gateway.                                                       |

This example shows the output from the show scada tcp and show scada statistics commands:

```
Router#show scada tcp
DNP3 network channel [test]: 4 max simultaneous connections
conn: local-ip: 3.3.3.21 local-port 20000 remote-ip 3.3.3.15 data-socket
1
Total:
1 current client connections
0 total closed connections
```

```
Router#show scada statistics
DNP3 network Channel [test]:
5 messages sent, 2 messages received
0 timeouts, 0 aborts, 0 rejections
2 protocol errors, 2 link errors, 0 address errors
DNP3 serial Channel [test]:
152 messages sent, 152 messages received
1 timeouts, 0 aborts, 0 rejections
0 protocol errors, 0 link errors, 0 address errors
```

```
Router#show scada database
----- Scada Gateway Database -----
Configuration Root
 State -- 0x3
 MaxEvents -- 0x258
 Retry -- 0x3
 DegradedFrequency -- 0x2710
 Timeout -- 0x2710
 PointsAvailableToAlloc -- 0x470
 From Master
 IEC 104
```

```

Line(2) status:DOWN
Link(2) status:DOWN InUse(0)
Request(-99):NOT running
function(1)id(1)Triggered(0)MustRun(0)Attempt(4)diff(3604)Freq(100)
RTU(101) status:DOWN InUse(0) Online(0)
Object(Single Input)
DI(100)
Value -- 0x0
Quality -- 0x4
DI(101)
Value -- 0x0
Quality -- 0x4
DI(102)
Value -- 0x0
Quality -- 0x4

```

## Debug Commands

This section lists some debug commands that are helpful when troubleshooting.

- SCADA device to trace debug commands:

```

#debug scada device ?
network Network device to trace
none No device to trace
serial Serial device to trace

#debug scada device network ?
<0-65535> Address of device to trace

#debug scada device none ?
<cr> <cr>

#debug scada device serial ?
<0-65535> Address of device to trace

```

- SCADA function level debug commands:

```

#debug scada function ?
analog analog output trace
clock clock trace
config config trace
control control trace
datalink datalink trace
driver-event Driver event debug
driver-packet Driver Packet debug
error error trace
event event trace
file file trace
freeze freeze trace
general general debug
physical physical trace
poll poll trace
protocol protocol trace
request request trace
stack stack trace
status status trace
tcp-event TCP event debug
timer timer trace
transport transport trace
umode umode trace

```





## CHAPTER 14

# Raw Socket Transport

Raw Socket Transport transports streams of characters from one serial interface to another over an IP network for utility applications.

This document describes Raw Socket Transport for the IR8340 and provides a reference section describing the Raw Socket Transport commands.

This document includes the following sections:

- [Information About Raw Socket Transport, on page 173](#)
- [Prerequisites, on page 176](#)
- [Guidelines and Limitations, on page 176](#)
- [Default Settings, on page 176](#)
- [Configuring Raw Socket Transport, on page 176](#)
- [Verifying Configuration, on page 182](#)
- [Configuration Example, on page 183](#)
- [Show Line Details for Configuring Raw-TCP/UDP, on page 186](#)
- [Raw-Socket Show and Debug Commands, on page 187](#)

## Information About Raw Socket Transport

Raw Socket is a method for transporting serial data through an IP network. The feature can be used to transport Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). This method is an alternative to the Block Serial Tunnel (BSTUN) protocol.

Raw Socket Transport supports TCP or UDP as the transport protocol. An interface can be configured to use either protocol but not both at the same time. TCP transport is suitable for applications such as control applications that require acknowledged and sequenced delivery of data. For latency-sensitive applications such as line SEL relays, UDP transport provides faster transport of serial data than TCP.

Raw Socket Transport supports the following for the asynchronous serial interface:

- TCP as the transport protocol, with built-in auto TCP connection retry mechanism.
- Up to 32 TCP sessions and 32 UDP sessions.
- Interface configuration as a server, client, or a combination of both.
- One server interface, but multiple clients.

- VRF-awareness, which enables the router to send Raw Socket Transport traffic to a server host connected through a Virtual Private Network (VPN) Virtual Routing and Forwarding (VRF) interface.

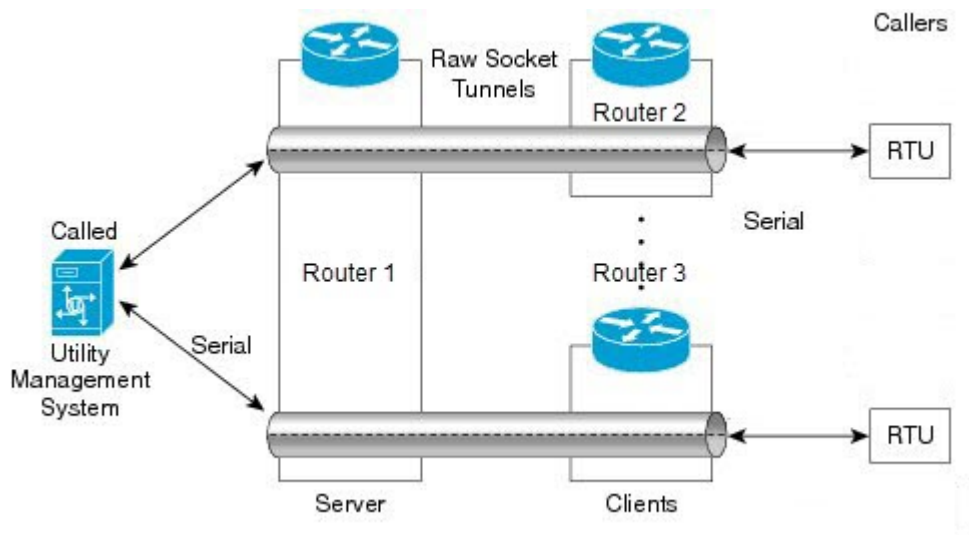
This section includes the following topics:

## TCP Transport

TCP Raw Socket transport uses a client-server model. At most one server and multiple clients can be configured on a single asynchronous serial line. In client mode, the IR8340 can initiate up to 32 TCP sessions to Raw Socket servers, which can be other IR8340 routers or third-party devices.

The following figure shows a sample Raw Socket TCP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes several IR8340 routers. One IR8340 router (Router 1) acts as a Raw Socket server, listening for TCP connection requests from the other IR8340 routers (Router 2 and Router 3), which are configured as Raw Socket clients.

A Raw Socket client receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The Raw Socket client initiates a TCP connection with the Raw Socket server and sends the packetized data across the IP network to the Raw Socket server, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.



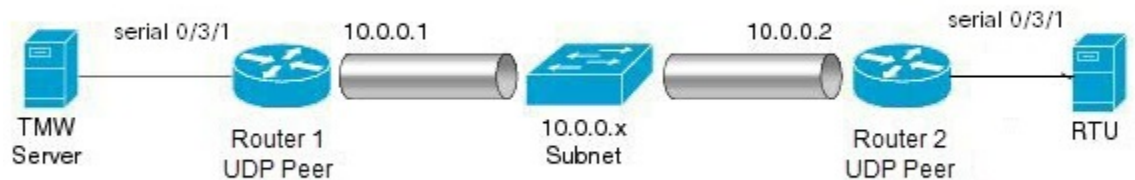
**Note** When you configure the serial link interface on the router as a server, the interface's peer is the serial link interface on the client router and vice versa.

## UDP Transport

UDP transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line. IR8340 can support up to 32 UDP sessions.

The following figure shows a sample Raw Socket UDP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes two routers that are configured as Raw Socket UDP peers.

In this example, the Raw Socket UDP peer receives streams of serial data from the RTUs and accumulates this data in its buffer, then places the data into packets, based on user-specified packetization criteria. The Raw Socket UDP peer sends the packetized data across the IP network to the Raw Socket peer at the other end, which retrieves the serial data from the packets and sends it to the serial interface, and on to the utility management system.



## Serial Data Processing

When the default serial protocol, Asynchronous Communication Protocol, is used, the streams of serial data received by a Raw Socket peer can be packetized based on the following criteria:

- **Packet length**—You can specify a packet length that triggers the IR8340 to transmit the serial data to the peer. Once the IR8340 collects this much data in its buffer, it packetizes the accumulated data and forwards it to the Raw Socket peer.
- **Packet-timer value**—The packet timer specifies the amount of time the IR8340 waits to receive the next character in a stream. If a character is not received by the time the packet timer expires, the data the IR8340 has accumulated in its buffer is packetized and forwarded to the Raw Socket peer.
- **Special character**—You can specify a character that will trigger the IR8340 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR8340 packetizes the accumulated data and sends it to the Raw Socket peer.

See [Configuring Common Raw Socket Line Options, on page 177](#) for information about configuring the processing options.

## VRF-Aware Raw Socket

The VRF-aware Raw Socket Transport feature enables you to isolate Raw Socket traffic using a VRF for efficient management and control of serial data. After configuring a VRF, you can associate the serial interface configured for Raw Socket Transport with the VRF. See [Raw Socket VRF, on page 185](#) for a configuration example.

## Prerequisites

Determine how you want Raw Socket traffic transported in your network, including the network devices and interfaces to use, how the router packetizes the serial data, and whether to use VRF.

## Guidelines and Limitations

Typically, UDP traffic is blocked by firewalls in the network. If the network has such firewalls, make sure to configure pinholes to allow the raw socket UDP traffic.

## Default Settings

| Feature              | Default Setting                                       |
|----------------------|-------------------------------------------------------|
| Raw Socket Transport | Disabled.                                             |
| Packet length        | No packet length is configured.                       |
| Serial Protocol      | Asynchronous Communication Protocol                   |
| Packet timeout       | 15 ms.                                                |
| Special character    | No special character is configured.                   |
| Raw Socket mode      | Best-effort mode is off, not supported on the IR8340. |
| TCP idle timeout     | 5 minutes.                                            |

## Configuring Raw Socket Transport

This section includes the following topics:

### Enabling Raw Socket Transport on the Serial Interface

To enable Raw Socket Transport on the IR8340 router, you must first enable an asynchronous serial port and enable Raw Socket TCP or UDP encapsulation for that port.

#### Before you begin

Determine availability of the serial port on the IR8340.

**Procedure**

|               | Command or Action                                                                                | Purpose                                                                        |
|---------------|--------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                        | Enters global configuration mode.                                              |
| <b>Step 2</b> | <b>interface serial</b> <i>slot/subslot/port</i>                                                 | Enters the interface command mode for the serial interface.                    |
| <b>Step 3</b> | <b>physical-layer async</b>                                                                      | Configure the serial interface to Asynchronous mode.                           |
| <b>Step 4</b> | <b>no ip address</b>                                                                             | Disables IP processing on the interface.                                       |
| <b>Step 5</b> | Do one of the following:<br><br>• <b>encapsulation raw-tcp</b><br>• <b>encapsulation raw-udp</b> | Enables Raw Socket TCP encapsulation or UDP encapsulation for the serial port. |

**Example**

```

router# configure terminal
router(config)# interface serial 0/3/2
router(config)# physical-layer async
router(config-if)# no ip address
router(config-if)# encapsulation raw-tcp
router(config-if)# exit

```

## Configuring Common Raw Socket Line Options

You can configure options common to all connections on a line. The common options apply to both TCP and UDP.

**Before you begin**

Enable Raw Socket Transport as described in [Enabling Raw Socket Transport on the Serial Interface, on page 176](#).

**Procedure**

|               | Command or Action                             | Purpose                                                                                                                                |
|---------------|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                     | Enters global configuration mode.                                                                                                      |
| <b>Step 2</b> | <b>line</b> <i>0/slot /port</i>               | Enters line command mode for the serial slot/port.                                                                                     |
| <b>Step 3</b> | <b>raw-socket packet-length</b> <i>length</i> | Specifies the packet size that triggers the IR8340 to transmit the data to the peer. When the IR8340 accumulates this much data in its |

|               | Command or Action                             | Purpose                                                                                                                                                                                                                                                                                                                |
|---------------|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                               | buffer, it packetizes the data and forwards it to the Raw Socket peer.<br><br><i>length</i> — 2 to 1400 bytes.<br><br>By default, the packet-length trigger is disabled.                                                                                                                                               |
| <b>Step 4</b> | <b>raw-socket packet-timer</b> <i>timeout</i> | Specifies the maximum time in milliseconds the IR8340 waits to receive the next character in a stream. If a character is not received by the time the packet-timer expires, the accumulated data is packetized and forwarded to the Raw Socket peer.<br><br><i>timeout</i> —3 to 1000 ms.<br><br>The default is 15 ms. |
| <b>Step 5</b> | <b>raw-socket spec-char</b> <i>ascii_char</i> | Specifies a character that will trigger the IR8340 to packetize the data accumulated in its buffer and send it to the Raw Socket peer.<br><br><i>ascii_char</i> — 0 to 255.<br><br>By default, the special character trigger is disabled.                                                                              |

### Example

```

router# configure terminal
router(config)# line 0/3/2
router(config-line)# raw-socket packet-length 32
router(config-line)# raw-socket packet-timer 500
router(config-line)# raw-socket special-char 3
router(config-line)# parity even
router(config-line)# stopbits 1
router(config-line)# speed 9600

```

### What to do next

Use the **no** form of these commands to return to the default values.

## Configuring Raw Socket TCP

After enabling Raw Socket TCP encapsulation, you configure the TCP server and/or clients.

### Configuring the Raw Socket TCP Server

#### Before you begin

Enable a serial port and Raw Socket TCP encapsulation for that port, as described in [Enabling Raw Socket Transport on the Serial Interface, on page 176](#).

## Procedure

|               | Command or Action                                  | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------|----------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                          | Enters configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 2</b> | <b>line 0/slot /port</b>                           | Enters line command mode for the serial slot/port.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 3</b> | <b>raw-socket tcp server port [ip_address ]</b>    | Starts the Raw Socket Transport TCP server for an asynchronous line interface. In Raw Socket server mode, the IR8340 listens for incoming connection requests from Raw Socket clients.<br><br><i>port</i> –Port number the server listens on.<br><br><i>ip_address</i> –(Optional) Local IP address on which the server listens for connection requests.                                                                                                                                                       |
| <b>Step 4</b> | <b>raw-socket tcp idle-timeout session_timeout</b> | Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session closes. The client then automatically attempts to reestablish the TCP session with the server.<br><br>This timeout setting applies to all Raw Socket Transport TCP sessions under this particular line.<br><br><i>session_timeout</i> –Currently configured session idle timeout in minutes. The default is 5 minutes. |

## Example

```

router# configure terminal

router(config)# line 0/3/2
router(config-line)# raw-socket tcp server 4000 10.0.0.1
router(config-line)# raw-socket tcp idle-timeout 10
router(config-line)# exit
router(config)#

```

## What to do next

To remove a Raw Socket TCP server, use the **no raw-socket tcp server** command.

## Configuring the Raw Socket TCP Client

### Before you begin

Enable a serial port and Raw Socket TCP encapsulation for that port, as described in [Enabling Raw Socket Transport on the Serial Interface, on page 176](#).

### Procedure

|               | Command or Action                                                                                                         | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                                 | Enters configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 2</b> | <b>line 0/slot /port</b>                                                                                                  | Enters line command mode for the serial slot/port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 3</b> | <b>raw-socket tcp client</b> <i>dest_ip_address</i><br><i>dest_port</i> [ <i>local_ip_address</i> ] [ <i>local_port</i> ] | Specifies settings for Raw Socket Transport TCP client sessions.<br><br><i>dest_ip_address</i> –Destination IP address of the remote Raw Socket server.<br><br><i>dest_port</i> –Destination port number to use for the TCP connection to the remote server.<br><br><i>local_ip_address</i> –(Optional) Local IP address that the client can also bind to.<br><br><i>local_port</i> –(Optional) Local port number that the client can also bind to.                                                               |
| <b>Step 4</b> | <b>raw-socket tcp idle-timeout</b> <i>session_timeout</i>                                                                 | Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session is closed. The client then automatically attempts to reestablish the TCP session with the server.<br><br>This timeout setting applies to all Raw Socket Transport TCP sessions under this particular line.<br><br><i>session_timeout</i> –Currently configured session idle timeout in minutes. The default is 5 minutes. |
| <b>Step 5</b> | <b>raw-socket tcp keepalive</b> <i>interval</i>                                                                           | Sets the Raw Socket Transport TCP session keepalive interval for the asynchronous line interface. The router sends keepalive messages based on the configured interval. You may need to configure this interval, for example, when sending raw TCP traffic over a cellular interface.                                                                                                                                                                                                                             |

|  | Command or Action | Purpose                                                                                                                  |
|--|-------------------|--------------------------------------------------------------------------------------------------------------------------|
|  |                   | <i>interval</i> –Currently configured keepalive interval in seconds. Range is 1-864000 seconds. The default is 1 second. |

### Example

This example shows how to configure a Raw Socket TCP client for an asynchronous serial line. The IR8340 (router), serving as a Raw Socket client, initiates TCP sessions with a Raw Socket server and forwards packetized serial data to it. The router collects streams of serial data in its buffer; when it accumulates 827 bytes in its buffer, the router packetizes the data and forwards it to the Raw Socket server. If the router and the Raw Socket server do not exchange any data for 10 minutes, then the TCP session with the Raw Socket server closes, and the router attempts to reestablish the session with the Raw Socket server.

```
router# configure terminal

router(config)# line 0/3/2
router(config-line)# raw-socket tcp client 10.0.0.1 4000
router(config-line)# raw-socket packet-length 827
router(config-line)# raw-socket tcp idle-timeout 10
router(config-line)# exit
router(config)#
```

### What to do next

To remove a Raw Socket TCP client, use the **no raw-socket tcp client** command.

## Configuring a Raw Socket UDP Peer-to-Peer Connection

After enabling Raw Socket UDP encapsulation and the common line options, you configure the Raw Socket UDP peer-to-peer connection. The local port on one end of the connection should be the destination port on the other end.

### Before you begin

Enable a serial port and Raw Socket UDP encapsulation for that port, as described in [Enabling Raw Socket Transport on the Serial Interface, on page 176](#).

### Procedure

|               | Command or Action                                                                                          | Purpose                                                      |
|---------------|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| <b>Step 1</b> | <b>configure terminal</b>                                                                                  | Enters configuration mode.                                   |
| <b>Step 2</b> | <b>line 0/slot /port</b>                                                                                   | Enters line command mode for the serial slot/port.           |
| <b>Step 3</b> | <b>raw-socket udp connection</b> <i>dest_ip_address</i><br><i>dest_port local_port [local_ip_address ]</i> | Specifies settings for Raw Socket Transport UDP connections. |

|  | Command or Action | Purpose                                                                                                                                                                                                                                                                                                   |
|--|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  |                   | <i>dest_ip_address</i> –Destination IP address to use for the UDP connection.<br><i>dest_port</i> –Destination port number to use for the UDP connection.<br><i>local_port</i> –Local port number for the UDP connection.<br><i>local_ip_address</i> –(Optional) Local IP address for the UDP connection. |

### Example

This example shows how to configure a Raw Socket UDP connection between router A (local IP address 192.168.0.8) and router B (local IP address 192.168.0.2).

#### Router A

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket udp connection 192.168.0.2 5000 7000
router(config-line)# exit
router(config)#
```

#### Router B

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket udp connection 192.168.0.8 7000 5000
router(config-line)# exit
router(config)#
```

### What to do next

To remove a Raw Socket UDP connection, use the **no raw-socket udp connection** command.

## Verifying Configuration

| Command                               | Purpose                                                                                             |
|---------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>show running-config</b>            | Shows the configuration of the IR8340, including those features that are active and their settings. |
| <b>show raw-socket tcp detail</b>     | Displays information about Raw Socket Transport TCP activity.                                       |
| <b>show raw-socket tcp sessions</b>   | Displays information about Raw Socket Transport TCP sessions.                                       |
| <b>show raw-socket tcp statistics</b> | Displays Raw Socket Transport TCP statistics for each asynchronous serial line.                     |

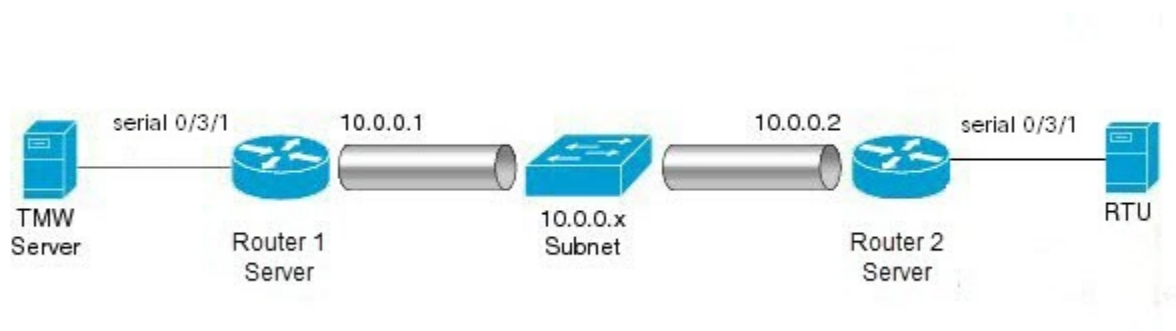
| Command                               | Purpose                                                                                                   |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------|
| <b>show raw-socket udp detail</b>     | Displays information about Raw Socket Transport UDP activity.                                             |
| <b>show raw-socket udp sessions</b>   | Displays information about Raw Socket Transport UDP sessions.                                             |
| <b>show raw-socket udp statistics</b> | Displays Raw Socket Transport UDP statistics for each asynchronous serial line.                           |
| <b>clear raw-socket statistics</b>    | Clears Raw Socket Transport statistics for a specific TTY interface or for all asynchronous serial lines. |

## Configuration Example

The following sections include Raw Socket Transport configuration examples:

### Raw Socket TCP

The following example shows a Raw Socket Transport configuration in which an IR8340 router (Router 1) acts as the server, and another IR8340 (Router 2) acts as the client.



The following table displays the configuration of the server and client IR8340s highlighted in the above figure:

| IR8340 Server Configuration                                                                                                                                                                                              | IR8340 Client Configuration                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre> ... interface serial 0/3/1  physical-layer async  no ip address  encapsulation raw-tcp ! ... line 0/3/1  raw-socket tcp server 5000 10.0.0.1   raw-socket packet-timer 3  raw-socket tcp idle-timeout 5 ... </pre> | <pre> ... interface serial 0/3/1  physical-layer async  no ip address  encapsulation raw-tcp ! interface serial 0/3/2  physical-layer async  no ip address  encapsulation raw-tcp ! ... line 0/3/1  raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9000   raw-socket packet-length 32  raw-socket tcp idle-timeout 5 line 0/3/2  raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9001   raw-socket packet-length 32  raw-socket tcp idle-timeout 5 </pre> |

## Raw Socket UDP

This example shows the configuration for a Raw Socket UDP connection between two IR8340 routers:

### From Router1

```

interface GigabitEthernet 0/1/1
ip address 192.168.0.8 255.255.255.0
duplex auto
speed auto
interface serial 0/3/2
 physical-layer async
 no ip address
 encapsulation raw-udp
 line 0/3/2
 raw-socket udp connection 192.168.0.2 4000 4000

```

### From Router2

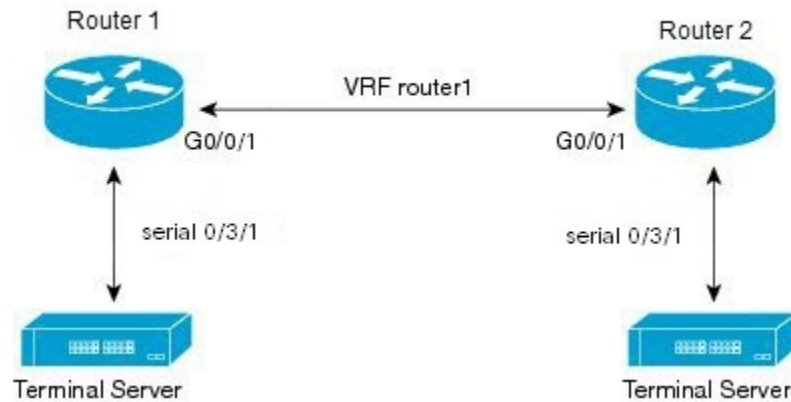
```

interface GigabitEthernet0/1/2
ip address 192.168.0.2 255.255.255.0
load-interval 60
duplex auto
speed auto
no keepalive
interface serial 0/3/2
 physical-layer async
 no ip address
 encapsulation raw-udp
 line 0/3/2
 raw-socket udp connection 192.168.0.8 4000 4000

```

## Raw Socket VRF

The following example shows a Raw Socket VRF configuration in which two routers, configured for Raw Socket Transport, connect through a VRF. Router1 is an IR8340, serves as the Raw Socket TCP server, and Router2 is an IR8340 serves as the Raw Socket TCP client.



Following are the configurations of Router1 and Router2 as shown in the above figure:

### Router1 Configuration

Defining VRF on the router:

```
vrf definition router1
 rd 100:1
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family
```

Applying VRF configuration on the interface:

```
interface GigabitEthernet0/0/1
 vrf forwarding router1
 ip address 100.100.100.2 255.255.255.0
 duplex auto
 speed auto
```

Applying raw-tcp on the serial interface:

```
interface serial 0/3/1
 physical-layer async
 vrf forwarding router1
 no ip address
 encapsulation raw-tcp
```

Applying raw-tcp on the line:

```
line 0/3/1
 raw-socket tcp server 5000 4.4.4.4
```

### Router2 Configuration

Defining VRF on the router:

```
vrf definition router1
 rd 100:1
 route-target export 100:3
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family
```

Applying VRF configuration on the interface:

```
interface GigabitEthernet0/0/1
 vrf forwarding router1
 ip address 100.100.100.1 255.255.255.0
 duplex auto
 speed auto
```

Applying raw-tcp on the serial interface:

```
interface serial 0/3/1
 physical-layer async
 vrf forwarding router1
 no ip address
 encapsulation raw-tcp
```

Applying raw-tcp on line:

```
line 0/3/1
 raw-socket tcp client 4.4.4.4 5000
```

## Show Line Details for Configuring Raw-TCP/UDP

The **show line** command shows all TTY line summary information. The output contains information about mapping between async interface and line number, the line speed, uses, noise, and so on. The line that begins with the asterisk "\*" indicates that the line is in use.

By enabling the physical layer Async on the serial port, the corresponding line will be activated and it will be displayed in the **show line** output. In the following example, 0/3/0 and 0/3/4 are configured as async mode and displayed.

```
U1#show line
```

| Tty | Line  | Typ     | Tx/Rx     | A | Modem | Roty | AccO | AccI | Uses | Noise | Overruns | Int     |
|-----|-------|---------|-----------|---|-------|------|------|------|------|-------|----------|---------|
| *   | 0     | 0 CTY   |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 1     | 1 AUX   | 9600/9600 | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 0/3/0 | 50 TTY  | 9600/9600 | - | -     | -    | -    | -    | 0    | 17    | 0/0      | Se0/3/0 |
|     | 0/3/4 | 54 TTY  | 9600/9600 | - | -     | -    | -    | -    | 0    | 0     | 0/0      | Se0/3/4 |
|     | 866   | 866 VTY |           | - | -     | -    | -    | -    | 3    | 0     | 0/0      | -       |
|     | 867   | 867 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 868   | 868 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 869   | 869 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 870   | 870 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 871   | 871 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 872   | 872 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 873   | 873 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 874   | 874 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 875   | 875 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 876   | 876 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 877   | 877 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 878   | 878 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 879   | 879 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |
|     | 880   | 880 VTY |           | - | -     | -    | -    | -    | 0    | 0     | 0/0      | -       |

Line(s) not in async mode -or- with no hardware support:

2-49, 51-53, 55-865  
U1#

## Raw-Socket Show and Debug Commands

Use the following show commands for the verification:

- **show raw-socket {tcp|udp} session**
- **show raw-socket {tcp|udp} statistic**

Use the following commands to debug:

**debug raw-socket ?**

driver        Driver level debug  
transport    Raw-socket over any transport

**debug raw-socket driver ?**

event        Driver event trace  
packet       Driver packet trace

**debug raw-socket driver event ?**

<cr> <cr>

**debug raw-socket driver packet ?**

line        Serial/Async line  
<cr> <cr>

**debug raw-socket driver packet line ?**

<0-726>    First Line range  
console    Primary terminal line  
tty        Terminal controller  
vty        Virtual terminal  
x/y/z      Slot/Subslot/Port for Modems

**debug raw-socket transport ?**

event       TCP or UDP event trace  
packet      TCP or UDP packet trace

**debug raw-socket transport event ?**

<cr> <cr>

**debug raw-socket transport packet ?**

line        Serial/Async line  
<cr> <cr>

**debug raw-socket transport packet line ?**

<0-726>    First Line range  
console    Primary terminal line  
tty        Terminal controller  
vty        Virtual terminal  
x/y/z      Slot/Subslot/Port for Modems





## CHAPTER 15

# Configuring Security for VPNs with IPsec

This chapter describes how to configure basic IPsec VPNs. IPsec is a framework of open standards developed by the IETF. It provides security for the transmission of sensitive information over unprotected networks such as the Internet. IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices (“peers”), such as Cisco routers.



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption](#) (NGE) white paper.

- [Information About Configuring Security for VPNs with IPsec, on page 189](#)
- [How to Configure IPsec VPNs, on page 192](#)

## Information About Configuring Security for VPNs with IPsec

### Supported Standards

Cisco implements the following standards with this feature:

- **IPsec**—IPsec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPsec provides these security services at the IP layer; IPsec uses IKE to handle negotiation of protocols and algorithms based on the local policy, and generate the encryption and authentication keys to be used by IPsec. IPsec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.



**Note** The term IPsec is sometimes used to describe the entire protocol of IPsec data services and IKE security protocols, and is also sometimes used to describe only the data services.

- **IKE (IKEv1 and IKEv2)**—A hybrid protocol that implements Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. While IKE is

used with other protocols, its initial implementation is with the IPsec protocol. IKE provides authentication of IPsec peers, negotiates IPsec security associations, and establishes IPsec keys.

The component technologies implemented for IPsec include:



**Note** Cisco no longer recommends using DES, 3DES, MD5 (including HMAC variant), and Diffie-Hellman (DH) groups 1, 2 and 5; instead, you should use AES, SHA and DH Groups 14 or higher. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption](#) (NGE) white paper.

- **AES**—Advanced Encryption Standard. A cryptographic algorithm that protects sensitive, unclassified information. AES is a privacy transform for IPsec and IKE and has been developed to replace DES. AES is designed to be more secure than DES. AES offers a larger key size, while ensuring that the only known approach to decrypt a message is for an intruder to try every possible key. AES has a variable key length—the algorithm can specify a 128-bit key (the default), a 192-bit key, or a 256-bit key.
- **DES**—Data Encryption Standard. An algorithm that is used to encrypt packet data. Cisco software implements the mandatory 56-bit DES-CBC with Explicit IV. Cipher Block Chaining (CBC) requires an initialization vector (IV) to start encryption. The IV is explicitly given in the IPsec packet. For backwards compatibility, Cisco IOS IPsec also implements the RFC 1829 version of ESP DES-CBC.

Cisco IOS also implements Triple DES (168-bit) encryption, depending on the software versions available for a specific platform. Cisco no longer recommends Triple DES (3DES).



**Note** Cisco IOS images with strong encryption (including, but not limited to 56-bit data encryption feature sets) are subject to United States government export controls, and have a limited distribution. Images to be installed outside the United States require an export license. Customer orders might be denied or subject to delay due to United States government regulations. Contact your sales representative or distributor for more information, or send an e-mail to [export@cisco.com](mailto:export@cisco.com).

- **SHA-2 and SHA-1 family (HMAC variant)**—Secure Hash Algorithm (SHA) 1 and 2. Both SHA-1 and SHA-2 are hash algorithms used to authenticate packet data and verify the integrity verification mechanisms for the IKE protocol. HMAC is a variant that provides an additional level of hashing. SHA-2 family adds the SHA-256 bit hash algorithm and SHA-384 bit hash algorithm. This functionality is part of the Suite-B requirements that comprises four user interface suites of cryptographic algorithms for use with IKE and IPsec that are described in RFC 4869. Each suite consists of an encryption algorithm, a digital signature algorithm, a key agreement algorithm, and a hash or message digest algorithm. See the Configuring Security for VPNs with IPsec feature module for more detailed information about Cisco IOS Suite-B support. SHA-2 for ISAKMP is supported in Cisco IOS XE 15.3(3)S and later.
- **Diffie-Hellman**—A public-key cryptography protocol that allows two parties to establish a shared secret over an unsecure communications channel. Diffie-Hellman is used within IKE to establish session keys. It supports 768-bit (the default), 1024-bit, 1536-bit, 2048-bit, 3072-bit, and 4096-bit DH groups. It also supports a 2048-bit DH group with a 256-bit subgroup, and 256-bit and 384-bit elliptic curve DH (ECDH). Cisco recommends using 2048-bit or larger DH key exchange, or ECDH key exchange.
- **MD5 (Hash-based Message Authentication Code (HMAC) variant)**—Message digest algorithm 5 (MD5) is a hash algorithm. HMAC is a keyed hash variant used to authenticate data.

IPsec as implemented in Cisco software supports the following additional standards:

- AH—Authentication Header. A security protocol, which provides data authentication and optional anti-replay services. AH is embedded in the data to be protected (a full IP datagram).
- ESP—Encapsulating Security Payload. A security protocol, which provides data privacy services and optional data authentication, and anti-replay services. ESP encapsulates the data to be protected.

## Supported Encapsulation

IPsec works with the following serial encapsulations: Frame Relay, High-Level Data-Links Control (HDLC), and PPP.

IPsec also works with Generic Routing Encapsulation (GRE) and IPinIP Layer 3, Data Link Switching+ (DLSw+), and Source Route Bridging (SRB) tunneling protocols; however, multipoint tunnels are not supported. Other Layer 3 tunneling protocols may not be supported for use with IPsec.

## IPsec Functionality Overview

IPsec provides the following network security services. (In general, the local security policy dictates the use of one or more of these services.)

- Data confidentiality—The IPsec sender can encrypt packets before transmitting them across a network.
- Data integrity—The IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission.
- Data origin authentication—The IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service.
- Anti-replay—The IPsec receiver can detect and reject replayed packets.

IPsec provides secure *tunnels* between two peers, such as two routers. You define which packets are considered sensitive and should be sent through these secure tunnels, and you define the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. (The use of the term *tunnel* in this chapter does not refer to using IPsec in tunnel mode.)

More accurately, these *tunnels* are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the router. “Applicable” packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.

Multiple IPsec tunnels can exist between two peers to secure different data streams, with each tunnel using a separate set of SAs. For example, some data streams only need to be authenticated, while other data streams must both be encrypted and authenticated.

## IKEv1 Transform Sets

An Internet Key Exchange version 1 (IKEv1) transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

## IKEv2 Transform Sets

An Internet Key Exchange version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE\_SA\_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation. The default proposal is a collection of commonly used algorithms which are as follows:

```
encryption aes-cbc-128 3des
integrity sha1 md5
group 5 2
```

Although the **crypto ikev2 proposal** command is similar to the **crypto isakmp policy priority** command, the IKEv2 proposal differs as follows:

- An IKEv2 proposal allows configuration of one or more transforms for each transform type.
- An IKEv2 proposal does not have any associated priority.



### Note

To use IKEv2 proposals in negotiation, they must be attached to IKEv2 policies. If a proposal is not configured, then the default IKEv2 proposal is used with the default IKEv2 policy.

# How to Configure IPsec VPNs

## Creating Crypto Access Lists

### Procedure

|               | Command or Action                                                                                                                              | Purpose                                                                                                               |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Router> <b>enable</b>                                                                                      | Enables privileged EXEC mode.<br><ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                              | Enters global configuration mode.                                                                                     |
| <b>Step 3</b> | Do one of the following: <b>access-list</b><br><i>access-list-number {deny   permit} protocol</i><br><i>source source-wildcard destination</i> | Specifies conditions to determine which IP packets are protected.                                                     |

|               | Command or Action                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <p><i>destination-wildcard</i> [log] or <b>ip access-list extended</b> <i>name</i></p> <p><b>Example:</b></p> <pre>Router(config)# access-list 100 permit ip 10.0.68.0 0.0.0.255 10.1.1.0 0.0.0.255 Router(config)# ip access-list extended vpn-tunnel</pre> | <ul style="list-style-type: none"> <li>You specify conditions using an IP access list designated by either a number or a name. The <b>access-list</b> command designates a numbered extended access list; the <b>ip access-list extended</b> command designates a named access list.</li> <li>Enable or disable crypto for traffic that matches these conditions.</li> </ul> <p><b>Tip</b><br/>Cisco recommends that you configure “mirror image” crypto access lists for use by IPsec and that you avoid using the <b>any</b> keyword.</p> |
| <b>Step 4</b> | Repeat Step 3 for each crypto access list you want to create.                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

### What to do next

After at least one crypto access list is created, a transform set needs to be defined as described in [Configuring Transform Sets for IKEv1 and IKEv2 Proposals, on page 193](#).

Next the crypto access lists need to be associated to particular interfaces when you configure and apply crypto map sets to the interfaces. (Follow the instructions in [Creating Crypto Map Sets, on page 197](#) and [Applying Crypto Map Sets to Interfaces, on page 205](#)).

## Configuring Transform Sets for IKEv1 and IKEv2 Proposals

Perform this task to define a transform set that is to be used by the IPsec peers during IPsec security association negotiations with IKEv1 and IKEv2 proposals.

### Restrictions

If you are specifying SEAL encryption, note the following restrictions:

- Your router and the other peer must not have a hardware IPsec encryption.
- Your router and the other peer must support IPsec.
- Your router and the other peer must support the k9 subsystem.
- SEAL encryption is available only on Cisco equipment. Therefore, interoperability is not possible.
- Unlike IKEv1, the authentication method and SA lifetime are not negotiable in IKEv2, and because of this, these parameters cannot be configured under the IKEv2 proposal.

## Configuring Transform Sets for IKEv1

### Procedure

|               | Command or Action                                                                                                                                                                                 | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                                                                                                                            |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 3</b> | <b>crypto ipsec transform-set transform-set-name transform1 [transform2 [transform3]]</b><br><b>Example:</b><br>Router(config)# <b>crypto ipsec transform-set aesset esp-aes 256 esp-sha-hmac</b> | Defines a transform set and enters crypto transform configuration mode. <ul style="list-style-type: none"> <li>• There are complex rules defining the entries that you can use for transform arguments. These rules are explained in the command description for the <b>crypto ipsec transform-set</b> command, and the table in “<a href="#">About Transform Sets</a>” section provides a list of allowed transform combinations.</li> </ul> |
| <b>Step 4</b> | <b>mode [tunnel   transport]</b><br><b>Example:</b><br>Router(cfg-crypto-tran)# <b>mode transport</b>                                                                                             | (Optional) Changes the mode associated with the transform set. <ul style="list-style-type: none"> <li>• The mode setting is applicable only to traffic whose source and destination addresses are the IPsec peer addresses; it is ignored for all other traffic. (All other traffic is in tunnel mode only.)</li> </ul>                                                                                                                       |
| <b>Step 5</b> | <b>end</b><br><b>Example:</b><br>Router(cfg-crypto-tran)# <b>end</b>                                                                                                                              | Exits crypto transform configuration mode and enters privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 6</b> | <b>clear crypto sa [peer {ip-address   peer-name}   sa map map-name   sa entry destination-address protocol spi]</b><br><b>Example:</b><br>Router# <b>clear crypto sa</b>                         | (Optional) Clears existing IPsec security associations so that any changes to a transform set takes effect on subsequently established security associations. <p>Manually established SAs are reestablished immediately.</p> <ul style="list-style-type: none"> <li>• Using the <b>clear crypto sa</b> command without parameters clears out the full SA database, which clears out active security sessions.</li> </ul>                      |

|               | Command or Action                                                                                                                                 | Purpose                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                   | <ul style="list-style-type: none"> <li>You may also specify the <b>peer</b>, <b>map</b>, or <b>entry</b> keywords to clear out only a subset of the SA database.</li> </ul> |
| <b>Step 7</b> | <b>show crypto ipsec transform-set</b> [ <i>tag transform-set-name</i> ]<br><br><b>Example:</b><br>Router# <b>show crypto ipsec transform-set</b> | (Optional) Displays the configured transform sets.                                                                                                                          |

### What to do next

After you have defined a transform set, you should create a crypto map as specified in [Creating Crypto Map Sets, on page 197](#).

## Configuring Transform Sets for IKEv2

### Procedure

|               | Command or Action                                                                                                                                    | Purpose                                                                                                                                                                                                                                                                                                                               |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                        | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>                                                                                                                                                                                                                      |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                | Enters global configuration mode.                                                                                                                                                                                                                                                                                                     |
| <b>Step 3</b> | <b>crypto ikev2 proposal</b> <i>proposal-name</i><br><br><b>Example:</b><br>Router(config)# <b>crypto ikev2 proposal proposal-1</b>                  | Specifies the name of the proposal and enters crypto IKEv2 proposal configuration mode. <ul style="list-style-type: none"> <li>The proposals are referred in IKEv2 policies through the proposal name.</li> </ul>                                                                                                                     |
| <b>Step 4</b> | <b>encryption</b> <i>transform1</i> [ <i>transform2</i> ] ...<br><br><b>Example:</b><br>Router(config-ikev2-proposal)# <b>encryption aes-cbc-128</b> | (Optional) Specifies one or more transforms of the following encryption type: <ul style="list-style-type: none"> <li>AES-CBC 128—128-bit AES-CBC</li> <li>AES-CBC 192—192-bit AES-CBC</li> <li>AES-CBC 256—256-bit AES-CBC</li> <li>3DES—168-bit DES (No longer recommended. AES is the recommended encryption algorithm).</li> </ul> |

|               | Command or Action                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b> | <b>integrity</b> <i>transform1</i> [ <i>transform2</i> ] ...<br><b>Example:</b><br><pre>Router(config-ikev2-proposal) # integrity sha1</pre> | (Optional) Specifies one or more transforms of the following integrity type: <ul style="list-style-type: none"> <li>• The <b>sha256</b> keyword specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.</li> <li>• The <b>sha384</b> keyword specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.</li> <li>• The <b>sha512</b> keyword specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.</li> <li>• The <b>sha1</b> keyword specifies the SHA-1 (HMAC variant) as the hash algorithm.</li> <li>• The <b>md5</b> keyword specifies MD5 (HMAC variant) as the hash algorithm. (No longer recommended. SHA-1 is the recommended replacement.)</li> </ul> |
| <b>Step 6</b> | <b>group</b> <i>transform1</i> [ <i>transform2</i> ] ...<br><b>Example:</b><br><pre>Router(config-ikev2-proposal) # group 14</pre>           | (Optional) Specifies one or more transforms of the possible DH group type: <ul style="list-style-type: none"> <li>• <b>1</b>—768-bit DH (No longer recommended.)</li> <li>• <b>2</b>—1024-bit DH (No longer recommended)</li> <li>• <b>5</b>—1536-bit DH (No longer recommended)</li> <li>• <b>14</b>—Specifies the 2048-bit DH group.</li> <li>• <b>15</b>—Specifies the 3072-bit DH group.</li> <li>• <b>16</b>—Specifies the 4096-bit DH group.</li> <li>• <b>19</b>—Specifies the 256-bit elliptic curve DH (ECDH) group.</li> <li>• <b>20</b>—Specifies the 384-bit ECDH group.</li> <li>• <b>24</b>—Specifies the 2048-bit DH/DSA group.</li> </ul>                                             |
| <b>Step 7</b> | <b>end</b><br><b>Example:</b><br><pre>Router(config-ikev2-proposal) # end</pre>                                                              | Exits crypto IKEv2 proposal configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|               | Command or Action                                                                                     | Purpose                                                     |
|---------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------|
| <b>Step 8</b> | <b>show crypto ikev2 proposal</b><br><br><b>Example:</b><br>Router# <b>show crypto ikev2 proposal</b> | (Optional) Displays the parameters for each IKEv2 proposal. |

## Creating Crypto Map Sets

### Creating Static Crypto Maps

When IKE is used to establish SAs, the IPsec peers can negotiate the settings they use for the new security associations. This means that you can specify lists (such as lists of acceptable transforms) within the crypto map entry.

Perform this task to create crypto map entries that use IKE to establish SAs. To create IPv6 crypto map entries, you must use the **ipv6** keyword with the **crypto map** command. For IPv4 crypto maps, use the **crypto map** command without the **ipv6** keyword.



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption](#) (NGE) white paper.

### Procedure

|               | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                   |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                          | Enters global configuration mode.                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>crypto map [ipv6] map-name seq-num [ipsec-isakmp]</b><br><br><b>Example:</b><br>Router(config)# <b>crypto map static-map 1 ipsec-isakmp</b> | Creates or modifies a crypto map entry, and enters crypto map configuration mode. <ul style="list-style-type: none"> <li>• For IPv4 crypto maps, use the command without the <b>ipv6</b> keyword.</li> </ul>                                                         |
| <b>Step 4</b> | <b>match address access-list-id</b><br><br><b>Example:</b><br>Router(config-crypto-m)# <b>match address vpn-tunnel</b>                         | Names an extended access list. <ul style="list-style-type: none"> <li>• This access list determines the traffic that should be protected by IPsec and the traffic that should not be protected by IPsec security in the context of this crypto map entry.</li> </ul> |

|                | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b>  | <b>set-peer</b> {hostname   ip-address}<br><b>Example:</b><br>Router(config-crypto-m) # <b>set-peer</b> 192.168.101.1                                                                                      | Specifies a remote IPsec peer—the peer to which IPsec protected traffic can be forwarded. <ul style="list-style-type: none"> <li>• Repeat for multiple remote peers.</li> </ul>                                                                                                                                                                                                                                                              |
| <b>Step 6</b>  | <b>crypto ipsec security-association dummy</b> {pps rate   seconds seconds}<br><b>Example:</b><br>Router(config-crypto-m) # <b>set security-association dummy seconds 5</b>                                | Enables generating dummy packets. These dummy packets are generated for all flows created in the crypto map.                                                                                                                                                                                                                                                                                                                                 |
| <b>Step 7</b>  | <b>set transform-set</b> transform-set-name1 [transform-set-name2...transform-set-name6]<br><b>Example:</b><br>Router(config-crypto-m) # <b>set transform-set aaset</b>                                    | Specifies the transform sets that are allowed for this crypto map entry. <ul style="list-style-type: none"> <li>• List multiple transform sets in the order of priority (highest priority first).</li> </ul>                                                                                                                                                                                                                                 |
| <b>Step 8</b>  | <b>set security-association lifetime</b> {seconds seconds   kilobytes kilobytes   kilobytes disable}<br><b>Example:</b><br>Router(config-crypto-m) # <b>set security-association lifetime seconds 2700</b> | (Optional) Specifies a SA lifetime for the crypto map entry. <ul style="list-style-type: none"> <li>• By default, the SAs of the crypto map are negotiated according to the global lifetimes, which can be disabled.</li> </ul>                                                                                                                                                                                                              |
| <b>Step 9</b>  | <b>set security-association level per-host</b><br><b>Example:</b><br>Router(config-crypto-m) # <b>set security-association level per-host</b>                                                              | (Optional) Specifies that separate SAs should be established for each source and destination host pair. <ul style="list-style-type: none"> <li>• By default, a single IPsec “tunnel” can carry traffic for multiple source hosts and multiple destination hosts.</li> </ul> <p><b>Caution</b><br/>           Use this command with care because multiple streams between given subnets can rapidly consume resources.</p>                    |
| <b>Step 10</b> | <b>set pfs</b> [group1   group14   group15   group16   group19   group2   group20   group24   group5]<br><b>Example:</b><br>Router(config-crypto-m) # <b>set pfs group14</b>                               | (Optional) Specifies that IPsec either should ask for password forward secrecy (PFS) when requesting new SAs for this crypto map entry or should demand PFS in requests received from the IPsec peer. <ul style="list-style-type: none"> <li>• Group 1 specifies the 768-bit Diffie-Hellman (DH) identifier (default). (No longer recommended).</li> <li>• Group 2 specifies the 1024-bit DH identifier. (No longer recommended).</li> </ul> |

|                | Command or Action                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                |                                                                                                                                | <ul style="list-style-type: none"> <li>• Group 5 specifies the 1536-bit DH identifier. (No longer recommended)</li> <li>• Group 14 specifies the 2048-bit DH identifier.</li> <li>• Group 15 specifies the 3072-bit DH identifier.</li> <li>• Group 16 specifies the 4096-bit DH identifier.</li> <li>• Group 19 specifies the 256-bit elliptic curve DH (ECDH) identifier.</li> <li>• Group 20 specifies the 384-bit ECDH identifier.</li> <li>• Group 24 specifies the 2048-bit DH/DSA identifier</li> <li>• By default, PFS is not requested. If no group is specified with this command, group 1 is used as the default.</li> </ul> |
| <b>Step 11</b> | <b>end</b><br><b>Example:</b><br>Router(config-crypto-m) # <b>end</b>                                                          | Exits crypto map configuration mode and returns to privileged EXEC mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Step 12</b> | <b>show crypto map [interface <i>interface</i>   tag <i>map-name</i>]</b><br><b>Example:</b><br>Router# <b>show crypto map</b> | Displays your crypto map configuration.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

Certain configuration changes take effect only when negotiating subsequent SAs. If you want the new settings to take immediate effect, you must clear the existing SAs so that they are reestablished with the changed configuration. If the router is actively processing IPsec traffic, clear only the portion of the SA database that would be affected by the configuration changes (that is, clear only the SAs established by a given crypto map set). Clearing the full SA database should be reserved for large-scale changes, or when the router is processing very little other IPsec traffic.

To clear IPsec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears out the full SA database, which clears active security sessions.)

### What to do next

After you have successfully created a static crypto map, you must apply the crypto map set to each interface through which IPsec traffic flows. To complete this task, see [Applying Crypto Map Sets to Interfaces, on page 205](#).

## Creating Dynamic Crypto Maps

Dynamic crypto map entries specify crypto access lists that limit traffic for which IPsec SAs can be established. A dynamic crypto map entry that does not specify an access list is ignored during traffic filtering. A dynamic crypto map entry with an empty access list causes traffic to be dropped. If there is only one dynamic crypto map entry in the crypto map set, it must specify the acceptable transform sets.

Perform this task to create dynamic crypto map entries that use IKE to establish the SAs.



**Note** IPv6 addresses are not supported on dynamic crypto maps.



**Note** Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the [Next Generation Encryption](#) (NGE) white paper.

### Procedure

|               | Command or Action                                                                                                                                                                       | Purpose                                                                                                                                                                                                                                                                             |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                               | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>                                                                                                                                                                  |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                                       | Enters global configuration mode.                                                                                                                                                                                                                                                   |
| <b>Step 3</b> | <b>crypto dynamic-map</b> <i>dynamic-map-name</i> <i>dynamic-seq-num</i><br><b>Example:</b><br>Router(config)# <b>crypto dynamic-map test-map 1</b>                                     | Creates a dynamic crypto map entry and enters crypto map configuration mode.                                                                                                                                                                                                        |
| <b>Step 4</b> | <b>set transform-set</b> <i>transform-set-name1</i> [ <i>transform-set-name2...transform-set-name6</i> ]<br><b>Example:</b><br>Router(config-crypto-m)# <b>set transform-set aasset</b> | Specifies the transform sets allowed for the crypto map entry. <ul style="list-style-type: none"> <li>• List multiple transform sets in the order of priority (highest priority first). This is the only configuration statement required in dynamic crypto map entries.</li> </ul> |
| <b>Step 5</b> | <b>match address</b> <i>access-list-id</i><br><b>Example:</b><br>Router(config-crypto-m)# <b>match address 101</b>                                                                      | (Optional) Specifies the list number or name of an extended access list. <ul style="list-style-type: none"> <li>• This access list determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec</li> </ul>                              |

|               | Command or Action                                                                                                                                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               |                                                                                                                                                                                                                       | <p>security in the context of this crypto map entry.</p> <p><b>Note</b><br/>Although access lists are optional for dynamic crypto maps, they are highly recommended.</p> <ul style="list-style-type: none"> <li>• If an access list is configured, the data flow identity proposed by the IPsec peer must fall within a <b>permit</b> statement for this crypto access list.</li> <li>• If an access list is not configured, the device accepts any data flow identity proposed by the IPsec peer. However, if an access list is configured but the specified access list does not exist or is empty, the device drops all packets. This is similar to static crypto maps, which require access lists to be specified.</li> <li>• Care must be taken if the <b>any</b> keyword is used in the access list, because the access list is used for packet filtering as well as for negotiation.</li> <li>• You must configure a match address; otherwise, the behavior is not secure, and you cannot enable TED because packets are sent in the clear (unencrypted.)</li> </ul> |
| <b>Step 6</b> | <p><b>set-peer</b> {hostname   ip-address}</p> <p><b>Example:</b></p> <pre>Router(config-crypto-m) # set-peer 192.168.101.1</pre>                                                                                     | <p>(Optional) Specifies a remote IPsec peer. Repeat this step for multiple remote peers.</p> <p><b>Note</b><br/>This is rarely configured in dynamic crypto map entries. Dynamic crypto map entries are often used for unknown remote peers.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 7</b> | <p><b>set security-association lifetime</b> {seconds seconds   kilobytes kilobytes   kilobytes disable}</p> <p><b>Example:</b></p> <pre>Router(config-crypto-m) # set security-association lifetime seconds 720</pre> | <p>(Optional) Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IP Security SAs.</p> <p><b>Note</b><br/>To minimize the possibility of packet loss when rekeying in high bandwidth environments, you can disable the rekey request triggered by a volume lifetime expiry.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|                | Command or Action                                                                                                                                                                | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 8</b>  | <b>set pfs [group1   group14   group15   group16   group19   group2   group20   group24   group5]</b><br><br><b>Example:</b><br>Router(config-crypto-m) # <b>set pfs group14</b> | (Optional) Specifies that IPsec should ask for PFS when requesting new security associations for this crypto map entry or should demand PFS in requests received from the IPsec peer. <ul style="list-style-type: none"> <li>• Group 1 specifies the 768-bit Diffie-Hellman (DH) identifier (default). (No longer recommended).</li> <li>• Group 2 specifies the 1024-bit DH identifier. (No longer recommended).</li> <li>• Group 5 specifies the 1536-bit DH identifier. (No longer recommended)</li> <li>• Group 14 specifies the 2048-bit DH identifier.</li> <li>• Group 15 specifies the 3072-bit DH identifier.</li> <li>• Group 16 specifies the 4096-bit DH identifier.</li> <li>• Group 19 specifies the 256-bit elliptic curve DH (ECDH) identifier.</li> <li>• Group 20 specifies the 384-bit ECDH identifier.</li> <li>• Group 24 specifies the 2048-bit DH/DSA identifier</li> <li>• By default, PFS is not requested. If no group is specified with this command, <b>group1</b> is used as the default.</li> </ul> |
| <b>Step 9</b>  | <b>exit</b><br><br><b>Example:</b><br>Router(config-crypto-m) # <b>exit</b>                                                                                                      | Exits crypto map configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Step 10</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config) # <b>exit</b>                                                                                                               | Exits global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 11</b> | <b>show crypto dynamic-map [tag map-name]</b><br><br><b>Example:</b><br>Router# <b>show crypto dynamic-map</b>                                                                   | (Optional) Displays information about dynamic crypto maps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Step 12</b> | <b>configure terminal</b><br><br><b>Example:</b>                                                                                                                                 | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                | Command or Action                                                                                                                                                                                                                              | Purpose                                                                                                                                                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | Router# <b>configure terminal</b>                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                                                |
| <b>Step 13</b> | <b>crypto map</b> <i>map-name seq-num ipsec-isakmp</i><br><b>dynamic</b> <i>dynamic-map-name</i> [ <b>discover</b> ]<br><br><b>Example:</b><br>Router(config)# <b>crypto map static-map</b><br><b>1 ipsec-isakmp dynamic test-map discover</b> | (Optional) Adds a dynamic crypto map to a crypto map set.<br><br><ul style="list-style-type: none"> <li>You should set the crypto map entries referencing dynamic maps to the lowest priority entries in a crypto map set.</li> </ul> <b>Note</b><br>You must enter the <b>discover</b> keyword to enable TED. |
| <b>Step 14</b> | <b>exit</b><br><br><b>Example:</b><br>Router(config)# <b>exit</b>                                                                                                                                                                              | Exits global configuration mode.                                                                                                                                                                                                                                                                               |

Certain configuration changes take effect only when negotiating subsequent SAs. If you want the new settings to take immediate effect, you must clear the existing SAs so that they are reestablished with the changed configuration. If the router is actively processing IPsec traffic, clear only the portion of the SA database that would be affected by the configuration changes (that is, clear only the SAs established by a given crypto map set). Clearing the entire SA database must be reserved for large-scale changes, or when the router is processing minimal IPsec traffic.

To clear IPsec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears the full SA database, which clears active security sessions.)

### What to do next

After you have successfully created a crypto map set, you must apply the crypto map set to each interface through which IPsec traffic flows. To complete this task, see [Applying Crypto Map Sets to Interfaces, on page 205](#).

## Creating Crypto Map Entries to Establish Manual SAs

Perform this task to create crypto map entries to establish manual SAs (that is, when IKE is not used to establish the SAs). To create IPv6 crypto maps entries, you must use the **ipv6** keyword with the **crypto map** command. For IPv4 crypto maps, use the **crypto map** command without the **ipv6** keyword.

### Procedure

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

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                      | Purpose                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Router# <b>configure terminal</b>                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | <b>crypto map [ipv6] map-name seq-num [ipsec-manual]</b><br><br><b>Example:</b><br>Router(config)# <b>crypto map mymap 10 ipsec-manual</b>                                                                                                                                                                                                                             | Specifies the crypto map entry to be created or modified and enters crypto map configuration mode. <ul style="list-style-type: none"> <li>For IPv4 crypto maps, use the <b>crypto map</b> command without the <b>ipv6</b> keyword.</li> </ul>                                                                      |
| <b>Step 4</b> | <b>match address access-list-id</b><br><br><b>Example:</b><br>Router(config-crypto-m)# <b>match address 102</b>                                                                                                                                                                                                                                                        | Names an IPsec access list that determines which traffic should be protected by IPsec and which traffic should not be protected by IPsec in the context of this crypto map entry. <ul style="list-style-type: none"> <li>The access list can specify only one <b>permit</b> entry when IKE is not used.</li> </ul> |
| <b>Step 5</b> | <b>set peer {hostname   ip-address}</b><br><br><b>Example:</b><br>Router(config-crypto-m)# <b>set peer 10.0.0.5</b>                                                                                                                                                                                                                                                    | Specifies the remote IPsec peer. This is the peer to which IPsec protected traffic should be forwarded. <ul style="list-style-type: none"> <li>Only one peer can be specified when IKE is not used.</li> </ul>                                                                                                     |
| <b>Step 6</b> | <b>set transform-set transform-set-name</b><br><br><b>Example:</b><br>Router(config-crypto-m)# <b>set transform-set someset</b>                                                                                                                                                                                                                                        | Specifies which transform set should be used. <ul style="list-style-type: none"> <li>This must be the same transform set that is specified in the remote peer's corresponding crypto map entry.</li> </ul> <p><b>Note</b><br/>Only one transform set can be specified when IKE is not used.</p>                    |
| <b>Step 7</b> | Do one of the following: <b>set session-key inbound ah spi hex-key-string</b> or <b>set session-key outbound ah spi hex-key-string</b><br><br><b>Example:</b><br>Router(config-crypto-m)# <b>set session-key inbound ah 256 98765432109876549876543210987654</b><br>Router(config-crypto-m)# <b>set session-key outbound ah 256 fedcbafedcbafedcbafedcbafedcbafedc</b> | Sets the AH security parameter indexes (SPIs) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the AH protocol. <ul style="list-style-type: none"> <li>This manually specifies the AH security association to be used with protected traffic.</li> </ul>        |
| <b>Step 8</b> | Do one of the following: <b>set session-key inbound ah esp spi cipher hex-key-string [authenticator hex-key-string]</b> or <b>set session-key outbound ah esp spi cipher hex-key-string [authenticator hex-key-string]</b><br><br><b>Example:</b>                                                                                                                      | Sets the Encapsulating Security Payload (ESP) Security Parameter Indexes (SPI) and keys to apply to inbound and outbound protected traffic if the specified transform set includes the ESP protocol. <p>Or</p>                                                                                                     |

|                | Command or Action                                                                                                                                                                   | Purpose                                                                                                                                                                                                                                                                                                                          |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <pre>Router(config-crypto-m) # set session-key inbound esp 256 cipher 0123456789012345 Router(config-crypto-m) # set session-key outbound esp 256 cipher abcdefghijklmnopabcd</pre> | <p>Specifies the cipher keys if the transform set includes an ESP cipher algorithm. Specifies the authenticator keys if the transform set includes an ESP authenticator algorithm.</p> <ul style="list-style-type: none"> <li>This manually specifies the ESP security association to be used with protected traffic.</li> </ul> |
| <b>Step 9</b>  | <p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-crypto-m) # exit</pre>                                                                                                 | Exits crypto map configuration mode and returns to global configuration mode.                                                                                                                                                                                                                                                    |
| <b>Step 10</b> | <p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config) # exit</pre>                                                                                                          | Exits global configuration mode.                                                                                                                                                                                                                                                                                                 |
| <b>Step 11</b> | <p><b>show crypto map [interface <i>interface</i>] tag <i>map-name</i>]</b></p> <p><b>Example:</b></p> <pre>Router# show crypto map</pre>                                           | Displays your crypto map configuration.                                                                                                                                                                                                                                                                                          |

For manually established SAs, you must clear and reinitialize the SAs for the changes to take effect. To clear IPsec SAs, use the **clear crypto sa** command with appropriate parameters. (Omitting all parameters clears the entire SA database, which clears active security sessions.)

### What to do next

After you have successfully created a crypto map set, you must apply the crypto map set to each interface through which IPsec traffic flows. To complete this task, see [Applying Crypto Map Sets to Interfaces, on page 205](#).

## Applying Crypto Map Sets to Interfaces

You must apply a crypto map set to each interface through which IPsec traffic flows. Applying the crypto map set to an interface instructs the device to evaluate the interface's traffic against the crypto map set and to use the specified policy during connection or security association negotiation on behalf of traffic to be protected by the crypto map.

Perform this task to apply a crypto map to an interface.

### Procedure

|               | Command or Action                           | Purpose                                                                                                                 |
|---------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <p><b>enable</b></p> <p><b>Example:</b></p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul> |

|               | Command or Action                                                                                                                                                          | Purpose                                                                                             |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
|               | Router> <b>enable</b>                                                                                                                                                      |                                                                                                     |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                          | Enters global configuration mode.                                                                   |
| <b>Step 3</b> | <b>interface</b> <i>type/number</i><br><b>Example:</b><br>Router# <b>(config)# interface Gi 0/0/1</b>                                                                      | Configures an interface and enters interface configuration mode.                                    |
| <b>Step 4</b> | <b>crypto map</b> <i>map-name</i><br><b>Example:</b><br>Router(config-if)# <b>crypto map mymap</b>                                                                         | Applies a crypto map set to an interface.                                                           |
| <b>Step 5</b> | <b>exit</b><br><b>Example:</b><br>Router(config-if)# <b>exit</b>                                                                                                           | Exits interface configuration mode and returns to global configuration mode.                        |
| <b>Step 6</b> | <b>crypto map</b> <i>map-name</i> <b>local-address</b> <i>interface-id</i><br><b>Example:</b><br>Router(config)# <b>crypto map mymap</b><br><b>local-address loopback0</b> | (Optional) Permits redundant interfaces to share the same crypto map using the same local identity. |
| <b>Step 7</b> | <b>exit</b><br><b>Example:</b><br>Router(config)# <b>exit</b>                                                                                                              | (Optional) Exits global configuration mode.                                                         |
| <b>Step 8</b> | <b>show crypto map</b> [ <b>interface</b> <i>interface</i> ]<br><b>Example:</b><br>Router# <b>show crypto map</b>                                                          | Displays your crypto map configuration.                                                             |



## CHAPTER 16

# Configuring Resilient Ethernet Protocol (REP)

Resilient Ethernet Protocol (REP) is a Cisco proprietary protocol that provides an alternative to Spanning Tree Protocol (STP) to control network loops, handle link failures, and improve convergence time.

For detailed information on configuring REP, see the [Configuring Resilient Ethernet Protocol](#) chapter in *Redundancy Protocol Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches*.



**Note** The following features are not supported on IR8340:

- REP Fast
- REP Day Zero
- REP Segment Id Auto Discovery
- REP Negotiated





## CHAPTER 17

# System Messages

This chapter contains the following sections:

- [Information About Process Management, on page 209](#)
- [How to Find Error Message Details, on page 209](#)

## 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: <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a> . With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <a href="http://www.cisco.com/cisco/psn/bssprt/bss">http://www.cisco.com/cisco/psn/bssprt/bss</a> . If you still require assistance, open a case with the Technical Assistance Center at: <a href="http://tools.cisco.com/ServiceRequestTool/create/">http://tools.cisco.com/ServiceRequestTool/create/</a> , 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 <b>show logging</b> and <b>show tech-support</b> commands and your pertinent troubleshooting logs. |

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

| Explanation | Recommended Action |
|-------------|--------------------|
|-------------|--------------------|

A process that does not affect the forwarding of traffic has failed.

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

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

#### Explanation

The process has failed as the result of an error.

#### Recommended Action

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

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

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

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

| Explanation                                                                                                 | Recommended Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The process was restarted too many times with repeated failures and has been placed in the hold-down state. | This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a> . With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <a href="http://www.cisco.com/cisco/psn/bssprt/bss">http://www.cisco.com/cisco/psn/bssprt/bss</a> . If you still require assistance, open a case with the Technical Assistance Center at: <a href="http://tools.cisco.com/ServiceRequestTool/create/">http://tools.cisco.com/ServiceRequestTool/create/</a> , 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 <b>show logging</b> and <b>show tech-support</b> 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-PROCSTART : 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

---

This chapter contains the following sections:

- [Environmental Monitoring, on page 215](#)
- [Environmental Monitoring and Reporting Functions, on page 215](#)
- [Environmental Monitoring Functions, on page 216](#)
- [Environmental Reporting Functions, on page 217](#)
- [Additional References, on page 217](#)

## 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 216](#)
- [Environmental Reporting Functions, on page 217](#)

# 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

- Operating Temperature: -40°F to 140°F (-40°C to 60°C)
- Operating Humidity: 5% to 95% relative humidity (non-condensing)
- Operating Altitude: Up to 10,000 ft (3048 m)



**Note** Refer to the *Cisco Catalyst IR8340 Rugged Series Router Hardware Installation Guide* for restricted ranges of the environmental operating conditions for exceptions which is specially applicable for harsh industrial deployments.

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

**Table 13: 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.

## 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> . |

## Technical Assistance

| Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Link                                                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | <p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p> |



## CHAPTER 19

# IOx Application Hosting

---

This section contains the following topics:

- [Application Hosting, on page 219](#)
- [Information About Application Hosting, on page 219](#)
- [Application Hosting on the IR8340 Router, on page 221](#)
- [How to Configure Application Hosting, on page 223](#)
- [Installing and Uninstalling Apps, on page 228](#)
- [Overriding the App Resource Configuration, on page 229](#)
- [IOx Configuration with ERSPAN, on page 230](#)
- [Verifying the Application Hosting Configuration, on page 231](#)
- [Configuration Examples for Application Hosting, on page 233](#)
- [Signed Application Support, on page 234](#)
- [Cisco Cyber Vision, on page 234](#)

## 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 chapter describes the Application Hosting feature and how to enable it.

## Information About Application Hosting

This section provides 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 installation requires Cisco supported SD flash on device with size greater than or equal to 4 GB. The SD card should be formatted to ext4 format with the following command:

```
#format sdcard: ext4
```

The SD card can not be used as a storage for any files or sync option. The application package or tar file need to be placed in the flash: or any supported external storage for configuring via CLI.

## Cisco Application Hosting Overview

The IR8340 allows you to deploy applications using the application hosting CLI commands. You can also deploy applications using the Local Manager.

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 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

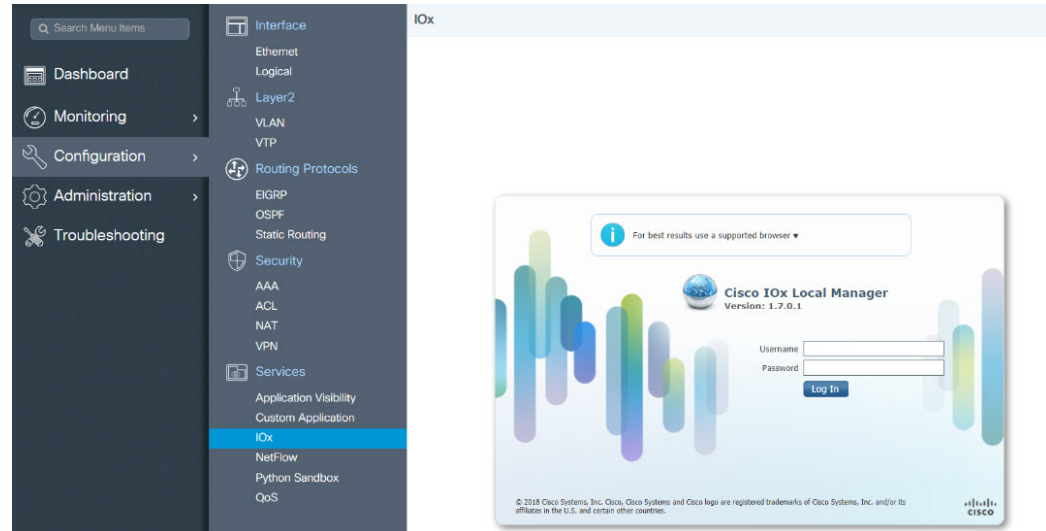
IOXMAN is a process that establishes a tracing infrastructure to provide logging or tracing services for guest applications, except Libvirt, that emulates serial devices. IOXMAN is based on the lifecycle of the guest application to enable and disable the tracing service, to send logging data to IOS syslog, to save tracing data to IOx tracelog, and to maintain IOx tracelog for each guest application.

# Application Hosting on the IR8340 Router

This section describes the application hosting characteristics specific to the IR8340 router.

Application hosting can be achieved using the application hosting CLI commands as well as using Local Manager. 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.

**Figure 2: 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](#).

The next section explains the deployment of an application using the application hosting CLI commands.

## Application Hosting on Layer 2 and Layer 3 Interfaces

The application configurations have two interfaces to support L2 and L3 traffic from the LAN and WAN ports respectively.

For application hosting, you can configure the L2 and L3 interfaces as following:

- L2 interfaces are configured with AppGigabitEthernet and VLAN with IP address in the same VLAN network, which are used or forwarding the L2 app traffic. Dedicated VLAN range 2340 - 2349 must be used for configuring L2 interfaces of application and to communicate the application for L2 traffic.

You should configure the AppGigEthernet interface as a trunk interface.

- L3 interfaces or gateway interfaces are configured with Virtual port group, and IP address in the same network as VPG, which are used for forwarding the L3 traffic to applications.

## VirtualPortGroup

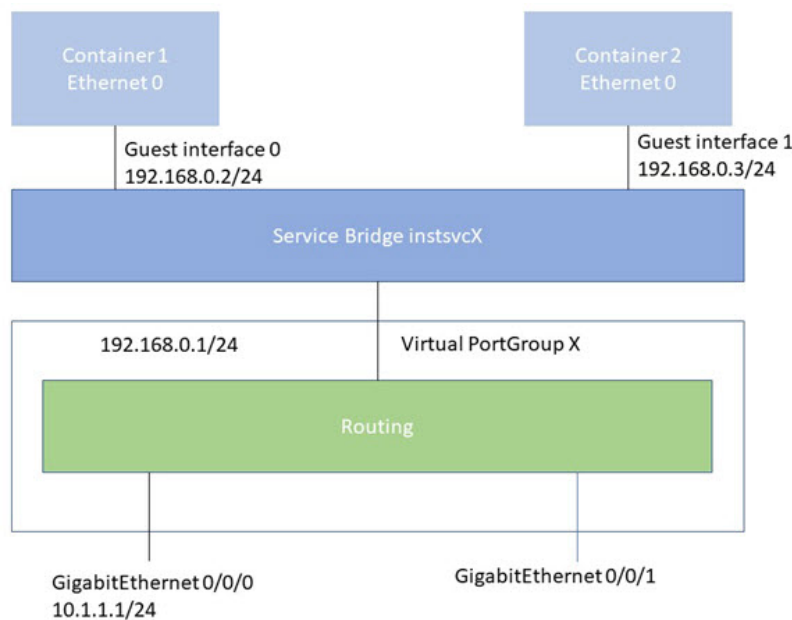
The VirtualPortGroup is a software construct on Cisco IOS that maps to a Linux bridge IP address. As such, the VirtualPortGroup represents the switch virtual interface (SVI) of the Linux container. Each bridge can contain multiple interfaces; each mapping to a different container. Each container can 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.

**Figure 3: 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

The following sections provide information about the various tasks that comprise the configuration of 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.

### Procedure

|               | Command or Action                                                                                                                                                                  | Purpose                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Router> <b>enable</b>                                                                                                                      | Enables privileged EXEC mode.<br><br>Enter your password if prompted.                                                                              |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                                                                              | Enters global configuration mode.                                                                                                                  |
| <b>Step 3</b> | <b>iox</b><br><br><b>Example:</b><br>Router(config)# <b>iox</b>                                                                                                                    | Enables IOx.                                                                                                                                       |
| <b>Step 4</b> | <b>ip http server</b><br><br><b>Example:</b><br>Router(config)# <b>ip http server</b>                                                                                              | Enables the HTTP server on your IP or IPv6 system.                                                                                                 |
| <b>Step 5</b> | <b>ip http secure-server</b><br><br><b>Example:</b><br>Router(config)# <b>ip http secure-server</b>                                                                                | Enables a secure HTTP (HTTPS) server.                                                                                                              |
| <b>Step 6</b> | <b>username name privilege level secret {0   7   user-password} encrypted-password</b><br><br><b>Example:</b><br>Router(config)# <b>username cisco privilege 15 secret 0 cisco</b> | Establishes a username-based authentication system and privilege level for the user.<br><br>The username privilege level must be configured as 15. |

|               | Command or Action                                               | Purpose                                                                 |
|---------------|-----------------------------------------------------------------|-------------------------------------------------------------------------|
| <b>Step 7</b> | <b>end</b><br><br><b>Example:</b><br>Router(config)# <b>end</b> | Exits interface configuration mode and returns to privileged EXEC mode. |

## Configuring Application Hosting to Layer 2 Interfaces

Follow these steps to configure application hosting to Layer 2 interfaces.

### Procedure

|               | Command or Action                                                                                                                       | Purpose                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Device> <b>enable</b>                                                                           | Enables privileged EXEC mode. Enter your password if prompted.                                                    |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Device# <b>configure terminal</b>                                                   | Enters global configuration mode.                                                                                 |
| <b>Step 3</b> | <b>interface AppGigEthernet <i>number</i></b><br><br><b>Example:</b><br>Device(config)# <b>interface AppGigabitEthernet 0/1/1</b>       | Configures the AppGigabitEthernet and enters interface configuration mode.                                        |
| <b>Step 4</b> | <b>switchport mode trunk</b><br><br><b>Example:</b><br>Device(config-if)# <b>switchport mode trunk</b>                                  | Sets the interface into permanent trunking mode and negotiates to convert the neighboring link into a trunk link. |
| <b>Step 5</b> | <b>exit</b><br><br><b>Example:</b><br>Device(config-if)# <b>exit</b>                                                                    | Exits interface configuration mode and returns to global configuration mode.                                      |
| <b>Step 6</b> | <b>app-hosting appid <i>name</i></b><br><br><b>Example:</b><br>Device(config)# <b>app-hosting appid iperf_3</b>                         | Configures the application and enters the application hosting configuration mode.                                 |
| <b>Step 7</b> | <b>app-vnic AppGigabitEthernet trunk</b><br><br><b>Example:</b><br>Device(config-app-hosting)# <b>app-vnic AppGigabitEthernet trunk</b> | Configures a trunk port for an application, and enters application-hosting trunk-configuration mode.              |

|                | Command or Action                                                                                                                                                                                      | Purpose                                                                                             |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| <b>Step 8</b>  | <b>vlan</b> <i>vlan-ID</i> <b>guest-interface</b> <i>guest-interface-number</i><br><b>Example:</b><br>Device (config-app-hosting-trunk) # <b>vlan</b> 2340 <b>guest-interface</b> 1                    | Configures a VLAN guest interface and enters application-hosting VLAN-access IP configuration mode. |
| <b>Step 9</b>  | <b>guest-ipaddress</b> <i>ip-address</i> <b>netmask</b> <i>netmask</i><br><b>Example:</b><br>Device (config-app-hosting-vlan-access-ip) # <b>guest-ipaddress</b> 20.1.1.2 <b>netmask</b> 255.255.255.0 | Configures a static IP address.                                                                     |
| <b>Step 10</b> | <b>end</b><br><b>Example:</b><br>Device (config-config-app-hosting-vlan-access-ip) # <b>end</b>                                                                                                        | Exits application-hosting VLAN-access IP 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. VirtualPortGroups and Layer 3 data ports must be on different subnets.

Enable the **ip routing** command to allow external routing on the Layer 3 data-port.

### Procedure

|               | Command or Action                                                                                           | Purpose                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Device> <b>enable</b>                                                   | Enables privileged EXEC mode. Enter your password if prompted.                                                            |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Device# <b>configure terminal</b>                           | Enters global configuration mode.                                                                                         |
| <b>Step 3</b> | <b>ip routing</b><br><b>Example:</b><br>Device (config) # <b>ip routing</b>                                 | Enables IP routing.<br><br>The <b>ip routing</b> command must be enabled to allow external routing on Layer 3 data ports. |
| <b>Step 4</b> | <b>interface type number</b><br><b>Example:</b><br>Device (config) # <b>interface</b> gigabitethernet 0/0/0 | Configures an interface and enters interface configuration mode                                                           |

|                | Command or Action                                                                                                     | Purpose                                                                                                            |
|----------------|-----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b>  | <b>no switchport</b><br><b>Example:</b><br>Device (config-if) # <b>no switchport</b>                                  | Places the interface in Layer 3 mode, and makes it operate more like a router interface rather than a switch port. |
| <b>Step 6</b>  | <b>ip address ip-address mask</b><br><b>Example:</b><br>Device (config-if) # <b>ip address 10.1.1.1 255.255.255.0</b> | Configures an IP address for the interface.                                                                        |
| <b>Step 7</b>  | <b>exit</b><br><b>Example:</b><br>Device (config-if) # <b>exit</b>                                                    | Exits interface configuration mode and returns to global configuration mode.                                       |
| <b>Step 8</b>  | <b>interface type number</b><br><b>Example:</b><br>Device (config) # <b>interface virtualportgroup 0</b>              | Configures an interface and enters interface configuration mode.                                                   |
| <b>Step 9</b>  | <b>ip address ip-address mask</b><br><b>Example:</b><br>Device (config-if) # <b>ip address 20.1.2.1 255.255.255.0</b> | Configures an IP address for the interface.                                                                        |
| <b>Step 10</b> | <b>end</b><br><b>Example:</b><br>Device (config-if) # <b>end</b>                                                      | Exits interface configuration mode and returns to privileged EXEC mode.                                            |
| <b>Step 11</b> | <b>configure terminal</b><br><b>Example:</b><br>Device# <b>configure terminal</b>                                     | Enters global configuration mode.                                                                                  |
| <b>Step 12</b> | <b>interface vlan vlan-id</b><br><b>Example:</b><br>Device (config-if) # <b>interface vlan 2340</b>                   | Configure the SVI interface for supporting L2 traffic. VLAN range: 2340 - 2349.                                    |
| <b>Step 13</b> | <b>ip address ip-address mask</b><br><b>Example:</b><br>Device (config-if) # <b>ip address 20.1.1.1 255.255.255.0</b> | Configures an IP address and IP subnet mask.                                                                       |
| <b>Step 14</b> | <b>end</b><br><b>Example:</b><br>Device (config-if) # <b>end</b>                                                      | Exits interface configuration mode and returns to privileged EXEC mode.                                            |

|                | Command or Action                                                                                                                                                                 | Purpose                                                                                                                                       |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 15</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Device# <b>configure terminal</b>                                                                                             | Enters global configuration mode.                                                                                                             |
| <b>Step 16</b> | <b>app-hosting appid name</b><br><br><b>Example:</b><br>Device(config)# <b>app-hosting appid iperf_3</b>                                                                          | Configures the application and enters the application hosting configuration mode.                                                             |
| <b>Step 17</b> | <b>app-vnic gateway2 virtualportgroup 0 guest-interface 2</b><br><br><b>Example:</b><br>Device(config-app-hosting)# <b>app-vnic gateway2 virtualportgroup 0 guest-interface 2</b> | Configures the application interface and the gateway of the application. You can create multiple interfaces with different virtualportgroups. |
| <b>Step 18</b> | <b>guest-ipaddress ip-address netmask netmask</b><br><br><b>Example:</b><br>Device(config-app-hosting-gateway0)# <b>guest-ipaddress 20.1.2.2 netmask 255.255.255.0</b>            | Configures the application Ethernet interface ip address.                                                                                     |
| <b>Step 19</b> | <b>app-default-gateway ip-address guest-interface 2</b><br><br><b>Example:</b><br>Device(config-app-hosting-gateway0)# <b>app-default-gateway 20.1.2.1 guest-interface 2</b>      | Configures the default gateway for the application. Only one gateway is supported.                                                            |
| <b>Step 20</b> | <b>end</b><br><br><b>Example:</b><br>Device# <b>end</b>                                                                                                                           | Exits global configuration mode and returns to privileged EXEC configuration mode.                                                            |

## Configuring Docker Run Time Options

### Procedure

|               | Command or Action                                                                     | Purpose                                                               |
|---------------|---------------------------------------------------------------------------------------|-----------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><br><b>Example:</b><br>Device > <b>enable</b>                        | Enables privileged EXEC mode.<br><br>Enter your password if prompted. |
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Device# <b>configure terminal</b> | Enters global configuration mode.                                     |

|               | Command or Action                                                                                                                     | Purpose                                                                                                                                      |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 3</b> | <b>app-hosting appid</b> <i>name</i><br><b>Example:</b><br>Router(config)# <b>app-hosting appid appl</b>                              | Enables application hosting and enters application hosting configuration mode.                                                               |
| <b>Step 4</b> | <b>app-hosting docker</b><br><b>Example:</b><br>Device(config-app-hosting) # <b>app-resource docker</b>                               | Enters application-hosting docker-configuration mode to specify application resource updates.<br>Application start-up scripts are activated. |
| <b>Step 5</b> | <b>run-opts</b> <i>options</i><br><b>Example:</b><br>Device(config-app-hosting-docker) #<br><b>run-opts 1 "-v \$(APP_DATA):/data"</b> | Specifies the Docker run time options.                                                                                                       |
| <b>Step 6</b> | <b>end</b><br><b>Example:</b><br>Device(config-app-hosting-docker) # <b>end</b>                                                       | Exits application-hosting docker-configuration mode and returns to privileged EXEC mode.                                                     |

**Example**

```
app-hosting appid appl
app-resource docker
run-opts 1 "--tmpfs /tmp:rw,size=128m"
```

## Installing and Uninstalling Apps

Follow these steps to install or uninstall apps:

**Procedure**

|               | Command or Action                                                                                                                                                                                  | Purpose                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Device > <b>enable</b>                                                                                                                                         | Enables privileged EXEC mode.<br>Enter your password if prompted.                                                                                  |
| <b>Step 2</b> | <b>app-hosting install appid</b> <i>application-name</i><br><b>package</b> <i>package-path</i><br><b>Example:</b><br>Device# <b>app-hosting install appid lxc_app package flash:my_iox_app.tar</b> | Installs an app from the specified location.<br>The app can be installed from any local storage location such as, flash, bootflash, and usbflash0. |
| <b>Step 3</b> | <b>app-hosting activate appid</b> <i>application-name</i><br><b>Example:</b>                                                                                                                       | Activates the application.                                                                                                                         |

|               | Command or Action                                                                                                                  | Purpose                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | Device# <b>app-hosting activate appid app1</b>                                                                                     | This command validates all application resource requests, and if all resources are available the application is activated; if not, the activation fails. |
| <b>Step 4</b> | <b>app-hosting start appid <i>application-name</i></b><br><b>Example:</b><br>Device# <b>app-hosting start appid app1</b>           | Starts the application.<br>Application start-up scripts are activated.                                                                                   |
| <b>Step 5</b> | <b>app-hosting stop appid <i>application-name</i></b><br><b>Example:</b><br>Device# <b>app-hosting stop appid app1</b>             | Stops the application.                                                                                                                                   |
| <b>Step 6</b> | <b>app-hosting deactivate appid <i>application-name</i></b><br><b>Example:</b><br>Device# <b>app-hosting deactivate appid app1</b> | Deactivates all resources allocated for the application.                                                                                                 |
| <b>Step 7</b> | <b>app-hosting uninstall appid <i>application-name</i></b><br><b>Example:</b><br>Device# <b>app-hosting uninstall appid app1</b>   | Uninstalls the application.<br>Uninstalls all packaging and images stored.<br>All changes and updates to the application are also removed.               |

#### What to do next



**Note** The app traffic to VirtualPortGroup interfaces will be blocked after you uninstall the app and reinstall it again with the same IP addresses, because the ARP entry for VirtualPortGroup interface is not updated after the app is reinstalled. You must clear the ARP cache for those IP addresses to be manually refreshed for the ARP.

## Overriding the App Resource Configuration

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

#### Procedure

|               | Command or Action                                         | Purpose                                                           |
|---------------|-----------------------------------------------------------|-------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Router> <b>enable</b> | Enables privileged EXEC mode.<br>Enter your password if prompted. |

|               | Command or Action                                                                                                         | Purpose                                                                                                                                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | <b>configure terminal</b><br><br><b>Example:</b><br>Router# <b>configure terminal</b>                                     | Enters global configuration mode.                                                                                                                                                                               |
| <b>Step 3</b> | <b>app-hosting appid name</b><br><br><b>Example:</b><br>Router(config)# <b>app-hosting appid app1</b>                     | Enables application hosting and enters application hosting configuration mode.                                                                                                                                  |
| <b>Step 4</b> | <b>app-resource profile name</b><br><br><b>Example:</b><br>Router(config-app-hosting)# <b>app-resource profile custom</b> | Configures the custom application resource profile, and enters custom application resource profile configuration mode.<br><br>Only the custom profile name is supported.                                        |
| <b>Step 5</b> | <b>cpu unit</b><br><br><b>Example:</b><br>Router(config-app-resource-profile-custom)#<br><b>cpu 800</b>                   | Changes the default CPU allocation for the application.<br><br>Resource values are application-specific, and any adjustment to these values must ensure that the application can run reliably with the changes. |
| <b>Step 6</b> | <b>memory memory</b><br><br><b>Example:</b><br>Router(config-app-resource-profile-custom)#<br><b>memory 512</b>           | Changes the default memory allocation.                                                                                                                                                                          |
| <b>Step 7</b> | <b>vcpu number</b><br><br><b>Example:</b><br>Router(config-app-resource-profile-custom)#<br><b>vcpu 2</b>                 | Changes the virtual CPU (vCPU) allocation for the application.                                                                                                                                                  |
| <b>Step 8</b> | <b>end</b><br><br><b>Example:</b><br>Router(config-app-resource-profile-custom)#<br><b>end</b>                            | Exits custom application resource profile configuration mode and returns to privileged EXEC mode.                                                                                                               |

## IOx Configuration with ERSpan

The traffic can be spanned to IOX applications with the ERSpan configurations on LAN or WAN ports. ACL can be applied on traffic like ERSpan with FSPAN.

### Procedure

- 
- Step 1** Create ACL like any extended access-list.

**Example:**

```
ip access-list extended ACL120
10 permit ip host 120.1.1.1 host 120.120.120.120
```

**Step 2** Configure ERSPAN session for LAN or WAN ports to span data to the application.

- Configure ERSPAN session for LAN ports to span data to the application.

**Note**

ERSPAN Session ID 1 - 4 are only supported on LAN ports.

```
monitor session 1 type erspan-source
source interface Gi0/1/10 rx
filter access-group ACL120
destination
erspan-id 1
ip address 20.1.2.2 <== Ip address of L2/VLAN interface on APP
origin ip address 68.68.68.68
```

- configuring ERSPAN session for WAN ports to span data to the application.

```
monitor session 1 type erspan-source
source interface Gi0/0/0 rx
filter access-group ACL120
destination
erspan-id 1
ip address 20.1.1.2 <== Ip address of L3 interface on APP
origin ip address 68.68.68.68
```

## Verifying the Application Hosting Configuration

**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
Libvirt 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 appid iperf_3
App id : iperf_3
Owner : iox
State : RUNNING
Application
Type : docker
Name : networkstatic/iperf3
Version : latest
Description :
Author : Brent
Path : bootflash:iperf3x86.tar
URL Path :
Activated profile name : custom

Resource reservation
Memory : 500 MB
Disk : 500 MB
CPU : 173 units
CPU-percent : 5 %
VCPU : 1

Platform resource profiles
Profile Name CPU(unit) Memory(MB) Disk(MB)

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:67:81:6f
IPv6 address : ::
Network name : mgmt-bridge300
eth3:
MAC address : 52:54:dd:b2:4d:86
IPv4 address : 20.1.2.2
IPv6 address : ::
Network name : VPG0
eth1:
MAC address : 52:54:dd:f2:29:67
IPv4 address : 20.1.1.2
IPv6 address : 2001:1::5054:ddff:fef2:2967
Network name : mgmt-bridge-v2340

Docker

Run-time information
Command :
Entry-point : /bin/sleep 10000
Run options in use : --entrypoint '/bin/sleep 10000'
Package run options :
Application health information
Status : 0
Last probe error :
Last probe output :

```

```
Device#
```

#### 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 secret 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
```

## Signed Application Support

To install a signed application, signed verification has to be enabled on the device. Signed verification can be enabled or disabled by the following command:

```
#app-hosting verification {enable|disable}
```

The signed verification enabled or disabled status can be verified by the **show app-hosting infra** command:

```
#show app-hosting infra
IOX version: 2.6.0.0
App signature verification: disabled
Internal working directory: /vol/usb1/iox

Application Interface Mapping
AppGigabitEthernet Port # Interface Name Port Type Bandwidth
1 AppGigabitEthernet0/1/1 KR Port - Internal 10G
```

```
CPU:
Quota: 99(Percentage)
Available: 99(Percentage)
Quota: 3465(Units)
Available: 2842(Units)
```

When signed verification is enabled, any unsigned app can not be activated, and signed app can move to different states irrespective of the app sign verification enabled or disabled.

After enabling the signed verification, follow the instructions in [Installing and Uninstalling Apps](#), on page 228 to install the application.

## Cisco Cyber Vision

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 Cyber Vision release is 4.1.1 to work with the IR8340. For more information about CVC, see the release notes in the following URL:

<https://www.cisco.com/c/en/us/support/security/cyber-vision/products-release-notes-list.html>

For more information about CVC installation and ERSPAN with CVC, see the following:

[Cyber Vision Support](#) and [ERSPAN Support](#)



## CHAPTER 20

# ROM Monitor Overview

---

- [ROM Monitor Overview, on page 235](#)
- [Access ROM Monitor Mode, on page 236](#)
- [Displaying the Configuration Register Setting, on page 238](#)
- [Environment Variable Settings, on page 239](#)
- [Exiting ROM Monitor Mode, on page 240](#)

## 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.



---

**Caution** Be cautious to change ROMMON variables, because it may cause unexpected consequences.

---

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 IR8340 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 v0.33, DEVELOPMENT SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.
Compiled Mon Jul 12 18:53:57 2021 by gilchen

Router# show romvar
ROMMON variables:
PS1 = rommon ! >
DEVICE_MANAGED_MODE = autonomous
CRYPTO_BI_THPUT = 50000
TEMPLATE = advanced
DISABLE_USB_FLASH = no
```

```

DISABLE_CC_AUTH = 1
DISABLE_SD_FLASH = no
PASSWD_RECOVERY = no
ENABLE_BREAK = no
ENABLE_FLASH_PRIMARY_BOOT = no
BAUD = 9600
LICENSE_BOOT_LEVEL =
SKIP_CHIPGUARD = 1
RET_2_RTS =
BOOT =
flash:ir8340-universalk9.BLD_POLARIS_DEV_LATEST_20210322_153228.SSA.bin,12;flash:ir8340-universalk9.BLD_POLARIS_DEV_LATEST_20210323_184154.SSA.bin,12;
BSI = 0
RET_2_RCALTS =
RANDOM_NUM = 404654831

```

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 2 >set
BOOT=flash:ir8340-universalk9.BLD_POLARIS_DEV_LATEST_20210710_191629_V17_7_0_60.SSA.bin,12;
BSI=0
CRYPTO_BI_THPUT=50000
DEVICE_MANAGED_MODE=autonomous
LICENSE_BOOT_LEVEL=
PS1=rommon ! >
RANDOM_NUM=1822515242
RET_2_RCALTS=1630484680
RET_2_RTS=
SKIP_CHIPGUARD=1
TEMPLATE=advanced
rommon 3 >

```

## 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 14: 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.                                                        |

| ROMMON Command | Description                                |
|----------------|--------------------------------------------|
| <b>unset</b>   | Removes an environmental variable setting. |

## Examples

The following example shows what appears when you enter the **?** command on a router:

```
rommon 3 >?

alias set and/or display command aliases
boot boot up an external process
cpuinfo display processor information
confreg configuration register utility
ctchallenge Generate a challenge for dev key install
ctinstkey Parse the response and install dev key
ctiskeyinstalled checks if devkey installed and display it
ctremkey Remove the devkey from Aikido
ctrespsave Store parts of incoming response
dev display the device table
dir list files in a file system
efi_shell launch the UEFI SHELL enviroment
flwr burn new BIOS onto the bootrom
help monitor built-in command(s) help
history display monitor command history
meminfo display main memory information
repeat repeat a monitor command
reset system reset
set display the monitor environment
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 variable from the monitor environment
rommon 4 >
```

## 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 4 >PS1="IR8340 rommon ! >"
IR8340 rommon 5 >
```

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 “IR8340 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 **showmon** command without parameters as follows:

```
IR8340 rommon 8 >showmon
```

```
System Bootstrap, Version v0.33, DEVELOPMENT SOFTWARE
```

```
Copyright (c) 1994-2021 by cisco Systems, Inc.
Compiled Mon Jul 12 18:53:57 2021 by root
```

```
!!! DEBUG SECURE-BOOT CPLD Version Installed. For INTERNAL USE ONLY !!!
```

```
Current image running : Boot ROM0
```

```
Last reset cause (0x00000002): LocalSoft
IR8340-K9 platform with 8388608 Kbytes of main memory
```

```
IR8340 rommon 9 >
```

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 IR8340 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 15: Frequently Used ROM Monitor Environmental Variables**

| Environmental variable | Description                                                                                                |
|------------------------|------------------------------------------------------------------------------------------------------------|
| <b>BOOT</b> =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 :

```
IR8340 rommon 8 >showmon
```

```
System Bootstrap, Version v0.33, DEVELOPMENT SOFTWARE
Copyright (c) 1994-2021 by cisco Systems, Inc.
Compiled Mon Jul 12 18:53:57 2021 by root
```

```
!!! DEBUG SECURE-BOOT CPLD Version Installed. For INTERNAL USE ONLY !!!

Current image running : Boot ROM0

Last reset cause (0x00000002): LocalSoft
IR8340-K9 platform with 8388608 Kbytes of main memory

IR8340 rommon 9 >
```

## 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 = IR8340-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 | <b>confreg</b><br><b>Example:</b><br><br>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 | <b>reset</b><br><b>Example:</b><br><br>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 IR8340-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

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | (Optional) Run the <b>show rom-monitor slot</b> command on the router to see the current release numbers of ROMmon on the hardware. See the <a href="#">Checking the Current ROMMON Version, on page 236</a> for information about interpreting the output of the command that you run.                                                                                                    |
| <b>Step 2</b> | If autoboot has not been enabled by using the <b>config-register 0x2102</b> command, run the <b>boot filesystem:/file-location</b> command at the ROMmon prompt to boot the Cisco IOS XE image, where <i>filesystem:/file-location</i> 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. |
| <b>Step 3</b> | Run the <b>enable</b> command at the user prompt to enter the privileged EXEC mode after the boot is complete.                                                                                                                                                                                                                                                                             |
| <b>Step 4</b> | Run the <b>show rom-monitor slot</b> command to verify whether the ROMmon has been upgraded.                                                                                                                                                                                                                                                                                               |
-





## CHAPTER 21

# Process Health Monitoring

---

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

- [Monitoring Control Plane Resources, on page 243](#)
- [Monitoring Hardware Using Alarms, on page 255](#)

## 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 243](#)
- [Cisco IOS Process Resources, on page 243](#)
- [Overall Control Plane Resources, on page 253](#)

## 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#ac03ca5b9748c51baa2971d7a417e55e

```
Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 7F74107C4048 3807080396 239658308 3567422088 661095820 3145727908
reserve P 7F74107C40A0 102404 92 102312 102312 102312
lsmpi_io 7F740259B1A8 6295128 6294304 824 824 412
Dynamic heap limit(MB) 3000 Use(MB) 0
```

Processor memory

```
Address Bytes Prev Next Ref PrevF NextF what Alloc PC
7F74107C4048 0000102408 00000000 7F74107DD0A8 001 ----- *Init*
:559FB88BD000+5E73061
7F74107DD0A8 0000000056 7F74107C4048 7F74107DD138 001 ----- *Init*
:559FB88BD000+5E7307F
7F74107DD138 0000008224 7F74107DD0A8 7F74107DF1B0 001 ----- *Init*
:559FB88BD000+5E7309A
7F74107DF1B0 0000000296 7F74107DD138 7F74107DF330 001 ----- *Init*
:559FB88BD000+9093511
7F74107DF330 0000000568 7F74107DF1B0 7F74107DF5C0 001 ----- *Init*
:559FB88BD000+9099C4A
7F74107DF5C0 0000032776 7F74107DF330 7F74107E7620 001 ----- Managed Chunk Q
:559FB88BD000+90832BF
7F74107E7620 0000000056 7F74107DF5C0 7F74107E76B0 001 ----- *Init*
:559FB88BD000+5EC98DD
7F74107E76B0 0000032776 7F74107E7620 7F74107EF710 001 ----- Queue Pair - Q
:559FB88BD000+90B02EF
7F74107EF710 0000012808 7F74107E76B0 7F74107F2970 001 ----- *Init*
:559FB88BD000+13BF988B
7F74107F2970 0000032776 7F74107EF710 7F74107FA9D0 001 ----- List Elements
:559FB88BD000+904DB29
7F74107FA9D0 0000032776 7F74107F2970 7F7410802A30 001 ----- List Headers
:559FB88BD000+904DB77
7F7410802A30 0000032776 7F74107FA9D0 7F741080AA90 001 ----- IOSXE Process S
:559FB88BD000+A664348
7F741080AA90 0000032776 7F7410802A30 7F7410812AF0 001 ----- IOSXE Queue Pro
:559FB88BD000+A66438A
7F7410812AF0 0000065544 7F741080AA90 7F7410822B50 001 ----- IOSXE Queue Bal
:559FB88BD000+A6643C5
7F7410822B50 0000000328 7F7410812AF0 7F7410822CF0 001 ----- *Init*
:559FB88BD000+13BF1567
7F7410822CF0 0000000328 7F7410822B50 7F7410822E90 001 ----- *Init*
:559FB88BD000+13BF1567
7F7410822E90 0000000192 7F7410822CF0 7F7410822FA8 001 ----- *Init*
:559FB88BD000+90C3F74
7F7410822FA8 0000036872 7F7410822E90 7F741082C008 001 ----- *Init*
:559FB88BD000+A65A3A8
7F741082C008 0000010008 7F7410822FA8 7F741082E778 001 ----- Platform VM Pag
:559FB88BD000+A68A8A3
7F741082E778 0000002008 7F741082C008 7F741082EFA8 001 ----- *Init*
iosd_crb_crankshaft_unix:7F7460E22000+7D8CB
7F741082EFA8 0000200712 7F741082E778 7F7410860008 001 ----- Interrupt Stack
:559FB88BD000+A65A3A8
7F7410860008 0000000328 7F741082EFA8 7F74108601A8 001 ----- *Init*
:559FB88BD000+13BF1567
7F74108601A8 0000003008 7F7410860008 7F7410860DC0 001 ----- Watched Semapho
:559FB88BD000+90BBCE8
7F7410860DC0 0000000400 7F74108601A8 7F7410860FA8 001 ----- *Init*
:559FB88BD000+13BF1567
7F7410860FA8 0000036872 7F7410860DC0 7F741086A008 001 ----- *Init*
```

```

:559FB88BD000+A65A3A8
7F741086A008 0000000328 7F7410860FA8 7F741086A1A8 001 ----- *Init*
:559FB88BD000+13BF1567
7F741086A1A8 0000000184 7F741086A008 7F741086A2B8 001 ----- *Init*
:559FB88BD000+90A4B10
7F741086A2B8 0000000184 7F741086A1A8 7F741086A3C8 001 ----- *Init*
:559FB88BD000+90A4B10
7F741086A3C8 0000000184 7F741086A2B8 7F741086A4D8 001 ----- *Init*
:559FB88BD000+90A4B10
7F741086A4D8 0000000184 7F741086A3C8 7F741086A5E8 001 ----- *Init*
:559FB88BD000+90A4B10
7F741086A5E8 0000000184 7F741086A4D8 7F741086A6F8 001 ----- *Init*
:559FB88BD000+90A4B10
7F741086A6F8 0000000096 7F741086A5E8 7F741086A7B0 001 ----- *Init*
:559FB88BD000+90A4AA4
7F741086A7B0 0000000152 7F741086A6F8 7F741086A8A0 001 ----- Crypto CA
:559FB88BD000+98E58BF
7F741086A8A0 0000000152 7F741086A7B0 7F741086A990 001 ----- Crypto CA
:559FB88BD000+98E58BF
7F741086A990 0000000152 7F741086A8A0 7F741086AA80 001 ----- Crypto CA
:559FB88BD000+98E58BF
7F741086AA80 0000000152 7F741086A990 7F741086AB70 001 ----- Crypto CA
:559FB88BD000+98E58BF
7F741086AB70 0000000176 7F741086AA80 7F741086AC78 001 ----- Crypto CA
:559FB88BD000+98E58BF
7F741086AC78 0000000272 7F741086AB70 7F741086ADE0 001 ----- Crypto CA
:559FB88BD000+98E5875
7F741086ADE0 0000000096 7F741086AC78 7F741086AE98 000 7F741C306070 7F7415EC2CE8 (fragment)
:559FB88BD000+98E5875
7F741086AE98 0000000184 7F741086ADE0 7F741086AFA8 001 ----- Init
:559FB88BD000+52443C9
7F741086AFA8 0000036872 7F741086AE98 7F7410874008 001 ----- *Init*
:559FB88BD000+A65A3A8
7F7410874008 0000000328 7F741086AFA8 7F74108741A8 001 ----- *Init*
:559FB88BD000+13BF1567
7F74108741A8 0000000184 7F7410874008 7F74108742B8 001 ----- *Init*
:559FB88BD000+90A4B10
7F74108742B8 0000000064 7F74108741A8 7F7410874350 001 ----- Parser Linkage
:559FB88BD000+5D90EDA
7F7410874350 0000000216 7F74108742B8 7F7410874480 001 ----- IPv4 FIB subblo
:559FB88BD000+5A2947A
7F7410874480 0000000224 7F7410874350 7F74108745B8 001 ----- *Init*
:559FB88BD000+9060A7C
7F74108745B8 0000000224 7F7410874480 7F74108746F0 001 ----- *Init*
:559FB88BD000+9060A7C
7F74108746F0 0000000328 7F74108745B8 7F7410874890 001 ----- *Init*
:559FB88BD000+9060A7C
7F7410874890 0000000328 7F74108746F0 7F7410874A30 001 ----- *Init*
:559FB88BD000+9060A7C
7F7410874A30 0000000328 7F7410874890 7F7410874BD0 001 ----- *Init*
:559FB88BD000+9060A7C
7F7410874BD0 0000000896 7F7410874A30 7F7410874FA8 001 ----- *Init*
:559FB88BD000+9060A7C
7F7410874FA8 0000200712 7F7410874BD0 7F74108A6008 001 ----- Interrupt Stack
:559FB88BD000+A65A3A8
7F74108A6008 0000000968 7F7410874FA8 7F74108A6428 001 ----- *Init*
iosd_crb_crankshaft_unix:7F7460E22000+3AC76
7F74108A6428 0000002008 7F74108A6008 7F74108A6C58 001 ----- Watcher Message
:559FB88BD000+90BBDB7B
7F74108A6C58 0000000360 7F74108A6428 7F74108A6E18 001 ----- Process Events
:559FB88BD000+90B6840
7F74108A6E18 0000000096 7F74108A6C58 7F74108A6ED0 001 ----- SWIDB_SB_PTP
:559FB88BD000+5324CAA
7F74108A6ED0 0000000128 7F74108A6E18 7F74108A6FA8 001 ----- *Init*

```

```

:559FB88BD000+9060A7C
7F74108A6FA8 0000036872 7F74108A6ED0 7F74108B0008 001 ----- *Init*
:559FB88BD000+A65A3A8
7F74108B0008 0000002840 7F74108A6FA8 7F74108B0B78 001 ----- *Init*
:559FB88BD000+B529B9D
7F74108B0B78 0000000984 7F74108B0008 7F74108B0FA8 001 ----- Watched Message
:559FB88BD000+90BBD4A
7F74108B0FA8 0000200712 7F74108B0B78 7F74108E2008 001 ----- Interrupt Stack
:559FB88BD000+A65A3A8
7F74108E2008 0000002336 7F74108B0FA8 7F74108E2980 001 ----- Process Array
:559FB88BD000+90C3DC0
7F74108E2980 0000000360 7F74108E2008 7F74108E2B40 001 ----- Process Events
:559FB88BD000+90B6840
7F74108E2B40 0000000328 7F74108E2980 7F74108E2CE0 001 ----- *Init*
:559FB88BD000+13BF1567
7F74108E2CE0 0000000120 7F74108E2B40 7F74108E2DB0 001 ----- *Init*
:559FB88BD000+90A4347
7F74108E2DB0 0000000184 7F74108E2CE0 7F74108E2EC0 001 ----- *Init*
:559FB88BD000+90A4B10
7F74108E2EC0 0000000144 7F74108E2DB0 7F74108E2FA8 001 ----- *Init*
:559FB88BD000+4FFE35D
7F74108E2FA8 0000036872 7F74108E2EC0 7F74108EC008 001 ----- *Init*
:559FB88BD000+A65A3A8
7F74108EC008 0000001232 7F74108E2FA8 7F74108EC530 001 ----- Process
:559FB88BD000+90C3F05
7F74108EC530 0000001232 7F74108EC008 7F74108ECA58 001 ----- Process
:559FB88BD000+90C3F05
7F74108ECA58 0000000096 7F74108EC530 7F74108ECB10 001 ----- Init
:559FB88BD000+8FF0694
7F74108ECB10 0000000184 7F74108ECA58 7F74108ECC20 001 ----- *Init*
:559FB88BD000+90A4B10
7F74108ECC20 0000000184 7F74108ECB10 7F74108ECD30 001 ----- *Init*
:559FB88BD000+90A4B10
7F74108ECD30 0000000184 7F74108ECC20 7F74108ECE40 001 ----- *Init*
:559FB88BD000+90A4B10
7F74108ECE40 0000000272 7F74108ECD30 7F74108ECFA8 001 ----- *Init*
:559FB88BD000+90A4B10
7F74108ECFA8 0000200712 7F74108ECE40 7F741091E008 001 ----- Interrupt Stack
:559FB88BD000+A65A3A8
7F741091E008 0000000184 7F74108ECFA8 7F741091E118 001 ----- *Init*
:559FB88BD000+90A4B10
7F741091E118 0000003008 7F741091E008 7F741091ED30 001 ----- Reg Function Li
:559FB88BD000+905FC68
7F741091ED30 0000000064 7F741091E118 7F741091EDC8 001 ----- Parser Linkage
:559FB88BD000+5D90C9A
7F741091EDC8 0000000064 7F741091ED30 7F741091EE60 001 ----- Parser Linkage
:559FB88BD000+5D90EDA
7F741091EE60 0000000064 7F741091EDC8 7F741091EEF8 001 ----- Parser Linkage
:559FB88BD000+5D90C9A
7F741091EEF8 0000000088 7F741091EE60 7F741091EFA8 001 ----- *Init*
:559FB88BD000+5EC98DD
7F741091EFA8 0000036872 7F741091EEF8 7F7410928008 001 ----- *Init*
:559FB88BD000+A65A3A8
7F7410928008 0000000184 7F741091EFA8 7F7410928118 001 ----- *Init*
:559FB88BD000+90A4B10
7F7410928118 0000001504 7F7410928008 7F7410928750 001 ----- Reg Function Se
:559FB88BD000+905FCC2
7F7410928750 0000001504 7F7410928118 7F7410928D88 001 ----- Reg Function Ca
:559FB88BD000+905FCEF
7F7410928D88 0000000064 7F7410928750 7F7410928E20 001 ----- Parser Linkage
:559FB88BD000+5D90C9A
7F7410928E20 0000000064 7F7410928D88 7F7410928EB8 001 ----- Parser Linkage
:559FB88BD000+5D90EDA
7F7410928EB8 0000000152 7F7410928E20 7F7410928FA8 001 ----- Init

```

```

:559FB88BD000+500508B
7F7410928FA8 0000200712 7F7410928EB8 7F741095A008 001 ----- Interrupt Stack
:559FB88BD000+A65A3A8
7F741095A008 0000006888 7F7410928FA8 7F741095BB48 001 ----- TTY data
:559FB88BD000+8F75806
7F741095BB48 0000004104 7F741095A008 7F741095CBA8 001 ----- TTY Input Buf
:559FB88BD000+8F77B6F
7F741095CBA8 0000004104 7F741095BB48 7F741095DC08 001 ----- TTY Output Buf
:559FB88BD000+8F77BC7
7F741095DC08 0000024584 7F741095CBA8 7F7410963C68 001 ----- proc_hist_lmt_v
:559FB88BD000+D06DC00
7F7410963C68 0000008200 7F741095DC08 7F7410965CC8 001 ----- proc_hist_lmt_v
:559FB88BD000+D06DC48
7F7410965CC8 0000008200 7F7410963C68 7F7410967D28 001 ----- proc_hist_lmt_v
:559FB88BD000+D06DC82
7F7410967D28 0000005008 7F7410965CC8 7F7410969110 001 ----- messages
:559FB88BD000+90BBB5
7F7410969110 0000005008 7F7410967D28 7F741096A4F8 001 ----- Watched message
:559FB88BD000+90BBED
7F741096A4F8 0000020008 7F7410969110 7F741096F378 001 ----- Watched Queue
:559FB88BD000+90BBC1E
7F741096F378 0000065544 7F741096A4F8 7F741097F3D8 001 ----- Watched Queue I
:559FB88BD000+90BBC55
7F741097F3D8 0000020008 7F741096F378 7F7410984258 001 ----- Watched Boolean
:559FB88BD000+90BBC86
7F7410984258 0000020008 7F741097F3D8 7F74109890D8 001 ----- Watched Bitfiel
:559FB88BD000+90BBCB7
7F74109890D8 0000010008 7F7410984258 7F741098B848 001 ----- Watcher Info
:559FB88BD000+90BBD19
7F741098B848 0000010008 7F74109890D8 7F741098DFB8 001 ----- Read/Write Lock
:559FB88BD000+90BBDAC
7F741098DFB8 0000000184 7F741098B848 7F741098E0C8 001 ----- *Init*
:559FB88BD000+90A4B10
7F741098E0C8 0000000064 7F741098DFB8 7F741098E160 001 ----- Init
:559FB88BD000+98AD5C3
7F741098E160 0000000576 7F741098E0C8 7F741098E3F8 001 ----- *Init*
:559FB88BD000+9060A7C
7F741098E3F8 0000000400 7F741098E160 7F741098E5E0 001 ----- *Init*
:559FB88BD000+9060A7C
7F741098E5E0 0000001240 7F741098E3F8 7F741098EB10 001 ----- *Init*
:559FB88BD000+9060A7C
7F741098EB10 0000000488 7F741098E5E0 7F741098ED50 001 ----- *Init*
:559FB88BD000+9060A7C
7F741098ED50 0000000072 7F741098EB10 7F741098EDF0 001 ----- Init
:559FB88BD000+98DB044
7F741098EDF0 0000000056 7F741098ED50 7F741098EE80 001 ----- Init
:559FB88BD000+5D94FF6
7F741098EE80 0000000208 7F741098EDF0 7F741098EFA8 001 ----- *Init*
:559FB88BD000+C1E0292
7F741098EFA8 0000028104 7F741098EE80 7F7410995DC8 001 ----- Process Stack
:559FB88BD000+A65A3A8
7F7410995DC8 0000000152 7F741098EFA8 7F7410995EB8 001 ----- *Init*
:559FB88BD000+90C3F74
7F7410995EB8 0000000152 7F7410995DC8 7F7410995FA8 001 ----- *Init*
:559FB88BD000+9060A7C
7F7410995FA8 0000016104 7F7410995EB8 7F7410999EE8 001 ----- Process Stack
:559FB88BD000+A65A3A8
7F7410999EE8 0000032776 7F7410995FA8 7F74109A1F48 001 ----- List Elements
:559FB88BD000+904DF98
7F74109A1F48 0000032776 7F7410999EE8 7F74109A9FA8 001 ----- List Elements
:559FB88BD000+904DF98
7F74109A9FA8 0000032776 7F74109A1F48 7F74109B2008 001 ----- List Elements
:559FB88BD000+904DF98
7F74109B2008 0000032776 7F74109A9FA8 7F74109BA068 001 ----- List Elements

```

```
:559FB88BD000+904DF98
7F74109BA068 0000032776 7F74109B2008 7F74109C20C8 001 ----- List Elements
:559FB88BD000+904DF98
7F74109C20C8 0000032776 7F74109BA068 7F74109CA128 001 ----- List Elements
:559FB88BD000+904DF98
7F74109CA128 0000032776 7F74109C20C8 7F74109D2188 001 ----- List Element
```

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

```
Router# show process cpu
CPU utilization for five seconds: 1%/0%; one minute: 1%; five minutes: 1%
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
PID Runtime(ms) Invoked uSecs 5Sec 1Min 5Min TTY Process
1 3 21 142 0.00% 0.00% 0.00% 0 Chunk Manager
2 166 399 416 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 17 14 1214 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 1017 304 3345 0.47% 0.06% 0.03% 0 Check heaps
10 5 34 147 0.00% 0.00% 0.00% 0 Pool Manager
11 0 1 0 0.00% 0.00% 0.00% 0 DiscardQ Backgro
12 1 2 500 0.00% 0.00% 0.00% 0 Timers
13 0 53 0 0.00% 0.00% 0.00% 0 WATCH_AFS
14 0 1 0 0.00% 0.00% 0.00% 0 MEMLEAK_PROCESS
15 4 18 222 0.00% 0.00% 0.00% 0 ARP Input
16 37 2132 17 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
23 130 50 2600 0.00% 0.00% 0.00% 0 Entity MIB API
24 179 83 2156 0.00% 0.00% 0.00% 0 PrstVbl
25 2 247 8 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 10 1000 10 0.00% 0.00% 0.00% 0 IOSXE heartbeat
30 31 1023 30 0.00% 0.00% 0.00% 0 DB Lock Manager
31 33 1989 16 0.00% 0.00% 0.00% 0 GraphIt
32 0 1 0 0.00% 0.00% 0.00% 0 DB Notification
33 0 1 0 0.00% 0.00% 0.00% 0 IPC Apps Task
34 0 1 0 0.00% 0.00% 0.00% 0 ifIndex Receive
35 5 401 12 0.00% 0.00% 0.00% 0 IPC Event Notifi
36 32 1952 16 0.00% 0.00% 0.00% 0 IPC Mcast Pendin
37 0 1 0 0.00% 0.00% 0.00% 0 Platform appsess
38 0 34 0 0.00% 0.00% 0.00% 0 IPC Dynamic Cach
39 1 401 2 0.00% 0.00% 0.00% 0 IPC Service NonC
40 0 1 0 0.00% 0.00% 0.00% 0 IPC Zone Manager
41 16 1952 8 0.00% 0.00% 0.00% 0 IPC Periodic Tim
42 19 1952 9 0.00% 0.00% 0.00% 0 IPC Deferred Por
43 0 1 0 0.00% 0.00% 0.00% 0 IPC Process leve
44 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat Manager
45 0 115 0 0.00% 0.00% 0.00% 0 IPC Check Queue
46 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat RX Cont
47 0 1 0 0.00% 0.00% 0.00% 0 IPC Seat TX Cont
48 10 201 49 0.00% 0.00% 0.00% 0 IPC Keep Alive M
49 33 401 82 0.00% 0.00% 0.00% 0 IPC Loadometer
50 0 1 0 0.00% 0.00% 0.00% 0 IPC Session Deta
51 0 1 0 0.00% 0.00% 0.00% 0 SENSOR-MGR event
52 2 201 9 0.00% 0.00% 0.00% 0 Compute SRP rate
```

```

53 0 1 0 0.00% 0.00% 0.00% 0 IFS Agent Manage
54 0 1 0 0.00% 0.00% 0.00% 0 License IPC stat
55 0 1 0 0.00% 0.00% 0.00% 0 License IPC serv
56 0 7 0 0.00% 0.00% 0.00% 0 Net Input
57 0 2 0 0.00% 0.00% 0.00% 0 Dialer event
58 0 1 0 0.00% 0.00% 0.00% 0 SERIAL A'detect
59 0 1 0 0.00% 0.00% 0.00% 0 IOSXE signals IO
60 0 1 0 0.00% 0.00% 0.00% 0 client_entity_se
61 1 1 1000 0.00% 0.00% 0.00% 0 RF SCTPthread
62 0 1 0 0.00% 0.00% 0.00% 0 CHKPT RG SCTPthr
63 0 2 0 0.00% 0.00% 0.00% 0 XML Proxy Client
64 0 1 0 0.00% 0.00% 0.00% 0 ARP Snoop
65 28 1999 14 0.00% 0.00% 0.00% 0 Dynamic ARP Insp
66 1216 110 11054 0.00% 0.00% 0.00% 0 crypto sw pk pro
67 0 2 0 0.00% 0.00% 0.00% 0 License Client N
68 0 1 0 0.00% 0.00% 0.00% 0 Image License br
69 24 133 180 0.00% 0.00% 0.00% 0 SAEventLog
70 11 2 5500 0.00% 0.00% 0.00% 0 SASStorage
71 1 4 250 0.00% 0.00% 0.00% 0 SASConnect
72 41 1165 35 0.00% 0.00% 0.00% 0 SASRcvWQ
73 2 5 400 0.00% 0.00% 0.00% 0 SACConnect
74 30 1183 25 0.00% 0.00% 0.00% 0 SACRcvWQ
75 8 68 117 0.00% 0.00% 0.00% 0 Licensing Auto U
76 0 1 0 0.00% 0.00% 0.00% 0 License HA Consi
77 0 1 0 0.00% 0.00% 0.00% 0 Token Daemon
78 0 1 0 0.00% 0.00% 0.00% 0 Critical Bkgnd
79 221 1374 160 0.00% 0.00% 0.00% 0 Net Background
80 0 3 0 0.00% 0.00% 0.00% 0 IDB Work
81 8 101 79 0.00% 0.00% 0.00% 0 Logger
82 71 1985 35 0.00% 0.00% 0.00% 0 TTY Background
83 53 24 2208 0.00% 0.00% 0.00% 0 CTS CORE
84 1 3 333 0.00% 0.00% 0.00% 0 SXP CORE
85 56 1164 48 0.00% 0.00% 0.00% 0 SASRcvWQWrk1
86 3 14 214 0.00% 0.00% 0.00% 0 IF-MGR control p
87 0 28 0 0.00% 0.00% 0.00% 0 IF-MGR event pro
88 0 2 0 0.00% 0.00% 0.00% 0 CTS HA
89 0 2 0 0.00% 0.00% 0.00% 0 CTS HA IPC flow
90 0 1 0 0.00% 0.00% 0.00% 0 CTS HA operation
91 5357 18052 296 0.15% 0.20% 0.20% 0 IOSD ipc task
92 213 5786 36 0.00% 0.00% 0.00% 0 IOSD chasfs task
93 0 2 0 0.00% 0.00% 0.00% 0 Crimson interfac
94 274 19 14421 0.00% 0.00% 0.00% 0 Crimson Database
95 681 2548 267 0.00% 0.02% 0.00% 0 Crimson flush tr
96 4 287 13 0.00% 0.00% 0.00% 0 REDUNDANCY FSM
97 0 1 0 0.00% 0.00% 0.00% 0 Punt FP Stats Du
98 171 953 179 0.00% 0.00% 0.00% 0 PuntInject Keepa
99 0 16 0 0.00% 0.00% 0.00% 0 ESG MATM Learnin
100 141 401 351 0.00% 0.00% 0.00% 0 CMAN RP Msg Proc
101 118 1998 59 0.00% 0.00% 0.00% 0 Environmental Mo
102 42 1998 21 0.00% 0.00% 0.00% 0 RP HA Periodic
103 0 2 0 0.00% 0.00% 0.00% 0 cpf_msg_holdq_pr
104 0 1 0 0.00% 0.00% 0.00% 0 cpf_msg_rcvq_pro
105 0 1 0 0.00% 0.00% 0.00% 0 cpf_process_tpQ
106 0 1 0 0.00% 0.00% 0.00% 0 CEF RRP RF waite
107 0 1 0 0.00% 0.00% 0.00% 0 CONSOLE helper p
108 175 50 3500 0.00% 0.00% 0.00% 0 DBAL EVENTS
109 0 1 0 0.00% 0.00% 0.00% 0 XDR RRP RF waite
110 50 1999 25 0.00% 0.00% 0.00% 0 REDUNDANCY peer
111 337 19959 16 0.00% 0.00% 0.00% 0 100ms check
112 0 1 0 0.00% 0.00% 0.00% 0 CWAN APS HA Proc
113 1 34 29 0.00% 0.00% 0.00% 0 RF CWAN HA Proce
114 0 1 0 0.00% 0.00% 0.00% 0 CWAN IF EVENT HA
115 0 4 0 0.00% 0.00% 0.00% 0 ANCP HA
116 0 2 0 0.00% 0.00% 0.00% 0 ANCP HA IPC flow

```

```

117 0 1 0 0.00% 0.00% 0.00% 0 QoS HA ID RETAIN
118 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
119 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
120 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
121 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
122 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
123 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
124 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
125 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
126 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
127 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
128 0 1 0 0.00% 0.00% 0.00% 0 CHKPT Test clien
129 0 1 0 0.00% 0.00% 0.00% 0 DHCPC HA
130 0 1 0 0.00% 0.00% 0.00% 0 DHCPD HA
131 0 1 0 0.00% 0.00% 0.00% 0 DHCPv6 Relay HA
132 0 1 0 0.00% 0.00% 0.00% 0 DHCPv6 Server HA
133 0 2 0 0.00% 0.00% 0.00% 0 SISF HA Process
134 0 5 0 0.00% 0.00% 0.00% 0 ARP HA
135 0 1 0 0.00% 0.00% 0.00% 0 IOSXE-RP Punt Se
136 0 1 0 0.00% 0.00% 0.00% 0 IOSXE-RP Punt IP
137 0 1 0 0.00% 0.00% 0.00% 0 ACL Log Punt Ser
138 0 1 0 0.00% 0.00% 0.00% 0 ACL deny punt se
139 1576 124342 12 0.07% 0.06% 0.07% 0 L2 LISP Punt Pro
140 0 1 0 0.00% 0.00% 0.00% 0 OFSDN Punject Pr
141 1653 124341 13 0.15% 0.08% 0.07% 0 SIS Punt Process
142 0 1 0 0.00% 0.00% 0.00% 0 IOSXE-RP SPA TSM
143 0 1 0 0.00% 0.00% 0.00% 0 IOSXE-RP QFP HA
144 0 1 0 0.00% 0.00% 0.00% 0 Network-rf Notif
145 0 1 0 0.00% 0.00% 0.00% 0 DHCP Snooping cl
146 1 18 55 0.00% 0.00% 0.00% 0 DHCP Snooping
147 0 1 0 0.00% 0.00% 0.00% 0 DHCP Snooping db
148 0 1 0 0.00% 0.00% 0.00% 0 IKE HA Mgr
149 0 1 0 0.00% 0.00% 0.00% 0 IPSEC HA Mgr
150 0 1 0 0.00% 0.00% 0.00% 0 Crypto PKI-HA
151 3 12 250 0.00% 0.00% 0.00% 0 RF Master Main T
152 0 7 0 0.00% 0.00% 0.00% 0 RF Master Status
153 39 1009 38 0.00% 0.00% 0.00% 0 SACRcvWQWrk1
154 28 1009 27 0.00% 0.00% 0.00% 0 SACRcvWQWrk2
155 103 1185 86 0.00% 0.00% 0.00% 0 SACRcvWQWrk3
156 0 1 0 0.00% 0.00% 0.00% 0 BACK CHECK
157 323 210 1538 0.00% 0.00% 0.00% 0 SAMsgThread
158 25 202 123 0.00% 0.00% 0.00% 0 Compute load avg
159 515 107 4813 0.00% 0.02% 0.00% 0 Per-minute Jobs
160 167 2009 83 0.00% 0.00% 0.00% 0 Per-Second Jobs
161 0 1 0 0.00% 0.00% 0.00% 0 Transport Port A
162 167 9 18555 0.00% 0.00% 0.00% 0 ACT2 Crypto Engi
163 0 1 0 0.00% 0.00% 0.00% 0 AggMgr Process
164 0 4 0 0.00% 0.00% 0.00% 0 EEM ED MAT
165 4 73 54 0.00% 0.00% 0.00% 0 EEM ED ND
166 0 1 0 0.00% 0.00% 0.00% 0 MACSEC POST rest
167 0 1 0 0.00% 0.00% 0.00% 0 MACSEC POST hand
168 0 1 0 0.00% 0.00% 0.00% 0 MACSEC POST hand
169 0 1 0 0.00% 0.00% 0.00% 0 IOSXE-RP FastPat
170 0 6 0 0.00% 0.00% 0.00% 0 NGIO_BRI_POLL_DE
171 0 1 0 0.00% 0.00% 0.00% 0 ASYNC Input
172 21 2001 10 0.00% 0.00% 0.00% 0 IR8340 Alarm Con
173 0 2 0 0.00% 0.00% 0.00% 0 dialer isdn sess
174 0 1 0 0.00% 0.00% 0.00% 0 DSX3MIB ll handl
175 29 1961 14 0.00% 0.00% 0.00% 0 fanrp_l2fib
176 0 1 0 0.00% 0.00% 0.00% 0 POS APS Event Pr
177 0 2 0 0.00% 0.00% 0.00% 0 netclk_process
178 0 1 0 0.00% 0.00% 0.00% 0 netclk_ha_proces

```

Router#show process cpu platform sorted

```

CPU utilization for five seconds: 21%, one minute: 22%, five minutes: 22%
Core 0: CPU utilization for five seconds: 4%, one minute: 5%, five minutes: 5%
Core 1: CPU utilization for five seconds: 2%, one minute: 5%, five minutes: 5%
Core 2: CPU utilization for five seconds: 4%, one minute: 6%, five minutes: 6%
Core 3: CPU utilization for five seconds: 4%, one minute: 6%, five minutes: 6%
Core 4: CPU utilization for five seconds: 5%, one minute: 5%, five minutes: 5%
Core 5: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 6: CPU utilization for five seconds: 41%, one minute: 42%, five minutes: 43%
Core 7: CPU utilization for five seconds: 100%, one minute: 100%, five minutes: 100%
Pid PPid 5Sec 1Min 5Min Status Size Name

15435 15419 158% 158% 157% S 226748 ucode_pkt_PPE0
16998 16972 7% 6% 7% S 14252 btman
56 2 3% 5% 5% S 0 ksmd
15179 15139 2% 2% 2% S 171524 fman_fp_image
3821 3807 2% 3% 3% S 584524 linux_iosd-imag
26565 26536 1% 1% 1% S 52764 fman_cc
29044 2 0% 0% 0% I 0 kworker/u32:0-events
26536 16605 0% 0% 0% S 3788 pman
25912 25906 0% 0% 0% S 116208 fed main event
25906 16605 0% 0% 0% S 3796 pman
25689 25684 0% 0% 0% S 5036 nginx
25688 25684 0% 0% 0% S 5868 nginx
25684 25678 0% 0% 0% S 9980 nginx
25678 2784 0% 0% 0% S 3792 pman
25359 25349 0% 0% 0% S 8448 ngiolite
25349 16605 0% 0% 0% S 3792 pman
25048 25043 0% 0% 0% S 9876 ngiolite
25043 16605 0% 0% 0% S 3792 pman
24784 24779 0% 0% 0% S 12352 ngiolite
24779 16605 0% 0% 0% S 3824 pman
24713 2 0% 0% 0% I 0 kworker/1:2H
24688 24446 0% 0% 0% S 432 sleep
24446 1 0% 0% 0% S 2100 memory_monitor.
24341 24333 0% 0% 0% S 12300 ngiolite
24333 16605 0% 0% 0% S 3824 pman
24164 2 0% 0% 0% S 0 SarIosdMond
22339 2 0% 0% 0% I 0 gobisetpower-2-
22338 2 0% 0% 0% I 0 gobireadcb-2-2-
22337 2 0% 0% 0% I 0 gobiprobe-2-2-3
22139 22129 0% 0% 0% S 62172 iomd
22129 16605 0% 0% 0% S 3768 pman
21734 21723 0% 0% 0% S 62064 iomd
21723 16605 0% 0% 0% S 3768 pman
21566 2 0% 0% 0% I 0 kworker/1:3-gobiread
21466 21458 0% 0% 0% S 61992 iomd
21458 16605 0% 0% 0% S 3768 pman
21135 2 0% 0% 0% I 0 gobisetpower-1-
21131 2 0% 0% 0% I 0 gobireadcb-1-2-
21129 2 0% 0% 0% I 0 gobiprobe-1-2-2
21128 2 0% 0% 0% I 0 gobisetpower-0-
21127 2 0% 0% 0% I 0 gobireadcb-0-2-
21126 2 0% 0% 0% I 0 gobiprobe-0-2-2
21120 21113 0% 0% 0% S 74960 iomd
21113 16605 0% 0% 0% S 3820 pman
20788 20780 0% 0% 0% S 63312 iomd
20780 16605 0% 0% 0% S 3768 pman
19604 19582 0% 0% 0% S 18360 btman
19582 16605 0% 0% 0% S 3772 pman
19136 2 0% 0% 0% I 0 kworker/7:2H
18966 18953 0% 0% 0% S 23472 cmcc
18953 16605 0% 0% 0% S 3768 pman
18687 18674 0% 0% 0% S 12420 hman
18674 16605 0% 0% 0% S 3768 pman

```

```

18341 18320 0% 0% 0% S 7020 pttcd
18320 2784 0% 0% 0% S 3776 pman
18046 18031 0% 0% 0% S 78104 pubd
18031 2784 0% 0% 0% S 3776 pman
17396 2 0% 0% 0% I 0 kworker/5:0H
17301 16605 0% 0% 0% S 712 inotifywait
17057 1 0% 0% 0% S 3356 rotee
16972 14118 0% 0% 0% S 3768 pman
16605 1 0% 0% 0% S 8020 pvp.sh
16567 16545 0% 0% 0% S 19688 cman_fp
16545 14118 0% 0% 0% S 3768 pman
16331 16317 0% 0% 0% S 170672 cpp_cp_svr
16317 14118 0% 0% 0% S 3768 pman
16108 16095 0% 0% 0% S 66440 cpp_driver
16095 14118 0% 0% 0% S 3768 pman
15888 15873 0% 0% 0% S 70160 cpp_ha_top_leve
15873 14118 0% 0% 0% S 3772 pman
15660 15646 0% 0% 0% S 80592 cpp_sp_svr
15646 14118 0% 0% 0% S 3768 pman
15419 14118 0% 0% 0% S 3772 pman
15139 14118 0% 0% 0% S 3768 pman
14861 14844 0% 0% 0% S 12420 hman
14844 14118 0% 0% 0% S 3768 pman
14745 14731 0% 0% 0% S 1676 sort_files_by_i
14731 2784 0% 0% 0% S 3756 pman
14405 14118 0% 0% 0% S 712 inotifywait
14282 1 0% 0% 0% S 3356 rotee
14118 1 0% 0% 0% S 7988 pvp.sh
13169 13160 0% 0% 0% S 4224 flash_check.sh
13160 2784 0% 0% 0% S 3764 pman
12444 12435 0% 0% 0% S 14176 lman
12435 2784 0% 0% 0% S 3772 pman
12306 5095 0% 0% 0% S 3108 journalctl
10703 2784 0% 0% 0% S 712 inotifywait
10439 10345 0% 0% 0% S 712 inotifywait
10431 1 0% 0% 0% S 3360 rotee
10347 1 0% 0% 0% S 1180 xinetd
10346 1 0% 0% 0% S 1188 xinetd
10345 1 0% 0% 0% S 12168 rollback_timer.
10343 1 0% 0% 0% S 2068 auxinit.sh
9415 1 0% 0% 0% S 1012 xinetd
9412 1 0% 0% 0% S 1176 xinetd
9150 2 0% 0% 0% I 0 kworker/2:2H-kblockd
8448 1 0% 0% 0% S 6240 dhcpd
8198 8176 0% 0% 0% S 6784 tam_svcs_esg_cf
8176 2784 0% 0% 0% S 3776 pman
7929 7914 0% 0% 0% S 8432 tamd_proc
7914 2784 0% 0% 0% S 3776 pman
7673 7658 0% 0% 0% S 7904 tams_proc
7658 2784 0% 0% 0% S 3776 pman
7422 7405 0% 0% 0% S 32684 btman
7405 2784 0% 0% 0% S 3772 pman
7127 7106 0% 0% 0% S 26272 cli_agent
7106 2784 0% 0% 0% S 3780 pman
6878 6862 0% 1% 1% S 27788 cmand
6862 2784 0% 0% 0% S 3776 pman
6600 6583 0% 0% 0% S 92300 dbm
6583 2784 0% 0% 0% S 3772 pman
6059 6025 0% 0% 0% S 84992 fman_rp
6025 2784 0% 0% 0% S 3772 pman
5779 2 0% 0% 0% S 0 lfts_sar_aux
5778 5763 0% 0% 0% R 15868 hman
5763 2784 0% 0% 0% S 3772 pman
5568 5103 0% 0% 0% S 712 inotifywait

```

```

5560 1 0% 0% 0% S 3356 rotee
5412 5388 0% 0% 0% S 11452 keyman
5388 2784 0% 0% 0% S 3772 pman
5287 1 0% 0% 0% S 3360 rotee
5103 1 0% 0% 0% S 5640 iptbl.sh
5095 5086 0% 0% 0% S 10900 plogd
5086 2784 0% 0% 0% S 3780 pman
5054 13169 0% 0% 0% S 440 sleep
5043 4729 0% 0% 0% S 716 inotifywait
5030 14745 0% 0% 0% S 432 sleep
4940 1 0% 0% 0% S 3424 rotee

```

Router#

## 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 2 seconds ago
Load Average: healthy
1-Min: 2.07, status: healthy, under 9.30
5-Min: 2.03, status: healthy, under 9.30
15-Min: 1.92, status: healthy, under 9.30
Memory (kb): healthy
Total: 8000724
Used: 2565652 (32%), status: healthy
Free: 5435072 (68%)
Committed: 3263176 (41%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 0.80, System: 4.00, Nice: 0.00, Idle: 95.19
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 2.50, System: 1.60, Nice: 0.00, Idle: 95.90
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 2.90, System: 1.80, Nice: 0.00, Idle: 95.30
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 1.49, System: 7.79, Nice: 0.00, Idle: 90.70
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU4: CPU Utilization (percentage of time spent)
User: 4.60, System: 1.80, Nice: 0.00, Idle: 93.59
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU5: CPU Utilization (percentage of time spent)
User: 0.99, System: 1.89, Nice: 0.00, Idle: 97.10
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU6: CPU Utilization (percentage of time spent)
User: 24.10, System: 18.30, Nice: 0.00, Idle: 57.60
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
CPU7: CPU Utilization (percentage of time spent)
User: 92.50, System: 7.50, Nice: 0.00, Idle: 0.00
IRQ: 0.00, SIRQ: 0.00, IOWait: 0.00
```

```
Router#

Router# show platform software status control-processor brief
Load Average
Slot Status 1-Min 5-Min 15-Min
RP0 Healthy 2.01 2.01 1.91

Memory (kB)
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
RP0 Healthy 8000724 2565240 (32%) 5435484 (68%) 3263124 (41%)

CPU Utilization
Slot CPU User System Nice Idle IRQ SIRQ IOWait
RP0 0 0.70 3.30 0.00 96.00 0.00 0.00 0.00
1 4.39 7.39 0.00 88.11 0.00 0.09 0.00
2 4.80 9.30 0.00 85.80 0.00 0.10 0.00
3 3.39 8.69 0.00 87.91 0.00 0.00 0.00
4 4.40 1.80 0.00 93.80 0.00 0.00 0.00
5 1.00 1.90 0.00 97.10 0.00 0.00 0.00
6 24.64 23.54 0.00 51.80 0.00 0.00 0.00
7 92.60 7.40 0.00 0.00 0.00 0.00 0.00

Router#
```

# 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 22

# Troubleshooting

---

- [Troubleshooting, on page 257](#)
- [Understanding Diagnostic Mode, on page 257](#)
- [Before Contacting Cisco or Your Reseller, on page 258](#)
- [show interfaces Troubleshooting Command, on page 258](#)
- [Software Upgrade Methods, on page 258](#)
- [Change the Configuration Register, on page 259](#)
- [Recovering a Lost Password, on page 262](#)

## 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 IR8340 supports the following interfaces:

- GigabitEthernet 0/0/0 and 0/0/1
- Cellular 0/4/0, Cellular 0/4/1, Cellular 0/5/0, and Cellular 0/5/1
- msata

## 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_V177_THROTTLE_LATEST_20210827_030512_V17_7_0_91
Cisco IOS Software [Bengaluru], ir8340 Software (X86_64_LINUX_IOSD-UNIVERSALK9_IOT-M),
Experimental Version 17.7.20210827:033430
[S2C-build-v177_throttle-289-/nobackup/mcpre/BLD-BLD_V177_THROTTLE_LATEST_20210827_030512
154]
Copyright (c) 1986-2021 by Cisco Systems, Inc.
Compiled Fri 27-Aug-21 15:58 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: v0.33

```
Router uptime is 1 week, 1 day, 23 hours, 9 minutes
Uptime for this control processor is 1 week, 1 day, 23 hours, 10 minutes
System returned to ROM by Reload Command
System image file is
"flash:ir8340-universalk9.BLD_V177_THROTTLE_LATEST_20210827_030512_V17_7_0_91.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](mailto: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 crypto throughput level is 250000 kbps

Smart Licensing Status: Registration Not Applicable/Not Applicable

```
cisco IR8340-K9 (2RU) processor with 3717851K/6147K bytes of memory.
Processor board ID FDO2502JF0L
Router operating mode: Autonomous
1 Virtual Ethernet interface
14 Gigabit Ethernet interfaces
8 Serial interfaces
8 terminal lines
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
7574982K bytes of flash memory at bootflash:.
33554432K bytes of mSATA at msata:.
929715K bytes of sdcard flash at sdcard:.
30031856K bytes of USB flash at usb0:.
```

Configuration register is 0x0

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 0x142
```

**Step 3** Sync the configuration changes with the **sync** command.

**Example:**

```
rommon 3>sync
```

**Step 4** Reset the router to apply confreg. The router will reload with the reset.

**Example:**

```
rommon 4>reset
```

```
resetting...
```

**Step 5** 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 6** Boot the image with the confreg 0x2142.

**Example:**

```
rommon 2> boot
flash:ir8340-universalk9.BLD_V177_THROTTLE_LATEST_20210827_030512_V17_7_0_91.SSA.bin
```

---

## Recovering a Lost Password

To recover a lost password, follow these steps. Refer to [Reset the Router, on page 261](#) 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br><pre>Router&gt; enable</pre>                                                                                          | Enables privileged EXEC mode.<br>Enter your password if prompted.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br><pre>Router# configure terminal</pre>                                                                     | Enters global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 3</b> | <b>transport-map type console</b><br><i>transport-map-name</i><br><b>Example:</b><br><pre>Router(config)# transport-map type console consolehandler</pre> | Creates and names a transport map for handling console connections, and enters transport map configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 4</b> | <b>connection wait [allow [interruptible]   none [disconnect]]</b><br><b>Example:</b><br><pre>Router(config-tmap)# connection wait none</pre>             | Specifies how a console connection will be handled using this transport map. <ul style="list-style-type: none"> <li>• <b>allow interruptible</b>—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.</li> </ul> <b>Note</b><br>Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b> . <ul style="list-style-type: none"> <li>• <b>none</b>—The console connection immediately enters diagnostic mode.</li> </ul> |

|               | Command or Action                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 5</b> | <p>(Optional) <b>banner</b> [<b>diagnostic</b>   <b>wait</b>]<br/><i>banner-message</i></p> <p><b>Example:</b></p> <pre>Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. --Welcome to Diagnostic Mode-- X Router(config-tmap)#</pre> | <p>(Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.</p> <ul style="list-style-type: none"> <li>• <b>diagnostic</b>—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.</li> </ul> <p><b>Note</b><br/>Users can interrupt a waiting connection by entering <b>Ctrl-C</b> or <b>Ctrl-Shift-6</b>.</p> <ul style="list-style-type: none"> <li>• <b>wait</b>—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.</li> <li>• <i>banner-message</i>—Banner message, which begins and ends with the same delimiting character.</li> </ul> |
| <b>Step 6</b> | <p><b>exit</b></p> <p><b>Example:</b></p> <pre>Router(config-tmap)# exit</pre>                                                                                                                                                                                               | Exits transport map configuration mode to re-enter global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 7</b> | <p><b>transport type console</b><br/><i>console-line-number input</i><br/><i>transport-map-name</i></p> <p><b>Example:</b></p> <pre>Router(config)# transport type console 0 input consolehandler</pre>                                                                      | <p>Applies the settings defined in the transport map to the console interface.</p> <p>The <i>transport-map-name</i> for this command must match the <i>transport-map-name</i> defined in the <b>transport-map type console</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

## Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

## Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

**show transport-map** [**all** | **name** *transport-map-name* | **type** [**console** ]]

This command can be used either in user EXEC mode or privileged EXEC mode.

### Example

The following example shows transport maps that are configured on the router: console port (*consolehandler*):

```
Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode
```

```
Router# show transport-map type console
Transport Map:
Name: consolehandler
```

```
REVIEW DRAFT - CISCO CONFIDENTIAL
```

```
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

```
Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode
```

Use the **show platform software configuration access policy** command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides

the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the **show transport-map** command, the **show platform software configuration access policy** command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

### Example

The following example shows the **show platform software configuration access policy** command.

```
Router# show platform software configuration access policy
The current access-policies

Method : telnet
Rule : wait with interrupt Shell banner:
Welcome to Diagnostic Mode

Wait banner :
Waiting for IOS Process

Method : ssh Rule : wait Shell banner: Wait banner :

Method : console
Rule : wait with interrupt Shell banner:
Wait banner :
```

## Using the factory reset Commands

The **factory reset** commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.



#### Caution

Use of the factory reset command should not be done lightly. All customer configurations will be deleted and the platform will boot up as if new from the factory.



#### Note

factory-reset all does not work if IOS-XE is running in controller mode. Please refer to SDWAN configuration information.

```
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.

