# Cisco 1000 Series Software Configuration Guide, Cisco IOS XE 17

**First Published:** 2019-11-18

**Last Modified:** 2022-08-29

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

© 2021-2022 Cisco Systems, Inc. All rights reserved.

# CONTENTS


CHAPTER 1 **Overview** 1

Introduction to Cisco 1000 Series Integrated Services Routers 1

CHAPTER 2 **Using Cisco IOS XE Software** 3

Accessing the CLI Using a Router Console 3

Accessing the CLI Using a Directly-Connected Console 3

Connecting to the Console Port 3

Use the Console Interface 4

Using SSH to Access Console 4

Accessing the CLI from a Remote Console Using Telnet 5

Preparing to Connect to the Router Console Using Telnet 5

Using Telnet to Access a Console Interface 6

Accessing the CLI from a Remote Console Using a Modem 6

Accessing the CLI from a Micro USB Serial Console Port 7

Keyboard Shortcuts 7

Using the History Buffer to Recall Commands 7

Understanding Command Modes 8

Understanding Diagnostic Mode 9

Getting Help 10

Using the no and default Forms of Commands 14

Using the factory reset Commands 14

Saving Configuration Changes 14

Managing Configuration Files 15

Filtering Output from the show and more Commands 15

Powering Off a Router 16

Finding Support Information for Platforms and Cisco Software Images 16

Using Cisco Feature Navigator 16
Using Software Advisor 16
Using Software Release Notes 16
CLI Session Management 16
Information About CLI Session Management 17
Changing the CLI Session Timeout 17
Locking a CLI Session 17
Initial Bootup Security 18

CHAPTER 3 **Installing the Software** 21
Installing the Software 21
Guestshell Installation 22
Licensing 23
Cisco Software Licensing 23
Consolidated Packages 23
Technology Packages 24
Unlicensed Feature: Example 25
LED Indicators 25
Related Documentation 25
How to Install and Upgrade the Software 26
Managing and Configuring a Router to Run Using Individual Packages 30
How to Install and Upgrade the Software for Cisco IOS XE Denali Release 16.3 36
Installing a Firmware Subpackage 42
Upgrading the Firmware on xDSL NIMs 48
Provisioning Files 57
File Systems 58
Autogenerated File Directories and Files 58
Flash Storage 59
Configuring the Configuration Register for Autoboot 59
Crypto Throughput Licensing 60
Unlicensed Feature: Example 62
LED Indicators 62
Related Documentation 62
How to Install and Upgrade the Software 63

Managing and Configuring a Router to Run Using a Consolidated Package 63
Managing and Configuring a Consolidated Package Using copy and boot Commands 63
Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example 64
Managing and Configuring a Router to Run Using Individual Packages 70
Installing Subpackages from a Consolidated Package 70
Installing Subpackages from a Consolidated Package on a Flash Drive 79
How to Install and Upgrade the Software for Cisco IOS XE Everest Release 16.6 79
Upgrading to Cisco IOS XE Everest 16.6.2 Release 79

CHAPTER 4 **Configuring ROMMON** 81
ROMMON Images 81

CHAPTER 5 **Basic Router Configuration** 83
Default Configuration 83
Configuring Global Parameters 86
Configuring Gigabit Ethernet Interfaces 86
Configuring a Loopback Interface 87
Configuring Module Interfaces 89
Enabling Cisco Discovery Protocol 89
Configuring Command-Line Access 89
Configuring Static Routes 91
Configuring Dynamic Routes 92
Configuring Routing Information Protocol 92
Configuring Enhanced Interior Gateway Routing Protocol 97

CHAPTER 6 **Control Router Access with Passwords and Privilege Levels** 99
Restrictions and Guidelines for Reversible Password Types 99
Restrictions and Guidelines for Irreversible Password Types 100
Information About Controlling Router Access with Passwords and Privileges 100
Preventing Unauthorized Access 100
Default Password and Privilege Level Configuration 101
Additional Password Security 101
Password Recovery 102

Terminal Line Telnet Configuration 102
Username and Password Pairs 102
Privilege Levels 102
AES Password Encryption and Primary Encryption Keys 103
How to Configure Switch Access with Passwords and Privileges 103
Setting or Changing a Static Enable Password 103
Protecting Enable and Enable Secret Passwords with Encryption 104
Disabling Password Recovery 107
Setting a Telnet Password for a Terminal Line 108
Configuring Username and Password Pairs 109
Setting the Privilege Level for a Command 110
Changing the Default Privilege Level for Lines 111
Logging in to and Exiting a Privilege Level 112
Configuring an Encrypted Preshared Key 113
Monitoring Switch Access with Passwords and Privileges 114
Configuration Examples for Switch Access with Passwords and Privilege Levels 114
Example: Setting or Changing a Static Enable Password 114
Example: Protecting Enable and Enable Secret Passwords with Encryption 114
Example: Setting a Telnet Password for a Terminal Line 114
Example: Setting the Privilege Level for a Command 114
Example: Configuring an Encrypted Preshared Key 115
Additional References for Switch Access with Passwords and Privilege Levels 115
Feature Information for Controlling Router Access with Passwords and Privileges 115

CHAPTER 7 **Change of Authorization** 117
Feature Information for Change of Authorization 117
Information About Change of Authorization 118
Change of Authorization-Reauthentication Procedure 118
Change of Authorization 120
Restrictions for Change of Authorization 120
How to Configure Change of Authorization 121
Essential dot1x | SANet Configuration 121
Configure Change of Authorization 121
Configuration Examples for Change of Authorization 122

Example: Check if the RADIUS Server is Active 122
Example: Device Tracking Policy 122

CHAPTER 8 Console Port, Telnet, SSH Handling, and Reset Button 125
Restrictions and Notes for Console Port, Telnet, and SSH 125
Console Port Overview 125
Console Port Handling Overview 125
Telnet and SSH Overview 126
Reset Button Overview 126
Information About Reset Button Functionality 126
Prerequisites for Enabling the Reset Button Functionality 127
Restrictions for Reset Button in Controller Mode 128
How to Enable the Reset Button Functionality 128
Example: Enable and Disable the Reset Button Functionality 129
Configuring a Console Port Transport Map 129
Viewing Console Port, SSH, and Telnet Handling Configurations 131
Configuring Console Port for Modem Connection 133

CHAPTER 9 Setting Up Factory Default Device Using WebUI 135
Using Basic or Advanced Mode Setup Wizard 136
Configure LAN Settings 136
Configure Primary WAN Settings 137
Configure Secondary WAN Settings 138
Configure Security Settings 138
Using Web User Interface for Day One Setup 139
Monitor and Troubleshoot Device Plug and Play (PnP) Onboarding using WebUI 140

CHAPTER 10 Process Health Monitoring 143
Monitoring Control Plane Resources 143
Avoiding Problems Through Regular Monitoring 143
Cisco IOS Process Resources 143
Overall Control Plane Resources 145
Monitoring Hardware Using Alarms 147
Router Design and Monitoring Hardware 147

BootFlash Disk Monitoring 147
Approaches for Monitoring Hardware Alarms 147
Viewing the Console or Syslog for Alarm Messages 147
Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP 149

CHAPTER 11 **Packet Trace** 151
Information About Packet Trace 151
Usage Guidelines for Configuring Packet Trace 152
Configuring Packet Trace 152
Displaying Packet-Trace Information 154
Removing Packet-Trace Data 154
Configuration Examples for Packet Trace 155
Example: Configuring Packet Trace 155
Example: Using Packet Trace 157
Additional References 162
Feature Information for Packet Trace 163

CHAPTER 12 **G.Fast and VDSL2 35b Profile** 165
Feature Information for G.fast and VDSL2 35b Profile 165
Restrictions for G.Fast and VDSL2 35b 166
Information About G.Fast and VDSL2 35b 166
Overview of G.fast and VDSL2 35b 166
Benefits of Implementing G.fast 167
Key DSL features on G.fast and VDSL2 35b 167
Configure G.Fast and VDSL2 35b 168
Configuring G.fast on the Cisco 1000 ISR 168
Example: G.Fast and VDSL2 35b 168
Example: The following is sample output for VDSL2 35b 168
Example: The following is sample output for G.fast 169
Additional References for G.fast or VDSL2 35b 171

CHAPTER 13 **Encrypted Traffic Analytics** 173
Feature Information for Encrypted Traffic Analytics 173

Restrictions for Encrypted Traffic Analytics 174
Information About Encrypted Traffic Analytics 174
Data Elements for Encrypted Traffic 174
How to Configure Encrypted Traffic Analytics 175
Enabling ET-Analytics on an Interface 175
Applying an ACL in the Allowed list 175
Verifying the ET-Analytics Configuration 176

CHAPTER 14 **Configuring Traffic Storm Control** 179
Information About Traffic Storm Control 179
Prerequisites for Traffic Storm Control 179
Limitations of Traffic Storm Control 179
Configuring Traffic Storm Control 180
Example: Configuring a Traffic Storm Control 181
Feature Information for Traffic Storm Control 181

CHAPTER 15 **Smart Licensing** 183
Smart Licensing Client 183
Prerequisites for Cisco Smart Licensing Client 183
Restrictions for Cisco Smart Licensing Client 183
Information About Cisco Smart Licensing Client 183
Cisco Smart Licensing - An Overview 183
HSECK9 184
Transitioning from CSL to Smart Licensing 184
Cisco One Suites 184
How to Activate Cisco Smart Licensing Client 185
Enable Smart Licensing 185
Device Registration 186
Install and Upgrade Licenses Using Software Activation Commands 186
Troubleshooting for Cisco Smart Licensing Client 188
Configuration Examples for Cisco Smart Licensing Client 189
Example: Displays summary information about all licenses 189
Example: Enabling Smart Licensing 189

CHAPTER 16 **Configuring Bridge Domain Interfaces** 191

Restrictions for Bridge Domain Interfaces 191

Information About Bridge Domain Interface 192

Ethernet Virtual Circuit Overview 192

Bridge Domain Interface Encapsulation 193

Assigning a MAC Address 193

Support for IP Protocols 193

Support for IP Forwarding 194

Packet Forwarding 194

Layer 2 to Layer 3 194

Layer 3 to Layer 2 194

Link States of a Bridge Domain and a Bridge Domain Interface 195

BDI Initial State 195

BDI Link State 195

Bridge Domain Interface Statistics 195

Creating or Deleting a Bridge Domain Interface 196

Bridge Domain Interface Scalability 196

Bridge-Domain Virtual IP Interface 196

How to Configure a Bridge Domain Interface 197

Example 198

Displaying and Verifying Bridge Domain Interface Configuration 199

Configuring Bridge-Domain Virtual IP Interface 200

Associating VIF Interface with a Bridge Domain 200

Verifying Bridge-Domain Virtual IP Interface 200

Example Configuration Bridge-Domain Virtual IP Interface 201

Configuring Flexible NetFlow over a Bridge Domain Virtual IP Interface 201

Examples: Flexible NetFlow over a Bridge Domain Virtual IP Interface 202

Additional References 206

Feature Information for Configuring Bridge Domain Interfaces 207

CHAPTER 17 **Configuring VDSL2 and ADSL2/22 Plus for Cisco C1100 Series ISRs** 209

DSL Feature Specifications 210

Configuring DSL 211

Configuring ADSL 211
Configuring Auto Mode 212
Configuring ADSL1 and ADSL2/2+ plus Annex A and Annex M Mode 212
Configuring VDSL2 213
Examples of DSL Interface Configuration 214
Features Supported in xDSL 215
ATM Conditional Debug Support 215
ATM OAM Loopback Mode Detection 215
ATM Oversubscription for DSL 215
ATM Routed Bridge Encapsulation (RBE)Concept 217
Default Route on a PPP Virtual Access Interface 217
Dynamic Bandwidth Change for ATM PVCs 217
Enabling ATM Dynamic Bandwidth 218
Disabling ATM Dynamic Bandwidth 219
How the ATM Dynamic Bandwidth Feature Works 219
Upgrading the Firmware on DSL Interface 221
IP to ATM CoS, Per-VC WFQ and CBWFQ QoS: PPPoE QoS Markings of .1P Bits in S (AOL) 227
Low Latency Queueing 227
Modular QoS CLI (MQC) Unconditional Packet Discard 227
MQC Policy Map Support on Configured VC Range ATM 227
Multilink PPP (MLPPP) bundling 227
PPPoE Enhancement with RFC 4638 228
PPPoEoA over ATM AAL5Mux 228
PPP Over ATM (IETF-Compliant) 228
PPPoE Specification Conformance with PADT Message 228
QoS on Dialer 228
QoS: PPPoE QoS Markings of .1P Bits 229
RBE Client Side Encapsulation with QoS 229
VC Bundling 229
Show and Debug Commands 229
Module Specific Show Commands 234
Packet Flow Specific to ATM PVC Related Show and Debug Commands 242
Collecting DSL Training Logs 244
Sample Configurations 247

Sample MLPPP Configurations and Show Commands 247
Sample PPPoA Configuration 250
Sample PPPoEoA Configuration 251

CHAPTER 18 **Cisco LTE/5G on Cisco 1000 Series Integrated Services Router** 253
Finding Feature Information 253
Overview of Cisco LTE/5G 254
Prerequisites for Configuring Cisco LTE/5G 256
Restrictions for Configuring Cisco LTE/5G 256
Features not Supported in Cisco LTE/5G 256
Cisco LTE/5G Features 257
4G GPS and NMEA 257
Example: Connecting to a Server Hosting a GPS Application 258
Dual SIM Card 258
Auto SIM 259
Enable Auto SIM 259
Example: List the firmware when Auto-SIM is Enabled 259
Disable Auto SIM 260
Example: List the firmware when Auto-SIM is Disabled 260
Using a SIM Card 260
Changing the PIN 261
Locking and Unlocking a SIM Card Using a PIN 261
Configure CHV1 for Unencrypted Level 0 262
Configure CHV1 for Unencrypted Level7 262
Configure CHV1 for Unencrypted Level7 264
Short Message Service (SMS) Capabilities 265
Data Account Provisioning 266
IP Multimedia Subsystem Profiles 266
LTE/5G LEDs 266
Configuring Cisco LTE/5G 267
Verifying Modem Signal Strength and Service Availability 267
Guidelines for Creating, Modifying, or Deleting Modem Data Profiles 268
Creating, Modifying, or Deleting Data Profiles Using EXEC Mode 269
Creating, Modifying, or Deleting Data Profiles in Configuration Mode 271

Configuration Examples 272
Configuration Example 273
Configure Radio Band Selection 274
Multiple PDN Contexts 275
Configuring a SIM for Data Calls 278
Locking and Unlocking a SIM Card Using a PIN Code 278
Changing the PIN Code 278
Verifying the Security Information of a Modem 278
Configuring Automatic Authentication for a Locked SIM 279
Configuring an Encrypted PIN for a SIM 280
Applying a Modem Profile in a SIM Configuration 281
Data Call Setup 282
Configuring the Cellular Interface 282
Configuring DDR 283
Enabling 4G GPS and NMEA Data Streaming 285
Configuring 4G SMS Messaging 287
Configuring Modem DM Log Collection 289
Example 291
Enabling Modem Crashdump Collection 292
Displaying Modem Log Error and Dump Information 293
Verifying the LTE/5G Router Information 294
Configuring Cellular Modem Link Recovery 296
Cellular Modem Link Recovery Parameters 297
Verifying the Cellular Modem Link Recovery Configuration 298
Configuration Examples for 3G and 4G Serviceability Enhancement 300
Example: Sample Output for the show cellular logs dm-log Command 300
Example: Sample Output for the show cellular logs modem-crashdump Command 300
Configuration Examples for LTE/5G 301
Example: Basic Cellular Interface Configuration: Cisco LTE/5G 301
Configuration Examples for Cisco LTE/5G 301
Cellular Back-off: Example 303
Example: GRE Tunnel over Cellular Interface Configuration 305
Example: LTE/5G as Backup with NAT and IPSec 305
Example: SIM Configuration 307

Locking the SIM Card 307
Unlocking the SIM Card 307
Automatic SIM Authentication 308
Changing the PIN Code 309
Configuring an Encrypted PIN 310
Upgrading the Modem Firmware 310
Upgrading the Modem Firmware Manually With CLI 311
EM74xx Manual Modem Firmware Upgrade: Example 311
Configuring dm-log to Utility Flash: Example 313
SNMP MIBs 313
SNMP LTE/5G Configuration: Example 314
Troubleshooting 315
Verifying Data Call Setup 315
Checking Signal Strength 316
Verifying Service Availability 316
Successful Call Setup 321
Modem Troubleshooting Using Integrated Modem DM Logging 321
Modem Settings for North America and Carriers Operating on 700 MHz Band 321
Changing Modem Settings 321
Electronic Serial Number (ESN) 321
Additional References 322

CHAPTER 19 **Configuring Ethernet Switch Ports** 325
Configuring VLANs 325
Configuring VTP 326
Configuring 802.1x Authentication 327
Configuring Spanning Tree Protocol 328
Configuring MAC Address Table Manipulation 330
Configuring Switch Port Analyzer 330
Configuring IGMP Snooping 331
Configuring LACP 332
EtherChannel Overview 332
Channel Groups and Port-Channel Interfaces 332
Link Aggregation Control Protocol 332

Auto-LAG 332
Configuring Layer 2 EtherChannels 333
334
Configuring EtherChannel Load-Balancing 335
Configuring the LACP Port Channel Min-Links Feature 336
Configuring LACP Fast Rate Timer 337
Configuring Auto-LAG Globally 338
Configuring HSRP 339
Configuring VRRP 340

CHAPTER 20 **Slot and Subslot Configuration** 343
Configuring the Interfaces 343
Configuring the Interfaces: Example 343
Viewing a List of All Interfaces: Example 343
Viewing Information About an Interface: Example 344

CHAPTER 21 **Online Insertion and Removal** 347
Soft OIR Procedures 347
Manage OIR for Pluggable LTE Modules 347

CHAPTER 22 **Cisco Multimode G.SHDSL EFM-ATM in Cisco ISR 1000 Series Routers** 349
Connecting Cisco G.SHDSL EFM or ATM to the Network 349
Cisco G.SHDSL EFM or ATM 349
Configuring Cisco G.SHDSL EFM or ATM in CPE/CO Mode 350
Configuring NIM-4SHDSL-EA as CPE 350
Configuring Bonding on CPE 350
Verify the Configuration 351
Additional References 351
Technical Assistance 351

CHAPTER 23 **Configuring SFP Auto-Failover** 353
Enabling Auto-Detect 353
Configuring Auto-Detect 353
Configuring the Primary and Secondary Media 354

CHAPTER 24 **Configuring Cellular IPv6 Address** 357

Cellular IPv6 Address 357

IPv6 Unicast Routing 357

Link-Lock Address 357

Global Address 358

Configuring Cellular IPv6 Address 358

CHAPTER 25 **Dying Gasp Through SNMP, Syslog, and Ethernet OAM** 361

Prerequisites for Dying Gasp Support 361

Restrictions for Dying Gasp Support 361

Information About Dying Gasp Through SNMP, Syslog and Ethernet OAM 362

Dying Gasp 362

How to Configure Dying Gasp Through SNMP, Syslog and Ethernet OAM 362

Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations 362

Environmental Settings on the Network Management Server 362

Message Displayed on the Peer Router on Receiving Dying Gasp Notification 363

Displaying SNMP Configuration for Receiving Dying Gasp Notification 363

Configuration Examples for Dying Gasp Through SNMP, Syslog and Ethernet OAM 363

Example: Configuring SNMP Community Strings on a Router 363

Example: Configuring SNMP-Server Host Details on the Router Console 364

Feature Information for Dying Gasp Support 364

CHAPTER 26 **Cisco Umbrella Integration** 365

Feature Information for Cisco Umbrella Integration 365

Prerequisites for Cisco Umbrella Integration 366

Restrictions for Cisco Umbrella Integration 366

Cloud-based Security Service Using Cisco Umbrella Integration 367

Encrypting the DNS Packet 367

Benefits of Cisco Umbrella Integration 368

How to Configure Cisco Umbrella Connector 368

Configure the Cisco Umbrella Connector 368

Register the Cisco Umbrella Tag 369

Configure Cisco 1000 Series ISR as a Pass-through Server 370

Verify the Cisco Umbrella Connector Configuration 370
Show Commands 371
Show Commands at FP Layer 371
Show Commands at Cisco Packet Processor Layer 371
Data Path Show Commands 371
Clear Command 371
Troubleshoot the Cisco Umbrella Integration 371
Configuration Examples 372
Deploy the Cisco Umbrella Integration using Cisco Prime CLI Templates 372
Additional References for Cisco Umbrella Integration 373

CHAPTER 27 **Wireless Device Overview** 375
Wireless Connectivity for Cisco 1100 Series ISR 375
Module Managment 376
Slot and Subslots for WLAN 376
Supported WiFi Cards 377
Implementing Modules on Your Router 378
Accessing Your Module Through a Console Connection 378
Deactivating a Module 378
Deactivating Modules and Interfaces in Different Command Modes 379
Reactivating a Module 380
Access Points 381
Configuring and Deploying the Access Point 381
The Controller Discovery Process 382
Deploying the Access Point on the Wireless Network 383
Checking the Wireless LAN LED 383
Miscellaneous Usage and Configuration Guidelines 385
Important Information for Controller-Based Deployments 385
Deploying Cisco Mobility Express 386
Pre-Requisites for Deploying Mobility Express Solution 386
Connecting Mobility Express Capable Access Point to the Network 386
Determining image on the Access Point 388
Converting Access Point from CAPWAP to Cisco Mobility Express 390
Converting Access Point from Cisco Mobility Express to CAPWAP 393

Configuring Cisco Mobility Express controller 394
CLI Setup Wizard 394
Over-the-Air Setup Wizard 395
Network Plug and Play 397
Introduction 397
Pre-Requisites 397
APIC-EM Discovery Options 398
Configuring APIC-EM / Network PnP Server 398
APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express 400
APIC-EM controller in Private Cloud 400
Cloud Plug and Play Connect Redirect to APIC-EM Controller 400
Cloud Plug and Play Device Redirect Provisioning Workflow 400
Connecting Cisco Mobility Access Points 405
Using internal DHCP server on Cisco Mobility Express 405
Creating a DHCP Scope 405
Configuring Cisco Mobility Express for Site Survey 407
Introduction 407
Configuring Mobility Express for Site Survey Using CLI 408
Creating Wireless Networks 411
Creating Employee WLANs 412
Creating Employee WLAN with WPA2 Personal 412
Creating Employee WLAN using WPA2 Enterprise with External Radius Server 412
Creating Employee WLAN with WPA2 Enterprise and Authentication Server as AP 412
Creating Employee WLAN with WPA2 Enterprise/External RADIUS and MAC Filtering 413
Creating Guest WLANs 414
Creating Guest WLAN with Captive Portal on CMX Connect 414
Creating Guest WLAN with Internal Splash Page 414
Creating Guest WLAN with External Splash Page 416
Internal Splash Page for Web Authentication 417
Using Default Internal Guest Portal 417
Using Customized Internal Guest Portal 418
Managing WLAN Users 418
Adding MAC for Local MAC Filtering on WLANs 419
Managing Services with Cisco Mobility Express 420

Application Visibility and Control 420
Enabling Application Visibility on WLAN 420
Enabling Application Control on WLAN 420
iOS Optimized WiFi Connectivity and Fast Lane 421
Configuring Optimized WiFi Connectivity 421
Configuring Fast Lane 422
Cisco Mobility Express with CMX Cloud 423
Cisco CMX Cloud 423
Cisco CMX Cloud Solution Compatibility Matrix 423
Minimum Requirements for Cisco CMX Cloud Deployment 423
Enabling CMX Cloud Service on Mobility Express for Presence Analytics 423
Configuring Site on CMX Cloud for Presence Analytics 424
Managing the Cisco Mobility Express Deployment 425
Managing Access Points 425
Primary AP Failover and Electing a New Primary 427
Primary AP Failover 427
Electing a new Primary Access Point 427

CHAPTER 28 **Configuring Wi-Fi 6** 429
Wireless Device Overview 429
Wireless Connectivity for Cisco 1100 Series ISR 429
Module Managment 430
Slot and Subslots for WLAN 430
Supported WiFi Cards 430
Implementing Modules on Your Router 431
Accessing Your Module Through a Console Connection 431
Deactivating a Module 432
Deactivating Modules and Interfaces in Different Command Modes 432
Reactivating a Module 433
Deploying Cisco Embedded Wireless Controller (EWC) 433
Prerequisites for Deploying Embedded Wireless Controller (EWC) Solution 433
Prerequisites for Configuring the AP on the Router 434
Configuring the AP Using Day 0 Provisioning 436
Connecting Cisco Embedded Wireless Controller (EWC) Capable Access Point to the Network 437

Converting Access Point from CAPWAP to Cisco Embedded Wireless Controller (EWC) 438
Converting Access Point from Cisco Embedded Wireless Controller (EWC) to CAPWAP 441
Determining image on the Access Point 441
Configuring Cisco Embedded Wireless Controller (EWC) 443
Configuring the controller using day 0 wizard 443
Using internal DHCP server on Cisco Mobility Express 444
Creating a DHCP Scope 444
Access Points 446
Configuring and Deploying the Access Point 446
The Controller Discovery Process 447
Deploying the Access Point on the Wireless Network 448
Checking the Wireless LAN LED 448
Miscellaneous Usage and Configuration Guidelines 449
Important Information for Controller-Based Deployments 449

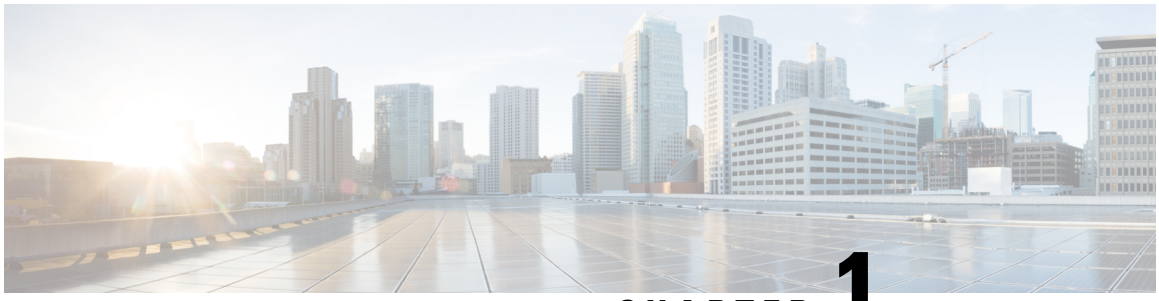
CHAPTER 29 **Small Form-Factor Pluggables for Cisco ISR1000** 451
Configuring Third-Party SFPs 451

CHAPTER 30 **Security Group Tagging** 453
Limitations for Security Group Tag 454
Configuring Security Group Tagging for Dynamic SGT and SGACL 455
Configuring SGT Tagging 459
Example 1: Static Security Group Tagging and Security Group ACL 461
Example 2: Dynamic Security Group Tagging and Security Group ACL 461
Troubleshoot the Security Group Tagging Configuration 462
Feature History for Cisco TrustSec 462

CHAPTER 31 **System Messages** 465
Information About Process Management 465
How to Find Error Message Details 465

CHAPTER 32 **Troubleshooting** 471
Before Contacting Cisco or Your Reseller 471
ADSL Troubleshooting 472

SHDSL Troubleshooting 472
VDSL2 Troubleshooting 472
show interfaces Troubleshooting Command 473
ATM Troubleshooting Commands 475
ping atm interface Command 475
show atm interface Command 476
debug atm Commands 476
Guidelines for Using Debug Commands 476
debug atm errors Command 477
debug atm events Command 477
debug atm packet Command 478
System Report 479
Software Upgrade Methods 480
Recovering a Lost Password 481
Change the Configuration Register 481
Reset the Router 482
Reset the Router 484
Reset the Password and Save Your Changes 485
Reset the Configuration Register Value 486
References 486



CHAPTER 1

# Overview

This chapter contains the following sections:


- Introduction to Cisco 1000 Series Integrated Services Routers, on page 1


# Introduction to Cisco 1000 Series Integrated Services Routers

The Cisco 1100 Series Integrated Services Routers (ISRs) are fixed branch routers based on the Cisco IOS XE Everest 16.6.2 operating system, multi-core Data Plane.

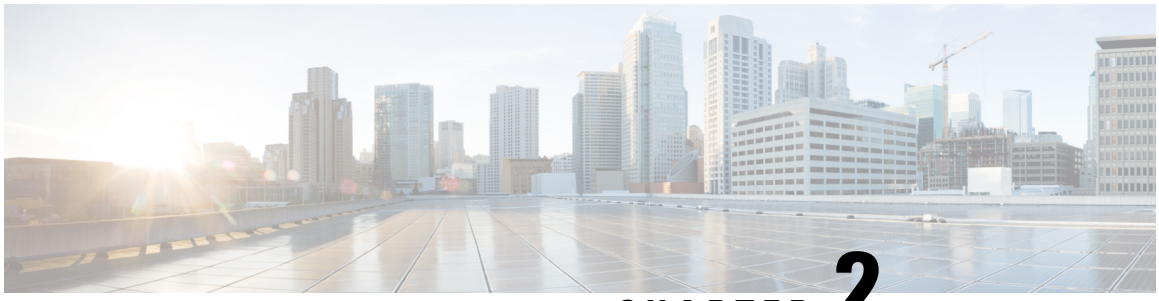
The two types of platforms supported on Cisco 1100 Series ISRs are 8-port and 4-port platforms.

The 8-port platforms are high-performance managed service provider and enterprise platforms having:

- 8-port integrated front panel switch ports
- Optional POE on LAN daughter card with support up to 4PoE/2PoE+ ports
- Optional WLAN support - 802.11ac WAVE 2
- 4G LTE-Advanced support with carrier aggregation

The 4-port platforms are midrange performance managed service provider platforms and enterprise platforms with the following specifications:

- 4-port integrated front panel switch ports
- VDSL2 and ADSL2/2+ support
- (Optional) PoE on LAN daughter card supporting 2PoE/1PoE+ ports
- (Optional) WLAN support - 802.11ac WAVE 2
- 4G LTE-Advanced support with carrier aggregation



CHAPTER 2

# Using Cisco IOS XE Software

This chapter contains the following sections:


- Accessing the CLI Using a Router Console, on page 3
- Initial Bootup Security , on page 18


# Accessing the CLI Using a Router Console

Cisco 1100 series routers have console port with modem support.

The following sections describe the main methods of accessing the router:


- Accessing the CLI Using a Directly-Connected Console, on page 3
- Using SSH to Access Console, on page 4
- Accessing the CLI from a Remote Console Using Telnet, on page 5
- Accessing the CLI from a Remote Console Using a Modem, on page 6


## Accessing the CLI Using a Directly-Connected Console

The CON port is an EIA/TIA-232 asynchronous, serial connection with no-flow control and an RJ-45 connector. The CON port is located on the front panel of the chassis.

The following sections describe the procedure to access the control interface:

### Connecting to the Console Port

**Procedure**

**Step 1** Configure your terminal emulation software with the following settings:

- 9600 bits per second (bps)
- 8 data bits
- No parity

- No flow control

**Step 2** Connect to the CON port using the RJ-45-to-RJ-45 cable and the RJ-45-to-DB-25 DTE adapter or the RJ-45-to-DB-9 DTE adapter (labeled Terminal).

## Use 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** If you enter the **setup** command, see "Using Cisco Setup Command Facility" in the "Initial Configuration" section of the Hardware Installation Guide for the Cisco 1100 Series Integrated Services Router.

**Step 4** To exit the console session, enter the **exit** command:

```
Router# exit
```

# Using SSH to Access Console

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. To enable SSH support on the device:

### Procedure

**Step 1** Configure the hostname:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#hostname xxx_lab
```

Here, *host name* is the router hostname or IP address.

**Step 2** Configure the DNS domain of the router:

```
xxx_lab(config)# xxx.cisco.com
```

**Step 3** Generate an SSH key to be used with SSH:

```
xxx_lab(config)#  crypto key generate rsa
The name for the keys will be: xxx_lab.xxx.cisco.com Choose the size of the key modulus in
 the range
of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may
take a few
minutes.
How many bits in the modulus [512]: 1024 % Generating 1024 bit RSA keys, keys will be
non-exportable...
[OK] (elapsed time was 0 seconds)
xxx_lab(config)#
```

**Step 4** By default, the vtys? transport is Telnet. In this case, Telnet is disabled and only SSH is supported:

```
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)#transport input SSH
```

**Step 5** Create a username for SSH authentication and enable login authentication:

```
xxx_lab(config)# username jsmith privilege 15 secret 0 p@ss3456
xxx_lab(config)#line vty 0 4
xxx_lab(config-line)# login local
```

**Step 6** Verify remote connection to the device using SSH.

# Accessing the CLI from a Remote Console Using Telnet

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

## Preparing to Connect to the Router Console Using Telnet

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

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

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

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

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

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

## Using Telnet to Access a Console Interface

### 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.

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

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

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

**Step 2** Enter your login password:

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

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

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

```
Router> enable
```

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

```
Password: enablepass
```

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

```
Router#
```

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

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

```
Router# logout
```

# Accessing the CLI from a Remote Console Using a Modem

To access the router remotely using a modem through an asynchronous connection, connect the modem to the port. For more information, see the "Configuring Console Port for Modem Connection" section.

# Accessing the CLI from a Micro USB Serial Console Port

The router provides an additional mechanism for configuring the system: a micro USB serial console that supports remote administration of the router using a micro USB-compliant cable. See the "Connecting to a Console Terminal or Modem" section in the Hardware Installation Guide for the Cisco 1100 Series Integrated Services Router.

# 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 1: Keyboard Shortcuts***

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

# Using the 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 2: History Substitution Commands***

| Command | Purpose |
|---|---|
| **Ctrl-P** or the **Up Arrow** key[1] | Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands. |
| **Ctrl-N** or the **Down Arrow** key[1] | Returns to more recent commands in the history buffer after recalling commands with **Ctrl-P** or the **Up Arrow** key. |
| Router# show history | While in EXEC mode, lists the last few commands you entered. |

| Command | Purpose |
|---|---|

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

## 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 3: Accessing and Exiting Command Modes***

| Command Mode | Access Method | Prompt | Exit Method |
|---|---|---|---|
| User EXEC | Log in. | `Router>` | Use the **logout** command. |
| Privileged EXEC | From user EXEC mode, use the **enable** command. | `Router#` | To return to user EXEC mode, use the **disable** command. |
| Global configuration | From privileged EXEC mode, use the **configure terminal** command. | `Router(config)#` | To return to privileged EXEC mode from global configuration mode, use the **exit** or **end** command. |
| Interface configuration | From global configuration mode, specify an interface using an **interface** command. | `Router(config-if)#` | To return to global configuration mode, use the **exit** command.<br>To return to privileged EXEC mode, use the **end** command. |

| Command Mode | Access Method | Prompt | Exit Method |
|---|---|---|---|
| Diagnostic | The router boots up or accesses diagnostic mode in the following scenarios:<br>• In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload.<br>• A user-configured access policy is configured using the **transport-map** command that directs a user into diagnostic mode.<br>• A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) is entered and the router is configured to go to diagnostic mode when the break signal is received. | `Router(diag)#` | If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode.<br>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI. |
| ROM monitor | From privileged EXEC mode, use the **reload** EXEC command. Press the **Break** key during the first 60 seconds while the system is booting. | `rommon#>` | To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded. |

## 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.

## Getting Help

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

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

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

### Finding Command Options: Example

This section provides information about how to display the syntax for a command. The syntax can consist of optional or required keywords and arguments. To display keywords and arguments for a command, enter a question mark (**?**) at the configuration prompt or after entering a part of a command followed by a space. The

Cisco IOS XE software displays a list and brief descriptions of the available keywords and arguments. For example, if you are in global configuration mode and want to see all the keywords and arguments for the **arap** command, you should type **arap ?**.

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

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

***Table 4: Finding Command Options***

| Command | Comment |
|---|---|
| `Router> enable`<br>`Password: <password>`<br>`Router#` | Enter the **enable** command and password to access privileged EXEC commands. You are in privileged EXEC mode when the prompt changes to a " # " from the " > ", for example, `Router>` to `Router#` |
| `Router# configure terminal`<br>`Enter configuration commands, one per line. End with CNTL/Z.`<br>`Router(config)#` | Enter the **configure terminal** privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to `Router (config)#` |
| `Router(config)# interface GigabitEthernet ?`<br>`<0-0> GigabitEthernet interface number`<br><br>`Router(config)# interface GigabitEthernet 0/?`<br>`<0-5> Port Adapter number`<br><br>`Router (config)# interface GigabitEthernet 0/0/?`<br>`<0-63> GigabitEthernet interface number`<br><br>`Router (config)# interface GigabitEthernet 0/0/0?`<br>`.  <0-71>`<br><br>`Router(config-if)#` | Enter interface configuration mode by specifying the interface that you want to configure, using the **interface GigabitEthernet** global configuration command.<br><br>Enter **?** to display what you must enter next on the command line.<br><br>When the <cr> symbol is displayed, you can press **Enter** 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  Interface Internet Protocol`<br>`  config commands`<br>`  keepalive  Enable keepalive`<br>`  lan-name  LAN Name command`<br>`  llc2  LLC2 Interface Subcommands`<br>`  load-interval  Specify interval for load calculation`<br>`  for an interface`<br>`  locaddr-priority  Assign a priority group`<br>`  logging  Configure logging for interface`<br>`  loopback  Configure internal loopback on an`<br>`  interface`<br>`  mac-address  Manually set interface MAC address`<br>`  mls  mls router sub/interface commands`<br>`  mpoa  MPOA interface configuration commands`<br>`  mtu  Set the interface Maximum Transmission Unit (MTU)`<br>`  netbios  Use a defined NETBIOS access list`<br>`  or enable name-caching`<br>`  no  Negate a command or set its defaults`<br>`  nrzi-encoding  Enable use of NRZI encoding`<br>`  ntp  Configure NTP`<br>`  .`<br>`  .`<br>`  .`<br>`Router(config-if)#` | Enter **?** to display a list of all the interface configuration commands available for the interface. This example shows only some of the available interface configuration commands. |

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

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

# 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 factory reset Commands

The **factory reset** commands are used to remove all the customer specific data on a router/switch that has been added. The data can be configuration, log files, boot variables, core files, and so on.

The **factory-reset all** command erases the bootflash, nvram, rommon variables, licenses, and logs.

```
Router#factory-reset all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
*Enter*

*May 12 09:55:45.831: %SYS-5-RELOAD: Reload requested by Exec. Reload Reason: Factory Reset.

***Return to ROMMON Prompt
```

# Saving Configuration Changes

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

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

It may take a few minutes to save the configuration. After the configuration has been saved, the following output is displayed:

```
[OK]
Router#
```

This task saves the configuration to the NVRAM.

# 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.

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.

# Filtering Output from the show and more Commands

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

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

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

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

### Example

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

```
Router# show interface | include protocol
GigabitEthernet0/0/0 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/1 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/2 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0/0/3 is administratively down, line protocol is down
     0 unknown protocol drops
GigabitEthernet0 is up, line protocol is up
     0 unknown protocol drops
Loopback0 is up, line protocol is up
     0 unknown protocol drops
```

# Powering Off a Router

### Before you begin

The router can be safely turned off at any time by moving the router's power supply switch to the Off position. However, any changes to the running config since the last WRITE of the config to the NVRAM is lost.

Ensure that any configuration needed after startup is saved before powering off the router. The **copy running-config startup-config** command saves the configuration in NVRAM and after the router is powered up, the router initializes with the saved configuration.

# 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. 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 Release Notes for Cisco IOS XE.

## 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.

## 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 document for the Cisco 4000 Series for information about the following:

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

Release notes are intended to be release-specific for the most current release, and the information provided in these documents may not be cumulative in providing information about features that first appeared in previous releases. For cumulative feature information, refer to the Cisco Feature Navigator at: http://www.cisco.com/go/cfn/.

# CLI Session Management

An inactivity timeout is configurable and can be enforced. Session locking provides protection from two users overwriting changes that the other has made. To prevent an internal process from using all the available

capacity, some spare capacity is reserved for CLI session access. For example, this allows a user to remotely access a router.

## Information About CLI Session Management

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

## Changing the CLI Session Timeout

### Procedure

**Step 1** `configure terminal`

Enters global configuration mode

**Step 2** `line console 0`

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

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

**Step 4** `show line console 0`

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

## Locking a CLI Session

### Before you begin

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

### Procedure

**Step 1** `Router# configure terminal`

Enters global configuration mode.

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

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

**Step 3** `Router(config)# lockable`

Enables the line to be locked.

**Step 4** `Router(config)# exit`

**Step 5** `Router# lock`

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

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

# Initial Bootup Security

This section contains the following:

### Enforce Changing Default Password

The Enforce Changing Default Password feature allows you to change the default password and set a new password for a better encryption algorithm. The enable secret is a command that allows you to set a new password which helps to protect the access to different modes such as a privileged EXEC and configuration mode.

With the earlier software versions, you can bypass the option to set a new enabled password. When the device first boots up after the factory reset or fresh from the factory, the following prompt is displayed on the console:

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

The earlier versions of the software allow you to answer **no** and the device changes to the **Router>** prompt with a blank enable password. At this point, you can configure the device and bring it into service with a blank enable password.

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

Starting with Cisco IOS XE Release 17.5.1, the initial dialog is changed to force setting a new enable password and also using the **enable secret** command instead. The following is an example:

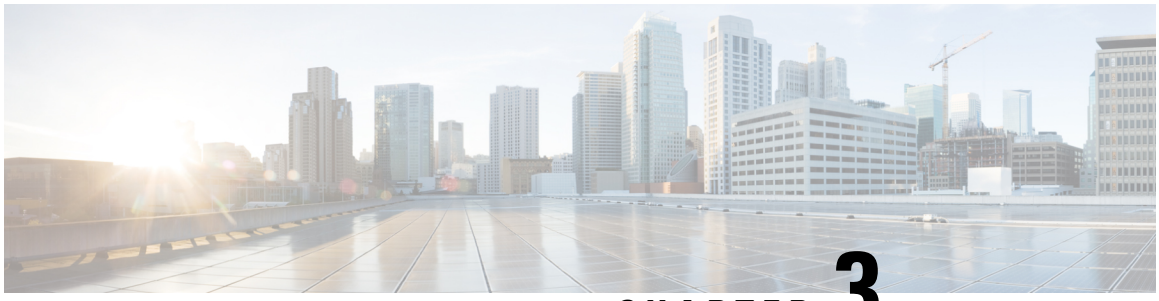
```
Would you like to enter basic management setup? [yes/no]:yes
Configuring global parameters

Enter host name [Router]:router-1

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 enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
Enter enable password: ********

The virtual terminal password is used to protect
  access to the router over a network interface.
Enter virtual terminal password:********
Configure SNMP Network Management?no
```

```
Enter interface name used to connect to the
management network from the above interface summary:Ethernet0/0

Configuring interface Ethernet0/0
Configure IP on this interface? [yes]:no

The following configuration command script was created:
hostname router-1
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
.
.
[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
.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
enable password password-1
```

The following is an example of what happens if you answer **no** to the initial configuration dialog:

```
Would you like to enter the initial configuration dialog? [yes/no]:no
The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret:********
  Confirm enable secret:********
Would you like to terminate autoinstall? [yes]:yes

.
.
router-1>en
Password:
router-1#sh run | sec enable
enable secret 9 $9$emUzIshVXwlUaE$nTzhgi9STdZKzQc4VJ0kEaCqafjUNdCD7ZUf37SY9qg
```

After the enable secret is prompted during the first login, you can enter a password and this password is always masked. If you enter a weak password, the device will prompt again to enter a strong password. For example, you must use the standard mix of upper-case and lower-case characters, special characters, numbers, and so on. The device will continue to prompt until you enter a strong password. You should enter the strong secret password twice for confirming and configuring the device."



CHAPTER 3

# Installing the Software

This chapter contains the following sections:


- Installing the Software, on page 21
- Provisioning Files, on page 57
- File Systems, on page 58
- Autogenerated File Directories and Files, on page 58
- Flash Storage, on page 59
- Configuring the Configuration Register for Autoboot, on page 59
- Crypto Throughput Licensing, on page 60
- Unlicensed Feature: Example, on page 62
- LED Indicators, on page 62
- Related Documentation, on page 62
- How to Install and Upgrade the Software, on page 63
- Managing and Configuring a Router to Run Using Individual Packages, on page 70
- How to Install and Upgrade the Software for Cisco IOS XE Everest Release 16.6, on page 79


# 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.

These are the two main methods to install the software:

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

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

# Guestshell Installation

The guestshell is removed from the IOS XE software image from the Cisco IOS XE 17.9 release. If you need to use guestshell, then you can download it from https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads.

The Guest Shell is a virtualized Linux-based environment, designed to run custom Linux applications, including Python for automated control and management of Cisco devices. Using the Guest Shell, the user can also install, update, and operate third-party Linux applications and access the IOS CLI.

The Guest Shell environment is intended for tools, Linux utilities, and manageability rather than networking.

Guest Shell shares the kernel with the host (router) system. Users can access the Linux shell of Guest Shell and update scripts and software packages in the container rootfs. However, users within the Guest Shell cannot modify the host file system and processes.

The Guest Shell container is managed using IOx. IOx is Cisco's Application Hosting Infrastructure for Cisco IOS XE devices. IOx enables hosting of applications and services developed by Cisco, partners, and third-party developers in network edge devices, seamlessly across diverse and disparate hardware platforms.

With these users in mind, guestshell will be made available as a single tar file which can then be downloaded and installed on the system like any other IOX application. As a result, there won't be any increase in the size of the universal release image.

**Note** Day 0 guestshell provisioning will not work with this approach.

Sample guestshell configuration can be found on this page: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/178/b_178_programmability_cg/m_178_prog_guestshell.html

To install guestshell on the device, copy the tar file to the router and run the following command:

```
app-hosting install appid guestshell package <path to tar file>
```

Use the following command to check the status:

```
show app-hosting list
```

Once guestshell has been deployed successfully, standard guestshell commands such as **guestshell enable**, **guestshell run bash**, and **guestshell run python3** should work.

The following resource talks about running python scripts using guestshell:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/prog/configuration/178/b_178_programmability_cg/m_178_prog_eem_python.html

**Note** Only python3 is supported in 17.5.1.

### Important - Before You Install

Before attempting to install Guest shell on your device, please verify that the device has IOx container keys programmed on it by running the following command:

```
Router#show software authenticity keys | i Name
Product Name : ISR900_BL
Product Name : ISR900_BL
Product Name : ISR900
Product Name : ISR900
Product Name : ISR900_Containers
Product Name : ISR900_Containers
Product Name : CISCO
```

The output should contain one or more lines with the Product Name “ISR900_Containers”. If the device does not have container keys programmed on it, then you will not be able to install guest shell.

You will see an error like the following:

```
*Aug 26 15:47:21.484: %IOSXE-3-PLATFORM: R0/0: IOx: App signature verification failed with
 non-zero exit code
*Aug 26 15:47:21.588: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install failed: App
package signature (package.sign)
verification failed for package manifest file package.mf. Re-sign the application and then
 deploy again.
```

The guest shell tar file is published along with the IOS-XE image for a given release. More information can be found here:https://developer.cisco.com/docs/iox/#!iox-resource-downloads/downloads

# Licensing

## Cisco Software Licensing

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

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

An evaluation license is automatically converted to a Right to Use model after 60 days and this license is valid permanently. The conversion to a permanent license applies only to evaluation licenses. For other features supported on your router, you must purchase a permanent license.

See the "Configuring the Cisco IOS Software Activation Feature" chapter of the Software Activation Configuration Guide, Cisco IOS XE Release 3S.

## Consolidated Packages

One of the following two consolidated packages (images) is preinstalled on the router:

- **universalk9**—Contains the **ipbasek9** base package and the **securityk9**, **uck9**, and **appxk9** technology packages.
- **universalk9_npe**—Contains the **ipbasek9** base package and the **securityk9_npe**, **uck9**, and **appxk9** technology packages. This image has limited crypto functionality.

**Note** The term npe stands for No Payload Encryption.

**Note** The terms super package and image also refer to a consolidated package.

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

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.

Apart from the **universalk9** and **universalk9_npe** images, a Boot ROMMON image is available. For more information, see *ROMMON Images* section.

For more information about identifying digitally signed Cisco software and how to show the digital signature information of an image file, see the "Digitally Signed Cisco Software" section in the Loading and Managing System Images Configuration Guide, Cisco IOS XE Release 3S.

The following examples show how to obtain software authenticity information and internal details of a package:

- *Displaying Digitally Signed Cisco Software Signature Information* section
- *Obtaining the Description of a Module or Consolidated Package* section

Many features within the consolidated package are contained in the **ipbasek9** base package. The license key for the **ipbasek9** package is activated by default.

## Technology Packages

Technology packages contain software features within a consolidated package. To use different sets of features, enable the licenses of selected technology packages. You can enable the licenses for any combination of technology packages.

Each technology package has an evaluation license that converts to a Right to Use (RTU) license after 60 days and is then valid permanently.

The following is a list of technology packages:

**Note** In Cisco 1000 Series Integrated Series Routers, although L2TPv2 sessions comes up without appxk9, you need the appxk9 license for the traffic to go through the sessions. You also need the appxk9 license to apply the QoS policies to the L2TPv2 sessions.

### securityk9

The **securityk9** technology package includes all crypto features, including IPsec, SSL/SSH, Firewall, and Secure VPN.

The **securityk9_npe** package (npe = No Payload Encryption) includes all the features in the **securityk9** technology package without the payload-encryption functionality. This is to fulfill export restriction requirements. The **securityk9_npe** package is available only in the **universalk9_npe** image. The difference in features between the **securityk9** package and the **securityk9_npe** package is therefore the set of payload-encryption-enabling features such as IPsec and Secure VPN.

### uck9

The Unified Communications technology package is required to enable Cisco Unified Border Element (Cisco UBE) functionality. To use Cisco UBE features, you will require session licenses and a Security technology package to secure the media.

### appxk9

The **appxk9** technology package contains Application Experience features, which are similar to the features in the DATA package of the Cisco Integrated Services Routers Generation 2 routers. For more information, see: http://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/software-activation-on-integrated-services-routers-isr/white_paper_c11_556985.html#wp9000791.

There are many features in the **appxk9** package, including MPLS, PfR, L2/L3 VPN, Broadband, and AVC.

## Unlicensed Feature: Example

If you try to use a feature that is part of a package that is not enabled, an error message is displayed.

In the following example, the **crypto map** command is called during configuration and an error message is displayed. This is because, the feature associated with **crypto map** is part of the **securityk9** package and the **securityk9** package is not enabled.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto map
^
% Invalid input detected at '^' marker.
```

Use the **show license feature** command to view the license features that are enabled. In the following example, the **securityk9** and the **uck9** packages are not enabled.

**Note** **ipbasek9** is provided by default.

```
Router# show license feature
Feature name             Enforcement  Evaluation  Subscription   Enabled  RightToUse
appxk9                   yes          yes         no             yes      yes
uck9                     yes          yes         no             no       yes
securityk9               yes          yes         no             no       yes
ipbasek9                 no           no          no             yes      yes
```

## LED Indicators

For information on LEDs on the router, see "LED Indicators" in the "Overview" section of the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

For information on LEDs on the SSD Carrier Card NIM, see "Overview of the SSD Carrier Card NIM (NIM-SSD)" in the "Installing and Upgrading Internal Modules and FRUs" section of the Hardware Installation Guide for the Cisco 4000 Series Integrated Services Routers.

## Related Documentation

For further information on software licenses, see Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2.

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

## How to Install and Upgrade the Software

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

- Managing and Configuring a Router to Run Using a Consolidated Package, on page 26
- Managing and Configuring a Router to Run Using Individual Packages, on page 30

### Managing and Configuring a Router to Run Using a Consolidated Package

**Note** Do not use these procedures if you also need to install any optional subpackages or plan to upgrade individual subpackages. See Managing and Configuring a Router to Run Using Individual Packages, on page 30.

- Managing and Configuring a Consolidated Package Using copy and boot Commands, on page 26
- Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example, on page 27

#### *Managing and Configuring a Consolidated Package Using copy and boot Commands*

To upgrade a consolidated package, copy the consolidated package to the **bootflash:** directory on the router using the **copy** command. After making this copy of the consolidated package, configure the router to boot using the consolidated package file.

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

```
Router# dir bootflash:
Directory of bootflash:/
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer

928862208 bytes total (712273920 bytes free)

Router# copy tftp: bootflash:
Address or name of remote host []? 172.17.16.81
Source filename []? /auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
Destination filename [isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin]?
Accessing
tftp://172.17.16.81//auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
...
Loading /auto/tftp-users/user/isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin from
172.17.16.81 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00
isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
928862208 bytes total (503156736 bytes free)
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system flash bootflash:isr4400-universalk9.03.10.00.S.153-3.S-ext.SPA.bin
boot-end-marker
Router# copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
```

## Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot
boot-start-marker
boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with

reload chassis code


Initializing Hardware ...

System integrity status: c0000600
Failures detected:
Boot FPGA corrupt


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300
```

```
ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 424317088 (0x194a90a0) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
expected 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5116 msec
Image validated
%IOSXEBOOT-4-BOOT_ACTIVITY_LONG_TIME: (local/local): load_modules took: 2 seconds,
expected max time 2 seconds

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
```

```
cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
15.4(20140527:095327)
[v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Tue 27-May-14 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2014 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.



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.


Warning: the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.


Press RETURN to get started!


Router>
Router>
Router>enable
Router# show version
Cisco IOS XE Software, Version BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ext
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
15.4(20140527:095327)
v154_3_s_xe313_throttle-BLD-BLD_V154_3_S_XE313_THROTTLE_LATEST_20140527_070027-ios 156]

IOS XE Version: BLD_V154_3_S_XE313_THROTTLE_LATEST
```

```
Cisco IOS-XE software, Copyright (c) 2005-2014 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp://10.81.116.4/rtp-isr4400-54/isr4400.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.

License Level: adventerprise
License Type: EvalRightToUse
--More-- Next reload license Level: adventerprise

cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.

Configuration register is 0x2102
```

# Managing and Configuring a Router to Run Using Individual Packages

To choose between running individual packages or a consolidated package, see *Installing the Software - Overview* section.

The following topics are included in this section:

- Installing Subpackages from a Consolidated Package, on page 31
- Installing a Firmware Subpackage, on page 42
- Installing Subpackages from a Consolidated Package on a Flash Drive, on page 36

## Installing Subpackages from a Consolidated Package

Perform the following procedure to obtain the consolidated package from a TFTP server.

Another variation of this procedure obtains the consolidated package from a USB flash drive. This is described in Installing Subpackages from a Consolidated Package on a Flash Drive.

### Before you begin

Copy the consolidated package to the TFTP server.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show version**<br>**Example:**<br>`Router# show version`<br>`Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.3(20120627:221639) [build_151722 111]`<br>`Copyright (c) 1986-2012 by Cisco Systems, Inc.`<br>`Compiled Thu 28-Jun-12 15:17 by mcpre`<br>`.`<br>`.`<br>`.` | Shows the version of software running on the router. This can later be compared with the version of software to be installed. |
| **Step 2** | **dir bootflash:**<br>**Example:**<br>`Router# dir bootflash:` | Displays the previous version of software and that a package is present. |
| **Step 3** | **show platform**<br>**Example:**<br>`Router# show platform`<br>`Chassis type: ISR4451/K9` | Displays the inventory. |
| **Step 4** | **mkdir bootflash:** *URL-to-directory-name*<br>**Example:**<br>`Router# mkdir bootflash:mydir` | Creates a directory to save the expanded software image.<br>You can use the same name as the image to name the directory. |
| **Step 5** | **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*<br>**Example:**<br>`Router# request platform software package expand file bootflash:isr4400-universalk9-NIM.bin to bootflash:mydir` | Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in Step 4. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **reload**<br>**Example:**<br>`Router# reload`<br>`rommon >` | Enables ROMMON mode, which allows the software in the consolidated file to be activated. |
| **Step 7** | **boot** *URL-to-directory-name*/**packages.conf**<br>**Example:**<br>`rommon 1 > boot bootflash:mydir/packages.conf` | Boots the consolidated package, by specifying the path and name of the provisioning file: packages.conf. |
| **Step 8** | **show version installed**<br>**Example:**<br>`Router# show version installed`<br>`Package: Provisioning File, version: n/a, status: active` | Displays the version of the newly installed software. |

### Examples

The initial part of the example shows the consolidated package, isr4400-universalk9.164422SSA.bin, being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router# copy tftp:isr4400/isr4400-universalk9.164422SSA.bin bootflash:
Address or name of remote host []? 192.0.2.1
Destination filename [isr4400-universalk9.164422SSA.bin]?
Accessing tftp://192.0.2.1/isr4400/isr4400-universalk9.164422SSA.bin...
Loading isr4400/isr4400-universalk9.164422SSA.bin from 192.0.2.1 (via GigabitEthernet0):
!!!!!!!!
[OK - 410506248 bytes]

410506248 bytes copied in 338.556 secs (1212521 bytes/sec)


Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version

15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre

IOS XE Version: 2012-06-28_15.31_mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
```

```
Router uptime is 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp:isr4400/isr4400.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.

License Level: adventerprise
License Type: EvalRightToUse
Next reload license Level: adventerprise
cisco ISR4451/K9 (2RU) processor with 1136676K/6147K bytes of memory.
Processor board ID FGL161611AB
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.

Configuration register is 0x8000

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 May 3 2012 19:58:37 +00:00 lost+found
178465 drwx 4096 Jun 6 2012 15:20:20 +00:00 core
584065 drwx 4096 Jul 13 2012 19:19:00 +00:00 .prst_sync
405601 drwx 4096 May 3 2012 19:59:30 +00:00 .rollback_timer
113569 drwx 40960 Jul 13 2012 19:19:32 +00:00 tracelogs
64897 drwx 4096 May 3 2012 19:59:42 +00:00 .installer
13 -rw- 1305 May 7 2012 17:43:42 +00:00 startup-config
14 -rw- 1305 May 7 2012 17:43:55 +00:00 running-config
15 -r-- 1541 Jun 4 2012 18:32:41 +00:00 debug.conf
16 -rw- 1252 May 22 2012 19:58:39 +00:00 running-config-20120522
519169 drwx 4096 Jun 4 2012 15:29:01 +00:00 vman_fdb

7451738112 bytes total (7067635712 bytes free)



Router# show platform
Chassis type: ISR4451/K9

Slot         Type                State                 Insert time (ago)
---------    ------------------- --------------------- -----------------
0            ISR4451/K9          ok                    15:57:33
 0/0         ISR4451-6X1GE       ok                    15:55:24
1            ISR4451/K9          ok                    15:57:33
 1/0         SM-1T3/E3           ok                    15:55:24
2            ISR4451/K9          ok                    15:57:33
 2/0         SM-1T3/E3           ok                    15:55:24
```

```
R0           ISR4451/K9          ok, active            15:57:33
F0           ISR4451-FP          ok, active            15:57:33
P0           Unknown             ps, fail              never
P1           XXX-XXXX-XX         ok                    15:56:58
P2           ACS-4450-FANASSY    ok                    15:56:58

Slot         CPLD Version        Firmware Version
---------    ------------------- ---------------------------------------
0            12090323            15.3(01r)S [ciscouser-ISRRO...
1            12090323            15.3(01r)S [ciscouser-ISRRO...
2            12090323            15.3(01r)S [ciscouser-ISRRO...
R0           12090323            15.3(01r)S [ciscouser-ISRRO...
F0           12090323            15.3(01r)S [ciscouser-ISRRO...

Router# mkdir bootflash:isr4400-universalk9.dir1
Create directory filename [isr4400-universalk9.dir1]?
Created dir bootflash:/isr4400-universalk9.dir1
Router# request platform software package expand file bootflash:isr4400-universalk9.NIM.bin

to bootflash:isr4400-universalk9.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console.Reload Reason: Reload
Command.

rommon 1 > boot bootflash:isr4400-universalk9.dir1/packages.conf

File size is 0x00002836
Located isr4400-universalk9.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_shalhash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
###############################################################################################
File is comprised of 21 fragments (0%)
.....



Router# show version installed
Package: Provisioning File, version: n/a, status: active
File: bootflash:isr4400-universalk9.dir1/packages.conf, on: RP0
Built: n/a, by: n/a
File SHA1 checksum: ad09affd3f8820f4844f27acc1add502e0b8f459

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg, on:
 RP0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: active
```

```
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e
Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: dir1, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb
Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge-BLD-BLD_MCP_DEV_LATEST_20120710
_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpcontrol-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: 2012-07-10_16.23_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpios-universalk9-BLD-BLD_MCP_DEV_LATEST_
```

```
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb

Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpaccess-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpbase-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes-BLD-BLD_MCP_DEV_LATEST
_20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_sp2700-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
```

### Installing Subpackages from a Consolidated Package on a Flash Drive

The steps for installing subpackages from a consolidated package on a USB flash drive are similar to those described in Installing Subpackages from a Consolidated Pacakage section .

#### Procedure

**Step 1** **show version**

**Step 2** **dir usb***n*:

**Step 3** **show platform**

**Step 4** **mkdir bootflash:***URL-to-directory-name*

**Step 5** **request platform software package expand fileusb*n*: *package-name to URL-to-directory-name***

**Step 6** **reload**

**Step 7** **boot** *URL-to-directory-name/***packages.conf**

**Step 8** **show version installed**

## How to Install and Upgrade the Software for Cisco IOS XE Denali Release 16.3

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

- *Managing and Configuring a Router to Run Using a Consolidated Package* section

- *Managing and Configuring a Router to Run Using Individual Packages* section
- *Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example* section
- *Upgrading to Cisco IOS XE Denali Release 16.3* section

## Upgrading to Cisco IOS XE Denali Release 16.3

Upgrading the device to Cisco IOS XE Denali Release 16.3 for the first time uses the same procedures as specified in the earlier section. In addition, Cisco IOS XE Denali Release 16.3 requires a minimum ROMMON version. When the device boots up with Cisco IOS XE Denali 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)#boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
Router(config)#config-register 0x2102
Router(config)#exit
Router# show run | include boot
boot-start-marker
boot system tftp://10.81.116.4/rtp-isr4400-54/isr4400.bin
boot-end-marker
license boot level adventerprise
Router# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Router# reload
Proceed with reload? [confirm]
Sep 13 17:42:54.445 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with

reload chassis code


Initializing Hardware ...

System integrity status: c0000600


Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username
```

```
Current image running: Boot ROM0

Last reset cause: LocalSoft

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 504063931 (0x1e0b67bb) bytes

ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed
Self Tests Latency: 58 msec

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
calculated 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
expected 7294dffc:892a6c35:a7a133df:18c032fc:0670b303
Signed Header Version Based Image Detected

Using FLASH based Keys of type = PRIMARY KEY STORAGE
Using FLASH based Keys of type = ROLLOVER KEY STORAGE
RSA Signed DEVELOPMENT Image Signature Verification Successful.
Package Load Test Latency : 5116 msec
Image validated


Detected old ROMMON version 12.2(20150910:184432), upgrade required
Upgrading to newer ROMMON version required by this version of IOS-XE, do not power cycle
the system.  A reboot will automatically occur for the new ROMMON to take effect.
selected : 1
Booted : 1
Reset Reason: 1

Info: Upgrading entire flash from the rommon package
Switching to ROM 0
Upgrade image MD5 signature is b702a0a59a46a20a4924f9b17b8f0887
Upgrade image MD5 signature verification is b702a0a59a46a20a4924f9b17b8f0887
Switching back to ROM 1
ROMMON upgrade complete.

To make the new ROMMON permanent, you must restart the RP.
ROMMON upgrade successful.  Rebooting for upgrade to take effect.


Initializing Hardware ...
```

```
System integrity status: 00300610
Key Sectors:(Primary,GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 300

ROM:RSA Self Test Passed

Expected hash:
ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f

Obtained hash:
ddaf35a193617abacc417349ae204131
12e6fa4e89a97ea20a9eeee64b55d39a
2192992a274fc1a836ba3c23a3feebbd
454d4423643ce80e2a9ac94fa54ca49f
ROM:Sha512 Self Test Passed
Self Tests Latency: 418 msec
Rom image verified correctly


System Bootstrap, Version 12.2(20120618:163328) [username-ESGROM_20120618_GAMMA 101],
DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Mon 05/27/2014 12:39:32.05 by username

CPLD Version: 33 (MM/DD/YY): 06/23/14 Cisco ISR4351/K9 Slot:0

Current image running: Boot ROM1

Last reset cause: ResetRequest
Reading confreg 0x2102

Reading monitor variables from NVRAM
Enabling interrupts...done

Checking for PCIe device presence...done
Cisco ISR4351/K9 platform with 16777216 Kbytes of main memory

autoboot entry: NVRAM VALUES: bootconf: 0x0, autobootstate: 0
autobootcount: 0, autobootsptr: 0x0
Rommon upgrade requested
Flash upgrade reset 0 in progress
.......
Initializing Hardware ...

Checking for PCIe device presence...done
Reading confreg 2102
System integrity status: 0x300610
Key Sectors:(Primary, GOOD),(Backup,GOOD),(Revocation,GOOD)
Size of Primary = 2288 Backup = 2288 Revocation = 288
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
```

```
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Rom image verified correctly


System Bootstrap, Version 16.2(1r), RELEASE SOFTWARE
Copyright (c) 1994-2016  by cisco Systems, Inc.


Current image running: *Upgrade in progress* Boot ROM0

Last reset cause: BootRomUpgrade
ISR4351/K9 platform with 16777216 Kbytes of main memory

Cisco ISR 4400 platform with 4194304 Kbytes of main memory


IP_ADDRESS: 172.18.42.119
IP_SUBNET_MASK: 255.255.255.0
DEFAULT_GATEWAY: 172.18.42.1
TFTP_SERVER: 10.81.116.4
TFTP_FILE: rtp-isr4400-54/isr4400.bin
TFTP_MACADDR: a4:4c:11:9d:ad:97
TFTP_VERBOSE: Progress
TFTP_RETRY_COUNT: 18
TFTP_TIMEOUT: 7200
TFTP_CHECKSUM: Yes
ETHER_PORT: 0

ETHER_SPEED_MODE: Auto Detect
link up...
Receiving rtp-isr4400-54/isr4400.bin from 10.81.116.4
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot image size = 504063931 (0x1e0b67bb) bytes


Image Base is: 0x56834018
Image Size is: 0x1E089706
Package header rev 1 structure detected
Package type:30000, flags:0x0
IsoSize = 503874534
Parsing package TLV info:
000: 000000090000001D4B45595F544C565F -         KEY_TLV_
010: 5041434B4147455F434F4D5041544942 - PACKAGE_COMPATIB
020: 494C4954590000000000090000000B - ILITY
030: 4652555F52505F545950450000000009 - FRU_RP_TYPE
040: 000000184B45595F544C565F5041434B -     KEY_TLV_PACK
050: 4147455F424F4F544152434800000009 - AGE_BOOTARCH
060: 0000000E415243485F693638365F5459 -     ARCH_i686_TY
070: 5045000000000009000000144B45595F - PE          KEY_
080: 544C565F424F4152445F434F4D504154 - TLV_BOARD_COMPAT
090: 0000000900000012424F4152445F6973 -         BOARD_is
0A0: 72343330305F54595045000000000009 - r4300_TYPE
0B0: 000000184B45595F544C565F43525950 -     KEY_TLV_CRYP
0C0: 544F5F4B4559535452494E4700000009 - TO_KEYSTRING

TLV: T=9, L=29, V=KEY_TLV_PACKAGE_COMPATIBILITY
TLV: T=9, L=11, V=FRU_RP_TYPE
TLV: T=9, L=24, V=KEY_TLV_PACKAGE_BOOTARCH
TLV: T=9, L=14, V=ARCH_i686_TYPE
TLV: T=9, L=20, V=KEY_TLV_BOARD_COMPAT
TLV: T=9, L=18, V=BOARD_isr4300_TYPE
```

```
TLV: T=9, L=24, V=KEY_TLV_CRYPTO_KEYSTRING
TLV: T=9, L=10, V=EnCrYpTiOn
TLV: T=9, L=11, V=CW_BEGIN=$$
TLV: T=9, L=19, V=CW_FAMILY=$isr4300$
TLV: T=9, L=59, V=CW_IMAGE=$isr4300-universalk9.2016-06-29_23.31_paj.SSA.bin$
TLV: T=9, L=19, V=CW_VERSION=$16.3.1$
TLV: T=9, L=52, V=CW_DESCRIPTION=$Cisco IOS Software, IOS-XE Software$
TLV: T=9, L=9, V=CW_END=$$
Found DIGISIGN TLV type 12 length = 392
RSA Self Test Passed

Expected hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F

Obtained hash:
DDAF35A193617ABACC417349AE204131
12E6FA4E89A97EA20A9EEEE64B55D39A
2192992A274FC1A836BA3C23A3FEEBBD
454D4423643CE80E2A9AC94FA54CA49F
Sha512 Self Test Passed
Found package arch type ARCH_i686_TYPE
Found package FRU type FRU_RP_TYPE
Calculating SHA-1 hash...Validate package: SHA-1 hash:
 calculated 8B082C48:35C23C9E:8A091441:D6FACEE6:B5111533
 expected   8B082C48:35C23C9E:8A091441:D6FACEE6:B5111533

Image validated

Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version
16.3(20160527:095327)
[v163_throttle]
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Tue 27-May-16 21:28 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2016 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.
```

```
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.


Warning: the compile-time code checksum does not appear to be present.
cisco ISR4451/K9 (2RU) processor with 1133585K/6147K bytes of memory.
Processor board ID FGL1619100P
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.
7816688K bytes of USB flash at usb0:.


Press RETURN to get started!
```

# Installing a Firmware Subpackage

### Before you begin

Obtain a consolidated package that contains your required firmware package and expand the package. (See Managing and Configuring a Router to Run Using Individual Packages, on page 30.) Make a note of the location and name of the firmware package and use this information in the steps below for *URL-to-package-name*.

You can install a firmware subpackage if the router has been configured using, for example, Managing and Configuring a Router to Run Using Individual Packages, on page 30.

Firmware subpackages are not released individually. You can select a firmware package from within a consolidated package after expanding the consolidated package. The firmware package can then be installed as shown in the procedure below.

**Note** Read the Release Notes document pertaining to the consolidated package to verify that the firmware within the consolidated package is compatible with the version of Cisco IOS XE software that is currently installed on a router.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show version**<br>**Example:**<br>`Router# show version`<br>`Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version 15.3(20120627:221639) [build_151722 111]`<br>`Copyright (c) 1986-2012 by Cisco Systems, Inc.`<br>`Compiled Thu 28-Jun-12 15:17 by mcpre`<br>`.`<br>`.`<br>`.` | Shows the version of software running on the router. This can later be compared with the version of software to be installed. |
| **Step 2** | **dir bootflash:**<br>**Example:**<br>`Router# dir bootflash:` | Displays the previous version of software and that a package is present. |
| **Step 3** | **show platform**<br>**Example:**<br>`Router# show platform`<br>`Chassis type: ISR4451/K9` | Checks the inventory.<br>Also see the example in Installing Subpackages from a Consolidated Package section. |
| **Step 4** | **mkdir bootflash:** *URL-to-directory-name*<br>**Example:**<br>`Router# mkdir bootflash:mydir` | Creates a directory to save the expanded software image.<br>You can use the same name as the image to name the directory. |
| **Step 5** | **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*<br>**Example:**<br>`Router# request platform software package expand file bootflash:isr4400-universalk9-NIM.bin to bootflash:mydir` | Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in the Step 4. |
| **Step 6** | **reload**<br>**Example:**<br>`Router# reload`<br>`rommon >` | Enables ROMMON mode, which allows the software in the consolidated file to be activated. |
| **Step 7** | **boot** *URL-to-directory-name* **/packages.conf**<br>**Example:**<br>`rommon 1 > boot bootflash:mydir/packages.conf` | Boots the consolidated package by specifying the path and name of the provisioning file: packages.conf. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **show version installed**<br>**Example:**<br>`Router# show version installed`<br>`Package: Provisioning File, version: n/a, status: active` | Displays the version of the newly installed software. |

### Examples

The initial part of the following example shows the consolidated package, isr4400-universalk9.164422SSA.bin, being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router# tftp:isr4400/isr4400-universalk9.164422SSA.bin bootflash:
Address or name of remote host []? 192.0.2.1
Destination filename [isr4400-universalk9.164422SSA.bin]?
Accessing tftp://192.0.2.1/isr4400/isr4400-universalk9.164422SSA.bin...
Loading isr4400/isr4400-universalk9.164422SSA.bin from 192.0.2.1 (via GigabitEthernet0):
!!!!!!!!
[OK - 410506248 bytes]

410506248 bytes copied in 338.556 secs (1212521 bytes/sec)


Router# show version
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental Version

15.3(20120627:221639) [build_151722 111]
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Thu 28-Jun-12 15:17 by mcpre

IOS XE Version: 2012-06-28_15.31_mcpre

Cisco IOS-XE software, Copyright (c) 2005-2012 by cisco Systems, Inc.
All rights reserved. Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0. The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0. For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 0 minutes
Uptime for this control processor is 3 minutes
System returned to ROM by reload
System image file is "tftp:isr4400/isr4400.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.

License Level: adventerprise
License Type: EvalRightToUse
Next reload license Level: adventerprise
cisco ISR4451/K9 (2RU) processor with 1136676K/6147K bytes of memory.
Processor board ID FGL161611AB
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of Compact flash at bootflash:.

Configuration register is 0x8000

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 May 3 2012 19:58:37 +00:00 lost+found
178465 drwx 4096 Jun 6 2012 15:20:20 +00:00 core
584065 drwx 4096 Jul 13 2012 19:19:00 +00:00 .prst_sync
405601 drwx 4096 May 3 2012 19:59:30 +00:00 .rollback_timer
113569 drwx 40960 Jul 13 2012 19:19:32 +00:00 tracelogs
64897 drwx 4096 May 3 2012 19:59:42 +00:00 .installer
13 -rw- 1305 May 7 2012 17:43:42 +00:00 startup-config
14 -rw- 1305 May 7 2012 17:43:55 +00:00 running-config
15 -r-- 1541 Jun 4 2012 18:32:41 +00:00 debug.conf
16 -rw- 1252 May 22 2012 19:58:39 +00:00 running-config-20120522
519169 drwx 4096 Jun 4 2012 15:29:01 +00:00 vman_fdb

7451738112 bytes total (7067635712 bytes free)



Router# show platform
Chassis type: ISR4451/K9

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 ISR4451/K9 ok 15:57:33
0/0 ISR4451-6X1GE ok 15:55:24
1 ISR4451/K9 ok 15:57:33
1/0 SM-1T3/E3 ok 15:55:24
2 ISR4451/K9 ok 15:57:33
2/0 SM-1T3/E3 ok 15:55:24
R0 ISR4451/K9 ok, active 15:57:33
F0 ISR4451-FP ok, active 15:57:33
P0 Unknown ps, fail never
P1 XXX-XXXX-XX ok 15:56:58
P2 ACS-4450-FANASSY ok 15:56:58

Slot CPLD Version Firmware Version
--------- ------------------- ---------------------------------------
0 12090323 15.3(01r)S [ciscouser-ISRRO...
1 12090323 15.3(01r)S [ciscouser-ISRRO...
2 12090323 15.3(01r)S [ciscouser-ISRRO...
R0 12090323 15.3(01r)S [ciscouser-ISRRO...
F0 12090323 15.3(01r)S [ciscouser-ISRRO...
```

```
Router# mkdir bootflash:isr4400-universalk9.dir1
Create directory filename [isr4400-universalk9.dir1]?
Created dir bootflash:/isr4400-universalk9.dir1
Router# request platform software package expand file bootflash:isr4400-universalk9.NIM.bin
 to
 bootflash:isr4400-universalk9.dir1
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.

rommon 1 > boot bootflash:isr4400-universalk9.dir1/packages.conf

File size is 0x00002836
Located isr4400-universalk9.dir1/packages.conf
Image size 10294 inode num 324484, bks cnt 3 blk size 8*512
#
File is comprised of 1 fragments (33%)

is_valid_shalhash: SHA-1 hash:
calculated 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
expected 62f6235a:fc98eb3a:85ce183e:834f1cb3:8a1f71d1
File size is 0x04b3dc00
Located isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg
Image size 78896128 inode num 324491, bks cnt 19262 blk size 8*512
################################################################################################
File is comprised of 21 fragments (0%)
.....



Router# show version installed
Package: Provisioning File, version: n/a, status: active
File: bootflash:isr4400-universalk9.dir1/packages.conf, on: RP0
Built: n/a, by: n/a
File SHA1 checksum: ad09affd3f8820f4844f27acc1add502e0b8f459

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9-build_164422SSA.pkg, on:
 RP0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e
Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7
```

```
Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: dir1, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb
Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: active
File: bootflash:isr4400-universalk9.dir1/isr4400-mono-universalk9_164422SSA.pkg, on: RP0/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes_164422SSA.pkg, on:
RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_fpge-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: eb72900ab32c1c50652888ff486cf370ac901dd7

Package: firmware_sm_1t3e3, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_sm_1t3e3-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 803005f15d8ea71ab088647e2766727ac2269871

Package: rpcontrol, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpcontrol-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 980fd58fe581e9346c44417b451d1c09ebb640c2

Package: rpios-universalk9, version: 2012-07-10_16.23_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpios-universalk9-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.23, by: mcpre
File SHA1 checksum: 27084f7e30a1d69d45a33e05d1b00345040799fb

Package: rpaccess, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpaccess-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP0/1
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 0119802deda2da91c38473c47a998fb3ed423448

Package: rpbase, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-rpbase-BLD-BLD_MCP_DEV_LATEST_20120710_
164422SSA.pkg, on: RP1
Built: 2012-07-10_16.22, by: mcpre
```

```
File SHA1 checksum: 5e95c9cbc4eaf5a4a5a1ac846ee2d0f41d1a026b

Package: firmware_attributes, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_attributes-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 71614f2d9cbe7f96d3c6e99b67d514bd108c6c99

Package: firmware_dsp_sp2700, version: 2012-07-10_16.22_mcpre, status: n/a
File: bootflash:isr4400-universalk9.dir1/isr4400-firmware_dsp_sp2700-BLD-BLD_MCP_DEV_LATEST_
20120710_164422SSA.pkg, on: RP1/0
Built: 2012-07-10_16.22, by: mcpre
File SHA1 checksum: 8334565edf7843fe246783b1d5c6ed933d96d79e

Package: firmware_fpge, version: 2012-07-10_16.22_mcpre, status: n/a
```

## Upgrading the Firmware on xDSL NIMs

To upgrade the firmware on a xDSL Network Interface Module (NIM), perform these steps:

### Before you begin

When you boot the router in packages.conf mode with the Cisco IOS XE image (super package) during the installation period, you can upgrade or downgrade the firmware without reloading the router. You need to follow the steps described in Installing a Firmware Subpackage section before proceeding with the firmware upgrade.

If you do not boot the router in packages.conf mode with the Cisco IOS XE image, you need to follow the below prerequisites before proceeding with the firmware upgrade:

- Copy the firmware subpackage (NIM firmware) into bootflash:/mydir.
- Send a request to the platform software package expand file *boot flash:/mydir/<IOS-XE image>* to expand the super package.
- Reload the hardware module subslot to boot the module with the new firmware.
- Verify that the module is booted up with the new firmware using the **show platform software subslot x/y module firmware** command.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | copy Cisco IOS XE image into bootflash: **mydir**.<br>**Example:**<br>`Router# mkdir bootflash:mydir` | Creates a directory to save the expanded software image.<br>You can use the same name as the image to name the directory. |
| **Step 2** | **request platform software package expand file** *bootflash:/mydir /<IOS-XE image* to expand super package.<br>**Example:** | Expands the platform software package to super package. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# request platform software package expand file bootflash:/mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin` | |
| **Step 3** | **reload**.<br>**Example:**<br>`Router# reload`<br>`rommon >` | Enables ROMMON mode, which allows the software in the super package file to be activated. |
| **Step 4** | **boot bootflash:mydir/ /packages.conf**.<br>**Example:**<br>`rommon 1 > boot bootflash:mydir/packages.conf` | Boots the super package by specifying the path and name of the provisioning file: packages.conf. |
| **Step 5** | **copy** NIM firmware subpackage to the folder **bootflash:mydir/**.<br>**Example:**<br>`Router#copy bootflash:isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg`<br>`bootflash:mydir/` | Copies the NIM firmware subpackage into bootflash:mydir. |
| **Step 6** | **request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>*.<br>**Example:**<br>`Router#equest platform software package install rp 0 file bootflash:mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg` | Installs the software package. |
| **Step 7** | **hw-module subslot x/y reload** to boot the module with the new firmware.<br>**Example:**<br>`Router#hw-module subslot 0/2 reload` | Reloads the hardware module subslot and boots the module with the new firmware. |
| **Step 8** | **show platform software subslot 0/2 module firmware** to verify that the module is booted up with the new firmware.<br>**Example:**<br>`Router# show platform software subslot 0/2 module firmware`<br>`Pe` | Displays the version of the newly installed firmware. |

### Examples

The following example shows how to perform firmware upgrade in a router module:

```
Routermkdir bootflash:mydir
Create directory filename [mydir]?
```

```
Created dir bootflash:/mydir
Router#c
Router#copy bootflash:isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin bootflash:mydir/
Destination filename [mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCC
425288648 bytes copied in 44.826 secs (9487544 bytes/sec)
Router#
Router#
Router#dir bootflash:mydir
Directory of bootflash:/mydir/

632738  -rw-        425288648  Dec 12 2014 09:16:42 +00:00
isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin

7451738112 bytes total (474025984 bytes free)
Router#

Router#request platform software package
expand file bootflash:/mydir/isr4400-universalk9.03.14.00.S.155-1.S-std.SPA.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router#reload
Proceed with reload? [confirm]

*Dec 12 09:26:09.874: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
Reload Command.Dec 12 09:26:25.156 R0/0: %PMAN-5-EXITACTION: Process manager is exiting:
process exit with reload chassis code


Initializing Hardware ...

System integrity status: 00000610
 Rom image verified correctly
 System Bootstrap, Version 15.3(3r)S1, RELEASE SOFTWARE
Copyright (c) 1994-2013  by cisco Systems, Inc.

 Current image running: Boot ROM0

Last reset cause: LocalSoft
 Cisco ISR4451-X/K9 platform with 4194304 Kbytes of main memory


rommon 1  boot bootflash:mydir/packages.conf

 File size is 0x000028f1
 Located mydir/packages.conf
 Image size
10481 inode num 632741, bks cnt 3 blk size 8*512

#
 File size is 0x150ae3cc
 Located mydir/isr4400-mono-universalk9.03.14.00.S.155-1.S-std.SPA.pkg
 Image size 353035212 inode num 356929, bks cnt 86191 blk size 8*512
 ###################################################################
###################################################################
 Boot image size = 353035212 (0x150ae3cc) bytes
```

```
 Package header rev 1 structure detected
 Calculating SHA-1 hash...done
 validate_package: SHA-1 hash:
  calculated 8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3
  expected   8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3

 RSA Signed RELEASE Image Signature Verification Successful.
 Package Load Test Latency : 3799 msec
 Image validated
 Dec 12 09:28:50.338 R0/0: %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded
[free space is 61864 kB] - Please clean up files on bootflash.

             Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre



Cisco IOS-XE software, Copyright (c) 2005-2014 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.



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.

cisco ISR4451-X/K9 (2RU) processor with 1681388K/6147K bytes of memory.
Processor board ID FTX1736AJUT
```

```
2 Ethernet interfaces
4 Gigabit Ethernet interfaces
2 ATM interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
7393215K bytes of flash memory at bootflash:.

Press RETURN to get started!

*Dec 12 09:28:58.922:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = appxk9 and License = appxk9
*Dec 12 09:28:58.943:
%IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL:
Module name = esg Next reboot level = ipbasek9 and License = ipbasek9
*Dec 12 09:28:58.981:
 %ISR_THROUGHPUT-6-LEVEL: Throughput level has been set to 1000000 kbps
*Dec 12 09:29:13.302: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:14.142: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Dec 12 09:28:51.438: %CMRP-3-PFU_MISSING:cmand:  The platform does not detect a power
supply in slot 1
*Dec 12 09:29:01.256: %CMLIB-6-THROUGHPUT_VALUE:cmand:  Throughput license found, throughput
 set to 1000000 kbps
*Dec 12 09:29:03.223: %CPPHA-7-START:cpp_ha:  CPP 0 preparing ucode
*Dec 12 09:29:03.238: %CPPHA-7-START:cpp_ha:  CPP 0 startup init
*Dec 12 09:29:11.335: %CPPHA-7-START:cpp_ha:  CPP 0 running init
*Dec 12 09:29:11.645: %CPPHA-7-READY:cpp_ha:  CPP 0 loading and initialization complete
*Dec 12 09:29:11.711: %IOSXE-6-PLATFORM:cpp_cp:
Process CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 12 09:29:16.280:
%IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO:
Management vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id 0x1E000001
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state to up
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to down
*Dec 12 09:29:16.330:
%LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state to up
*Dec 12 09:29:17.521: %SYS-5-LOG_CONFIG_CHANGE: Buffer logging disabled
*Dec 12 09:29:18.867: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*Dec 12 09:29:18.870:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Dec 12 09:29:18.871:
%IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/2, interfaces disabled
*Dec 12 09:29:18.873:
%SPA_OIR-6-OFFLINECARD: SPA (ISR4451-X-4x1GE) offline in subslot 0/0
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VA-B) offline in subslot 0/1
*Dec 12 09:29:18.874: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:29:18.876: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*Dec 12 09:29:18.876: %IOSXE_OIR-6-ONLINECARD: Card (fp) online in slot F0
*Dec 12 09:29:18.882: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/0
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/1
*Dec 12 09:29:18.884: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/2
*Dec 12 09:29:18.935: %SYS-5-RESTART: System restarted --
Cisco IOS Software, ISR Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 15.5(1)S,
RELEASE SOFTWARE (fc5)
Technical Support: http://www.cisco.com/techsupport
```

```
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled Thu 20-Nov-14 18:28 by mcpre
*Dec 12 09:29:18.895: %SPA-3-ENVMON_NOT_MONITORED:iomd:  Environmental monitoring
is not enabled for ISR4451-X-4x1GE[0/0]
*Dec 12 09:29:19.878: %LINK-5-CHANGED: Interface GigabitEthernet0,

changed state to administratively down
*Dec 12 09:29:22.419: %SPA_OIR-6-ONLINECARD: SPA (ISR4451-X-4x1GE) online in subslot 0/0
*Dec 12 09:29:22.610: %SYS-6-BOOTTIME: Time taken to reboot after reload =  194 seconds
*Dec 12 09:29:24.354: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to down
*Dec 12 09:29:24.415: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
changed state to down
*Dec 12 09:29:24.417: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
changed state to down
*Dec 12 09:29:30.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0,
changed state to up
*Dec 12 09:29:30.925: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/2,
 changed state to up
*Dec 12 09:29:30.936: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/3,
 changed state to up
*Dec 12 09:29:31.919: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0, changed state to up
*Dec 12 09:29:31.930: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0/2, changed state to up
*Dec 12 09:29:31.936: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0/0/3, changed state to up
*Dec 12 09:29:34.147: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 12 09:30:29.152: %SPA_OIR-6-ONLINECARD: SPA (NIM-VA-B) online in subslot 0/1
*Dec 12 09:30:29.470: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface Ethernet0/1/0, changed state to down
*Dec 12 09:30:31.152: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:30:31.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
*Dec 12 09:31:03.074: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to up
*Dec 12 09:31:05.075: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to up
*Dec 12 09:31:06.076: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/2/0,
changed state to up
*Dec 12 09:31:12.559: %CONTROLLER-5-UPDOWN: Controller VDSL 0/1/0, changed state to up
*Dec 12 09:31:20.188: %LINK-3-UPDOWN: Interface ATM0/1/0, changed state to up
*Dec 12 09:31:21.188: %LINEPROTO-5-UPDOWN: Line protocol on Interface ATM0/1/0,
changed state to up
Router>
Router>en
Password:
Router#
Router#show controller vdsl 0/2/0
Controller VDSL 0/2/0 is UP

Daemon Status:  UP

   XTU-R (DS)  XTU-C (US)
Chip Vendor ID:  'BDCM'    'BDCM'
Chip Vendor Specific:   0x0000    0xA41B
Chip Vendor Country:    0xB500    0xB500
Modem Vendor ID: 'CSCO'    '    '
Modem Vendor Specific:  0x4602    0x0000
Modem Vendor Country:   0xB500    0x0000
Serial Number Near:     FOC18426DQ8 4451-X/K15.5(1)S
Serial Number Far:
Modem Version Near:     15.5(1)S
Modem Version Far:      0xa41b

Modem Status(L1): TC Sync (Showtime!)
```

```
DSL Config Mode: VDSL2
Trained Mode(L1): G.993.2 (VDSL2) Profile 30a

TC Mode:  PTM
Selftest Result: 0x00
DELT configuration: disabled
DELT state:  not running

Failed full inits: 0
Short inits:  0
Failed short inits: 0

Modem FW  Version: 4.14L.04
Modem PHY Version: A2pv6F039h.d24o_rc1

Line 1:

   XTU-R (DS)  XTU-C (US)
Trellis:   ON    ON
SRA:     disabled   disabled
SRA count:    0    0
Bit swap:    enabled   enabled
Bit swap count:   9    0
Profile 30a:    enabled
Line Attenuation:   3.5 dB    0.0 dB
Signal Attenuation:   0.0 dB    0.0 dB
Noise Margin:   30.9 dB  12.4 dB
Attainable Rate: 200000 kbits/s   121186 kbits/s
Actual Power:  13.3 dBm   7.2 dBm
Per Band Status:        D1  D2  D3  U0  U1  U2  U3
Line Attenuation(dB):   0.9 1.5 5.5 N/A 0.1 0.9 3.8
Signal Attenuation(dB): 0.8 1.5 5.5 N/A 0.0 0.2 3.2
Noise Margin(dB):       31.1 31.0 30.9 N/A 12.3 12.4 12.5
Total FECC:  0    0
Total ES:  0    0
Total SES:  0    0
Total LOSS:  0    0
Total UAS:  51    51
Total LPRS:  0    0
Total LOFS:  0    0
Total LOLS:  0    0


     DS Channel1   DS Channel0 US Channel1   US Channel0
Speed (kbps):    NA       100014  NA       100014
SRA Previous Speed:   NA            0  NA            0
Previous Speed:    NA            0  NA            0
Reed-Solomon EC:   NA            0  NA            0
CRC Errors:    NA           0  NA           0
Header Errors:    NA            0  NA            0
Interleave (ms):   NA         9.00  NA         0.00
Actual INP:    NA         4.00  NA         0.00

Training Log : Stopped
Training Log Filename : flash:vdsllog.bin

Router#
Router#

Router#copy bootflash:isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
 bootflash:mydir/
Destination filename [mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

```
6640604 bytes copied in 1.365 secs (4864911 bytes/sec)
Router#

Router#request platform software package install rp 0 file
bootflash:mydir/isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed isr4400-firmware_nim_xdsl.03.14.00.S.155-1.S-std.SPA.pkg
New files list:
  Added isr4400-firmware_nim_xdsl.2014-11-17_11.05_39n.SSA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
```

```
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
Skipping soft links for firmware upgrade
Skipping soft links for firmware upgrade
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19
/release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
  Replacing running software
  Replacing CLI software
  Restarting software
  Applying final IPC and database definitions
rsync: getaddrinfo: cc2-0 873: Name or service not known rsync error:
error in socket IO (code 10) at /auto/mcpbuilds19/
release/03.14.00.S/BLD-V03_14_00_S_FC5/contrib/rsync/clientserver.c(104) [sender=2.6.9]
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
Router#
Router#show platform software subslot 0/2 module firmware
Avg Load info
-----------------------------------------
1.83 1.78 1.44 3/45 607

Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2
(Buildroot 2011.11) ) #3 SMP PREEMPT Fri Nov 7 09:26:19 IST 2014

Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039h.d24o_rc1

Boot Loader: Secondry
-----------------------------------------
Version: 1.1

Modem Up time
-----------------------------------------
0D 0H 25M 38S

Router#

Router#hw-module subslot 0/2 reload
Proceed with reload of module? [confirm]
Router#
*Dec 12 09:55:59.645: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
reloaded on subslot 0/2
*Dec 12 09:55:59.646: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
*Dec 12 09:55:59.647: %CONTROLLER-5-UPDOWN: Controller VDSL 0/2/0, changed state to down
```

```
*Dec 12 09:57:22.514: new extended attributes received from iomd(slot 0 bay 2 board 0)
*Dec 12 09:57:22.514: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(NIM-VAB-A)
 reloaded on subslot 0/2
*Dec 12 09:57:22.515: %SPA_OIR-6-OFFLINECARD: SPA (NIM-VAB-A) offline in subslot 0/2
Router#
Router#
*Dec 12 09:58:35.471: %SPA_OIR-6-ONLINECARD: SPA (NIM-VAB-A) online in subslot 0/2
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface Ethernet0/2/0, changed state to down
*Dec 12 09:58:37.470: %LINK-3-UPDOWN: Interface ATM0/2/0, changed state to down
Router#

Router#show platform software subslot 0/2 module firmware
Avg Load info
-----------------------------------------
0.84 0.23 0.08 1/45 598

Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2 (Buildroot 2011.11) )
#6 SMP PREEMPT Mon Nov 17 10:51:41 IST 2014

Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039n.d24o_rc1

Boot Loader: Secondry
-----------------------------------------
Version: 1.1

Modem Up time
-----------------------------------------
0D 0H 0M 42S

Router#
```

# Provisioning Files

This section provides background information about the files and processes used in Managing and Configuring a Router to Run Using Individual Packages, on page 70.

The consolidated package on a router consists of a collection of subpackages and a provisioning file titled `packages.conf`. To run the software, the usual method used is to boot the consolidated package, which is copied into memory, expanded, mounted, and run within memory. The provisioning file's name can be renamed but subpackage file's names cannot be renamed. The provisioning file and subpackage files must be kept in the same directory. The provisioning file does not work properly if any individual subpackage file is contained within a different directory.

**Note** An exception to this is that if a new or upgraded module firmware package is subsequently installed, it need not be in the same directory as the provisioning file.

Configuring a router to boot, using the provisioning file packages.conf, is beneficial because no changes have to be made to the boot statement after the Cisco IOS XE software is upgraded.

# File Systems

The following table provides a list of file systems that can be seen on the Cisco 1100 series routers.

***Table 5: Router File Systems***

| File System | Description |
|---|---|
| bootflash: | Boot flash memory file system. |
| flash: | Alias to the boot flash memory file system above. |
| cns: | Cisco Networking Services file directory. |
| nvram: | Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM. |
| obfl: | File system for Onboard Failure Logging (OBFL) files. |
| system: | System memory file system, which includes the running configuration. |
| tar: | Archive file system. |
| tmpsys: | Temporary system files file system. |
| usb0: | The Universal Serial Bus (USB) flash drive file systems.<br>**Note** The USB flash drive file system is visible only if a USB drive is installed in usb0: port. |

Use the **?** help option, or use the **copy** command in command reference guides, if you find a file system that is not listed in the table above.

# Autogenerated File Directories and Files

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

***Table 6: Autogenerated Files***

| File or Directory | Description |
|---|---|
| crashinfo files | Crashinfo files may appear in the bootflash: file system.<br>These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router. |

| File or Directory | Description |
|---|---|
| core directory | The storage area for .core files.<br>If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased. |
| lost+found directory | This directory is created on bootup if a system check is performed. Its appearance is completely normal and does not indicate any issues with the router. |
| tracelogs directory | The storage area for trace files.<br>Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure.<br>Trace files, 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, core, and trace files can be deleted.

# Flash Storage

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

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

# Configuring the Configuration Register for Autoboot

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.

For more information about the configuration register, see Use of the Configuration Register on All Cisco Routers and Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example, on page 64.

**Note** Setting the configuration register to 0x2102 will set the router to autoboot the Cisco IOS XE software.

**Note** The console baud rate is set to 9600 after changing the **confreg** to 0x2102 or 0x0. If you cannot establish a console session after setting **confreg**, or garbage output appears, change the setting on your terminal emulation software to 9600.

# Crypto Throughput Licensing

The Cisco 1100 series routers currently support two levels of crypto throughput licensing. The default crypto throughput level is 50 Mbps.

- The licensed level for Cisco 1111-8P SKU is 250 Mbps.
- The licensed level for Cisco 1111-4P SKU is 150 Mbps.

The following example is for the Cisco 1111-4P SKU:

Verify the current crypto throughput level

```
Router#sh platform hardware throughput crypto
 The current crypto level is 50000 kb/s  <---- This indicates the current crypto throughput.
```

Make changes to the existing crypto throughput level

```
Router(config)#platform hardware throughput crypto ?
      150000  throughput in kbps
      50000   throughput in kbps

  Router(config)#platform hardware throughput crypto 150000
  Feature Name:throughput

PLEASE  READ THE  FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE  KEY  PROVIDED FOR  ANY CISCO  PRODUCT  FEATURE  OR  USING SUCH
PRODUCT  FEATURE  CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING
TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO  BE BOUND
BY ALL THE TERMS SET FORTH HEREIN.

Use of this product feature requires  an additional license from Cisco,
together with an additional  payment.  You may use this product feature
on an evaluation basis, without payment to Cisco, for 60 days. Your use
of the  product,  including  during the 60 day  evaluation  period,  is
subject to the Cisco end user license agreement
http://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html
If you use the product feature beyond the 60 day evaluation period, you
must submit the appropriate payment to Cisco for the license. After the
60 day  evaluation  period,  your  use of the  product  feature will be
governed  solely by the Cisco  end user license agreement (link above),
```

```
together  with any supplements  relating to such product  feature.  The
above  applies  even if the evaluation  license  is  not  automatically
terminated  and you do  not receive any notice of the expiration of the
evaluation  period.  It is your  responsibility  to  determine when the
evaluation  period is complete and you are required to make  payment to
Cisco for your use of the product feature beyond the evaluation period.

Your  acceptance  of  this agreement  for the software  features on one
product  shall be deemed  your  acceptance  with  respect  to all  such
software  on all Cisco  products  you purchase  which includes the same
software.  (The foregoing  notwithstanding, you must purchase a license
for each software  feature you use past the 60 days evaluation  period,
so  that  if you enable a software  feature on  1000  devices, you must
purchase 1000 licenses for use past  the 60 day evaluation period.)

Activation  of the  software command line interface will be evidence of
your acceptance of this agreement.


ACCEPT? (yes/[no]): yes

*Jul 14 08:12:41.898: %LICENSE-6-EULA_ACCEPTED: EULA for feature throughput 1.0 has been
accepted. UDI=C1111-8P:FGL212694M3; StoreIndex=3:Built-In License Storage% The config will
 take effect on next reboot


Check the show license feature, throughput license at this point would not be enabled.

Router#sh license feature
Feature name             Enforcement  Evaluation  Subscription   Enabled  RightToUse
appxk9                                yes               yes                no
     no              yes
securityk9                         yes           yes          no               yes
 yes
ipbasek9                      no            no           no                no
   no
FoundationSuiteK9          yes           yes          no               no
yes
throughput                    yes           yes          no               No<--        yes
internal_service              yes           no           no                no
 no
```

### Save the configuration

```
Router#wr mem
   Building configuration...

   [OK]
```

### Reload the router

```
Router#reload
   Proceed with reload? [confirm]
```

### Verify the new crypto throughput level

```
Router#sh platform hardware throughput crypto
   The current crypto level is 150000 kb/s.
```

### Verify if the throughput license is enabled

```
Router#sh license feature
Feature name             Enforcement  Evaluation  Subscription   Enabled  RightToUse
appxk9                                yes               yes                no
     no              yes
securityk9                         yes           yes          no               yes
```

```
 yes
ipbasek9                        no            no           no                no
   no
FoundationSuiteK9          yes           yes          no                no
yes
throughput                    yes           yes          no                yes<--
yes
internal_service              yes           no           no                no
 no

=============
```

# Unlicensed Feature: Example

If you try to use a feature that is part of a package that is not enabled, an error message is displayed.

In the following example, the **crypto map** command is called during configuration and an error message is displayed. This is because, the feature associated with **crypto map** is part of the **securityk9** package and the **securityk9** package is not enabled.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto map
^
% Invalid input detected at '^' marker.
```

Use the **show license feature** command to view the license features that are enabled. In the following example, the **securityk9** and the **uck9** packages are not enabled.

**Note** **ipbasek9** is provided by default.

```
Router# show license feature
Feature name             Enforcement  Evaluation  Subscription   Enabled  RightToUse
appxk9                   yes          yes         no             yes      yes
uck9                     yes          yes         no             no       yes
securityk9               yes          yes         no             no       yes
ipbasek9                 no           no          no             yes      yes
```

# LED Indicators

For information on LEDs on the router, see the "LED Indicators" section of the Hardware Installation Guide for the Cisco 1100 Series Integrated Services Routers.

# Related Documentation

For further information on software licenses, see Software Activation on Cisco Integrated Services Routers and Cisco Integrated Service Routers G2.

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

# How to Install and Upgrade the Software

To install or upgrade the software, use one of the following methods to use the software from a consolidated package or an individual package.

**Note** When a device is in the installation mode, formatting of the boot drive, bootflash/flash is not recommended. Formatting is blocked to ensure stability of the running image and to avoid any impact to upgrade of the software.

## Managing and Configuring a Router to Run Using a Consolidated Package

**Note** Do not use these procedures if you also need to install any optional subpackages or plan to upgrade individual subpackages. See Managing and Configuring a Router to Run Using Individual Packages, on page 70.

## Managing and Configuring a Consolidated Package Using copy and boot Commands

To upgrade a consolidated package, copy the consolidated package to the **bootflash:** directory on the router using the **copy** command. After making this copy of the consolidated package, configure the router to boot using the consolidated package file.

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

```
Router# dir bootflash:
Directory of bootflash:/
   11  drwx            16384  Jun 13 2017 14:13:26 +00:00  lost+found
105249  drwx             4096  Jul 12 2017 15:48:19 +00:00  .installer
48577  drwx              4096  Jun 13 2017 14:16:31 +00:00  core
56673  drwx              4096  Jul 12 2017 18:42:01 +00:00  .prst_sync
145729  drwx             4096  Jun 13 2017 14:14:47 +00:00  .rollback_timer
   12  -rw-                0  Jun 13 2017 14:14:58 +00:00  tracelogs.a4i
348129  drwx             8192  Jul 12 2017 19:47:16 +00:00  tracelogs
   13  -rw-               30  Jul 12 2017 18:42:01 +00:00  throughput_monitor_params
   14  -rw-               35  Jun 13 2017 15:32:49 +00:00  pnp-tech-time
   15  -rw-           134096  Jun 13 2017 15:32:50 +00:00  pnp-tech-discovery-summary
   16  -rw-          2425808  Jul 12 2017 17:18:59 +00:00
C1100-ROMMON-20170621-SecureBoot-Aikido-SSA.pkg
6650826752 bytes total (5914554368 bytes free)


Router# copy tftp: bootflash:Address or name of remote host []? 172.18.40.4
Destination filename [c1100.bin]?
```

```
Accessing tftp://172.18.40.4/user5/c1100.bin...
Loading user5/c1100.bin from 172.18.40.4 (via GigabitEthernet0/0/0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 379357675 bytes]

Router# dir bootflash:
Directory of bootflash:/

   11  drwx            16384  Jun 13 2017 14:13:26 +00:00  lost+found
105249  drwx             4096  Jul 12 2017 15:48:19 +00:00  .installer
48577  drwx             4096  Jun 13 2017 14:16:31 +00:00  core
56673  drwx             4096  Jul 12 2017 18:42:01 +00:00  .prst_sync
145729  drwx             4096  Jun 13 2017 14:14:47 +00:00  .rollback_timer
   12  -rw-               0  Jun 13 2017 14:14:58 +00:00  tracelogs.a4i
348129  drwx             8192  Jul 12 2017 19:47:16 +00:00  tracelogs
   13  -rw-               30  Jul 12 2017 18:42:01 +00:00  throughput_monitor_params
   14  -rw-               35  Jun 13 2017 15:32:49 +00:00  pnp-tech-time
   15  -rw-           134096  Jun 13 2017 15:32:50 +00:00  pnp-tech-discovery-summary
   16  -rw-          2425808  Jul 12 2017 17:18:59 +00:00
C1100-ROMMON-20170621-SecureBoot-Aikido-SSA.pkg
   17  -rw-        379357675  Jul 12 2017 19:00:30 +00:00  c1100.bin

6650826752 bytes total (5914554368 bytes free)
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# boot system flash bootflash:c1100.bin
Router(config)# config-reg 0x2102
Router(config)# exit
Router# show run | include boot
boot-start-marker
boot system flash bootflash:c1100.bin boot-end-marker
Router# copy run start
Destination filename [startup-config]? Building configuration...
[OK]
Router# reload
```

# Configuring a Router to Boot the Consolidated Package via TFTP Using the boot Command: Example

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system tftp://172.18.40.4/<path>/c1100.bin
Router(config)#config-register 0x2102
Router(config)#exit

Router# show run | include boot
boot-start-marker
boot system tftp /<path>/c1100-universalk9_ias.16.06.02.SPA.bin 223.255.254.254
boot-end-marker
diagnostic bootup level minimal
Router#

Router# copy running-config startup-config
Destination filename [startup-config]? Building configuration...
[OK]
Router# reload
The following license(s) are transitioning, expiring or have expired.
Features with expired licenses may not work after Reload.
```

```
Feature: internal_service               ,Status: expiring, Period Left: 270 wks 2  days
Proceed with reload? [confirm]

*Jul 12 19:56:22.981: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.UEFI firmware (version MARVELL devel-17.1.0 built at 01:11:40 on Jun 22 2017)

Armada Platform Init

Board is TSN-P2H
Comphy-0: SGMII2        3.125 Gbps
Comphy-1: SGMII3        1.25 Gbps
Comphy-2: USB3_HOST0    5 Gbps
Comphy-3: USB3_HOST1    5 Gbps
Comphy-4: SGMII0        1.25 Gbps
Comphy-5: PCIE2         5 Gbps

UtmiPhy: stage: Check PLL.. Passed
UTMI PHY 0 initialized to USB Host0
UtmiPhy: stage: Check PLL.. Passed
UTMI PHY 1 initialized to USB Host1
Succesfully installed controller 0 at 0xF2701000
Succesfully installed controller 1 at 0xF2701100
Succesfully installed controller 2 at 0xF2211000
PciEmulation: Skip SD/MMC device with index 0
Succesfully installed protocol interfaces
Y[=3hfsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096
fsw_ext4_volume_mount: success, blocksize 4096

Starting ROMMON...
Rom image verified correctly


System Bootstrap, Version 12.2[16.6(1r)RC3], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2017  by cisco Systems, Inc.
Compiled at Wed Jun 21 21:09:42 2017 by user2


!!! DEBUG CPLD Version Installed. For INTERNAL USE ONLY !!!

Current image running: Boot ROM1

Last reset cause: LocalSoft
C1111-8PLTEEAWE platform with 4194304 Kbytes of main memory


........


          IP_ADDRESS: 172.18.42.231
      IP_SUBNET_MASK: 255.255.255.0
     DEFAULT_GATEWAY: 172.18.42.1
```

```
         TFTP_SERVER: 172.18.40.4
           TFTP_FILE: user5/c1100.bin
        TFTP_MACADDR: D4:8C:B5:83:A3:6C
          ETHER_PORT: 0
Unable to get TFTP file size - Using maximum size of 1073741824 bytes.
```

```
Package header rev 3 structure detected
IsoSize = 344424448
Calculating SHA-1 hash...Validate package: SHA-1 hash:
        calculated 5361A704:82F2A7F9:200C5D02:1209D89B:14A7FAFB
        expected   5361A704:82F2A7F9:200C5D02:1209D89B:14A7FAFB

RSA Signed DEVELOPMENT Image Signature Verification Successful
Image validated
   DXE    809 ms
   BDS   1153 ms
   BDS     21 ms
Total Time = 1984 ms


Starting OS kernel...


              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706


Cisco IOS Software [Fuji], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Experimental
 Version 16.7.20170621:131015 [polaris_dev-/scratch/user5/tsn_0620 104]
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 21-Jun-17 09:12 by user5


Cisco IOS-XE software, Copyright (c) 2005-2017 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.


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.

cisco C1111-8PLTEEAWE (1RU) processor with 1463766K/6147K bytes of memory.
Processor board ID FGL21071SK5
1 Virtual Ethernet interface
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6598655K bytes of flash memory at bootflash:.
0K bytes of WebUI ODM Files at webui:.

%INIT: waited 0 seconds for NVRAM to be available



Press RETURN to get started!


*Jul 12 20:02:38.716: %SMART_LIC-6-AGENT_READY: Smart Agent for Licensing is initialized
*Jul 12 20:02:39.070: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = esg
Next reboot level = ipbasek9 and License = No valid license found
*Jul 12 20:02:40.781: %ISR_THROUGHPUT-6-CRYPTO: Crypto level has been set to 50000 kbps
*Jul 12 20:02:46.668: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
*Jul 12 20:02:46.855:  in NSH init
*Jul 12 20:02:47.097: %LINK-3-UPDOWN: Interface Lsmpi0, changed state to up
*Jul 12 20:02:47.098: %LINK-3-UPDOWN: Interface EOBC0, changed state to up
*Jul 12 20:02:47.098: %LINK-3-UPDOWN: Interface LIIN0, changed state to up
*Jul 12 20:02:47.142: aaa proxy process: dmiauthd mqipc init failed
*Jul 12 20:02:47.171: %PNP-6-PNP_DISCOVERY_STOPPED: PnP Discovery stopped (Startup Config
Present)
*Jul 12 20:01:43.752: %IOSXE-3-PLATFORM:  R0/0: kernel: [  105.413908] cpld_ioctl (line
1307): ioctl not implemented: type=122 number=180
*Jul 12 20:01:59.696: %IOSXE-1-PLATFORM:  R0/0: kernel: [  121.345752] moka_fpga_open
*Jul 12 20:02:42.243: %CMLIB-6-THROUGHPUT_VALUE:  R0/0: cmand:  Throughput license found,
throughput set to 50000 kbps
*Jul 12 20:02:48.098: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
 to down
*Jul 12 20:02:48.098: %LINEPROTO-5-UPDOWN: Line protocol on Interface Lsmpi0, changed state
 to up
*Jul 12 20:02:48.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface EOBC0, changed state
 to up
*Jul 12 20:02:48.099: %LINEPROTO-5-UPDOWN: Line protocol on Interface LIIN0, changed state
 to up
*Jul 12 20:02:52.867: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named TP-self-signed-3241146330
 has been generated or imported
*Jul 12 20:02:56.210: %SYS-2-PRIVCFG_DECRYPT: Successfully apply the private config file
*Jul 12 20:02:56.298: %SYS-5-CONFIG_I: Configured from memory by console
*Jul 12 20:02:56.311: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/0, interfaces disabled
*Jul 12 20:02:56.311: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/1, interfaces disabled
*Jul 12 20:02:56.311: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/2, interfaces disabled
*Jul 12 20:02:56.311: %IOSXE_OIR-6-REMSPA: SPA removed from subslot 0/3, interfaces disabled
*Jul 12 20:02:56.325: %SPA_OIR-6-OFFLINECARD: SPA (C1111-2x1GE) offline in subslot 0/0
*Jul 12 20:02:56.338: %SPA_OIR-6-OFFLINECARD: SPA (C1111-ES-8) offline in subslot 0/1
*Jul 12 20:02:56.339: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
*Jul 12 20:02:56.339: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
*Jul 12 20:02:56.340: %SPA_OIR-6-OFFLINECARD: SPA (C1111-LTE) offline in subslot 0/2
```

```
*Jul 12 20:02:56.340: %SPA_OIR-6-OFFLINECARD: SPA (ISR-AP1100AC-E) offline in subslot 0/3
*Jul 12 20:02:56.343: %IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F0
*Jul 12 20:02:58.205: %SYS-5-RESTART: System restarted --
Cisco IOS Software [Fuji], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Experimental
 Version 16.7.20170621:131015 [polaris_dev-/scratch/user5/tsn_0620 104]
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 21-Jun-17 09:12 by user5
*Jul 12 20:02:58.252: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Jul 12 20:02:58.464: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named
TP-self-signed-3241146330.server has been generated or imported
*Jul 12 20:03:01.059: %SYS-6-BOOTTIME: Time taken to reboot after reload =  400 seconds
*Jul 12 20:03:07.272: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named CISCO_IDEVID_SUDI has been
 generated or imported
*Jul 12 20:03:12.073: %SPA_OIR-6-ONLINECARD: SPA (C1111-ES-8) online in subslot 0/1
*Jul 12 20:03:12.140: %LINK-3-UPDOWN: Interface Cellular0/2/0, changed state to down
*Jul 12 20:03:12.141: %LINK-3-UPDOWN: Interface Cellular0/2/1, changed state to down
*Jul 12 20:03:12.286: %SPA_OIR-6-ONLINECARD: SPA (C1111-LTE) online in subslot 0/2
*Jul 12 20:03:12.342: new extended attributes received from iomd(slot 0 bay 3 board 0)
*Jul 12 20:03:12.349: %SPA_OIR-6-ONLINECARD: SPA (C1111-2x1GE) online in subslot 0/0
*Jul 12 20:03:12.774: %SPA_OIR-6-ONLINECARD: SPA (ISR-AP1100AC-E) online in subslot 0/3
*Jul 12 20:03:13.927: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/0, changed state to down
*Jul 12 20:03:13.961: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/1, changed state to down
*Jul 12 20:03:13.981: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/2, changed state to down
*Jul 12 20:03:14.005: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/3, changed state to down
*Jul 12 20:03:14.021: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/4, changed state to down
*Jul 12 20:03:14.033: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/5, changed state to down
*Jul 12 20:03:14.041: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/6, changed state to down
*Jul 12 20:03:14.045: %LINK-3-UPDOWN: Interface GigabitEthernet0/1/7, changed state to down
*Jul 12 20:03:14.055: %LINK-3-UPDOWN: Interface Wlan-GigabitEthernet0/1/8, changed state
to down
*Jul 12 20:03:14.297: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to down
*Jul 12 20:03:14.323: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/1, changed state to down
*Jul 12 20:03:17.613: %LINK-3-UPDOWN: Interface Wlan-GigabitEthernet0/1/8, changed state
to up
*Jul 12 20:03:18.613: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Wlan-GigabitEthernet0/1/8, changed state to up
*Jul 12 20:03:18.621: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state
 to up
*Jul 12 20:03:18.961: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed state to up
*Jul 12 20:03:19.962: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
 changed state to up
*Jul 12 20:03:40.876: %IOSXE-3-PLATFORM:  R0/0: ngiolite: Modem VID/PID: 1199 9071
*Jul 12 20:03:40.880: %IOSXE-3-PLATFORM:  R0/0: ngiolite: Modem is in connected state
*Jul 12 20:04:06.349: %CELLWAN-5-SIM_DETECT_START: [Cellular0/2/0]: SIM presence detection
 starts !!
*Jul 12 20:04:08.976: %CELLWAN-5-SIM_DETECT_COMPLETE: [Cellular0/2/0]: SIM presence detection
 has completed !!
*Jul 12 20:04:09.228: %CELLWAN-2-SIM_NOT_PRESENT: [Cellular0/2/0]: SIM is not present in
NIM SIM Slot.
*Jul 12 20:05:14.464: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
*Jul 12 20:05:14.665: %CELLWAN-2-MODEM_RADIO: Cellular0/2/0 Modem radio has been turned on

Router>
Router>enable
Router#show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
 16.6.2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 01-Nov-17 03:00 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
```

```
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 3 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "usb0:c1100-universalk9_ias.16.06.02.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.



Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot
--------------------------------------------------------------------------------
FoundationSuiteK9     None                  None           None
securityk9
appxk9


Technology Package License Information:

------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appxk9           None             None             None
securityk9       None             None             None
ipbase           ipbasek9         None             ipbasek9

cisco C1111-8PLTELAWN (1RU) processor with 1464345K/6147K bytes of memory.
Processor board ID FGL212392WT
8 Virtual Ethernet interfaces
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
```

```
6762495K bytes of flash memory at bootflash:.
7855044K bytes of USB flash at usb0:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2100

Router#
```

# Managing and Configuring a Router to Run Using Individual Packages

To choose between running individual packages or a consolidated package, see the *Installing the Software - Overview* section.

## Installing Subpackages from a Consolidated Package

Perform the following procedure to obtain the consolidated package from a TFTP server.

Another variation of this procedure obtains the consolidated package from a USB flash drive. This is described in the Installing Subpackages from a Consolidated Package on a Flash Drive.

### Before you begin

Copy the consolidated package to the TFTP server.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show version**<br>**Example:**<br>`Router# show version`<br>`Cisco IOS XE Software, Version 16.06.02`<br>`Cisco IOS Software [Everest], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Version 16.6.2, RELEASE SOFTWARE (fc2)`<br>`Technical Support: http://www.cisco.com/techsupport`<br>`Copyright (c) 1986-2017 by Cisco Systems, Inc.`<br>`Compiled Wed 01-Nov-17 03:00 by mcpre`<br><br>`Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.`<br>`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` | Shows the version of software running on the router. This can later be compared with the version of software to be installed. |

| | Command or Action | Purpose |
|---|---|---|
| | 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.<br><br>ROM: IOS-XE ROMMON<br><br>Router uptime is 3 minutes<br>Uptime for this control processor is 5 minutes<br>System returned to ROM by Reload Command<br>System image file is "usb0:c1100-universalk9_ias.16.06.02.SPA.bin"<br>Last reload reason: Reload Command<br><br>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.<br><br>A summary of U.S. laws governing Cisco cryptographic products may be found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html<br><br>If you require further assistance please contact us by sending email to export@cisco.com.<br><br>Suite License Information for Module:'esg'<br><br>---<br>Suite Suite Current<br>Type Suite Next reboot<br>---<br>FoundationSuiteK9 None<br>None None<br><br>securityk9<br>appxk9 | |

| | Command or Action | Purpose |
|---|---|---|
| | Technology Package License Information:<br><br>Technology Technology-package Technology-package Current Type Next reboot<br>appxk9 None None None<br>securityk9 None None None<br>ipbase ipbasek9 None ipbasek9<br><br>cisco C1111-8PLTELAWN (1RU) processor with 1464345K/6147K bytes of memory.<br>Processor board ID FGL212392WT<br>8 Virtual Ethernet interfaces<br>11 Gigabit Ethernet interfaces<br>2 Cellular interfaces<br>32768K bytes of non-volatile configuration memory.<br>4194304K bytes of physical memory.<br>6762495K bytes of flash memory at bootflash:.<br>7855044K bytes of USB flash at usb0:.<br>0K bytes of WebUI ODM Files at webui:.<br><br>Configuration register is 0x2100<br><br>Router#<br><br>. | |
| **Step 2** | **dir bootflash:**<br>**Example:**<br>`Router# dir bootflash:` | Displays the previous version of software and that a package is present. |
| **Step 3** | **show platform**<br>**Example:**<br>`Router# show platform`<br>`Chassis type: C1100` | Displays the inventory. |
| **Step 4** | **mkdir bootflash:** *URL-to-directory-name*<br>**Example:**<br>`Router# mkdir bootflash:mydir` | Creates a directory to save the expanded software image.<br>You can use the same name as the image to name the directory. |
| **Step 5** | **request platform software package expand file** *URL-to-consolidated-package* **to** *URL-to-directory-name*<br>**Example:** | Expands the software image from the TFTP server (*URL-to-consolidated-package*) into the directory used to save the image (*URL-to-directory-name*), which was created in Step 4. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# request platform software package expand file bootflash:c1100-universalk9-ias.bin to bootflash:mydir` | |
| **Step 6** | **reload**<br>**Example:**<br>`Router# reload`<br>`rommon >` | Enables ROMMON mode, which allows the software in the consolidated file to be activated. |
| **Step 7** | **boot** *URL-to-directory-name*/**packages.conf**<br>**Example:**<br>`rommon 1 > boot bootflash:mydir/packages.conf` | Boots the consolidated package, by specifying the path and name of the provisioning file: packages.conf. |
| **Step 8** | **show version installed**<br>**Example:**<br>`Router# show version installed`<br>`Package: Provisioning File, version: n/a, status: active` | Displays the version of the newly installed software. |

### Examples

The initial part of the example shows the consolidated package, c1100.bin, being copied to the TFTP server. This is a prerequisite step. The remaining part of the example shows the consolidated file, packages.conf, being booted.

```
Router# copy tftp:c1100.bin bootflash:
Address or name of remote host []? 172.18.40.4
Destination filename [c1100.bin]?
Accessing tftp://172.18.40.4/user5/c1100.bin...
Loading user5/c1100.bin from 172.18.40.4 (via GigabitEthernet0/0/0):
```

```
[OK - 379357675 bytes]

379357675 bytes copied in 382.880 secs (990800 bytes/sec)
```

```
Router# show version
Cisco IOS XE Software, Version 16.06.02
Cisco IOS Software [Everest], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M), Version
 16.6.2, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 01-Nov-17 03:00 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
```

```
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 3 minutes
Uptime for this control processor is 5 minutes
System returned to ROM by Reload Command
System image file is "usb0:c1100-universalk9_ias.16.06.02.SPA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.



Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot
--------------------------------------------------------------------------------
FoundationSuiteK9     None                  None           None
securityk9
appxk9


Technology Package License Information:

------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appxk9           None             None             None
securityk9       None             None             None
ipbase           ipbasek9         None             ipbasek9

cisco C1111-8PLTELAWN (1RU) processor with 1464345K/6147K bytes of memory.
Processor board ID FGL212392WT
8 Virtual Ethernet interfaces
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6762495K bytes of flash memory at bootflash:.
7855044K bytes of USB flash at usb0:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2100
```

```
Router#

Router# dir bootflash:
Directory of bootflash:/
Directory of bootflash:/

   11  drwx            16384  Jun 13 2017 14:13:26 +00:00  lost+found
105249  drwx             4096  Jul 12 2017 15:48:19 +00:00  .installer
48577  drwx             4096  Jun 13 2017 14:16:31 +00:00  core
56673  drwx             4096  Jun 13 2017 14:14:40 +00:00  .prst_sync
145729  drwx             4096  Jun 13 2017 14:14:47 +00:00  .rollback_timer
   12  -rw-                0  Jun 13 2017 14:14:58 +00:00  tracelogs.a4i
348129  drwx             4096  Jul 12 2017 15:53:50 +00:00  tracelogs
   13  -rw-               30  Jul 12 2017 15:49:42 +00:00  throughput_monitor_params
   14  -rw-               35  Jun 13 2017 15:32:49 +00:00  pnp-tech-time
   15  -rw-           134096  Jun 13 2017 15:32:50 +00:00  pnp-tech-discovery-summary

6650826752 bytes total (6297722880 bytes free)



Router# show platform
Chassis type: C1111-8PLTELAWN

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C1111-8PLTELAWN     ok                    00:04:56
 0/0      C1111-2x1GE         ok                    00:02:41
 0/1      C1111-ES-8          ok                    00:02:40
 0/2      C1111-LTE           ok                    00:02:41
 0/3      ISR-AP1100AC-N      ok                    00:02:41
R0        C1111-8PLTELAWN     ok, active            00:04:56
F0        C1111-8PLTELAWN     ok, active            00:04:56
P0        PWR-12V             ok                    00:04:30

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         17100501            16.6(1r)RC3
R0        17100501            16.6(1r)RC3
F0        17100501            16.6(1r)RC3

Router#

Router# mkdir bootflash:c1100.dir1
Create directory filename [c1100.dir1]? Created dir bootflash:/c1100.dir1
Router# request platform software package expand file bootflash:c1100.bin to
bootflash:c1100.dir1

Jul 12 20:18:28.059 RP0/0: %INSTALL-5-OPERATION_START_INFO: Started expand package
bootflash:c1100.bin
Verifying parameters
Expanding superpackage bootflash:c1100.bin
Validating package type

*Jul 12 20:18:28.029: %IOSXE-5-PLATFORM:  R0/0: Jul 12 20:18:28 packtool:
%INSTALL-5-OPERATION_START_INFO: Started expand package bootflash:c1100.binCopying package
 files
SUCCESS: Finished expanding all-in-one software package.
Jul 12 20:19:57.041 RP0/0: %INSTALL-5-OPERATION_COMPLETED_INFO: Completed expand package
bootflash:c1100.bin
```

```
Router# reload
Proceed with reload? [confirm]

*Jul 13 19:39:06.354: %SYS-5-RELOAD: Reload requested by console.Reload Reason: Reload
Command.

rommon 1 > boot bootflash:c1100.dir/packages.conf
                        Located packages.conf
###############################################################################################################

Package header rev 3 structure detected
IsoSize = 0
Calculating SHA-1 hash...Validate package: SHA-1 hash:
        calculated 9E5196BD:ED7FB430:538521E5:90175EED:B3AD33B7
        expected   9E5196BD:ED7FB430:538521E5:90175EED:B3AD33B7

RSA Signed DEVELOPMENT Image Signature Verification Successful
Image validated
   DXE    809 ms
   BDS   1153 ms
   BDS     21 ms
Total Time = 1984 ms
.....



Router# show version installed
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: bootflash:c1100.dir/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: a02d730877371ac9c033e90444094bb441adc8e5

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: active
  Role: rp_base
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: rpboot, version: 2017-06-21_09.16_user5, status: active
  Role: rp_boot
  File: bootflash:c1100.dir/c1100-rpboot.2017-06-21_09.16_user5.SSA.pkg, on: RP0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: n/a

Package: firmware_c1100_gfast, version: 2017-06-21_09.16_user5, status: active
  Role: firmware_c1100_gfast
  File: bootflash:c1100.dir/c1100-firmware_c1100_gfast.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 996bc2d56bdb9d4e13f45a613db1bc41d0b6d291

Package: firmware_c1100_vadsl, version: 2017-06-21_09.16_user5, status: active
  Role: firmware_c1100_vadsl
  File: bootflash:c1100.dir/c1100-firmware_c1100_vadsl.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: a2a7daf772c30fc4cec5befac29ff320d8d47152

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: active
  Role: rp_daemons
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
```

```
 RP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

                   Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status:
 active
  Role: rp_iosd
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: active
  Role: rp_security
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: active
  Role: rp_webui
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: firmware_c1100_gfast, version: 2017-06-21_09.16_user5, status: n/a
  Role: firmware_c1100_gfast
  File: bootflash:c1100.dir/c1100-firmware_c1100_gfast.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 996bc2d56bdb9d4e13f45a613db1bc41d0b6d291

Package: firmware_c1100_vadsl, version: 2017-06-21_09.16_user5, status: n/a
  Role: firmware_c1100_vadsl
  File: bootflash:c1100.dir/c1100-firmware_c1100_vadsl.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: a2a7daf772c30fc4cec5befac29ff320d8d47152

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
  Role: rp_daemons
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/1
  Built: 2017-06-21_09.16, by: user5
                     File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992
                   Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status:
 n/a
  Role: rp_iosd
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/1
                    File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
  Role: rp_security
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
  Role: rp_webui
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP0/1
```

```
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
  Role: rp_base
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 RP1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: rpboot, version: 2017-06-21_09.16_user5, status: n/a
  Role: rp_boot
  File: bootflash:c1100.dir/c1100-rpboot.2017-06-21_09.16_user5.SSA.pkg, on: RP1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: n/a

Package: firmware_c1100_gfast, version: 2017-06-21_09.16_user5, status: n/a
  Role: firmware_c1100_gfast
  File: bootflash:c1100.dir/c1100-firmware_c1100_gfast.2017-06-21_09.16_user5.SSA.pkg, on:
 RP1/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 996bc2d56bdb9d4e13f45a613db1bc41d0b6d291

Package: firmware_c1100_vadsl, version: 2017-06-21_09.16_user5, status: n/a
  Role: firmware_c1100_vadsl
  File: bootflash:c1100.dir/c1100-firmware_c1100_vadsl.2017-06-21_09.16_user5.SSA.pkg, on:
 RP1/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: a2a7daf772c30fc4cec5befac29ff320d8d47152

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
                   Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status:
 active
  Role: cc
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 SIP0/0
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: active
  Role: cc
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 SIP0/1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: cc, version: unknown, status: active
  Role: cc
  File: unknown, on: SIP0/2
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: cc, version: unknown, status: active
  Role: cc
  File: unknown, on: SIP0/3
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: cc, version: unknown, status: n/a
  Role: cc
  File: unknown, on: SIP0/4
  Built: unknown, by: unknown
  File SHA1 checksum: unknown
```

```
Package: cc, version: unknown, status: n/a
  Role: cc
  File: unknown, on: SIP0/5
  Built: unknown, by: unknown
  File SHA1 checksum: unknown

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
  Role: cc_spa
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 SIP1
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992

Package: mono-universalk9_ias, version: 2017-06-21_09.16_user5, status: n/a
  Role: cc_spa
  File: bootflash:c1100.dir/c1100-mono-universalk9_ias.2017-06-21_09.16_user5.SSA.pkg, on:
 SIP2
  Built: 2017-06-21_09.16, by: user5
  File SHA1 checksum: 1e44c63d734c574b986c9332c1bad8580f55e992
```

## Installing Subpackages from a Consolidated Package on a Flash Drive

The steps for installing subpackages from a consolidated package on a USB flash drive are similar to those described in the Installing Subpackages from a Consolidated Package section.

**Procedure**

**Step 1** **show version**

**Step 2** **dir usb***n*:

**Step 3** **show platform**

**Step 4** **mkdir bootflash:***URL-to-directory-name*

**Step 5** **request platform software package expand fileusb***n*: ***package-name to URL-to-directory-name***

**Step 6** **reload**

**Step 7** **boot** *URL-to-directory-name/***packages.conf**

**Step 8** **show version installed**

# How to Install and Upgrade the Software for Cisco IOS XE Everest Release 16.6

To install or upgrade the software, use one of the following methods to use the software from a consolidated package or an individual package.

## Upgrading to Cisco IOS XE Everest 16.6.2 Release

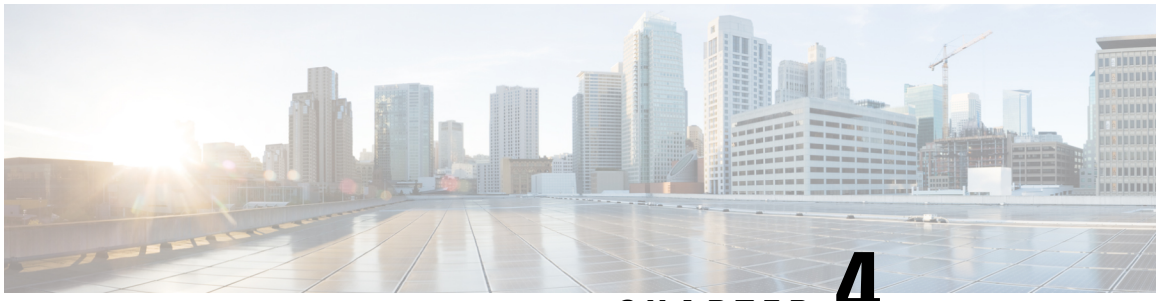
Upgrading the device to Cisco IOS XE Everest 16.6.2 release for the first time uses the same procedures as specified in the earlier section. In addition, Cisco IOS XE Everest 16.6.2 release requires a minimum ROMMON

version. When the device boots up with Cisco IOS XE Everest 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:

Not supported for C1100 in this release since C1100 is shipped with the minimum Rommon version.



CHAPTER 4

# Configuring ROMMON

This chapter contains the following sections:


- ROMMON Images, on page 81


## 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. For more information on ROMMON, see the "ROM Monitor Overview and Basic Procedures" section in the Cisco 1100 Series ISR Hardware and Installation Guide.

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.

*Table 7: Cisco ISR1000 ROMMON Compatibility Matrix*

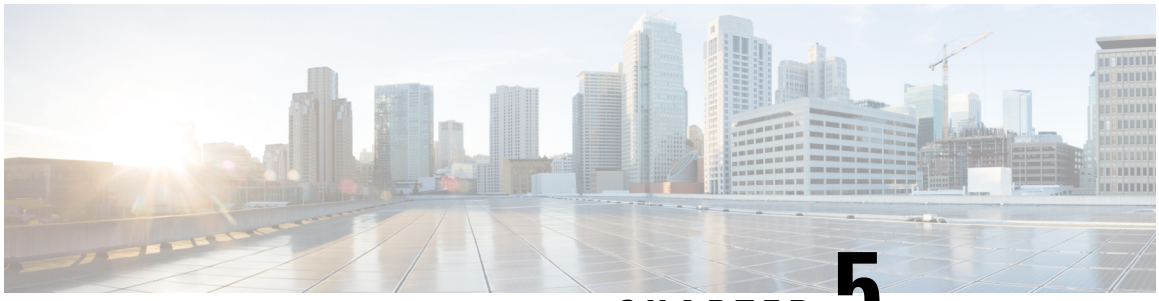
| Cisco IOS XE Release | Minimum ROMMON Release Supported for IOS XE | Recommended ROMMON Release Supported for IOS XE |
|---|---|---|
| 16.6.x | 16.6(1r) | 16.6(1r) |
| 16.7.x | 16.6(1r) | 16.6(1r) |
| 16.8.x | 16.8(1r) | 16.8(1r) |
| 16.9.x | 16.9(1r) | 16.9(1r) |
| 16.10.x | 16.9(1r) | 16.9(1r) |
| 16.11.x | 16.9(1r) | 16.9(1r) |
| 16.12.x | 16.9(1r) | 16.9(1r) |

| Cisco IOS XE Release | Minimum ROMMON Release Supported for IOS XE | Recommended ROMMON Release Supported for IOS XE |
|---|---|---|
| 17.2.x | 16.9(1r) | 16.9(1r) |
| 17.3.x | 16.12(2r) | 16.12(2r) |
| 17.4.x | 16.12(2r) | 16.12(2r) |
| 17.5.x | 17.5(1r) | 17.5(1r) |
| 17.6.x | 17.5(1r) | 17.5(1r) |

**Note** Starting from the following releases, the ROMMON image is not available for download on software.cisco.com:

- Cisco IOS XE Release 16.12.4 (16.x) onwards
- Cisco IOS XE Release 17.3.2 (17.x) onwards

Instead the ROMMON image is bundled along with the IOS XE image. When you install the IOS XE image, if the version of ROMMON bundled is higher than the existing version of ROMMON, an upgrade is performed automatically.



CHAPTER 5

# Basic Router Configuration

This chapter contains the following sections:


- Default Configuration, on page 83
- Configuring Global Parameters, on page 86
- Configuring Gigabit Ethernet Interfaces, on page 86
- Configuring a Loopback Interface, on page 87
- Configuring Module Interfaces, on page 89
- Enabling Cisco Discovery Protocol, on page 89
- Configuring Command-Line Access, on page 89
- Configuring Static Routes, on page 91
- Configuring Dynamic Routes, on page 92


## Default Configuration

When you boot up the router for the first time, the router looks for a default file name-the PID of the router. For example, the Cisco 1000 Series Integrated Services Routers look for a file named **isr1100.cfg**. The Cisco 1000 Series ISR looks for this file before finding the standard files-**router-confg** or the **ciscortr.cfg**.

The Cisco 1000 ISR looks for the **isr1100.cfg** file in the bootflash. If the file is not found in the bootflash, the router then looks for the standard files-**router-confg** and **ciscortr.cfg**. If none of the files are found, the router then checks for any inserted USB that may have stored these files in the same particular order.

**Note** If there is a configuration file with the PID as its name in an inserted USB, but one of the standard files are in bootflash, the system finds the standard file for use.

Use the **show running-config** command to view the initial configuration, as shown in the following example:

```
Router# show running-config

Building configuration...


Current configuration : 1749 bytes
!
! Last configuration change at 20:23:33 UTC Fri Nov 3 2017
!
version 16.6
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
!
hostname Router
!
boot-start-marker
boot-end-marker
!
!
!
no aaa new-model
!
!
!
!
!
!
!
!
!
!
!
subscriber templating
!
!
multilink bundle-name authenticated
!
!
!
crypto pki trustpoint TP-self-signed-4175586959
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4175586959
 revocation-check none
 rsakeypair TP-self-signed-4175586959
!
!
crypto pki certificate chain TP-self-signed-4175586959
!
!
license udi pid C1111-8PLTELA sn FGL212694ML
!
diagnostic bootup level minimal
spanning-tree extend system-id
!
!
!
redundancy
 mode none
!
controller Cellular 0/2/0
 lte modem link-recovery disable
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface GigabitEthernet0/0/0
 no ip address
```

```
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/1
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet0/1/0
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2
!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
!
interface GigabitEthernet0/1/7
!
interface Cellular0/2/0
 ip address negotiated
 ipv6 enable
!
interface Cellular0/2/1
 no ip address
 shutdown
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
!
!
!
!
!
control-plane
!
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 login
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
end
```

# Configuring Global Parameters

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

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router> enable`<br>`Router# configure terminal`<br>`Router(config)#` | Enters global configuration mode when using the console port.<br>Use the following to connect to the router with a remote terminal:<br>`telnet router-name or address`<br>`Login: login-id`<br>`Password: *********`<br>`Router> enable` |
| **Step 2** | **hostname** *name*<br>**Example:**<br>`Router(config)# hostname Router` | Specifies the name for the router. |
| **Step 3** | **enable password** *password*<br>**Example:**<br>`Router(config)# enable password cr1ny5ho` | Specifies a password to prevent unauthorized access to the router.<br>**Note** In this form of the command, password is not encrypted. |
| **Step 4** | **no ip domain-lookup**<br>**Example:**<br>`Router(config)# no ip domain-lookup` | Disables the router from translating unfamiliar words (typos) into IP addresses.<br>For complete information on global parameter commands, see the Cisco IOS Release Configuration Guide documentation set. |

# Configuring Gigabit Ethernet Interfaces

To manually define onboard Gigabit Ethernet interfaces, follow these steps, beginning from global configuration mode.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **interface** *slot/bay/port*<br>**Example:** | Enters the configuration mode for an interface on the router. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# interface 0/0/1` | |
| **Step 2** | **ip address** *ip-address mask*<br>**Example:**<br>`Router(config-if)# ip address 192.168.12.2 255.255.255.0` | Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address. |
| **Step 3** | **ipv6 address** *ipv6-address/prefix*<br>**Example:**<br>`Router(config-if)# ipv6 address 2001.db8::ffff:1/128` | Sets the IPv6 address and prefix for the specified interface. Use this step instead of Step 2, if you are configuring an IPv6 address. |
| **Step 4** | **no shutdown**<br>**Example:**<br>`Router(config-if)# no shutdown` | Enables the interface and changes its state from administratively down to administratively up. |
| **Step 5** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits the configuration mode of interface and returns to the global configuration mode. |

# Configuring a Loopback Interface

### Before you begin

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

To configure a loopback interface, follow these steps.

### Procedure

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | (Option 2) **ipv6 address** *ipv6-address/prefix*<br>**Example:**<br>`Router(config-if)# 2001:db8::ffff:1/128` | Sets the IPv6 address and prefix on the loopback interface. |
| **Step 4** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Exits configuration mode for the loopback interface and returns to global configuration mode. |

The loopback interface in this sample configuration is used to support Network Address Translation (NAT) on the virtual-template interface. This configuration example shows the loopback interface configured on the Gigabit Ethernet interface with an IP address of 192.0.2.0/16, which acts as a static IP address. The loopback interface points back to virtual-template1, which has a negotiated IP address.

```
!
interface loopback 0
ip address 192.0.2.1 255.255.0.0 (static IP address)
ip nat outside
!
interface Virtual-Template1
ip unnumbered loopback0
no ip directed-broadcast
ip nat outside
```

### 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 Module Interfaces

For detailed information about configuring service modules, see the Wireless Device Overview chapter and the Cisco Fourth-Generation LTE-Advanced chapter.

# Enabling Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is enabled by default on the router.

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.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **line** [ **console** \| **tty** \| **vty**] *line-number*<br>**Example:**<br>`Router(config)# line console 0` | Enters line configuration mode, and specifies the type of line.<br>The example provided here specifies a console terminal for access. |
| **Step 2** | **password** *password*<br>**Example:**<br>`Router(config-line)# password 5dr4Hepw3` | Specifies a unique password for the console terminal line. |
| **Step 3** | **login**<br>**Example:**<br>`Router(config-line)# login` | Enables password checking at terminal session login. |
| **Step 4** | **exec-timeout** *minutes* [*seconds*]<br>**Example:**<br>`Router(config-line)# exec-timeout 5 30`<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>The example provided here shows a timeout of 5 minutes and 30 seconds. Entering a timeout of **0 0** specifies never to time out. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **exit**<br>**Example:**<br>`Router(config-line)# exit` | Exits line configuration mode to re-enter global configuration mode. |
| **Step 6** | **line** [ **console** \| **tty** \| **vty**] *line-number*<br>**Example:**<br>`Router(config)# line vty 0 4`<br>`Router(config-line)#` | Specifies a virtual terminal for remote console access. |
| **Step 7** | **password** *password*<br>**Example:**<br>`Router(config-line)# password aldf2ad1` | Specifies a unique password for the virtual terminal line. |
| **Step 8** | **login**<br>**Example:**<br>`Router(config-line)# login` | Enables password checking at the virtual terminal session login. |
| **Step 9** | **end**<br>**Example:**<br>`Router(config-line)# end` | Exits line configuration mode, and returns to privileged EXEC mode. |

### Example

The following configuration shows the command-line access commands.

You do not have to input the commands marked **default**. These commands appear automatically in the configuration file that is generated when you use the **show running-config** command.

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

# Configuring Static Routes

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

To configure static routes, follow these steps.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | (Option 1) **ip route** *prefix mask* {*ip-address* \| *interface-type interface-number* [*ip-address*]}<br>**Example:**<br>`Router(config)# ip route 192.0.2.1 255.255.0.0 10.10.10.2` | Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the **ipv6 route** command described below.) |
| **Step 2** | (Option 2) **ipv6 route** *prefix/mask* {*ipv6-address* \| *interface-type interface-number* [*ipv6-address*]}<br>**Example:**<br>`Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0` | Specifies a static route for the IP packets. |
| **Step 3** | **end**<br>**Example:**<br>`Router(config)# end` | Exits global configuration mode and enters privileged EXEC mode. |

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

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

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

### Verifying Configuration

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

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

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

Gateway of last resort is not set

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

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

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

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

# Configuring Dynamic Routes

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

A router can use IP routing protocols, such as Routing Information Protocol (RIP) or Enhanced Interior Gateway Routing Protocol (EIGRP), to learn about routes dynamically.

## Configuring Routing Information Protocol

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

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **router rip**<br>**Example:**<br>`Router(config)# router rip` | Enters router configuration mode, and enables RIP on the router. |

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

The following configuration example shows RIP Version 2 enabled in IP networks 10.0.0.0 and 192.168.1.0. To see this configuration, use the **show running-config** command from privileged EXEC mode.

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


Current configuration : 5980 bytes
!
! Last configuration change at 13:56:48 PST Fri Nov 3 2017 by admin
!
version 16.6
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform shell
!
hostname Router
!
boot-start-marker
boot system tftp /auto/tftp-sjc-users5/c1100-universalk9_ias.16.06.02.SPA.bin 255.255.255.0
boot-end-marker
!
!
vrf definition VRF-example
 description VRF-example
!
```

```
no logging console
!
aaa new-model
!
!
!
aaa login success-track-conf-time 1
!
!
!
!
aaa session-id common
!
transport-map type persistent webui tsn_sol
 server
 secure-server
!
clock timezone PST -23 0
call-home
 contact-email-addr dsfdsfds@cisco.com
 profile "ewrewtrwrewr"
  destination address email cisco@cisco.com
!
!
ipv6 unicast-routing
ipv6 dhcp pool 234324
!
!
!
!
!
!
!
!
subscriber templating
!
!
multilink bundle-name authenticated
passthru-domain-list 34324
 match 3r4324
passthru-domain-list ewtrewr
 match asfdkdslkf.com
!
!
!
crypto pki trustpoint TP-self-signed-2994767669
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2994767669
 revocation-check none
 rsakeypair TP-self-signed-2994767669
!
crypto pki trustpoint TP-self-signed-3039537782
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3039537782
 revocation-check none
 rsakeypair TP-self-signed-3039537782
!
!
crypto pki certificate chain TP-self-signed-2994767669
crypto pki certificate chain TP-self-signed-3039537782
!
!
license udi pid C1111-8PLTELAWN sn FGL212392WT
!
```

```
redundancy
 mode none
!
controller Cellular 0/2/0
 lte modem link-recovery disable
!
!
vlan internal allocation policy ascending
!
!
!
!
!
!
interface Loopback3
 no ip address
!
interface Loopback50
 ip address 192.0.2.1 255.255.255.255
!
interface Loopback100
 no ip address
!
interface Loopback544534
 no ip address
!
interface Loopback32432532
 no ip address
!
interface Port-channel2
 no ip address
 no negotiation auto
!
interface GigabitEthernet0/0/0
 description Interface for WebUI access
 ip address 192.168.1.46 255.255.255.0
 negotiation auto
 spanning-tree portfast disable
!
interface GigabitEthernet0/0/1
 description Interface for TFTP
 ip address 192.0.2.1 255.255.255.0
 negotiation auto
 spanning-tree portfast disable
!
interface GigabitEthernet0/1/0
 spanning-tree portfast disable
!
interface GigabitEthernet0/1/1
!
interface GigabitEthernet0/1/2

!
interface GigabitEthernet0/1/3
!
interface GigabitEthernet0/1/4
!
interface GigabitEthernet0/1/5
!
interface GigabitEthernet0/1/6
!
interface GigabitEthernet0/1/7
!
interface Wlan-GigabitEthernet0/1/8
```

```
!
interface Cellular0/2/0
 pulse-time 1
!
interface Cellular0/2/1
 no ip address

!
interface Vlan1
 ip address 10.10.10.1 255.255.255.0
!
router rip
 version 2
 network 10.0.0.1
 network 192.168.1.0
!
 !
 address-family ipv4 unicast autonomous-system 44
  !
  af-interface GigabitEthernet0/0/0
   no split-horizon
  exit-af-interface
  !
  topology base
  exit-af-topology
 exit-address-family
!
!
!
!
control-plane
!
banner login ^CTSN_WebUI^C
!
line con 0
 transport input none
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 transport input telnet ssh
 transport output all
line vty 5 15
 transport input all
 transport output all
!
wsma agent exec
!
wsma agent config
!
wsma agent filesys
!
wsma agent notify
!
!
end

Router#
```

### 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    192.0.2.2/8 [120/1] via 192.0.2.1, 00:00:02, Ethernet0/0/0
```

# Configuring Enhanced Interior Gateway Routing Protocol

To configure Enhanced Interior Gateway Routing Protocol (EIGRP), follow these steps.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **router eigrp** *as-number*<br>**Example:**<br>`Router(config)# router eigrp 109` | Enters router configuration mode, and enables EIGRP on the router. The autonomous-system number identifies the route to other EIGRP routers and is used to tag the EIGRP information. |
| **Step 2** | **network** *ip-address*<br>**Example:**<br>`Router(config)# network 192.168.1.0`<br>`Router(config)# network 10.10.12.115` | Specifies a list of networks on which EIGRP is to be applied, using the IP address of the network of directly connected networks. |
| **Step 3** | **end**<br>**Example:**<br>`Router(config-router)# end` | Exits router configuration mode, and enters privileged EXEC mode. |

### Example

The following configuration example shows the EIGRP routing protocol enabled in IP networks 192.168.1.0 and 10.10.12.115. The EIGRP autonomous system number is 109. To see this configuration, use the **show running-config** command.

```
Router# show running-config
.
.
.
!
router eigrp 109
 network 192.168.1.0
  network 10.10.12.115
```

```
!
.
.
.
```

### Verifying Configuration

To verify that you have configured IP EIGRP correctly, enter the **show ip route** command, and look for EIGRP routes marked by the letter D. 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
D     3.0.0.0/8 [90/409600] via 2.2.2.1, 00:00:02, Ethernet0/0
```

CHAPTER 6

# Control Router Access with Passwords and Privilege Levels

One of the restriction for controlling router access with passwords and privileges is - disabling password recovery does not work if you have set the router to boot up manually by using the **boot manual** global configuration command. This command produces the boot loader prompt (*router:*) after the router is power cycled.


- Restrictions and Guidelines for Reversible Password Types, on page 99
- Restrictions and Guidelines for Irreversible Password Types, on page 100
- Information About Controlling Router Access with Passwords and Privileges, on page 100
- How to Configure Switch Access with Passwords and Privileges, on page 103
- Monitoring Switch Access with Passwords and Privileges, on page 114
- Configuration Examples for Switch Access with Passwords and Privilege Levels, on page 114
- Additional References for Switch Access with Passwords and Privilege Levels, on page 115
- Feature Information for Controlling Router Access with Passwords and Privileges, on page 115


## Restrictions and Guidelines for Reversible Password Types

- Password type 0 and 7 are replaced with password type 6. So password type 0 and 7, which were used for administrator login to the console, Telnet, SSH, webUI, and NETCONF must be migrated to password type 6. No action is required if username and password are type 0 and 7 for local authentication such as CHAP, EAP, and so on.

**Note** Type 6 encrypted password and Autoconversion to password type 6 are supported from is supported from Cisco IOS XE Amsterdam 17.2 and later releases.

- If the startup configuration of the device has type 6 password and you downgrade to a version in which type 6 password is not supported, you will be locked out of the device.

# Restrictions and Guidelines for Irreversible Password Types

- Username secret password type 5 and enable secret password type 5 must be migrated to the stronger password type 8 or 9. For more information, see Protecting Enable and Enable Secret Passwords with Encryption, on page 104.
- If the startup configuration of the device has convoluted type 9 secret (password that starts with $14$), then a downgrade can only be performed to a release in which the convoluted type 9 secret is supported. Convoluted type 9 secret is supported in Cisco IOS XE Gibraltar 16.11.2 and later releases. If the startup configuration has convoluted type 9 secret and you downgrade to any release earlier than Cisco IOS XE Amsterdam 17.2.1, you will be locked out of the device.

  Before you downgrade to any release in which convoluted type 9 secret is not supported, ensure that the type 9 secret (password that starts with $9$) must be part of the startup configuration instead of convoluted type 9 secret (password that starts with $14$) or type 5 secret (password that starts with $1$).

  If a device is upgraded from Cisco IOS XE Fuji 16.9.x, Cisco IOS XE Gibraltar 16.10.x, or Cisco IOS XE Gibraltar 16.11.x to Cisco IOS XE Gibraltar 16.12.x, the type 5 secret is auto-converted to convoluted type 9 secret (password that starts with $14$). For example: `username user1 secret 5 $1$dNmW$7jWhqdtZ2qBVz2R4CSZZC0` is auto-converted to `username user1 secret 9 $14$dNmW$QykGZEEGmiEGrE$C9D/fD0czicOtgaZAa1CTa2sgygi0Leyw3/cLqPY426`. After the device is upgraded, run the **write memory** command in privileged EXEC mode for the convoluted type 9 secret to be permanently written into the startup configuration.
- Plain text passwords are converted to nonreversible encrypted password type 9.

**Note** This is supported in Cisco IOS XE Amsterdam 17.2.1 and later releases.

- Secret password type 4 is not supported.

# Information About Controlling Router Access with Passwords and Privileges

This section provides information about controlling router access with passwords and privileges.

## Preventing Unauthorized Access

You can prevent unauthorized users from reconfiguring your switch and viewing configuration information. Typically, you want network administrators to have access to your switch while you restrict access to users who dial from outside the network through an asynchronous port, connect from outside the network through a serial port, or connect through a terminal or workstation from within the local network.

To prevent unauthorized access into your switch, you should configure one or more of these security features:

- At a minimum, you should configure passwords and privileges at each switch port. These passwords are locally stored on the switch. When users attempt to access the switch through a port or line, they must enter the password specified for the port or line before they can access the switch.

- For an additional layer of security, you can also configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.
- If you want to use username and password pairs, but you want to store them centrally on a server instead of locally, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if necessary, authorization) information.
- You can also enable the login enhancements feature, which logs both failed and unsuccessful login attempts. Login enhancements can also be configured to block future login attempts after a set number of unsuccessful attempts are made.

# Default Password and Privilege Level Configuration

A simple way of providing terminal access control in your network is to use passwords and assign privilege levels. Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.

This table shows the default password and privilege level configuration.

***Table 8: Default Password and Privilege Levels***

| Feature | Default Setting |
|---|---|
| Enable password and privilege level | No password is defined. The default is level 15 (privileged EXEC level). The password is not encrypted in the configuration file. |
| Enable secret password and privilege level | No password is defined. The default is level 15 (privileged EXEC level). The password is encrypted before it is written to the configuration file. |
| Line password | No password is defined. |

# Additional Password Security

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use either the **enable password** or **enable secret** global configuration commands. Both commands accomplish the same thing; that is, you can establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify.

We recommend that you use the **enable secret** command because it uses an improved encryption algorithm.

If you configure the **enable secret** command, it takes precedence over the **enable password** command; the two commands cannot be in effect simultaneously.

If you enable password encryption, it applies to all passwords including username passwords, authentication key passwords, the privileged command password, and console and virtual terminal line passwords.

# Password Recovery

By default, any end user with physical access to the switch can recover from a lost password by interrupting the boot process while the switch is powering on and then by entering a new password.

The password-recovery disable feature protects access to the switch password by disabling part of this functionality. When this feature is enabled, the end user can interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, you can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted.

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

To re-enable password recovery, use the **service password-recovery** global configuration command.

# Terminal Line Telnet Configuration

When you power-up your switch for the first time, an automatic setup program runs to assign IP information and to create a default configuration for continued use. The setup program also prompts you to configure your switch for Telnet access through a password. If you did not configure this password during the setup program, you can configure it when you set a Telnet password for a terminal line.

# Username and Password Pairs

You can configure username and password pairs, which are locally stored on the switch. These pairs are assigned to lines or ports and authenticate each user before that user can access the switch. If you have defined privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.

# Privilege Levels

Cisco devices use privilege levels to provide password security for different levels of switch operation. By default, the Cisco IOS XE software operates in two modes (privilege levels) of password security: user EXEC (Level 1) and privileged EXEC (Level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring multiple passwords, you can allow different sets of users to have access to specified commands.

### Privilege Levels on Lines

Users can override the privilege level you set using the **privilege level** line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

For example, if you want many users to have access to the **clear line** command, you can assign it level 2 security and distribute the level 2 password fairly widely. But if you want more restricted access to the **configure** command, you can assign it level 3 security and distribute that password to a more restricted group of users.

### Command Privilege Levels

When you set a command to a privilege level, all commands whose syntax is a subset of that command are also set to that level. For example, if you set the **show ip traffic** command to level 15, the **show** commands and **show ip** commands are automatically set to privilege level 15 unless you set them individually to different levels.

## AES Password Encryption and Primary Encryption Keys

You can enable strong, reversible 128-bit Advanced Encryption Standard (AES) password encryption, also known as type 6 encryption. To start using type 6 encryption, enable the AES Password Encryption feature and configure a primary encryption key to encrypt and decrypt passwords.

After you enable AES password encryption and configure a primary key, all the existing and newly created cleartext passwords for the supported applications are stored in type 6 encrypted format, unless you disable type 6 password encryption. You can also configure the device to convert all the existing weakly encrypted passwords to type 6 encrypted passwords.

Type 0 and 7 passwords can be autoconverted to type 6 if the AES Password Encryption feature and primary encryption key are configured.

**Note** Type 6 username and password are backward compatible to Cisco IOS XE Gibraltar 16.10.x. If you downgrade to any release earlier than Cisco IOS XE Gibraltar 16.10.1, the type 6 username and password are rejected. After autoconversion, to prevent an administrator password from getting rejected during a downgrade, migrate the passwords used for administrator logins (management access) to irreversible password types manually.

# How to Configure Switch Access with Passwords and Privileges

## Setting or Changing a Static Enable Password

The enable password controls access to the privileged EXEC mode. Follow these steps to set or change a static enable password:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **enable password** *password*<br>**Example:**<br>`Device(config)# enable password secret321` | Defines a new password or changes an existing password for access to privileged EXEC mode.<br>By default, no password is defined.<br>For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. It can contain the question mark (?) character if you precede the question mark with the key combination Crtl-v when you create the password; for example, to create the password abc?123, do this:<br>**a.** Enter **abc**.<br>**b.** Enter **Crtl-v**.<br>**c.** Enter **?123**.<br>When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Protecting Enable and Enable Secret Passwords with Encryption

Follow these steps to establish an encrypted password that users must enter to access privileged EXEC mode (the default) or any privilege level you specify:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password, if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | Use one of the following:<br>• **enable password** [**level** *level*] {*unencrypted-password* \| *encryption-type encrypted-password*}<br>• **enable secret** [**level** *level*] {*unencrypted-password* \| *encryption-type encrypted-password*}<br>**Example:**<br>`Device(config)# enable password level 12 example123`<br>or<br>`Device(config)# enable secret 9 $9$sMLBsTFXLnnHTk$0L82` | • Defines a new password or changes an existing password for access to privileged EXEC mode.<br>• Defines a secret password, which is saved using a nonreversible encryption method.<br>• (Optional) For *level*, the range is from 0 to 15. Level 1 is normal user EXEC mode privileges. The default level is 15 (privileged EXEC mode privileges).<br>• For *unencrypted-password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined.<br>• For *encryption-type*, the available options for **enable password** are type 0 and 7, and type 0, 5, 8, and 9 for **enable secret**. If you specify an encryption type, you must provide an encrypted password—an encrypted password that you copy from another switch configuration. Secret encryption type 9 is more secure, so we recommend that you select type 9 to avoid any issues while upgrading or downgrading. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note**<br>• If you do not specify an encryption type for the secret password, the password is auto converted to type 9. This is applicable in Cisco IOS XE Gibraltar 16.10.1 and later releases.<br>• If you specify an encryption type and then enter a clear text password, it will result in an error.<br>• You can also configure type 9 encryption for the secret password manually by using the **algorithm-type scrypt** command in global configuration mode. For example:<br>`Device(config)# username user1 algorithm-type scrypt secret cisco`<br>Or<br>`Device(config)# enable algorithm-type scrypt secret cisco`<br>Run the **write memory** command in privileged EXEC mode for the type 9 secret to be permanently written into the startup configuration. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **service password-encryption**<br>**Example:**<br>`Device(config)# service password-encryption` | (Optional) Encrypts the password when the password is defined or when the configuration is written.<br>Encryption prevents the password from being readable in the configuration file. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Disabling Password Recovery

Follow these steps to disable password recovery to protect the security of your switch:

### Before you begin

If you disable password recovery, we recommend that you keep a backup copy of the configuration file on a secure server in case the end user interrupts the boot process and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch. If the switch is operating in VTP transparent mode, we recommend that you also keep a backup copy of the VLAN database file on a secure server. When the switch is returned to the default system configuration, you can download the saved files to the switch by using the Xmodem protocol.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **system disable password recovery switch** {*all* \| *<1-9>*}<br>**Example:**<br>`Device(config)# system disable password recovery switch all` | Disables password recovery.<br>• *all*: Sets the configuration on switches in stack.<br>• *<1-9>*: Sets the configuration on the switch number selected. |

| | Command or Action | Purpose |
|---|---|---|
| | | This setting is saved in an area of the flash memory that is accessible by the boot loader and the Cisco IOS image, but is not a part of the file system and is not accessible by any user. |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

### What to do next

To remove **disable password recovery**, use the **no system disable password recovery switch all** global configuration command.

# Setting a Telnet Password for a Terminal Line

Beginning in user EXEC mode, follow these steps to set a Telnet password for the connected terminal line:

### Before you begin

- Attach a PC or workstation with emulation software to the switch console port, or attach a PC to the Ethernet management port.
- The default data characteristics of the console port are 9600, 8, 1, no parity. You might need to press the Return key several times to see the command-line prompt.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **line vty 0 15**<br>**Example:**<br>`Device(config)# line vty 0 15` | Configures the number of Telnet sessions (lines), and enters line configuration mode.<br>There are 16 possible sessions on a command-capable device. The 0 and 15 mean that you are configuring all 16 possible Telnet sessions. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **password** *password*<br>**Example:**<br>`Device(config-line)# password abcxyz543` | Sets a Telnet password for the line or lines.<br>For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-line)# end` | Returns to privileged EXEC mode. |

# Configuring Username and Password Pairs

Follow these steps to configure username and password pairs:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **username** *name* [**privilege** *level*] {**password** *encryption-type password*}<br>**Example:**<br>`Device(config)# username adamsample privilege 1 password secret456`<br>`Device(config)# username 111111111111 mac attribute` | Sets the username, privilege level, and password for each user.<br>• For *name*, specify the user ID as one word or the MAC address. Spaces and quotation marks are not allowed.<br>• You can configure a maximum of 12000 clients each, for both username and MAC filter.<br>• (Optional) For *level*, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 1 gives user EXEC mode access. |

| | Command or Action | Purpose |
|---|---|---|
| | | • For *encryption-type*, enter **0** to specify that an unencrypted password will follow. Enter **7** to specify that a hidden password will follow. Enter **6** to specify that an encrypted password will follow.<br>• For *password*, specify the password the user must enter to gain access to the device. The password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command. |
| **Step 4** | Use one of the following:<br>• **line console 0**<br>• **line vty 0 15**<br>**Example:**<br>`Device(config)# line console 0`<br>or<br>`Device(config)# line vty 15` | Enters line configuration mode, and configures the console port (line 0) or the VTY lines (line 0 to 15). |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-line)# end` | Exits line configuration mode and returns to privileged EXEC mode. |

# Setting the Privilege Level for a Command

Follow these steps to set the privilege level for a command:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **privilege** *mode* **level** *level command* | Sets the privilege level for a command. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Device(config)# privilege exec level 14 configure` | • For *mode*, enter **configure** for global configuration mode, **exec** for EXEC mode, **interface** for interface configuration mode, or **line** for line configuration mode.<br>• For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password.<br>• For *command*, specify the command to which you want to restrict access. |
| **Step 4** | **enable password level** *level password*<br>**Example:**<br>`Device(config)# enable password level 14 SecretPswd14` | Specifies the password to enable the privilege level.<br>• For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges.<br>• For *password*, specify a string from 1 to 25 alphanumeric characters. The string cannot start with a number, is case sensitive, and allows spaces but ignores leading spaces. By default, no password is defined. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Changing the Default Privilege Level for Lines

Follow these steps to change the default privilege level for the specified line:

**Procedure**

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **line vty** *line*<br>**Example:**<br>`Device(config)# line vty 10` | Selects the virtual terminal line on which to restrict access. |
| **Step 4** | **privilege exec level** *level*<br>**Example:**<br>`Device(config-line)# privilege exec level 15` | Changes the default privilege level for the line.<br>For *level*, the range is from 0 to 15. Level 1 is for normal user EXEC mode privileges. Level 15 is the level of access permitted by the **enable** password. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config-line)# end` | Exits line configuration mode and returns to privileged EXEC mode. |

### What to do next

Users can override the privilege level you set using the **privilege level** line configuration command by logging in to the line and enabling a different privilege level. They can lower the privilege level by using the **disable** command. If users know the password to a higher privilege level, they can use that password to enable the higher privilege level. You might specify a high level or privilege level for your console line to restrict line usage.

# Logging in to and Exiting a Privilege Level

Beginning in user EXEC mode, follow these steps to log into a specified privilege level and exit a specified privilege level.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** *level*<br>**Example:**<br>`Device> enable 15` | Logs in to a specified privilege level.<br>InI the example, Level 15 is privileged EXEC mode.<br>For *level*, the range is 0 to 15. |
| **Step 2** | **disable** *level*<br>**Example:**<br>`Device# disable 1` | Exits to a specified privilege level.<br>In the example, Level 1 is user EXEC mode.<br>For *level*, the range is 0 to 15. |

# Configuring an Encrypted Preshared Key

To configure an encrypted preshared key, perform the following steps.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **key config-key password-encrypt** [*text*]<br>**Example:**<br>`Device(config)# key config-key password-encrypt` | Stores a type 6 encryption key in private NVRAM.<br>• To key in interactively (using the **Enter** key) and an encrypted key already exists, you will be prompted for the following: Old key, New key, and Confirm key.<br>• To key in interactively, but an encryption key is not present, you will be prompted for the following: New key and Confirm key.<br>• When removing the password that is already encrypted, you will see the following prompt:<br>`WARNING: All type 6 encrypted keys will become unusable. Continue with master key deletion? [yes/no]:"` |
| **Step 4** | **password encryption aes**<br>**Example:**<br>`Device(config)# password encryption aes` | Enables the encrypted preshared key. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Exits global configuration mode and returns to privileged EXEC mode. |

# Monitoring Switch Access with Passwords and Privileges

*Table 9: Commands for Displaying Privilege-Level Information*

| Command | Information |
|---|---|
| **show privilege** | Displays the privilege level configuration. |

# Configuration Examples for Switch Access with Passwords and Privilege Levels

## Example: Setting or Changing a Static Enable Password

The following example shows how to change the enable password to *l1u2c3k4y5*. The password is not encrypted and provides access to level 15 (traditional privileged EXEC mode access):

```
Device> enable
Device# configure terminal
Device(config)# enable password l1u2c3k4y5
Device(config)# end
```

## Example: Protecting Enable and Enable Secret Passwords with Encryption

The following example shows how to configure the encrypted password *$9$sMLBsTFXLnnHTk$0L82* for privilege level 2:

```
Device> enable
Device# configure terminal
Device(config)# enable secret level 2 9 $9$sMLBsTFXLnnHTk$0L82
Device(config)# end
```

## Example: Setting a Telnet Password for a Terminal Line

The following example shows how to set the Telnet password to *let45me67in89*:

```
Device> enable
Device# configure terminal
Device(config)# line vty 10
Device(config-line)# password let45me67in89
Device(config-line)# end
```

## Example: Setting the Privilege Level for a Command

The following example shows how to set the **configure** command to privilege level 14 and define *SecretPswd14* as the password users must enter to use level 14 commands:

```
Device> enable
Device# configure terminal
Device(config)# privilege exec level 14 configure
Device(config)# enable password level 14 SecretPswd14
Device(config)# end
```

## Example: Configuring an Encrypted Preshared Key

The following example shows a configuration for which a type 6 preshared key has been encrypted. It includes the prompts and messages that a user might see.

```
Device> enable
Device# configure terminal
Device(config)# password encryption aes
Device(config)# key config-key password-encrypt
New key:
Confirm key:
Device(config)#
01:46:40: TYPE6_PASS: New Master key configured, encrypting the keys with
the new master key
Device(config)# end
```

# Additional References for Switch Access with Passwords and Privilege Levels

### Technical Assistance

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

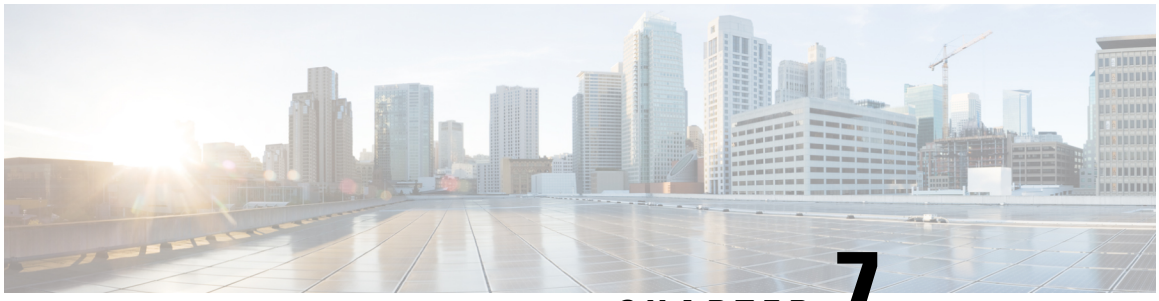
# Feature Information for Controlling Router Access with Passwords and Privileges

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

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

*Table 10: Feature Information for Controlling Router Access with Passwords and Privileges*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Controlling Switch Access with Passwords and Privileges | Cisco IOS XE Amsterdam 17.2.1r | Password protection restricts access to a network or network device. Privilege levels define what commands users can enter after they have logged into a network device.<br><br>Additionally, type 0 and type 7 Username and Password can be autoconverted to type 6. |



CHAPTER 7

# Change of Authorization

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated.

Identity-Based Networking Services supports change of authorization (CoA) commands for session query, reauthentication, and termination, port bounce and port shutdown, and service template activation and deactivation.


- Feature Information for Change of Authorization, on page 117
- Information About Change of Authorization, on page 118
- Restrictions for Change of Authorization, on page 120
- How to Configure Change of Authorization, on page 121
- Configuration Examples for Change of Authorization, on page 122


# Feature Information for Change of Authorization

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

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

***Table 11: Feature Information for Change of Authorization***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Change of Authorization | Cisco IOS XE Amsterdam 17.4.1 | The Change of Authorization<br>The following commands were introduced by this feature: **show aaa servers**, **show aaa group radius**, **show device-tracking policies**, **show device-tracking database show access-session interface** *interface-name* |
| Change of Authorization | Cisco IOS XE Amsterdam 17.3.1a | The Change of Authorization<br>The following commands were introduced by this feature: **show ip access-lists**, **show ip access-list interface** , **debug epm plugin acl event**, **debug epm plugin acl errors** |

# Information About Change of Authorization

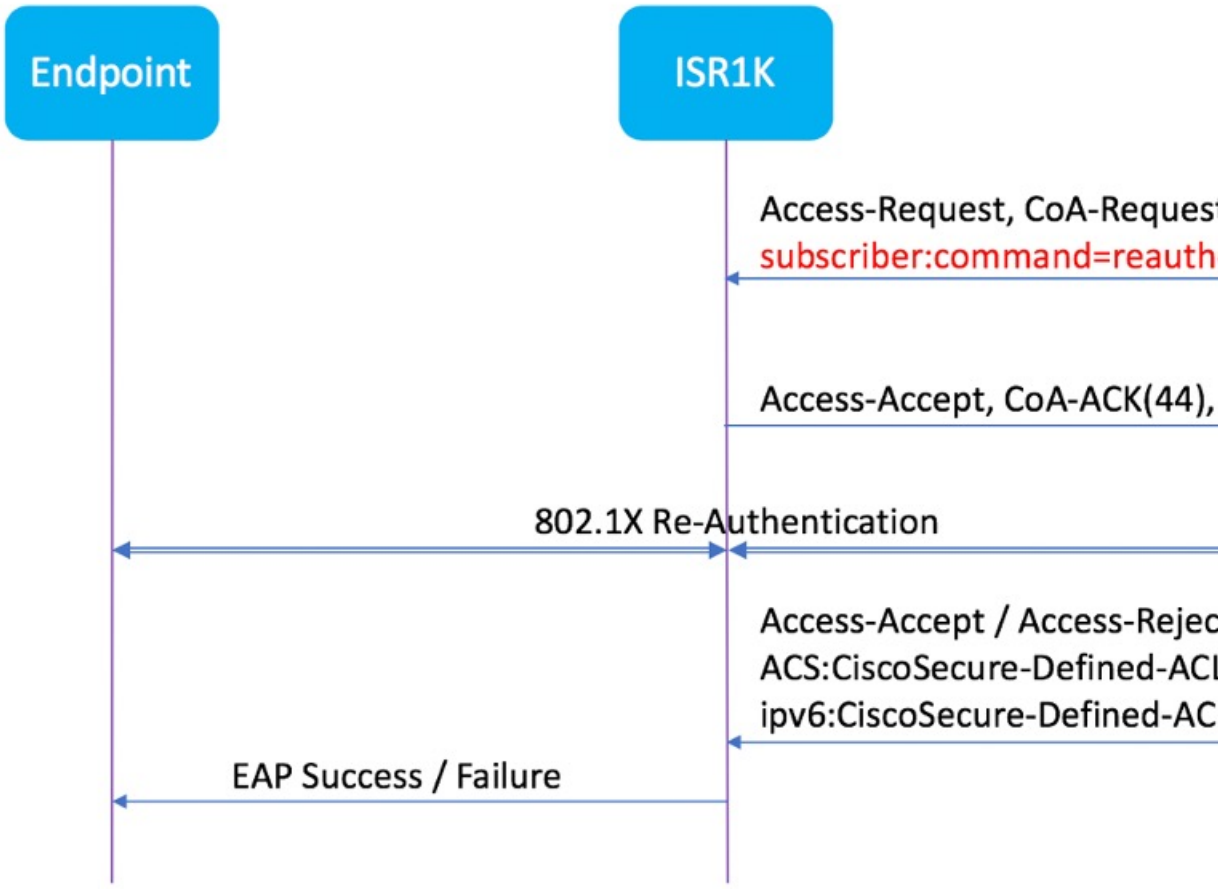
## Change of Authorization-Reauthentication Procedure

Change of Authorization (CoA) provides a mechanism to change the attributes of an authentication, authorization, and accounting (AAA) session after it is authenticated. The main steps in this procedure are:

- Authentication
- Posture Assessment
- CoA Re-Authentication
- Network Access Authorization

When a policy changes for a user or user group in AAA, administrators can send RADIUS CoA packets from the AAA server, such as a Cisco Identity Secure Engine (ISE) to reinitialize authentication and apply the new policy. This section provides an overview of the RADIUS interface including available primitives and how they are used during a CoA.

The RADIUS CoA provides a mechanism to change the attributes of an AAA session after it is authenticated. When policy changed on user or user group in RADIUS server, administrators can initiate RADIUS CoA process from RADIUS server to re-authenticate or re-authorize new policy




By default, the RADIUS interface is enabled on the device. However, some basic configuration is required for the following attributes:

- Security and Password
- Accounting

After posture assessment is succeessful, full network access is pushed down to the device for specific client through CoA re-authentication command based on its compliance state derived from last assessment. It is optional to enforce downloadable ACLs with Permit-ALL or limited access to certain resources to corresponding clients. Per-session CoA requests are supported for session identification, session termination, host reauthentication, port shutdown, and port bounce. This model comprises one request (CoA-Request) and two possible response codes:

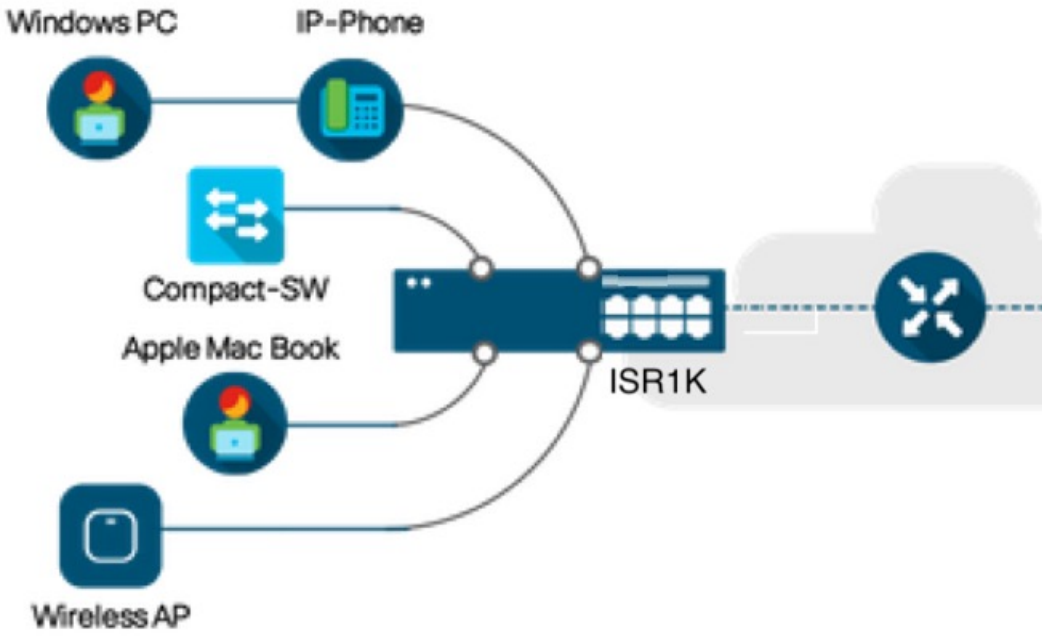
- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

# Change of Authorization

Change of Authorization (CoA) is a critical part of a solution to initiate re-authenticate or re-authorization to an endpoint's network access based on its posture assessment result. This feature is integrated with Cisco AnyConnect, version 4.8 and Cisco ISE, version 2.6.

The network topology below shows a typical Cisco 1000 Series Integrated Services Router as a branch router in a network for secure access with ISE and other network services deployed in Campus or Data Center.

***Figure 1: Cisco ISR1000 in a Network for Secure Access with ISE and other Network Services***




CoA is critical part of the solution to initiate re-authenticate or re-authorization to endpoint's network access based on its posture assessment result. Downloadable ACL is the Target/Purpose of the entire solution. The per-client basis customized security policies are achieved by it.

# Restrictions for Change of Authorization

- Only 8 ports SKUs have TCAM to support DACL and Redirect ACL
- xACL can only match exact value(>,<,>=,<= are not supported)
- Switch ASIC TCAM has only 255 entries (IPv4 ACL entries) in total
- No IPv4 option header support, no IP fragment support in ACL packet inspection
- IPv6 is not supported in this feature
- Port ACL is not supported in this feature
- SISF: Only support none-secure device-tracking (tracking policy with security level 'glean')
- Multi-auth vlan is not supported on Cisco 1000 Series Integrated Services Routers

- Tracking is not getting replaced by ‘enable tracking‘
- VLAN change does not happen consistently with multiple iterations on client interfaces

# How to Configure Change of Authorization

## Essential dot1x | SANet Configuration

```
aaa new-model
aaa authentication dot1x default group coa-ise
aaa authorization network default group coa-ise
dot1x system-auth-control
aaa group server radius coa-ise
 server name coa
radius server coa
 address ipv4 10.10.1.10 auth-port 1812 acct-port 1813
 key cisco123
policy-map type control subscriber simple_coa
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
interface gigabitethernet0/0/1
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticator
service-policy type control subscriber simple_coa
```

## Configure Change of Authorization

```
aaa server radius dynamic-author
 client
 server-key ******
 auth-type any
 ignore server-key
ip access-list extended redirect_acl
 20 deny udp any eq bootps any
 25 deny udp any eq domain any
 30 deny udp any any eq bootpc
 40 deny udp any eq bootpc any
 50 deny ip any host %{ise.ip}
 60 permit tcp any any eq www
 70 permit tcp any any eq 443
device-tracking tracking
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
interface 0/0/1
 device-tracking attach-policy tracking_test
```

# Configuration Examples for Change of Authorization

## Example: Check if the RADIUS Server is Active

```
Device# show aaa servers
RADIUS: id 1, priority 1, host 10.75.28.231, auth-port 1812, acct-port 1813, hostname host
     State: current UP, duration 188755s, previous duration 0s
     Dead: total time 0s, count 0
     Platform State from SMD: current UP, duration 188755s, previous duration 0s
```

## Example: Device Tracking Policy

```
Device# show aaa group radius coa3 **** port 1813 new-code
User successfully authenticated
USER ATTRIBUTES
username             0   "coa3"
```

To check if the parameters are enabled:

```
Device# show device-tracking policies
Target               Type  Policy               Feature        Target range
Gi0/1/1              PORT  tracking_test        Device-tracking vlan all
Gi0/1/2              PORT  tracking_test        Device-tracking vlan all
Gi0/1/3              PORT  tracking_test        Device-tracking vlan all
Gi0/1/4              PORT  tracking_test        Device-tracking vlan all
```

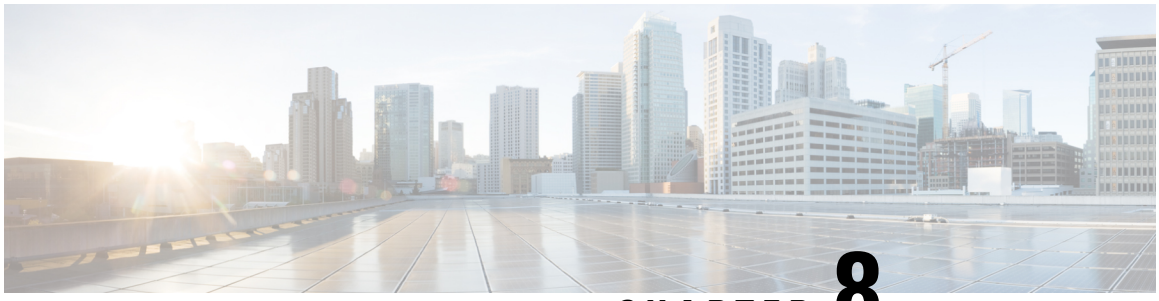
To check the SISF table:

```
Device# show device-tracking database
Binding Table has 1 entries, 1 dynamic (limit 100000)
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned
Network Address        Link Address       Interface  vlan  prlvl    age    state       Time
 left
ARP 10.11.22.20       0050.5683.3f97      Gi0/1/4     22    0005    11s   REACHABLE
295 s
```

To check if the access-session is authenticated and autorized:

```
Device# show access-session interface gigabitEthernet 0/1/7 detail
            Interface:  GigabitEthernet0/1/7
               IIF-ID:  0x0DB9315A
          MAC Address:  b496.913d.4f9b
         IPv6 Address:  Unknown
         IPv4 Address:  10.10.22.27
            User-Name:  coa2
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  611C4B0A00000053F483D7B0
```

```
   Acct Session ID:  Unknown
            Handle:  0x21000049
    Current Policy:  POLICY_COA
Server Policies:  Filter-ID: Filter_ID_COA2
Method status list:  Method           State
                     dot1x           Authc Success
```



CHAPTER 8

# Console Port, Telnet, SSH Handling, and Reset Button

This chapter contains the following sections:


- Restrictions and Notes for Console Port, Telnet, and SSH, on page 125
- Console Port Overview, on page 125
- Console Port Handling Overview, on page 125
- Telnet and SSH Overview, on page 126
- Reset Button Overview, on page 126
- Configuring a Console Port Transport Map, on page 129
- Viewing Console Port, SSH, and Telnet Handling Configurations, on page 131
- Configuring Console Port for Modem Connection , on page 133


## Restrictions and Notes for Console Port, Telnet, and SSH

- 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.

## Console Port Overview

The console port on the router is an EIA/TIA-232 asynchronous, serial connection with no flow control and an RJ-45 connector. The console port is used to access the router and is located on the front panel of the Route Processor.

For information on accessing the router using the console port, see Using Cisco IOS XE Software, on page 3.

## Console Port Handling Overview

If you are using the console port to access the router, you are automatically directed to the Cisco IOS command-line interface (CLI).

If you are trying to access the router through the console port and send a break signal (by entering **Ctrl-C** or **Ctrl-Shift-6**, or by entering the **send break** command at the Telnet prompt) before connecting to the CLI, you are directed to a diagnostic mode if the non-RPIOS subpackages are accessible. These settings can be changed by configuring a transport map for the console port and applying that transport map to the console interface.

# Telnet and SSH Overview

Telnet and SSH on the router can be configured and handled like Telnet and SSH on other Cisco platforms. For information on traditional Telnet, see the line command in the Cisco IOS Terminal Services Command Reference, Release 12.2 document.

For information on configuring traditional SSH, see the "Configuring Secure Shell" chapter in the Cisco IOS Terminal Services Command Reference, Release 12.2 document.

# Reset Button Overview

The Reset button functionality is configured on all Cisco 1000 Series Integrated Services Routers (ISRs) by default. You can use the Reset button to recover Cisco 1000 Series ISRs that become non-responsive due to incorrect configuration or when users are unable to login due to incorrect credentials.

## Information About Reset Button Functionality

To enable the Reset button functionality on these devices, configure the device with the password recovery service using the **service password-recovery** command, and to disable the feature, use either the **no service password-recovery** command or the **no service password-recovery strict** command.

You can enable the Reset button feature on the device only under any of these scenarios:

- during hardware initialization, or
- after the device is powered on, or
- at the **reload** command

In Cisco IOS XE Gibraltar 16.12 releases and earlier, you can enable the Reset button feature only if you use **service password-recovery** configuration. However, to disable the feature, use the **no service password-recovery** or **no service password-recovery strict** configurations.

From Cisco IOS XE Amsterdam 17.2.1r release and later, the Reset button feature is entirely disabled with the **no service password-recovery strict** configuration.

Below are the tables that show the behavior of the Reset button feature in various possible combinations under service password recovery and no service password recovery:

***Table 12: Service Password-Recovery***

| **Press Reset Button (STATUS)** | | | | **Behavior** | | | |
|---|---|---|---|---|---|---|---|
| **Sl. No** | **Golden Image** | **Golden Config** | **Start up config** | **Image** | **Config** | **Extra** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | Exists | Exists | Exists | Golden | Golden | - |
| 2 | Exists | Exists | None | Golden | Golden | - |
| 3 | Exists | None | Exists | Golden | PnP | Delete startup |
| 4 | Exists | None | None | Golden | PnP | - |
| 5 | None | Exists | Exists | Standard | Golden | - |
| 6 | None | Exists | None | Standard | Golden | - |
| 7 | None | None | Exists | Standard | PnP | Delete startup |
| 8 | None | None | None | Standard | PnP | - |

*Table 13: No Service Password-Recovery*

| **Press Reset Button (STATUS)** | | | | **Behavior** | | |
|---|---|---|---|---|---|---|
| **Sl. No** | **Golden Image** | **Golden Config** | **Start up config** | **Image** | **Config** | **Extra** |
| 1 | Exists | In NVRAM | Exists | Golden | PnP | Wipe |
| 2 | Exists | In Bootflash | Exists | Golden | Golden | Wipe |
| 3 | Exists | In NVRAM | None | Golden | PnP | Wipe |
| 4 | Exists | In Bootflash | None | Golden | Golden | Wipe |
| 5 | Exists | None | Exists | Golden | PnP | Wipe |
| 6 | Exists | None | None | Golden | PnP | Wipe |
| 7 | None | In NVRAM | Exists | Standard | PnP | Wipe |
| 8 | None | In Bootflash | Exists | Standard | Golden | Wipe |
| 9 | None | In NVRAM | None | Standard | PnP | Wipe |
| 10 | None | In Bootflash | None | Standard | Golden | Wipe |
| 11 | None | None | Exists | Standard | PnP | Wipe |
| 12 | None | None | None | Standard | PnP | Wipe |

## Prerequisites for Enabling the Reset Button Functionality

- Ensure that the ROMmon version on the device is at least 17.2(1r)
- Ensure to configure the golden.bin image and golden.cfg configuration.

## Restrictions for Reset Button in Controller Mode

- Thereset button can erase all SD-WAN configuration, or apply available ciscosdwan.cfg configuration as the default configuration in Cisco 1000 Series ISR devices. The reset button first attempts to boot the golden.bin image if available. If the golden.bin image is not available, the next attempt is the default bootup configuration. The golden.bin image is not mandatory for the reset feature. This functionality is supported in controllermode for the following releases:
  - Cisco IOS XE 17.6.x
  - Cisco IOS XE 17.8.x, and higher releases
- The Reset button must be entered immediately after setup is reset to ROMMON under auto reboot mode. The Reset feature does not work when the system is configured in ROMMON or IOS modes.

# How to Enable the Reset Button Functionality

This task describes how to enable Reset button feature on the Cisco 1000 Series ISR device:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **service password-recovery**<br>**Example:**<br>`Device(config)# service password-recovery` | Configures the password recovery service on the device. |
| **Step 3** | **no service password-recovery**<br>**Example:**<br>`Device(config)# no service password-recovery` | (Optional) Disables the Reset button feature on the device.<br>You can recover the non-responsive device; however, the device is reconfigured because all user configurations and keys are deleted.<br>**Note** Ensure that the device has a golden.bin and golden.cfg configurations on the device as a recovery mechanism so that the startup-config file on the IOS NVRAM is not deleted. |
| **Step 4** | **exit**<br>**Example:**<br>`Device(config)# exit` | Exits the configuration mode and returns to the priviledge exec mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **no service recovery-service strict**<br>**Example:**<br>`Device(config)# no service recovery-service strict`**`exit`** | Disables the Reset button feature on the device.<br>**Note** From Cisco IOS XE Amsterdam 17.2 release and later, if you use the **no service recovery-service strict** command, even with a golden.bin or golden.cfg configuration on the device, you will not be able to recover the device, and therefore has to be returned and replaced through Return Material Authorization (RMA) to Cisco. |

# Example: Enable and Disable the Reset Button Functionality

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Device(config)# service password-recovery
Executing this command enables the password recovery mechanism.
Device(config)#

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# no service password-recovery

WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.

Are you sure you want to continue? [yes]: yes
Device(config)#
```

# Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

### Procedure

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **transport-map type console** *transport-map-name*<br>**Example:**<br>`Router(config)# transport-map type console consolehandler` | Creates and names a transport map for handling console connections, and enters transport map configuration mode. |
| **Step 4** | **connection wait** [**allow** [**interruptible**] \| **none** [**disconnect**]]<br>**Example:**<br>`Router(config-tmap)# connection wait none` | Specifies how a console connection will be handled using this transport map.<br>• **allow interruptible**—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting.<br>**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.<br>• **none**—The console connection immediately enters diagnostic mode. |
| **Step 5** | (Optional) **banner** [**diagnostic** \| **wait**] *banner-message*<br>**Example:**<br>`Router(config-tmap)# banner diagnostic X`<br>`Enter TEXT message. End with the character 'X'.`<br>`--Welcome to Diagnostic Mode--`<br>`X`<br>`Router(config-tmap)#` | (Optional) Creates a banner message that will be seen by users entering diagnostic mode or waiting for the Cisco IOS VTY line because of the console transport map configuration.<br>• **diagnostic**—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.<br>**Note** Users can interrupt a waiting connection by entering **Ctrl-C** or **Ctrl-Shift-6**.<br>• **wait**—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.<br>• *banner-message*—Banner message, which begins and ends with the same delimiting character. |
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-tmap)# exit` | Exits transport map configuration mode to re-enter global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **transport type console** *console-line-number* **input** *transport-map-name*<br>**Example:**<br>`Router(config)# transport type console 0 input consolehandler` | Applies the settings defined in the transport map to the console interface.<br>The *transport-map-name* for this command must match the *transport-map-name* defined in the **transport-map type console** command. |

### Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

# Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- **show transport-map**
- **show platform software configuration access policy**

Use the **show transport-map** command to view transport map configurations.

**show transport-map** [**all** | **name** *transport-map-name* | **type** [**console** ]]

This command can be used either in user EXEC mode or privileged EXEC mode.

### Example

The following example shows transport maps that are configured on the router: console port (`consolehandler`):

```
Router# show transport-map allTransport 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 consoleTransport 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 sshTransport 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 policyThe 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 :
```

# Configuring Console Port for Modem Connection

Cisco 1100 Series router supports connecting a modem to the router console port for EXEC dial in connectivity. When a modem is connected to the console port, a remote user can dial in to the router and configure it. To configure a modem on the console port, perform these steps:

### Procedure

**Step 1** Connect the RJ-45 end of the adapter cable to the console port on the router.

**Step 2** Use the **show line** command to determine the async interface of the console port:

```
Router# show  line

 Router#show line
Tty Line Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
* 0 0 CTY - - - - - 0 0 0/0 -
866 866 VTY - - - - - 0 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 -
```

**Step 3** Use the following commands to configure the router console line::

```
Router(config)# line con 0

Router(config-line)#modem inOut
Router(config-line)#modem autoconfigure type usr_sportster
Router(config-line)#speed 115200  [Speed to be set according to the modem manual]
Router(config-line)#stopbits 1 [Stopbits to be set according to the modem manual]
Router(config-line)#transport input all
Router(config-line)#flowcontrol hardware [flowcontrol to be set according to the modem
manual]
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#end
Router(config)#enable password lab
```

**Step 4** Use the reverse telnet method on the modem to verify the modem connectivity and configuration string:

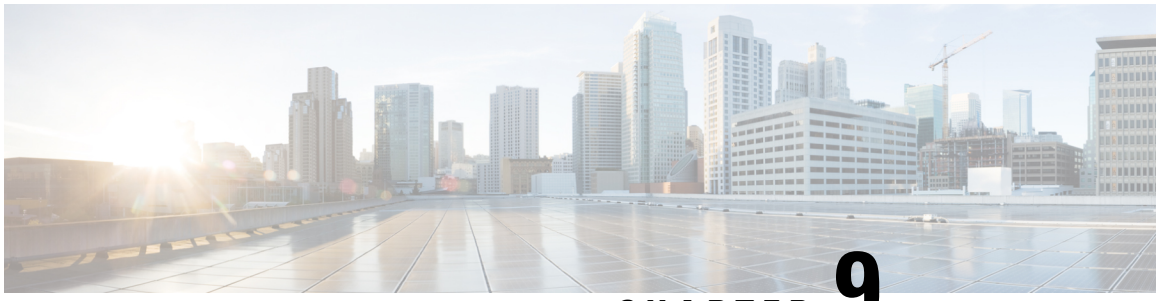
```
Router(config)#int loopback 0
Router(config-if)#ip add 192.0.2.1 255.255.255.0
Router(config-if)#end
Router#telnet 192.0.2.1 2001
Trying 1.1.1.1, 2001 ... Open

User Access Verification

Password: <enter the password given under line configuration>

at    <<<=== Modem command
OK  <<<=== This OK indicates that the modem is connected successully to the console port.
```

**Step 5** Use an analog phone to verify that the phone line is active and functions properly. Then, connect the analog phone line to the modem.

**Step 6** Initialize an EXEC modem call to the router from another device (PC) to test the modem connection.

**Step 7** When the connection is established, the dial in client is prompted for a password. Enter the correct password.

**Note**: This password should match the one that is configured on the console port line.



CHAPTER 9

# Setting Up Factory Default Device Using WebUI

Quick Setup Wizard allows you perform the basic router configuration. To configure the router:

**Note** Before you access the WebUI, you need to have the basic configuration on the device.

**Procedure**

**Step 1** Ensure that the router is in the factory fresh mode. If the router is not in the factory fresh mode, use the write erase option to erase all the configuration from the router.

**Step 2** Ensure that the following basic configuration is available on the device.

```
!
!
ip dhcp excluded-address 192.168.1.1 192.168.1.5
!
ip dhcp pool WEBUIPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.1
!
!
username webui privilege 15 secret cisco
!
interface Vlan1
ip address 192.168.1.1 255.255.255.0
ip nat inside
no shutdown
!
```

**Step 3** Connect the PC to any of the switch port which is the member of VLAN1. By default, all the ports will be the member of VLAN1 and the PC recieves the IP address from the pool WEBUIPool.

**Step 4** After your PC receives the IP address, launch the browser, type https://192.168.1.1/webui/#/dayZeroRouting or enter http://192.168.1.1/webui/#/dayZeroRouting.

**Step 5** Enter the default username (webui) and default password (cisco).


- Using Basic or Advanced Mode Setup Wizard, on page 136
- Configure LAN Settings, on page 136

• Configure Primary WAN Settings, on page 137
• Configure Secondary WAN Settings, on page 138
• Configure Security Settings, on page 138
• Using Web User Interface for Day One Setup, on page 139
• Monitor and Troubleshoot Device Plug and Play (PnP) Onboarding using WebUI , on page 140

# Using Basic or Advanced Mode Setup Wizard

To configure the router using the basic or advanced mode setup:

### Procedure

**Step 1** Choose the **Basic Mode** or **Advanced Mode** and click **Go To Account Creation Page**.

**Step 2** Enter the username and password. Reenter the password to confirm.

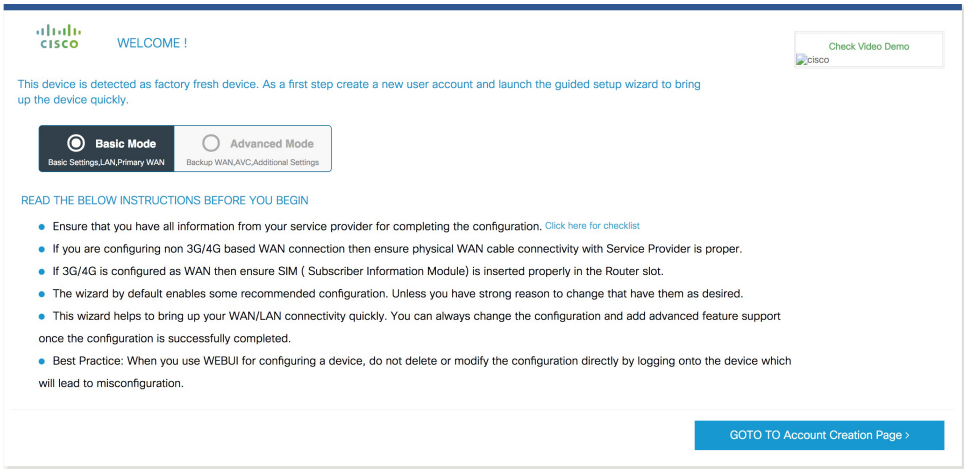
**Step 3** Click **Create and Launch Wizard**.

**Step 4** Enter the device name and domain name.

**Step 5** Select the appropriate time zone from the **Time Zone** drop-down list.

**Step 6** Select the appropriate date and time mode from the **Date and Time** drop-down list.

**Step 7** Click **LAN Settings**.




# Configure LAN Settings

### Procedure

**Step 1** Choose the **Web DHCP Pool/DHCP Pool** name or the **Create and Associate Access VLAN** option.

a) If you choose the Web DHCP Pool, specify the following:

**Pool Name**—Enter the DHCP Pool Name.

**Network**—Enter network address and the subnet mask.

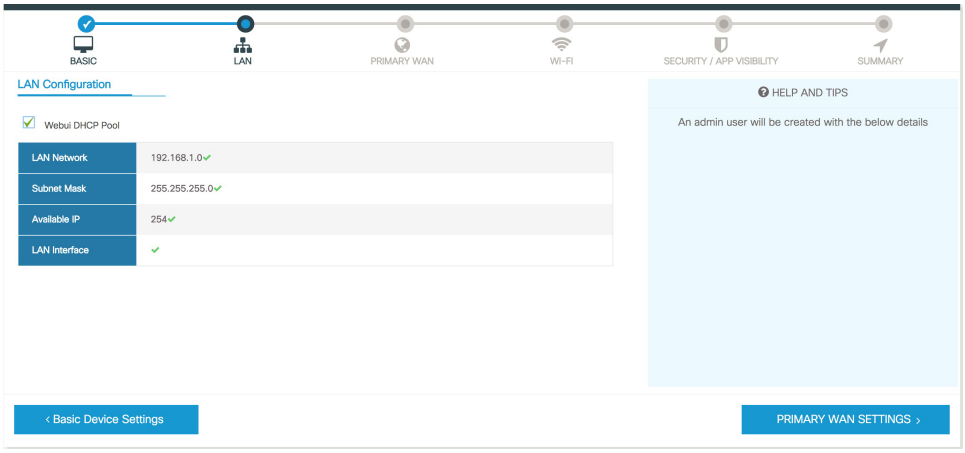
b) If you choose the Create and Associate Access VLAN option, specify the following:

**Access VLAN**—Enter the Access VLAN identification number. The range is from 1 to 4094.

**Network**—Enter the IP address of the VLAN.

**Management Interfaces**—Select the interface and move to the selected list box using the right and left arrows. You can also double click or drag and drop to move the interface to the selected list box.

**Step 2** Click **Primary WAN Settings**.




# Configure Primary WAN Settings

## Procedure

**Step 1** Select the primary WAN type. You can configure Serial, 3G/4G, Ethernet, or Broadband (xDSL) as primary WAN depending on the WAN types supported by the router.

**Step 2** Select the interface from the drop-down list.

**Step 3** Check the **Get DNS Server info directly from ISP** check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.

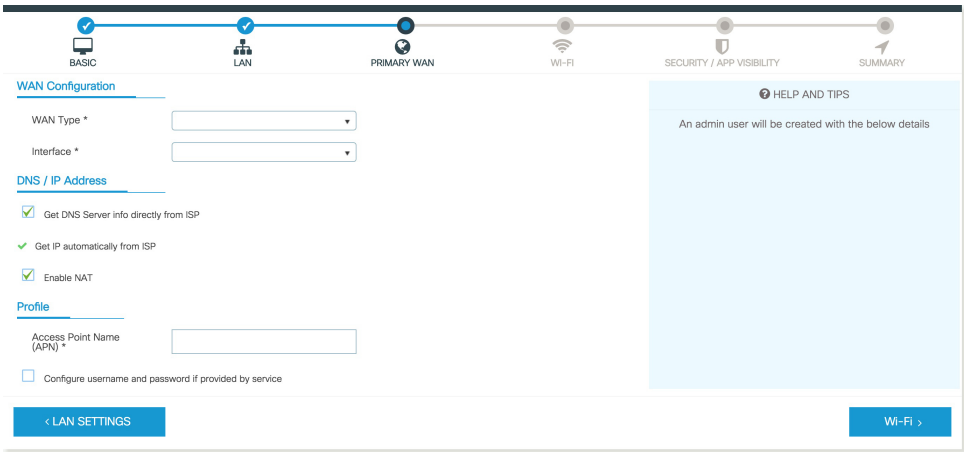
**Step 4** Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

**Step 5** Check the **Enable NAT** check box to enable NAT. It is recommended to enable NAT.

**Step 6** Check the **Enable PPPOE** check box to enable PPPoE. If you have enabled PPPoE, select the required authentication mode. The options are: **PAP** and **CHAP**.

**Step 7** Enter the username and password provided by the service provider.

**Step 8** Click **Security / APP Visibility WAN Settings**.




# Configure Secondary WAN Settings

For advanced configuration, you should configure the secondary WAN connection.

### Procedure

**Step 1** Select the secondary WAN type. You can configure Serial, 3G/4G, Ethernet, or Broadband (xDSL) as a secondary WAN depending on the WAN types supported by the router.

**Step 2** Select the interface from the drop-down list.

**Step 3** Check the **Get DNS Server info directly from ISP** check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.

**Step 4** Check the **Get IP automatically from ISP** check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

**Step 5** Check the **Enable NAT** check box to enable NAT. It is recommended to enable NAT.

**Step 6** Check the **Enable PPPOE** check box to enable PPPoE. If you have enabled PPPoE, select the required authentication mode. The options are **PAP** and **CHAP**.

**Step 7** Enter the username and password provided by the service provider.

**Step 8** Click **Security / APP Visibility WAN Settings**.

# Configure Security Settings

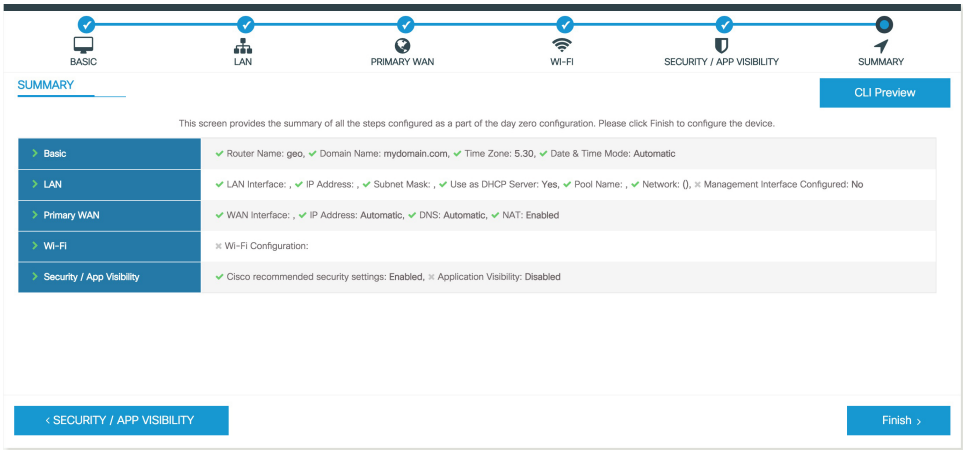
### Procedure

**Step 1** Check the **Enable Cisco Recommended Security Settings** check box to ensure that all passwords are not shown in plain text. The passwords are encrypted.

**Step 2** Click **Day 0 Config Summary**.

**Step 3** To preview the configuration, click **CLI Preview** to preview the configuration.

**Step 4** Click **Finish** to complete the Day Zero setup.




# Using Web User Interface for Day One Setup

To configure the Web user interface:

### Before you begin

- You need to configure at least 30 VTY lines on the device for the Web UI information to be displayed without errors.
- You need a user with privilege 15 to access the configuration screens on Web UI. If the privilege is less than 15, you can access only the Dashboard and Monitoring screens on Web UI.

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

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

### Procedure

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

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

**Step 2** Set up the authentication options to log into Web UI. You can use one of these methods to authenticate:

a) You can authenticate using local database. To use a local database for Web UI authentication, ensure to have the **ip http authentication local** command in the running configuration. This command is preconfigured on the device. If the command is not present, configure the device as shown in this example:

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

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

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

**Step 3** Launch the browser. In the address bar, type the IP address of the device. For a secure connection, type https://ip-address.

**Step 4** Enter the default username (webui) and default password (cisco).

**Step 5** Click **Log In**.

# Monitor and Troubleshoot Device Plug and Play (PnP) Onboarding using WebUI

*Table 14: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Monitor and Troubleshoot Device PnP Onboarding using WebUI | Cisco IOS XE Release 17.5.1a | You can now monitor and troubleshoot your Day-0 device onboarding using WebUI through PnP onboarding. If the automated PnP onboarding fails, you can manually onboard your device. |

A device can be automatically onboarded to Cisco vManage through either Zero Touch Provisioning (ZTP) or the Plug and Play (PnP) process. This section describes the procedure to monitor and troubleshoot device onboarding through the PnP method. This feature on WebUI enables you to monitor and troubleshoot the PnP onboarding process, and also see its real-time status. If this onboarding is stuck or fails, you can terminate the process and onboard your device manually.

### Prerequisites

- Your device (a computer that can run a web browser) running the WebUI and the device you are onboarding must be connected through an L2 switch port (NIM) on the device.
- The DHCP client-identifier on your device must be set to string "webui".
- Your device must support Cisco SD-WAN Day-0 device onboarding on WebUI.

### Troubleshoot Device PnP Onboarding

To troubleshoot device onboarding through PnP in controller mode:

1. Enter the controller mode in WebUI:

   - Switching from autonomous mode to controller mode:

     Usually, when you boot your device for the first time it is in autonomous mode. Go to the URL https://192.168.1.1/webui/ and log in using the default credentials— webui/cisco. If your device supports Cisco SD-WAN Day-0 device onboarding on WebUI, you can switch to the controller mode by selecting **Controller Mode.** A dialogue box appears, asking if you want to continue. Click **Yes.** Your device reloads to switch to controller mode.

   - Booting your device in controller mode:

     If your device is already in the controller mode, you do not have to make any changes to the mode. Go to the URL https://192.168.1.1 or https://192.168.1.1/webui. If your device supports Cisco SD-WAN Day-0 device onboarding on WebUI, the URL is redirected to https://192.168.1.1/ciscosdwan/ and you can log in using the default credentials for Cisco IOS XE SD-WAN devices - admin/admin.

**Note** If the device does not have start-up configuration at the time of PnP onboarding, the WebUI is enabled by default on supported devices.

2. On the **Welcome to Cisco SDWAN Onboarding Wizard** page, click **Reset Default Password.**

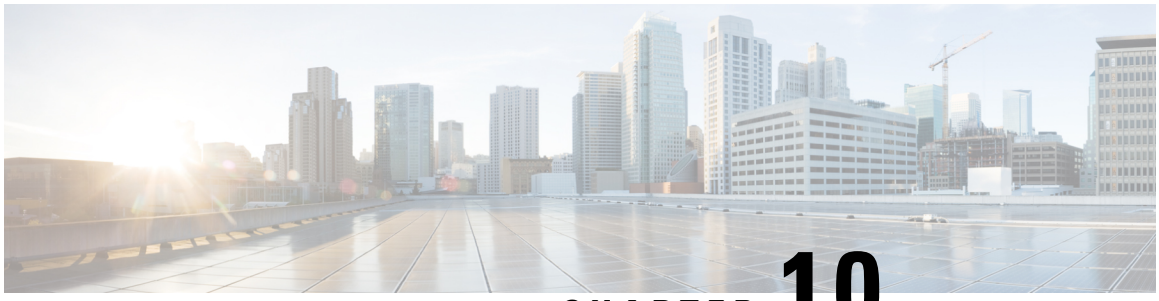
**Note** The default password of your Day-0 device is weak. Therefore, for a secure log in, you must reset the password when you first log in to the device on WebUI. The WebUI configuration is automatically deleted after the device is onboarded successfully. In rare cases where the template configuration for your device on Cisco vManage has the WebUI configuration, it is not deleted even after a successful device onboarding.

3. You are redirected to the Device hardware and software details page. Enter your password and click **Submit.**
4. The next page displays the onboarding progress and lists statuses of different components of the PnP Connect Portal and Cisco SD-WAN controllers. If the PnP IPv4 component fails, it indicates that the device PnP onboarding has failed.

   To view and download logs for the onboarding process, click the information icon on the right hand side of the SDWAN Onboarding Progress bar.
5. If the automated PnP onboarding fails, click **Terminate Automated Onboarding.** This allows you to onboard your device manually.
6. A dialogue box appears. To continue with the termination, click **Yes**. It might take a few minutes for the termination to complete.
7. On the Bootstrap Configuration page click **Select File** and choose the bootstrap file for your device. This file can be either a generic bootstrap file (common platform-specific file) or a full configuration

bootstrap file that you can download from Cisco vManage. This file must contain details such as the vBond number, UUID, WAN interface, root CA and configuration.

8. Click **Upload**.
9. After your file is successfully uploaded, click **Submit.**
10. You can see the SDWAN Onboarding Progress page again with statuses of the Cisco SD-WAN controllers. To open the Controller Connection History table click the information icon on the right hand side of the SDWAN Control Connections bar. In this table you can see the state of your onboarded device. After the onboarding is complete, the state of your device changes to **connect**.



CHAPTER 10

# 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 143
- Monitoring Hardware Using Alarms, on page 147


# 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 143
- Cisco IOS Process Resources, on page 143
- Overall Control Plane Resources, on page 145


## 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#24c450a57e03d03a6788866ae1d462e4
 Address      Bytes      Prev       Next    Ref   PrevF     NextF          what        Alloc
 PC

                Head    Total(b)     Used(b)     Free(b)   Lowest(b)  Largest(b)
Processor  7F51210010   1499843648   303330248   1196513400   786722360   713031588
 lsmpi_io  7F506281A8     6295128     6294304         824         824         412
Dynamic heap limit(MB) 680       Use(MB) 0



          Processor memory

 Address      Bytes      Prev       Next    Ref   PrevF     NextF          what
    Alloc PC
7F51210010 0000000568 00000000 7F512102A0 001  -------- -------- *Init*
:400000+896EB88
7F512102A0 0000032776 7F51210010 7F51218300 001  -------- -------- Managed Chunk Q
:400000+295B3C8
7F51218300 0000000056 7F512102A0 7F51218390 001  -------- -------- *Init*
:400000+896EB88
7F51218390 0000012808 7F51218300 7F5121B5F0 001  -------- -------- *Init*
:400000+896EB88
 Address      Bytes      Prev       Next    Ref   PrevF     NextF          what
    Alloc PC
7F5121B5F0 0000032776 7F51218390 7F51223650 001  -------- -------- List Elements
:400000+2948680
7F51223650 0000010008 7F5121B5F0 7F51225DC0 001  -------- -------- List Headers
:400000+2948680
7F51225DC0 0000032776 7F51223650 7F5122DE20 001  -------- -------- IOSXE Process S
:400000+295B3C8
7F5122DE20 0000032776 7F51225DC0 7F51235E80 001  -------- -------- IOSXE Queue Pro
:400000+295B3C8
7F51235E80 0000065544 7F5122DE20 7F51245EE0 001  -------- -------- IOSXE Queue Bal
:400000+295B3C8
7F51245EE0 0000000112 7F51235E80 7F51245FA8 001  -------- -------- *Init*
:400000+2951DE0
7F51245FA8 0000036872 7F51245EE0 7F5124F008 001  -------- -------- *Init*
:400000+2950FB4
7F5124F008 0000010008 7F51245FA8 7F51251778 001  -------- -------- Platform VM Pag
:400000+295B3C8
7F51251778 0000000328 7F5124F008 7F51251918 001  -------- -------- *Init*
:400000+896EB88
7F51251918 0000000328 7F51251778 7F51251AB8 001  -------- -------- *Init*
:400000+896EB88
7F51251AB8 0000000896 7F51251918 7F51251E90 001  -------- -------- Watched Message
:400000+295B3C8

...
```

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

```
Router# show process cpu
CPU utilization for five seconds: 1%/1%; one minute: 1%; five minutes: 1%
 PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
   1           0          21          0  0.00%  0.00%  0.00%   0 Chunk Manager
   2        5692       12584        452  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          16          12       1333  0.00%  0.00%  0.00%   0 RF Slave Main Th
   7           4           1       4000  0.00%  0.00%  0.00%   0 EDDRI_MAIN
```

```
  8           0           1           0  0.00%  0.00%  0.00%   0 RO Notify Timers
  9       38188        8525        4479  0.00%  0.04%  0.05%   0 Check heaps
 10          12        1069          11  0.00%  0.00%  0.00%   0 Pool Manager
 11           0           1           0  0.00%  0.00%  0.00%   0 DiscardQ Backgro
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 12           0           2           0  0.00%  0.00%  0.00%   0 Timers
 13           0          29           0  0.00%  0.00%  0.00%   0 WATCH_AFS
 14           0           1           0  0.00%  0.00%  0.00%   0 MEMLEAK PROCESS
 15        3840       23732         161  0.00%  0.00%  0.00%   0 ARP Input
 16        1156       65637          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
PID Runtime(ms)     Invoked      uSecs   5Sec   1Min   5Min TTY Process
 23          76          19        4000  0.00%  0.00%  0.00%   0 Entity MIB API
 24         124          38        3263  0.00%  0.00%  0.00%   0 PrstVbl
 25           0           2           0  0.00%  0.00%  0.00%   0 Serial Backgroun
 26           0           1           0  0.00%  0.00%  0.00%   0 RMI RM Notify Wa
 27           0           2           0  0.00%  0.00%  0.00%   0 ATM AutoVC Perio
 28           0           2           0  0.00%  0.00%  0.00%   0 ATM VC Auto Crea
 29         768       31455          24  0.00%  0.00%  0.00%   0 IOSXE heartbeat
 30         180        1866          96  0.00%  0.00%  0.00%   0 DB Lock Manager
 31           0           1           0  0.00%  0.00%  0.00%   0 DB Notification
 32           0           1           0  0.00%  0.00%  0.00%   0 IPC Apps Task
 33           0           1           0  0.00%  0.00%  0.00%   0 ifIndex Receive

...
```

# Overall Control Plane Resources

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

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

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

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

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

### Load Average

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

which is currently running. On a dual-core processor, a load of 7 would mean that seven processes are ready to run, two of which are currently running.

### Memory Utilization

Memory utilization is represented by the following fields:

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

### CPU Utilization

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

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

### 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 5 seconds ago
Load Average: healthy
  1-Min: 0.90, status: healthy, under 5.00
  5-Min: 0.87, status: healthy, under 5.00
  15-Min: 0.95, status: healthy, under 5.00
Memory (kb): healthy
  Total: 3448368
  Used: 1979068 (57%), status: healthy
  Free: 1469300 (43%)
  Committed: 2002904 (58%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
  User:  1.54, System:  1.33, Nice:  0.00, Idle: 97.11
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU1: CPU Utilization (percentage of time spent)
  User:  1.53, System:  0.82, Nice:  0.00, Idle: 97.64
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU2: CPU Utilization (percentage of time spent)
```

```
  User:  2.77, System:  9.38, Nice:  0.00, Idle: 87.84
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00
CPU3: CPU Utilization (percentage of time spent)
  User: 12.62, System: 64.63, Nice:  0.00, Idle: 22.74
  IRQ:  0.00, SIRQ:  0.00, IOwait:  0.00


Router# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.87   0.87   0.94

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  3448368  1996720 (58%)  1451648 (42%)   2003380 (58%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   1.54   0.92   0.00  97.53   0.00   0.00   0.00
         1   1.64   1.12   0.00  97.22   0.00   0.00   0.00
         2   3.32   8.36   0.00  88.30   0.00   0.00   0.00
         3  12.58  64.44   0.00  22.97   0.00   0.00   0.00
```

# 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.

## Examples of Alarm Messages

The following are examples of alarm messages that are sent to the console.

### Alarms

To view alarms, use the **show facility-alarm status** command. The following example shows a critical alarm for the power supply:

```
Device# show facility-alarm status
Source          Severity            Description [Index]
------                             --------      -------------------------
Cellular0/2/0   INFO                Physical Port Administrative State Down [2]
Cellular0/2/1   INFO                Physical Port Administrative State Down [2]
```

To view critical alarms, use the **show facility-alarm status critical** command, as shown in the following example:

```
Device# show facility-alarm status critical
ystem Totals Critical: 4 Major: 0 Minor: 0
Source               Time                 Severity Description           [Index]
------               ------               -------- ------------          -------
GigabitEthernet0/1/0 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/1/1 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/1/2 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
GigabitEthernet0/1/3 Jul 12 2017 22:27:25 CRITICAL Physical Port Link Down [1]
```

To view the operational state of the major hardware components on the Device, use the **show platform diag** command. This example shows that power supply P0 has failed:

```
Device# show platform diag

Chassis type: C1117-4PLTEEA

Slot: 0, C1117-4PLTEEA
  Running state               : ok
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:52 (09:02:14 ago)
  Software declared up time   : 00:03:12 (09:00:54 ago)
  CPLD version                : 17100501
  Firmware version            : 16.6(1r)RC3

Sub-slot: 0/0, C1117-1x1GE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)
```

```
Sub-slot: 0/1, C1117-ES-4
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)

Sub-slot: 0/2, C1117-LTE
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)

Sub-slot: 0/3, C1117-VADSL-A
  Operational status          : ok
  Internal state              : inserted
  Physical insert detect time : 00:04:34 (08:59:32 ago)
  Logical insert detect time  : 00:04:34 (08:59:32 ago)

Slot: R0, C1117-4PLTEEA
    Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:52 (09:02:14 ago)
  Software declared up time   : 00:01:52 (09:02:14 ago)
  CPLD version                : 17100501
  Firmware version            : 16.6(1r)RC3

Slot: F0, C1117-4PLTEEA
  Running state               : ok, active
  Internal state              : online
  Internal operational state  : ok
  Physical insert detect time : 00:01:52 (09:02:14 ago)
  Software declared up time   : 00:04:06 (09:00:00 ago)
  Hardware ready signal time  : 00:02:44 (09:01:22 ago)
  Packet ready signal time    : 00:04:31 (08:59:35 ago)
  CPLD version                : 17100501
  Firmware version            : 16.6(1r)RC3

Slot: P0, PWR-12V
  State                       : ok
  Physical insert detect time : 00:02:24 (09:01:43 ago)

Slot: GE-POE, Unknown
  State                       : NA
  Physical insert detect time : 00:00:00 (never ago)
```

### Reviewing and Analyzing Alarm Messages

To facilitate the review of alarm messages, you can write scripts to analyze alarm messages sent to the console or syslog. Scripts can provide reports on events such as alarms, security alerts, and interface status.

Syslog messages can also be accessed through Simple Network Management Protocol (SNMP) using the history table defined in the CISCO-SYSLOG-MIB.

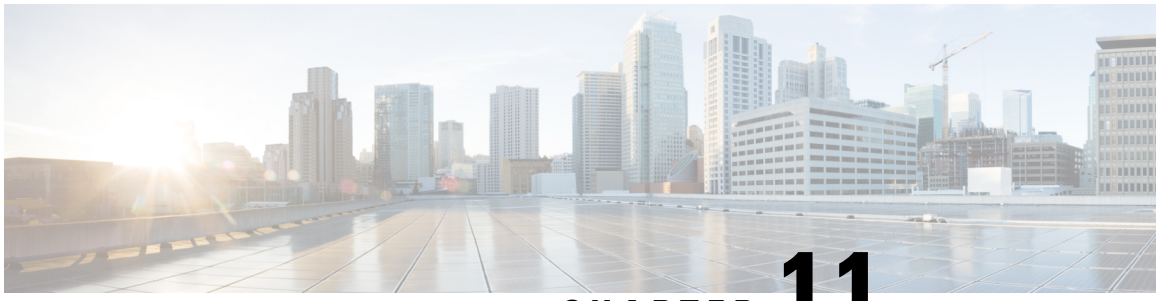
## Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP

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 11

# Packet Trace

First Published: August 03, 2016

The Packet-Trace feature provides a detailed understanding of how data packets are processed by the Cisco IOS XE platform, and thus helps customers to diagnose issues and troubleshoot them more efficiently. This module provides information about how to use the Packet-Trace feature.


- Information About Packet Trace, on page 151
- Usage Guidelines for Configuring Packet Trace, on page 152
- Configuring Packet Trace, on page 152
- Displaying Packet-Trace Information, on page 154
- Removing Packet-Trace Data, on page 154
- Configuration Examples for Packet Trace , on page 155
- Additional References, on page 162
- Feature Information for Packet Trace, on page 163


# Information About Packet Trace

The Packet-Trace feature provides three levels of inspection for packets: accounting, summary, and path data. Each level provides a detailed view of packet processing at the cost of some packet processing capability. However, Packet Trace limits inspection to packets that match the debug platform condition statements, and is a viable option even under heavy-traffic situations in customer environments.

The following table explains the three levels of inspection provided by packet trace.

***Table 15: Packet-Trace Level***

| Packet-Trace Level | Description |
|---|---|
| Accounting | Packet-Trace accounting provides a count of packets that enter and leave the network processor. Packet-Trace accounting is a lightweight performance activity, and runs continuously until it is disabled. |
| Summary | At the summary level of packet trace, data is collected for a finite number of packets. Packet-Trace summary tracks the input and output interfaces, the final packet state, and punt, drop, or inject packets, if any. Collecting summary data adds to additional performance compared to normal packet processing, and can help to isolate a troublesome interface. |

| Packet-Trace Level | Description |
|---|---|
| Path data | The packet-trace path data level provides the greatest level of detail in packet trace. Data is collected for a finite number of packets. Packet-Trace path data captures data, including a conditional debugging ID that is useful to correlate with feature debugs, a timestamp, and also feature-specific path-trace data.<br><br>Path data also has two optional capabilities: packet copy and Feature Invocation Array (FIA) trace. The packet-copy option enables you to copy input and output packets at various layers of the packet (layer 2, layer 3 or layer 4). The FIA- trace option tracks every feature entry invoked during packet processing and helps you to know what is happening during packet processing.<br><br>**Note** Collecting path data consumes more packet-processing resources, and the optional capabilities incrementally affect packet performance. Therefore, path-data level should be used in limited capacity or in situations where packet performance change is acceptable. |

# Usage Guidelines for Configuring Packet Trace

Consider the following best practices while configuring the Packet-Trace feature:

- Use of ingress conditions when using the Packet-Trace feature is recommended for a more comprehensive view of packets.
- Packet-trace configuration requires data-plane memory. On systems where data-plane memory is constrained, carefully consider how you will select the packet-trace values. A close approximation of the amount of memory consumed by packet trace is provided by the following equation:

memory required = (statistics overhead) + number of packets * (summary size + data size + packet copy size).

When the Packet-Trace feature is enabled, a small, fixed amount of memory is allocated for statistics. Similarly, when per-packet data is captured, a small, fixed amount of memory is required for each packet for summary data. However, as shown by the equation, you can significantly influence the amount of memory consumed by the number of packets you select to trace, and whether you collect path data and copies of packets.

# Configuring Packet Trace

Perform the following steps to configure the Packet-Trace feature.

**Note** The amount of memory consumed by the Packet-Trace feature is affected by the packet-trace configuration. You should carefully select the size of per-packet path data and copy buffers and the number of packets to be traced in order to avoid interrupting normal services. You can check the current data-plane DRAM memory consumption by using the **show platform hardware qfp active infrastructure exmem statistics** command.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables the privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **debug platform packet-trace packet** *pkt-num* **[fia-trace \| summary-only] [circular] [data-size** *data-size***]**<br>**Example:**<br>`Router# debug platform packet-trace packets 2048 summary-only` | Collects summary data for a specified number of packets. Captures feature path data by default, and optionally performs FIA trace.<br>*pkt-num*—Specifies the maximum number of packets maintained at a given time.<br>**fia-trace**—Provides detailed level of data capture, including summary data, feature-specific data. Also displays each feature entry visited during packet processing.<br>**summary-only**—Enables the capture of summary data with minimal details.<br>**circular**—Saves the data of the most recently traced packets.<br>*data-size*—Specifies the size of data buffers for storing feature and FIA trace data for each packet in bytes. When very heavy packet processing is performed on packets, users can increase the size of the data buffers if necessary. The default value is 2048. |
| **Step 3** | **debug platform packet-trace {punt \|inject\|copy\|drop\|packet\|statistics}**<br>**Example:**<br>`Router# debug platform packet-trace punt` | Enables tracing of punted packets from data to control plane. |
| **Step 4** | **debug platform condition [ipv4 \| ipv6] [interface** *interface***][access-list** *access-list -name* **\|** *ipv4-address* **/** *subnet-mask* **\|** *ipv6-address* **/** *subnet-mask***] [ingress \| egress \|both]**<br>**Example:**<br>`Router# debug platform condition interface g0/0/0 ingress` | Specifies the matching criteria for tracing packets. Provides the ability to filter by protocol, IP address and subnet mask, access control list (ACL), interface, and direction. |
| **Step 5** | **debug platform condition start**<br>**Example:**<br>`Router# debug platform condition start` | Enables the specified matching criteria and starts packet tracing. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **debug platform condition stop**<br>**Example:**<br>`Router# debug platform condition start` | Deactivates the condition and stops packet tracing. |
| **Step 7** | **show platform packet-trace {configuration \| statistics \| summary \| packet {all \| *pkt-num*}}**<br>**Example:**<br>`Router# show platform packet-trace 14` | Displays packet-trace data according to the specified option. See {start cross reference} Table 21-1 {end cross reference} for detailed information about the **show** command options. |
| **Step 8** | **clear platform condition all**<br>**Example:**<br>`Router(config)# clear platform condition all` | Removes the configurations provided by the **debug platform condition** and **debug platform packet-trace** commands. |
| **Step 9** | **exit**<br>**Example:**<br>`Router# exit` | Exits the privileged EXEC mode. |

# Displaying Packet-Trace Information

Use these **show** commands to display packet-trace information.

***Table 16: show Commands***

| Command | Description |
|---|---|
| **show platform packet-trace configuration** | Displays packet trace configuration, including any defaults. |
| **show platform packet-trace statistics** | Displays accounting data for all the traced packets. |
| **show platform packet-trace summary** | Displays summary data for the number of packets specified. |
| **show platform packet-trace {all \| *pkt-num*} [decode]** | Displays the path data for all the packets or the packet specified. The **decode** option attempts to decode the binary packet into a more human- readable form. |

# Removing Packet-Trace Data

Use these commands to clear packet-trace data.

*Table 17: clear Commands*

| Command | Description |
|---|---|
| **clear platform packet-trace statistics** | Clears the collected packet-trace data and statistics. |
| **clear platform packet-trace configuration** | Clears the packet-trace configuration and the statistics. |

# Configuration Examples for Packet Trace

This section provides the following configuration examples:

## Example: Configuring Packet Trace

This example describes how to configure packet trace and display the results. In this example, incoming packets to Gigabit Ethernet interface 0/0/1 are traced, and FIA-trace data is captured for the first 128 packets. Also, the input packets are copied. The **show platform packet-trace packet 0** command displays the summary data and each feature entry visited during packet processing for packet 0.

```
Router>
enable
Router# debug platform packet-trace packet 128 fia-trace
Router# debug platform packet-trace punt
Router# debug platform condition interface g0/0/1 ingress
Router# debug platform condition start
Router#! ping to UUT
Router# debug platform condition stop
Router# show platform packet-trace packet 0
Packet: 0           CBUG ID: 9
Summary
  Input     : GigabitEthernet0/0/1
  Output    : GigabitEthernet0/0/0
  State     : FWD
  Timestamp
    Start   : 1819281992118 ns (05/17/2014 06:42:01.207240 UTC)
    Stop    : 1819282095121 ns (05/17/2014 06:42:01.207343 UTC)
Path Trace
  Feature: IPV4
    Source      : 192.0.2.1
    Destination : 192.0.2.2
    Protocol    : 1 (ICMP)
  Feature: FIA_TRACE
    Entry     : 0x8059dbe8 - DEBUG_COND_INPUT_PKT
    Timestamp : 3685243309297
  Feature: FIA_TRACE
    Entry     : 0x82011a00 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Timestamp : 3685243311450
  Feature: FIA_TRACE
    Entry     : 0x82000170 - IPV4_INPUT_FOR_US_MARTIAN
    Timestamp : 3685243312427
  Feature: FIA_TRACE
    Entry     : 0x82004b68 - IPV4_OUTPUT_LOOKUP_PROCESS
    Timestamp : 3685243313230
  Feature: FIA_TRACE
    Entry     : 0x8034f210 - IPV4_INPUT_IPOPTIONS_PROCESS
    Timestamp : 3685243315033
```

```
  Feature: FIA_TRACE
    Entry     : 0x82013200 - IPV4_OUTPUT_GOTO_OUTPUT_FEATURE
    Timestamp : 3685243315787
  Feature: FIA_TRACE
    Entry     : 0x80321450 - IPV4_VFR_REFRAG
    Timestamp : 3685243316980
  Feature: FIA_TRACE
    Entry     : 0x82014700 - IPV6_INPUT_L2_REWRITE
    Timestamp : 3685243317713
  Feature: FIA_TRACE
    Entry     : 0x82000080 - IPV4_OUTPUT_FRAG
    Timestamp : 3685243319223
  Feature: FIA_TRACE
    Entry     : 0x8200e500 - IPV4_OUTPUT_DROP_POLICY
    Timestamp : 3685243319950
  Feature: FIA_TRACE
    Entry     : 0x8059aff4 - PACTRAC_OUTPUT_STATS
    Timestamp : 3685243323603
  Feature: FIA_TRACE
    Entry     : 0x82016100 - MARMOT_SPA_D_TRANSMIT_PKT
    Timestamp : 3685243326183

Router# clear platform condition all
Router# exit
```

Linux Forwarding Transport Service (LFTS) is a transport mechanism to forward packets punted from the CPP into applications other than IOSd. This example displays the LFTS-based intercepted packet destined for binos application.

```
Router# show platform packet-trace packet 10
Packet: 10     CBUG ID: 52
Summary
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  State  : PUNT 55 (For-us control)
  Timestamp
    Start : 597718358383 ns (06/06/2016 09:00:13.643341 UTC)
    Stop : 597718409650 ns (06/06/2016 09:00:13.643392 UTC)
Path Trace
  Feature: IPV4
    Input  : GigabitEthernet0/0/0
    Output : <unknown>
    Source : 10.64.68.2
    Destination : 10.0.0.102
    Protocol : 17 (UDP)
      SrcPort : 1985
      DstPort : 1985
  Feature: FIA_TRACE
    Input  : GigabitEthernet0/0/0
    Output : <unknown>
    Entry  : 0x8a0177bc - DEBUG_COND_INPUT_PKT
    Lapsed time : 426 ns
  Feature: FIA_TRACE
    Input  : GigabitEthernet0/0/0
    Output : <unknown>
    Entry  : 0x8a017788 - IPV4_INPUT_DST_LOOKUP_CONSUME
    Lapsed time : 386 ns
  Feature: FIA_TRACE
    Input  : GigabitEthernet0/0/0
    Output : <unknown>
    Entry  : 0x8a01778c - IPV4_INPUT_FOR_US_MARTIAN
    Lapsed time : 13653 ns
  Feature: FIA_TRACE
    Input  : GigabitEthernet0/0/0
```

```
  Output : internal0/0/rp:1
  Entry  : 0x8a017730 - IPV4_INPUT_LOOKUP_PROCESS_EXT
  Lapsed time : 2360 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017be0 - IPV4_INPUT_IPOPTIONS_PROCESS_EXT
  Lapsed time : 66 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017bfc - IPV4_INPUT_GOTO_OUTPUT_FEATURE_EXT
  Lapsed time : 680 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017d60 - IPV4_INTERNAL_ARL_SANITY_EXT
  Lapsed time : 320 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017a40 - IPV4_VFR_REFRAG_EXT
  Lapsed time : 106 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017d2c - IPV4_OUTPUT_DROP_POLICY_EXT
  Lapsed time : 1173 ns
Feature: FIA_TRACE
  Input  : GigabitEthernet0/0/0
  Output : internal0/0/rp:1
  Entry  : 0x8a017940 - INTERNAL_TRANSMIT_PKT_EXT
  Lapsed time : 20173 ns
LFTS Path Flow: Packet: 10    CBUG ID: 52
  Feature: LFTS
  Pkt Direction: IN
  Punt Cause  : 55
       subCause : 0
```

# Example: Using Packet Trace

This example provides a scenario in which packet trace is used to troubleshoot packet drops for a NAT configuration on a Cisco device. This example shows how you can effectively utilize the level of detail provided by the Packet-Trace feature to gather information about an issue, isolate the issue, and then find a solution.

In this scenario, you can detect that there are issues, but are not sure where to start troubleshooting. You should, therefore, consider accessing the Packet-Trace summary for a number of incoming packets.

```
Router# debug platform condition ingress
Router# debug platform packet-trace packet 2048 summary-only
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Pkt   Input             Output            State  Reason
0     Gi0/0/0           Gi0/0/0           DROP   402 (NoStatsUpdate)
1     internal0/0/rp:0  internal0/0/rp:0  PUNT   21  (RP<->QFP keepalive)
2     internal0/0/recycle:0  Gi0/0/0      FWD
```

The output shows that packets are dropped due to NAT configuration on Gigabit Ethernet interface 0/0/0, which enables you to understand that an issue is occurring on a specific interface. Using this information, you

can limit which packets to trace, reduce the number of packets for data capture, and increase the level of inspection.

```
Router# debug platform packet-trace packet 256
Router# debug platform packet-trace punt
Router# debug platform condition interface Gi0/0/0
Router# debug platform condition start
Router# debug platform condition stop
Router# show platform packet-trace summary
Router# show platform packet-trace 15
Packet: 15          CBUG ID: 238
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:1
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 1166288346725 ns (06/06/2016 09:09:42.202734 UTC)
    Stop    : 1166288383210 ns (06/06/2016 09:09:42.202770 UTC)
Path Trace
  Feature: IPV4
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.64.68.3
    Destination : 10.0.0.102
    Protocol    : 17 (UDP)
      SrcPort   : 1985
      DstPort   : 1985
IOSd Path Flow: Packet: 15    CBUG ID: 238
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From CPP
  Feature: IP
    Pkt Direction: IN
    Source      : 10.64.68.122
    Destination : 10.64.68.255
  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.64.68.122
    Destination : 10.64.68.255
    Interface   : GigabitEthernet0/0/0
  Feature: UDP
    Pkt Direction: IN
    src         : 10.64.68.122(1053)
    dst         : 10.64.68.255(1947)
    length      : 48

Router#show platform packet-trace packet 10
Packet: 10          CBUG ID: 10
Summary
  Input     : GigabitEthernet0/0/0
  Output    : internal0/0/rp:0
  State     : PUNT 55  (For-us control)
  Timestamp
    Start   : 274777907351 ns (01/10/2020 10:56:47.918494 UTC)
    Stop    : 274777922664 ns (01/10/2020 10:56:47.918509 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet0/0/0
    Output      : <unknown>
    Source      : 10.78.106.2
    Destination : 10.0.0.102
    Protocol    : 17 (UDP)
```

```
      SrcPort   : 1985
      DstPort   : 1985

IOSd Path Flow: Packet: 10    CBUG ID: 10
  Feature: INFRA
    Pkt Direction: IN
Packet Rcvd From DATAPLANE
 Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.78.106.2
    Destination : 10.0.0.102
    Interface   : GigabitEthernet0/0/0

  Feature: UDP
    Pkt Direction: IN DROP
    Pkt : DROPPED
    UDP: Discarding silently
    src        : 881 10.78.106.2(1985)
    dst        : 10.0.0.102(1985)
    length     : 60

Router#show platform packet-trace packet  12
Packet: 12          CBUG ID: 767
Summary
  Input     : GigabitEthernet3
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 16120990774814 ns (01/20/2020 12:38:02.816435 UTC)
    Stop    : 16120990801840 ns (01/20/2020 12:38:02.816462 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet3
    Output      : <unknown>
    Source      : 10.1.1.1
    Destination : 10.1.1.2
    Protocol    : 6 (TCP)
      SrcPort   : 46593
      DstPort   : 23
IOSd Path Flow: Packet: 12    CBUG ID: 767
  Feature: INFRA
    Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
    Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.1.1.1
    Destination : 10.1.1.2
    Interface   : GigabitEthernet3

  Feature: IP
    Pkt Direction: IN
    FORWARDEDTo transport layer
    Source        : 10.1.1.1
    Destination   : 10.1.1.2
    Interface     : GigabitEthernet3

  Feature: TCP
    Pkt Direction: IN
    tcp0: I NoTCB 10.1.1.1:46593 10.1.1.2:23 seq 1925377975 OPTS 4 SYN  WIN 4128

Router# show platform packet-trace summary
Pkt   Input                     Output                    State  Reason
```

```
0     INJ.2                     Gi1                       FWD
1     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
2     INJ.2                     Gi1                       FWD
3     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
4     INJ.2                     Gi1                       FWD
5     INJ.2                     Gi1                       FWD
6     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
7     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
8     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
9     Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
10    INJ.2                     Gi1                       FWD
11    INJ.2                     Gi1                       FWD
12    INJ.2                     Gi1                       FWD
13    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
14    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
15    Gi1                       internal0/0/rp:0          PUNT   11  (For-us data)
16    INJ.2                     Gi1                       FWD
```

The following example displays the packet trace data statistics.

```
Router#show platform packet-trace statistics
Packets Summary
  Matched  3
  Traced   3
Packets Received
  Ingress  0
  Inject   0
Packets Processed
  Forward  0
  Punt     3
    Count       Code  Cause
    3           56    RP injected for-us control
  Drop     0
  Consume  0

          PKT_DIR_IN
             Dropped       Consumed       Forwarded
INFRA            0             0             0
TCP              0             0             0
UDP              0             0             0
IP               0             0             0
IPV6             0             0             0
ARP              0             0             0

         PKT_DIR_OUT
             Dropped       Consumed       Forwarded
INFRA            0             0             0
TCP              0             0             0
UDP              0             0             0
IP               0             0             0
IPV6             0             0             0
ARP              0             0             0
```

The following example displays packets that are injected and punted to the forwarding processor from the control plane.

```
Router#debug platform condition ipv4 10.118.74.53/32 both
 Router#Router#debug platform condition start
Router#debug platform packet-trace packet 200
Packet count rounded up from 200 to 256

Router#show platform packet-tracer packet 0
show plat pack pa 0
Packet: 0           CBUG ID: 674
Summary
```

```
  Input     : GigabitEthernet1
  Output    : internal0/0/rp:0
  State     : PUNT 11  (For-us data)
  Timestamp
    Start   : 17756544435656 ns (06/29/2020 18:19:17.326313 UTC)
    Stop    : 17756544469451 ns (06/29/2020 18:19:17.326346 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet1
    Output      : <unknown>
    Source      : 10.118.74.53
    Destination : 172.18.124.38
    Protocol    : 17 (UDP)
      SrcPort   : 2640
      DstPort   : 500

IOSd Path Flow: Packet: 0    CBUG ID: 674
  Feature: INFRA
  Pkt Direction: IN
    Packet Rcvd From DATAPLANE

  Feature: IP
  Pkt Direction: IN
    Packet Enqueued in IP layer
    Source      : 10.118.74.53
    Destination : 172.18.124.38
    Interface   : GigabitEthernet1

  Feature: IP
  Pkt Direction: IN
  FORWARDED To transport layer
    Source        : 10.118.74.53
    Destination   : 172.18.124.38
    Interface     : GigabitEthernet1

  Feature: UDP
  Pkt Direction: IN
  DROPPED
 UDP: Checksum error: dropping
 Source      : 10.118.74.53(2640)
 Destination : 172.18.124.38(500)

Router#show platform packet-tracer packet 2
Packet: 2           CBUG ID: 2

IOSd Path Flow:
  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 172.18.124.38:22 172.18.124.55:52774 seq 3052140910
OPTS 4 ACK 2346709419 SYN  WIN 4128

  Feature: TCP
  Pkt Direction: OUT
  FORWARDED
 TCP: Connection is in SYNRCVD state
 ACK         : 2346709419
 SEQ         : 3052140910
 Source      : 172.18.124.38(22)
 Destination : 172.18.124.55(52774)


  Feature: IP
  Pkt Direction: OUTRoute out the generated packet.srcaddr: 172.18.124.38, dstaddr:
172.18.124.55
```

```
  Feature: IP
  Pkt Direction: OUTInject and forward successful srcaddr: 172.18.124.38, dstaddr:
172.18.124.55

  Feature: TCP
  Pkt Direction: OUTtcp0: O SYNRCVD 172.18.124.38:22 172.18.124.55:52774 seq 3052140910
OPTS 4 ACK 2346709419 SYN  WIN 4128
Summary
  Input     : INJ.2
  Output    : GigabitEthernet1
  State     : FWD
  Timestamp
    Start   : 490928006866 ns (06/29/2020 13:31:30.807879 UTC)
    Stop    : 490928038567 ns (06/29/2020 13:31:30.807911 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : internal0/0/rp:0
    Output      : <unknown>
    Source      : 172.18.124.38
    Destination : 172.18.124.55
    Protocol    : 6 (TCP)
      SrcPort   : 22
      DstPort   : 52774
  Feature: IPSec
    Result    : IPSEC_RESULT_DENY
    Action    : SEND_CLEAR
    SA Handle : 0
    Peer Addr : 10.124.18.172
    Local Addr: 10.124.18.172


Router#
```

# Additional References

### Standards

| Standard | Title |
|---|---|
| None | — |

### MIBs

| MIB | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at this URL:<br>{start hypertext}http://www.cisco.com/go/mibs{end hypertext} |

### RFCs

| RFC | Title |
|---|---|
| None | — |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | {start hypertext}http://www.cisco.com/cisco/web/support/index.html{end hypertext} |

# Feature Information for Packet Trace

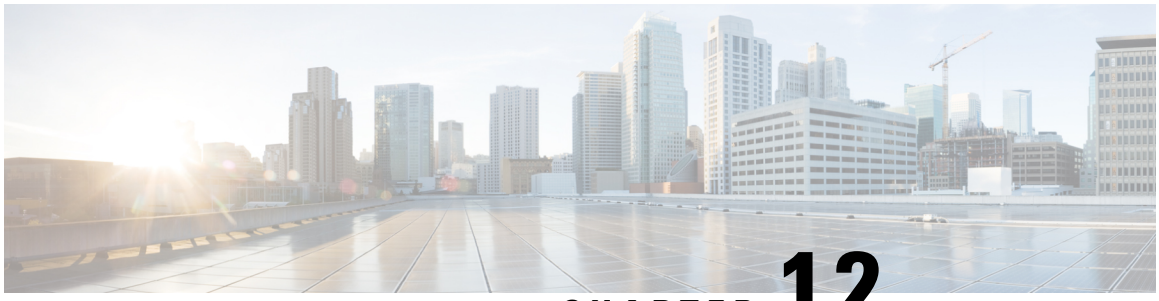
{start cross reference}Table 21-4{end cross reference} lists the features in this module and provides links to specific configuration information.

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

**Note** {start cross reference}Table 21-4{end cross reference} lists only the software releases that support a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 18: Feature Information for Packet Trace*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Packet Trace | Cisco IOS XE 3.10S | The Packet Trace feature provides information about how data packets are processed by the Cisco IOS XE software.<br>In Cisco IOS XE Release 3.10S, this feature was introduced.<br>The following commands were introduced or modified:<br>• **debug platform packet-trace packet** *pkt-num* [**fia-trace** \| **summary-only**] [**data-size** *data-size*] [**circular**]<br>• **debug platform packet-trace copy packet** {**input** \| **output** \| **both**} [**size** *num-bytes*] [**L2** \| **L3** \| **L4**]<br>• **show platform packet-trace** {**configuration** \| **statistics** \| **summary** \| **packet** {**all** \| *pkt-num*}} |
| | Cisco IOS XE 3.11S | In Cisco IOS XE Release 3.11S, this feature was enhanced to include the following features:<br>• Matched versus traced statistics.<br>• Trace stop timestamp in addition to trace start timestamp.<br>The following commands were introduced or modified:<br>• **debug platform packet-trace drop** [**code** *drop-num*]<br>• **show platform packet-trace packet** {**all** \| *pkt-num*} [*decode*] |
| | Cisco IOS XE Denali 16.3.1 | In Cisco IOS XE Denali 16.3.1, this feature was enhanced to include Layer3 packet tracing along with IOSd.<br>The following commands were introduced or modified: **debug platform packet-trace punt**. |
| | Cisco IOS XE Amsterdam 17.3.1 | The output of the **show platform packet-trace** command now includes additional trace information for packets either originated from IOSd or destined to IOSd or other BinOS processes. |



CHAPTER 12

# G.Fast and VDSL2 35b Profile

Cisco 1000 Series Intergration Services Routers (ISR) support single multimode G.fast and VDSL2 35b port, which are based on Fiber to X (FTTX) technology, to help accelerate ultra-broadband deployments at customer premises.

This chapter provides basic configuration procedures of the G.fast and VDSL2 35b and contains the following sections:


- Feature Information for G.fast and VDSL2 35b Profile, on page 165
- Restrictions for G.Fast and VDSL2 35b, on page 166
- Information About G.Fast and VDSL2 35b, on page 166
- Configure G.Fast and VDSL2 35b, on page 168
- Example: G.Fast and VDSL2 35b, on page 168
- Additional References for G.fast or VDSL2 35b, on page 171


## Feature Information for G.fast and VDSL2 35b Profile

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

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

*Table 19: Feature Information for G.Fast and VDSL2 35b*

| Feature Name | Releases | Feature Information |
|---|---|---|
| G.Fast and VDSL2 35b Profile | Cisco IOS XE Fuji Release 16.7.1 | Cisco 1000 Series Intergration Services Routers (ISR) uses G.fast and VDSL2 35b profiles, which are based on Fiber to X (FTTx) technology, to help accelerate ultra-broadband deployments at customer premises.<br>G.fast and VDSL2 35b are supported on the following platforms:<br>• Cisco ISR C1112<br>• Cisco ISR C1113<br>In this release, no commands were either introduced or modified by this feature. |

# Restrictions for G.Fast and VDSL2 35b

- G.Fast and VDSL2 35b profile is supported only on Cisco 1100 Series Integrated Services Routers (ISRs).

# Information About G.Fast and VDSL2 35b

## Overview of G.fast and VDSL2 35b

G.fast is a digital subscriber line (DSL) protocol standard for local loops shorter than 500 m, with performance targets between 150 Mbit/s and 1 Gbit/s, depending on loop length. G.fast uses the gigabit broadband access technology for plain old telephone service (POTS) services that provides ultra-broadband speeds over existing wired infrastructure.

According to ITU-T G.9701, G.fast supports asymmetric and symmetric transmission at an aggregate net data rate upto 1 Gbit per sec on twisted paired wires. G.fast uses a spectrum of upto 106 MHz with all the necessary functionalities to support far-end cross-talk (FEXT) cancellation between multiple paired wires, thereby facilitating low power operation.

VDSL2 35b operates on frequencies upto 35.324 MHz with subcarrier spacing of 4.3125 kHz, supports vectoring that is compatible with ITU-T G.993.2 profile 17a. VDSL2 35b supports service providers to optimize their network infrastructure, provides simplified deployment and provisioning options, thereby lowering the overall operational cost for implementing ITU-T G.993.2.

**Note** There is no specific command to implement G.fast on the Cisco 1000 Series Integrated Services Routers (ISRs).

## Benefits of Implementing G.fast

The ISR1000 series routers with G.fast technology provides better and improved performance using vectoring technology with dedicated speed upto 1 gigabits per sec.The infrastructural changes at customer premises is minimal because G.fast can co-exist with legacy xDSL. G.fast equipment can be deployed from fibre-fed distribution points (fibre to the distribution point, FTTdp) located very near the customer premises, or within buildings (fibre to the building, FTTB) where the existing copper wiring can be used.

# Key DSL features on G.fast and VDSL2 35b

- G.fast basic standards: ITU-T G.9700 [21], ITU-T G.9701 [22], ITU-T G.9701 Amendment 1 [23], ITU-T G.997.2 [24]
- 106a and 106b profiles are supported on all G.fast supported ISR1000 Series Integrated Services Routers.
- Firmware sub-package upgrade or downgrade
- Seamless Rate Adaptation (SRA)
- Fast Rate Adaption (FRA)
- Impulse noise protection
- DSL Line Train Logging
- Vectoring, G.993.5 (G.Vector)
- Dying gasp
- Bit Swap
- Auto-Sensing Support:
- G.fast/VDSL2 combo PHY
- G.fast US/DS ratio and start frequency range
- IOS CLI
- Controller Interface CLIs
- ATM/Ethernet Interface CLIs
- Show/Debug CLIs
- MIB Support
- ADSL-LINE MIB (RFC 2662)
- VDSL2-LINE-MIB (RFC 5650)
- ENTITY-MIB
- IF-MIB
- TR-069 (CWMP)

**Note** VDSL2 bonding is not supported on C1100 Series Integrated Services Routers.

SRA and Bit Swap are enabled by default.

For more information on firmware upgrade and training logs, refer to the Upgrading the Modem Firmware and Collecting DSL and Training Logs sections.

# Configure G.Fast and VDSL2 35b

## Configuring G.fast on the Cisco 1000 ISR

```
Device# configure terminal
   controller VDSL slot/subslot/port
   operating mode auto
end
```

### Before you begin

Configure the modem in the auto mode for the modem to work with G.fast and VDSL2 35b.

# Example: G.Fast and VDSL2 35b

## Example: The following is sample output for VDSL2 35b

```
Device# show controllers vdsL 0/3/0
Controller VDSL 0/3/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xC08A
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   '    '
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0x0000
Serial Number Near:     FGL215092KJ C1113-8P 16.8.20180
Serial Number Far:
Modem Version Near:     16.8.20180107:17011
Modem Version Far:      0xc08a

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.993.2 (VDSL2) Profile 35b

TC Mode:                PTM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running
```

```
Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.16L.05
Modem PHY Version:      A2pvfbH043j.d26r

Line 0:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     enabled                 enabled
SRA count:               0                       0
Bit swap:                enabled                 enabled
Bit swap count:          13                      0
Line Attenuation:         5.7 dB                  0.0 dB
Signal Attenuation:       6.4 dB                  0.0 dB
Noise Margin:             7.9 dB                 16.0 dB
Attainable Rate:        350000 kbits/s           61133 kbits/s
Actual Power:            7.0 dBm                 2.8 dBm
Per Band Status:        D1      D2      D3      U0      U1      U2      U3
Line Attenuation(dB):   3.2     3.6     6.7     N/A     0.0     0.0     N/A
Signal Attenuation(dB): 3.3     3.6     6.0     N/A     0.0     0.0     N/A
Noise Margin(dB):       8.1     8.0     7.9     N/A     19.1    14.8    N/A
Total FECC:             1968322                  1142
Total ES:               1005                     98
Total SES:              966                      88
Total LOSS:             77                       30
Total UAS:              50116                    48436
Total LPRS:             0                        0
Total LOFS:             1312                     0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):              NA          348077            NA             61133
SRA Previous Speed:        NA               0            NA                 0
Previous Speed:            NA          806105            NA            202881
Reed-Solomon EC:           NA           37263            NA                 0
CRC Errors:                NA             827            NA                63
Header Errors:             NA               0            NA                 0
Interleave (ms):           NA            0.00            NA              0.00
Actual INP:                NA           23.00            NA             22.00

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

# Example: The following is sample output for G.fast

```
Device# show controllers vdsL 0/3/0
Controller VDSL 0/3/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xC00E
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
```

**Example: The following is sample output for G.fast**

```
Serial Number Near:     FGL213191DQ C1113-8P 16.8.20171
Serial Number Far:      eq nr port:00  oemid softwarere
Modem Version Near:     16.8.20171023:08025
Modem Version Far:      0xc00e

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.9701 (GFAST) Profile 106b

TC Mode:                PTM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running

Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.16L.05
Modem PHY Version:      A2pvfbH043j.d26r

Line 0:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     enabled                 enabled
SRA count:               1                       5
Bit swap:                enabled                 enabled
Bit swap count:          0                       0
Line Attenuation:         0.0 dB                  0.0 dB
Signal Attenuation:       0.0 dB                  0.0 dB
Noise Margin:             6.4 dB                 8.9 dB
Attainable Rate:        833400 kbits/s          215007 kbits/s
Actual Power:            0.0 dBm                 4.1 dBm
RTX uc :                 0                       0
RTX tx :                 15                      26
BSW Completed :          1                       4
SRA Completed :          0                       2
FRA Completed :          0                       0
RPA Completed :          0                       0
TIGA Completed :         0                       0
Attainable Exp Thru:     833400                  214167
Error Free Thru :        805596                  202930
Total FECC:             351                     170
Total ES:               0                       0
Total SES:              0                       0
Total LOSS:             0                       0
Total UAS:              80545                   80545
Total LPRS:             0                       0
Total LOFS:             0                       0
Total LOLS:             0                       0

DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):              NA          805677            NA            202951
SRA Previous Speed:        NA          805687            NA            202920
Previous Speed:            NA          805677            NA            202920
Reed-Solomon EC:           NA             351            NA               170
CRC Errors:                NA               0            NA                 0
Header Errors:             NA               0            NA                 0
Interleave (ms):           NA         2810.82            NA              0.00
Actual INP:                NA            1.47            NA              0.00

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin
```

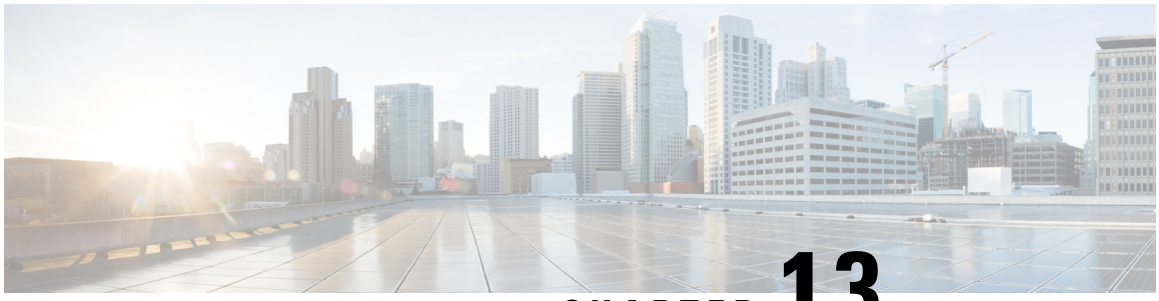
# Additional References for G.fast or VDSL2 35b

### MIBs

| MIB | MIBs Link |
|---|---|
| • CISCO-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the URL here:Cisco MIB Locator. |

### Technical Assistance

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



CHAPTER 13

# Encrypted Traffic Analytics

Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics uses Cisco NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time).


- Feature Information for Encrypted Traffic Analytics, on page 173
- Restrictions for Encrypted Traffic Analytics, on page 174
- Information About Encrypted Traffic Analytics, on page 174
- How to Configure Encrypted Traffic Analytics, on page 175
- Verifying the ET-Analytics Configuration, on page 176


# Feature Information for Encrypted Traffic Analytics

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

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

***Table 20: Feature Information for Encrypted Traffic Analytics (ET-Analytics)***

| Feature Name | Releases | Feature Information |
|---|---|---|
| Encrypted Traffic Analytics | | Encrypted Traffic Analytics (ET-Analytics) is used to identify malware communications in encrypted traffic. ET-Analytics uses passive monitoring, extraction of relevant data elements, and supervised machine learning with cloud-based global visibility. ET-Analytics uses Cisco NetFlow record fields to detect whether the packet flow has malware, and these NetFlow record fields include IDP (initial data packet) and SPLT (Sequence of Packet Length and Time). |

# Restrictions for Encrypted Traffic Analytics

ET-Analytics is not supported on management interfaces, VRF-Aware Software Infrastructure (VASI) interface, and internal interfaces.

# Information About Encrypted Traffic Analytics

## Data Elements for Encrypted Traffic

ET-Analytics uses intraflow metadata to identify malware components, maintaining the integrity of the encrypted traffic without the need for bulk decryption and without compromising on data integrity.

ET-Analytics extracts the following main data elements from the network flow: the sequence of packet lengths and times (SPLT), TLS-specific features, and the initial data packet (IDP). Cisco's Application-Specific Integrated Circuit (ASIC) architecture provides the ability to extract these data elements without slowing down the data network. Separate templates can be defined for each of the data elements.

Transport Layer Security (TLS) is a cryptographic protocol that provides privacy for applications. TLS is usually implemented with common protocols such as HTTP for web browsing or Simple Mail Transfer Protocol (SMTP) for email. HTTPS is the use of TLS over HTTP; this protocol is used to secure communication between a web server and client and is supported by most major web servers.

The TLS template is used to report several of the TLS parameters in use for a flow. These parameters help in finding the use of insecure cipher suites, out-of-date protocol version, and so on.

- Sequence of Packet Lengths and Times (SPLT) SPLT contains the length (number of bytes) of each packet's application payload for the first several packets of a flow, along with the inter-arrival times of those packets. SPLT can be represented as an array of packet sizes (in bytes) along with an array of times (in milliseconds) indicating the time since the previous packet was observed. The SPLT template is used to report packet size and timing information for a flow, which is useful to analyze encrypted traffic and find malicious flows or perform other classifications.
- Initial Data Packet (IDP) IDP obtains packet data from the first packet of a flow. It allows extraction of data such as an HTTP URL, DNS hostname/address, and other data elements. The TLS handshake is composed of several messages that contain unencrypted metadata used to extract data elements such as cipher suites, TLS versions, and the client's public key length. The IDP template is used to report packet data from the first data packet of a flow. This template allows collectors to perform application classification of a flow (for example, using Snort).

# How to Configure Encrypted Traffic Analytics

## Enabling ET-Analytics on an Interface

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal** | Enters global configuration mode. |
| **Step 3** | **et-analytics** | Enters encrypted traffic analytics configuration mode. |
| **Step 4** | **ip flow-record destination** *ip-address port* | Specifies NetFlow collector IP address and port number. A maximum of four exporters is supported. |
| **Step 5** | **exit** | Returns to global configuration mode. |
| **Step 6** | **interface** *interface-id* | Specifies the interface and port number and enters interface configuration mode. |
| **Step 7** | **et-analytics enable** | Enables encrypted traffic analytics on this interface. |
| **Step 8** | **end** | Returns to privileged EXEC mode. |

**Example**

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# ip flow-record destination 192.0.2.1 2055
Device(config-et-analytics)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# et-analytics enable
Device(config-if)# end
```

## Applying an ACL in the Allowed list

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable** | Enables privileged EXEC mode. |

| | Command or Action | Purpose |
|---|---|---|
| | | • Enter your password if prompted. |
| **Step 2** | **configure terminal** | Enters global configuration mode. |
| **Step 3** | **et-analytics** | Enters encrypted traffic analytics configuration mode. |
| **Step 4** | **whitelist acl** *access-list* | The allowed list specifies the access list traffic. The access list can be a standard, extended, or named ACL. |
| **Step 5** | **exit** | Returns to global configuration mode. |
| **Step 6** | **ip access-list extended** *access-list* | Specifies a named extended access list and enters extended access list configuration mode. |
| **Step 7** | **permit ip** {*ip-address* \| **any** \| **host** \| **object-group**} | Specifies the packets to forward to a source host or source IP address. |
| **Step 8** | **end** | Returns to privileged EXEC mode. |

### Example

```
Device> enable
Device# configure terminal
Device(config)# et-analytics
Device(config-et-analytics)# whitelist acl eta_whitelist
Device(config-et-analytics)# exit
Device(config)# ip access-list extended eta_whitelist
Device(config-ext-nacl)# permit ip host 198.51.100.1 any
Device(config-ext-nacl)# permit ip any host 198.51.100.1
Device(config-ext-nacl)# permit ip host 198.51.200.1 any
Device(config-ext-nacl)# permit ip any host 198.51.200.1
Device(config-ext-nacl)# end
```

# Verifying the ET-Analytics Configuration

The following **show** commands are used to see the platform ET-analytics, threat-visibility interfaces, FMAN FP global and interface information, and ET-analytics datapath information. Given below are the sample outputs of the **show** commands.

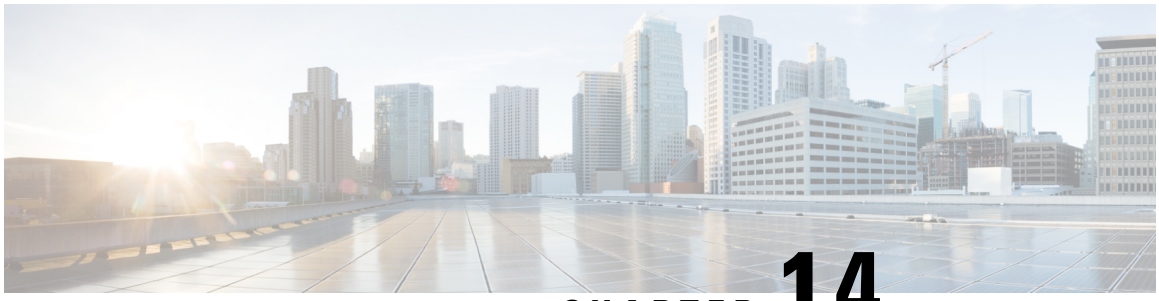
```
Device# show platform hardware qfp active feature et-analytics data interface gigabitEthernet
 2

uidb handle: 0x3fe
Interface Name: GigabitEthernet2
```

```
Device# show platform hardware qfp active feature et-analytics data memory

  ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 952903
   No. of FO frees       : 952902


Device# show platform hardware qfp active feature et-analytics data runtime

  ET-Analytics run-time information:

   Feature state         : initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   Flow CFG information  :   !Flow Table Infrastructure information internal to ETA!
       instance ID       : 0x0
       feature ID        : 0x0
       feature object ID : 0x0
       chunk ID          : 0x4


Device# show platform hardware qfp active feature et-analytics datapath stats export

  ET-Analytics 192.168.1.100:2055 Stats:
    Export statistics:
      Total records exported     : 2967386
      Total packets exported     : 1885447
      Total bytes exported       : 2056906120
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 805813
            responder->initiator : 418799
      Total SPLT records exported:
            initiator->responder : 805813
            responder->initiator : 418799
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 171332
            responder->initiator : 174860
ET-Analytics 172.27.56.99:2055 Stats:
    Export statistics:
      Total records exported     : 2967446
      Total packets exported     : 1885448
      Total bytes exported       : 2056909280
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
      Total IDP records exported :
            initiator->responder : 805813
            responder->initiator : 418799
      Total SPLT records exported:
            initiator->responder : 805813
```

```
          responder->initiator : 418799
   Total SALT records exported:
          initiator->responder : 0
          responder->initiator : 0
      Total BD records exported  :
          initiator->responder : 0
          responder->initiator : 0
      Total TLS records exported :
          initiator->responder : 171332
          responder->initiator : 174860
```

**Device# show platform hardware qfp active feature et-analytics datapath stats flow**

```
  ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```



CHAPTER 14

# Configuring Traffic Storm Control

This topic describes how to configure the Traffic Storm Control feature on a Cisco 1000 Series Integrated Services Router, and contains the following sections:


- Information About Traffic Storm Control, on page 179
- Prerequisites for Traffic Storm Control, on page 179
- Limitations of Traffic Storm Control, on page 179
- Configuring Traffic Storm Control, on page 180
- Example: Configuring a Traffic Storm Control, on page 181
- Feature Information for Traffic Storm Control, on page 181


## Information About Traffic Storm Control

A traffic storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance. This feature prevents LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces.

This feature when configured ensures that the rate does not exceed the configured policer rate. When the traffic exceeds the configured rate, packets are dropped to control the traffic.

## Prerequisites for Traffic Storm Control

Ensure that you configure a separate storm control policer for each of the unicast, broadcast, and multicast traffic types. It is important to configure traffic storm control policer for each traffic type. For example, multicast traffic will not be controlled traffic if you do not configure a storm control policer for it. If a storm control policer is not configured for multicast traffic, the traffic load may exceed which is the expected behavior and that adds load to the customer network, especially when this traffic is caused by any misconfiguration or a cyberattack.

## Limitations of Traffic Storm Control

- Only bandwidth as percentage is used to measure traffic activity.
- Storm control is detected based on interface counter or hardware module reports (depending on the platform).

- Storm control is specific to physical interfaces.
- Storm control is only supported for unicast, broadcast, and multicast ingress traffic.

# Configuring Traffic Storm Control

Perform the following steps to configure traffic storm control:

**Note** Traffic storm control is disabled by default.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router>enable` | Enables privileged EXEC mode. Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router#configure terminal` | Enters global configuration mode. |
| **Step 3** | **storm-control** {**unicast** \| **broadcast** \| **multicast**} **level** {*level_high*}{*level_low*}<br>**Example:**<br>• **Unicast control**<br>`Router(config-if)#storm-control unicast level 70.00 50.00`<br>• **Broadcast Control**<br>`Router(config-if)#storm-control broadcast level 70.00 50.00`<br>• **Multicast Control**<br>`Router(config-if)#storm-control multicast level 70.00 50.00` | Specifies the interface level unicast, broadcast, or multicast storm control suppression level as a percentage of the total bandwidth. Here, the bandwidth is dependent on the operational speed.<br>**Unicast**: Configures the known and unknown unicast storm control.<br>**Broadcast**: Configures broadcast storm control.<br>**Multicast**: Configures multicast storm control.<br>**Level**: Specifies the threshold levels for broadcast, multicast, or unicast traffic. |
| **Step 4** | **storm-control action** { **shutdown** \| **trap**}<br>**Example:**<br>`Router(config-if)#storm control action trap` | Specifies the action to take when a storm occurs on a port.<br>The traffic is blocked when it exceeds the threshold specified by configuration level, irrespective of the shutdown or SNMP trap being enabled or disabled. |

| | Command or Action | Purpose |
|---|---|---|
| | | • **shutdown**: The interface enters err-disable state when traffic exceeds the threshold specified by configuration level.<br>• **trap**: The interface sends an SNMP trap event when traffic exceeds the threshold specified by configuration level.<br>**Note** You can enable the **shutdown** and **trap** actions simultaneously. |
| **Step 5** | **exit** | Exits interface configuration mode and returns the router to global configuration mode. |

# Example: Configuring a Traffic Storm Control

### Example: Configuring a Traffic Storm Control

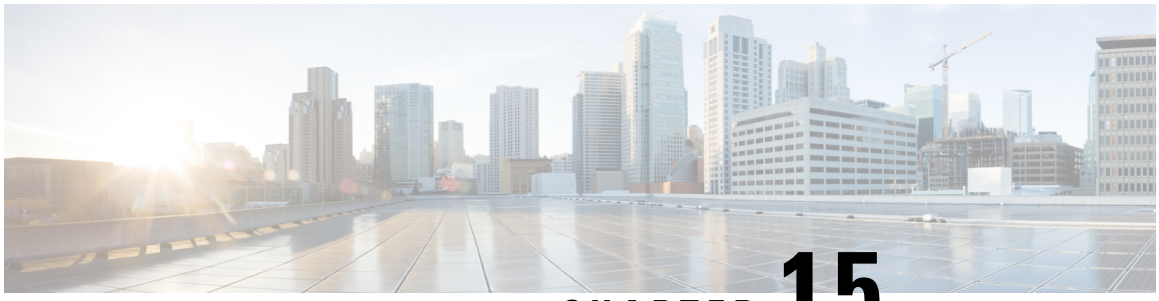
```
Router(config)#int gi0/1/0
Router(config-if)#storm-control unicast level 70.00 50.00
Router(config-if)#storm-control broadcast level 70.00 50.00
Router(config-if)#storm-control multicast level 70.00 50.00
Router(config-if)#storm-control action shutdown
Router(config-if)#storm-control action trap
```

# Feature Information for Traffic Storm Control

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

*Table 21: Feature Information for Traffic Storm Control*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Traffic storm control support on L2 switch ports | Cisco IOS XE Cupertino 17.8.1a Release | • Starting from Cisco IOS XE Cupertino 17.7.x, Traffic Storm Control is supported on all the existing C11xx (C110x, C111x, C112, C113x, C116x) models.<br>• Starting from Cisco IOS XE Cupertino 17.8.x, Traffic Storm Control is supported on C1113 and C1131 series.<br><br>Traffic storm control is configured to reduce excessive traffic when packets flood the LAN. Configuring traffic storm control helps in preventing LAN ports from being disrupted by a broadcast, multicast, or unicast traffic storm on physical interfaces. |



CHAPTER 15

# Smart Licensing

This chapter contains the following sections:


- Smart Licensing Client, on page 183


# Smart Licensing Client

Smart Licensing Client feature is a standardized licensing platform that simplifies the Cisco software experience and helps you to understand how Cisco software is used across your network. Smart Licensing is the next generation licensing platform for all Cisco software products.

## Prerequisites for Cisco Smart Licensing Client

- Ensure that Call Home is not disabled before using the Smart Licensing Client feature.

## Restrictions for Cisco Smart Licensing Client

- You require a virtual account in the Smart Licensing server for registration.

## Information About Cisco Smart Licensing Client

### Cisco Smart Licensing - An Overview

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

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

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (http://software.cisco.com/).

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

## HSECK9

The **HSECK9** license is required for a feature to have full crypto functionality. Without the **HSECK9** license, only 225 secure tunnels and 85 Mbps of crypto bandwidth would be available. The **HSECK9** license allows features in the **securityk9** technology package to use the maximum number of secure tunnels and crypto bandwidth. To enable the **HSECK9** license, purchase the **FL-44-HSEC-K9** license from Cisco.com and install it using the **license install** *license-files* command. For further information on obtaining and installing feature licenses, see configuring the Cisco IOS software activation.

**Note** The **HSECK9** feature does not have an evaluation license that converts to an RTU license after 60 days; a feature license must be obtained.

To enable the license for the **HSECK9** feature, use the **securityk9** technology package.

For more information on how to enable license boot level securityk9 or license feature hseck9, refer to Smart Licensing using Policy.

## Transitioning from CSL to Smart Licensing

In the Smart Licensing Model, customers can activate licensed objects without the use of a special software key or upgrade license file. The customers simply activate the new functionality using the appropriate product commands and configurations and the functionality is activated. A software reboot may or may not be required depending on the product capabilities and requirements.

Similarly, downgrading or removing an advanced feature, performance, or functionality would require a removal of the configuration or command.

Once either of these actions has been taken, the change in license state is noted by the Smart Software Manager upon next synchronization and an appropriate action is then taken.

### Cisco One Suites

Cisco ONE Suites is a new way for customers to purchase infrastructure software. Cisco ONE offers a simplified purchasing model, centered on common customer scenarios in the data center, wide area network, and local access networks.

# Cisco One Suites

Cisco ONE Suites is a new way for customers to purchase infrastructure software. Cisco ONE offers a simplified purchasing model, centered on common customer scenarios in the data center, wide area network, and local access networks.

# How to Activate Cisco Smart Licensing Client

## Enable Smart Licensing

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **license smart enable**<br>**Example:**<br>`Device# license smart enable` | Activates Smart Licensing on the device.<br>**Note** When you enable Smart Licensing, the Cisco Software License (CSL) and all licensing calls pass through the Smart Agent.<br>For the 'no' case, if Smart Licensing is already registered, the Smart Agent performs the "license smart deregister" operation that deactivates Smart Licensing. |
| **Step 4** | **exit**<br>**Example:**<br>`Device# exit` | Exits the global configuration mode. |
| **Step 5** | **write memory**<br>**Example:**<br>`Device# write memory` | Saves the running configuration to NVRAM. |
| **Step 6** | **show license all**<br>**Example:**<br>`Device# show license all` | (Optional) Displays summary information about all licenses. |

# Device Registration

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 2** | **license smart register idtoken** *idtoken* [**force**]<br>**Example:**<br>`Device# license smart register idtoken 123` | Registers the device with the back-end server. Token id can be obtained from your virtual a/c in the Smart Licensing server.<br>• **force**: To forcefully register your device irrespective of either the device is registered or not.<br>**Note** The device supplies the token ID to the Cisco server, which sends back a "Device Certificate" that is valid for 365 days. |
| **Step 3** | **license smart deregister**<br>**Example:**<br>`Device# license smart deregister` | Deregisters the device from the backend server. |
| **Step 4** | **license smart renew** [**ID** \| **auth**]<br>**Example:**<br>`Device# license smart renew ID` | (Optional) Manually renews the ID certification or authorization. |

# Install and Upgrade Licenses Using Software Activation Commands

### Before you begin

To install or upgrade a license by using the **license install** command, you must have already received the license file from the Cisco Product License Registration portal at http://www.cisco.com/go/license (or you already backed up the license by using the **license save** command).

If you use Microsoft Entourage and receive the license file from Cisco in an e-mail attachment, the license file will contain UTF-8 marking. These extra bytes in the license file cause it to be unusable during license installation. To work around this issue, you can use a text editor to remove the extra characters and then install the license file. For more information about UTF-8 encoding, go to this URL: http://www.w3.org/International/questions/qa-utf8-bom.

**Note** The installation process does not install duplicate licenses. This message appears when duplicate licenses are detected:

```
Installing...Feature:xxx-xxx-xxx...Skipped:Duplicate
```

**Note** A standby device reboots twice when there is a mismatch of licenses.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Obtain the PAK. | The PAK is provided to you when you order or purchase the right to use a feature set for a particular platform.<br>• The PAK serves as a receipt and is used as part of the process to obtain a license. |
| **Step 2** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>• Enter your password if prompted. |
| **Step 3** | **show license udi**<br>**Example:**<br>`Device# show license udi` | Displays all the UDI values that can be licensed in a system.<br>• You need the UDI of the device as part of the process to obtain a license. |
| **Step 4** | Convert the PAK to a license by entering the PAK and the UDI into the Cisco Product License Registration portal: http://www.cisco.com/go/license. | After entering the appropriate information, you will receive an e-mail containing the license information that you can use to install the license:<br>• Copy the license file received from the Cisco Product License Registration portal to the appropriate file system on the device.<br>or<br>• Click the **Install** button on the web page. |
| **Step 5** | **license install** *stored-location-url*<br>**Example:** | Installs the license.<br>• Accept the end-user license agreement if prompted. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device# license install tftp://infra-sun/<user>/license/5400/38a.lic` | |
| **Step 6** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters the global configuration mode. |
| **Step 7** | **license boot level** {**metroaggrservices**}<br>**Example:**<br>`Device(config)# license boot level metroaggrservices` | Activates the metroaggrservices license on the device upon the next reload. |
| **Step 8** | **write memory**<br>**Example:**<br>`Device# write memory` | Saves the running configuration to NVRAM. |
| **Step 9** | **reload**<br>**Example:**<br>`Device# reload` | (Optional) Restarts the device to enable the new feature set.<br>**Note** A reload is not required when moving from an evaluation license to a permanent license of the same license level on the devices. |

# Troubleshooting for Cisco Smart Licensing Client

You can troubleshoot Smart Licensing enabling issues using the following commands on the device:

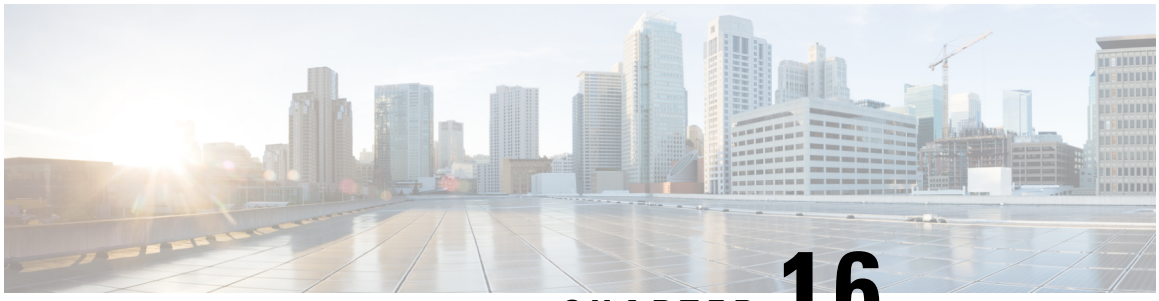
- **show version**
- **show running-config**
- **show license summary**
- **show license all**
- **show license tech support**
- **show license status**
- **debug smart_lic error**
- **debug smart_lic trace**

# Configuration Examples for Cisco Smart Licensing Client

## Example: Displays summary information about all licenses

## Example: Enabling Smart Licensing

Use the **license smart enable** command to confirm if Smart Licensing is enabled.



CHAPTER 16

# Configuring Bridge Domain Interfaces

The Cisco 1000 Series ISR devices support the bridge domain interface (BDI) feature for packaging Layer 2 Ethernet segments into Layer 3 IP address.


- Restrictions for Bridge Domain Interfaces, on page 191
- Information About Bridge Domain Interface, on page 192
- Configuring Bridge-Domain Virtual IP Interface, on page 200
- Additional References, on page 206
- Feature Information for Configuring Bridge Domain Interfaces, on page 207


## Restrictions for Bridge Domain Interfaces

The following are the restrictions pertaining to bridge domain interfaces:

- Only 4096 bridge domain interfaces are supported per system.
- For a bridge domain interface, the maximum transmission unit (MTU) size can be configured between 1500 and 9216 bytes.
- Bridge domain interfaces support only the following features:
  - IPv4 Multicast
  - QoS marking and policing. Shaping and queuing are not supported
  - IPv4 VRF
  - IPv6 unicast forwarding
  - Dynamic routing such as BGP, OSPF, EIGRP, RIP, IS-IS, and STATIC
  - Hot Standby Router Protocol (HSRP) from IOS XE 3.8.0 onwards.
  - Virtual Router Redundancy Protocol (VRRP) from IOS XE 3.8.0 onwards.
  - Flexible NetFlow

**Note** Flexible NetFlow is supported from Cisco IOS XE 17.7.1a and later releases.

- Bridge domain interfaces do not support the following features:
  - PPP over Ethernet (PPPoE)
  - Bidirectional Forwarding Detection (BFD) protocol
  - QoS
  - Network-Based Application Recognition (NBAR) or Advanced Video Coding (AVC)

# Information About Bridge Domain Interface

Bridge domain interface is a logical interface that allows bidirectional flow of traffic between a Layer 2 bridged network and a Layer 3 routed network traffic. Bridge domain interfaces are identified by the same index as the bridge domain. Each bridge domain represents a Layer 2 broadcast domain. Only one bridge domain interface can be associated with a bridge domain.

Bridge domain interface supports the following features:

- IP termination
- Layer 3 VPN termination
- Address Resolution Protocol (ARP), G-ARP, and P-ARP handling
- MAC address assignment

Prior to configuring a bridge domain interface, you must understand the following concepts:

- Ethernet Virtual Circuit Overview
- Bridge Domain Interface Encapsulation
- Assigning a MAC Address
- Support for IP Protocols
- Support for IP Forwarding
- Packet Forwarding
- Bridge Domain Interface Statistics

## Ethernet Virtual Circuit Overview

An Ethernet Virtual Circuit (EVC) is an end-to-end representation of a single instance of a Layer 2 service that is offered by a provider. It embodies the different parameters on which the service is being offered. In the Cisco EVC Framework, the bridge domains are made up of one or more Layer 2 interfaces known as service instances. A service instance is the instantiation of an EVC on a given port on a given router. Service instance is associated with a bridge domain based on the configuration.

An incoming frame can be classified as service instance based on the following criteria:

- Single 802.1Q VLAN tag, priority-tagged, or 802.1ad VLAN tag
- Both QinQ (inner and outer) VLAN tags, or both 802.1ad S-VLAN and C-VLAN tags

- Outer 802.1p CoS bits, inner 802.1p CoS bits, or both
- Payload Ethernet type (five choices are supported: IPv4, IPv6, PPPoE-all, PPoE-discovery, and PPPoE-session)

Service instance also supports alternative mapping criteria:

- Untagged—Mapping to all the frames lacking a 802.1Q or 802.1ad header
- Default—Mapping to all the frames

For more information on the EVC architecture, see the section *Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Router* in the Carrier Ethernet Configuration Guide .

# Bridge Domain Interface Encapsulation

Security Group classification includes both Source and Destination Group, which is specified by source SGT and DGT. SGT Based PBR feature provides the PBR route-map match clause for SGT/DGT based packet classification. SGT Based PBR feature supports configuration of unlimited number of tags, but it is recommended to configure the tags based on memory available in the platform.

An EVC provides the ability to employ different encapsulations on each Ethernet flow point (EFP) present in a bridge domain. A BDI egress point may not be aware of the encapsulation of an egress packet because the packet may have egressed from one or more EFPs with different encapsulations.

In a bridge domain, if all the EFPs have different encapsulations, the BDI must be untagged (using the no 802.1Q tag). Encapsulate all the traffic in the bridge domain (popped or pushed) at the EFPs. Configure rewrite at each EFP to enable encapsulation of the traffic on the bridge domain.

In a bridge domain, if all the EFPs have the same encapsulation, configure the encapsulations on the BDI using the encapsulation command. Enabling encapsulation at the BDI ensures effective pushing or popping of tags, thereby eliminating the need for configuring the rewrite command at the EFPs. For more information on configuring the encapsulations on the BDI, see the How to Configure a Bridge Domain Interface.

# Assigning a MAC Address

All the bridge domain interfaces on the Cisco 1000 Series ISR chassis share a common MAC address. The first bridge domain interface on a bridge domain is allocated a MAC address. Thereafter, the same MAC address is assigned to all the bridge domain interfaces that are created in that bridge domain.

**Note** You can configure a static MAC address on a bridge domain interface using the **mac-address** command.

# Support for IP Protocols

Bridge domain interfaces enable the Cisco 1000 Series ISR devices to act as a Layer 3 endpoint on the Layer 2 bridge domain for the following IP-related protocols:

- ARP
- DHCP

- HTTP
- ICMP
- NTP
- RARP
- SNMP
- TCP
- Telnet
- TFTP
- UDP

# Support for IP Forwarding

Bridge domain interface supports the following IP forwarding features:

- IPv4 input and output access control lists (ACL)
- IPv4 input and output QoS policies. The operations supported for the input and output service policies on a bridge domain interface are:
  - Classification
  - Marking
  - Policing
- IPv4 L3 VRFs

# Packet Forwarding

A bridge domain interface provides bridging and forwarding services between the Layer 2 and Layer 3 network infrastructure.

## Layer 2 to Layer 3

During a packet flow from a Layer 2 network to a Layer 3 network, if the destination MAC address of the incoming packet matches the bridge domain interface MAC address, or if the destination MAC address is a multicast address, the packet or a copy of the packet is forwarded to the bridge domain interface.

**Note** MAC address learning cannot not be performed on the bridge domain interface.

## Layer 3 to Layer 2

When a packet arrives at a Layer 3 physical interface of a router, a route lookup action is performed. If route lookup points to a bridge domain interface, then the bridge domain interface adds the layer 2 encapsulation and forwards the frame to the corresponding bridge domain. The byte counters are updated.

During a Layer 2 lookup on a bridge domain to which the bridge domain interface belongs, the bridge domain forwards the packets to the correct service instance based on the destination MAC address.

# Link States of a Bridge Domain and a Bridge Domain Interface

Bridge domain interface acts as a routable IOS interface on Layer 3 and as a port on a bridge domain. Both bridge domain interfaces and bridge domains operate with individual administrative states.

Shutting down a bridge domain interface stops the Layer 3 data service, but does not override or impact the state of the associated bridge domain.

Shutting down a bridge domain stops Layer 2 forwarding across all the associated members including service instances and bridge domain interfaces. The associated service instances influence the operational state of a bridge domain. Bridge domain interface cannot be operational unless one of the associated service instances is up.

**Note** Because a bridge domain interface is an internal interface, the operational state of bridge domain interface does not affect the bridge domain operational state.

## BDI Initial State

The initial administrative state of a BDI depends on how the BDI is created. When you create a BDI at boot time in the startup configuration, the default administrative state for the BDI is up. It will remain in this state unless the startup configuration includes the shutdown command. This behavior is consistent with all the other interfaces. When you create a BDI dynamically at command prompt, the default administrative state is down.

## BDI Link State

A BDI maintains a link state that comprises of three states: administratively down, operationally down, and up. The link state of a BDI is derived from two independent inputs: the BDI administrative state set by the corresponding users and the fault indication state from the lower levels of the interface states. It defines a BDI link state based on the state of the two inputs.

| **Fault Indication State** | **BDI Admin** | |
|---|---|---|
| {start emdash}{end emdash} | **Shutdown** | **No Shutdown** |
| **No faults asserted** | Admin-down | Up |
| **At least one fault asserted** | Admin-down | Operationally-Down |

# Bridge Domain Interface Statistics

For virtual interfaces, such as the bridge domain interface, protocol counters are periodically queried from the QFP.

When packets flow from a Layer 2 bridge domain network to a Layer 3 routing network through the bridge domain interface, the packets are treated as bridge domain interface input packets and bytes. When packets arrive at a Layer 3 interface and are forwarded through the bridge domain interface to a Layer 2 bridge domain, the packets are treated as output packets and bytes, and the counters are updated accordingly.

A BDI maintains a standard set of Layer 3 packet counters as the case with all Cisco IOS interfaces. Use the show interface command to view the Layer 3 packet counters.

The convention of the counters is relative to the Layer 3 cloud. For example, input refers to the traffic entry to the Layer 3 cloud from the Layer 2 BD, while output refers to the traffic exit from the Layer 3 cloud to the Layer 2 BD.

Use the **show interfaces accounting** command to display the statistics for the BDI status. Use the **show interface** <*if-name*> command to display the overall count of the packets and bytes that are transmitted and received.

# Creating or Deleting a Bridge Domain Interface

When you define an interface or subinterface for a Cisco IOS router, you name it and specify how it is assigned an IP address. You can create a bridge domain interface before adding a bridge domain to the system. This new bridge domain interface will be activated after the associated bridge domain is configured.

**Note** When a bridge domain interface is created, a bridge domain is automatically created.

When you create the bridge domain interface and the bridge domain, the system maintains the required associations for mapping the bridge domain-bridge domain interface pair.

The mapping of bridge domain and bridge domain interface is maintained in the system. The bridge domain interface uses the index of the associated bridge domain to show the association.

# Bridge Domain Interface Scalability

The following table lists the bridge domain interface scalability numbers, based on the type of Cisco 1000 Series ISR devices' Forwarding Processors (FPs).

***Table 22: Bridge Domain Interface Scalability Numbers Based on the Type of Cisco 1000 Series ISR devices' Forwarding Processor***

| Description | 0 |
|---|---|
| Maximum bridge domain interfaces per router | |

# Bridge-Domain Virtual IP Interface

The Virtual IP Interface (VIF) feature helps to associate multiple BDI interfaces with a BD instance. The BD-VIF interface inherits all the existing L3 features of IOS logical IP interface.

**Note** You must configure every BD-VIF interface with a unique MAC address and it should belong to a different VRF.

The Virtual IP Interface (VIF) feature has the following limitations:

- BD-VIF interface does not support IP multicast.

- Number of BD-VIF interfaces with automatically generated MAC address varies on the basis of platforms.
- BD-VIF Interface does not support MPLS.
- The maximum number of BD-VIF interfaces per bridge-domain and the total number of BD-VIF interface for per system vary based on the type of platforms.

The maximum number of BD-VIF supported on different platforms varies:

- ASR 1000 supports maximum 100 BD-VIF for a Bridge Domain
- CSR 1000v supports maximum 16 BD-VIF for a Bridge Domain
- ISR 4000 support maximum 16 BD-VIF for a Bridge Domain

From Cisco IOS XE 17.7.1a release, BD-VIF supports Flexible Netflow (FNF).

# How to Configure a Bridge Domain Interface

To configure a bridge domain interface, perform the following steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode. Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface BDI** *{interface number}*<br>**Example:**<br>`Router(config-if)# interface BDI3` | Specifies a bridge domain interface. |
| **Step 4** | **encapsulation** *encapsulation dot1q <first-tag> [second-dot1q <second-tag>]*<br>**Example:**<br>`Router(config-if)# encapsulation dot1Q 1 second-dot1q 2` | Defines the encapsulation type.<br>The example shows how to define dot1q as the encapsulation type. |
| **Step 5** | Do one of the following:<br>**Example:**<br>**ip address** *ip-address mask*<br>**Example:** | Specifies either the IPv4 or IPv6 address for the bridge domain interface. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>**ipv6 address** *{X:X:X:X::X* **link-local**\| *X:X:X:X::X/prefix* *[***anycast** \| **eui-64***]* \| **autoconfig** *[***default***]}*<br>**Example:**<br>`Router(config-if)# ip address 10.2.2.1 255.255.255.0`<br>**Example:**<br>**Example:**<br>`Router(config-if)# ipv6 address AB01:CD1:123:C::/64 eui-64` | |
| **Step 6** | **match security-group destination tag** *sgt-number*<br>**Example:**<br>`Router(config-route-map)# match security-group destination tag 150` | Configures the value for security-group destination security tag. |
| **Step 7** | **mac address** *{mac-address}*<br>**Example:**<br>`Router(config-if)# mac-address 1.1.3` | Specifies the MAC address for the bridge domain interface. |
| **Step 8** | **no shut**<br>**Example:**<br>`Router(config-if)# no shut` | Enables the bridge domain interface. |
| **Step 9** | **shut**<br>**Example:**<br>`Router(config-if)# shut` | Disables the bridge domain interface. |

# Example

The following example shows the configuration of a bridge domain interface at IP address 10.2.2.1 255.255.255.0:

```
Router# configure terminal
Router(config)# interface BDI3
Router(config-if)# encapsulation dot1Q 1 second-dot1q 2
```

```
Router(config-if)# ip address 10.2.2.1 255.255.255.0
Router(config-if)# mac-address 1.1.3
Router(config-if)# no shut
Router(config-if)# exit
```

# Displaying and Verifying Bridge Domain Interface Configuration

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Router> enable` | Enables privileged EXEC mode. Enter your password, if prompted. |
| **Step 2** | **show interfaces bdi**<br>**Example:**<br>`Router# show interfaces BDI3` | Displays the configuration summary of the corresponding BDI. |
| **Step 3** | **show platform software interface fp active name**<br>**Example:**<br>`Router# show platform software interface fp active name BDI4` | Displays the bridge domain interface configuration in a Forwarding Processor. |
| **Step 4** | **show platform hardware qfp active interface if-name**<br>**Example:**<br>`Router# show platform hardware qfp active interface if-name BDI4` | Displays the bridge domain interface configuration in a data path. |
| **Step 5** | **debug platform hardware qfp feature**<br>**Example:**<br>`Router# debug platform hardware qfp active feature l2bd client all` | The selected CPP L2BD Client debugging is on. |
| **Step 6** | **platform trace runtime process forwarding-manager module**<br>**Example:**<br>`Router(config)# platform trace runtime slot F0 bay 0 process` | Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Forwarding Manager process. |

| | Command or Action | Purpose |
|---|---|---|
| | **forwarding-manager module interfaces level info** | |
| **Step 7** | **platform trace boottime process forwarding-manager module interfaces**<br>**Example:**<br>`Router(config)# platform trace boottime slot R0 bay 1 process forwarding-manager forwarding-manager level max` | Enables the Forwarding Manager Route Processor and Embedded Service Processor trace messages for the Route Processor Forwarding Manager process during bootup. |

### What to do next

For additional information on the commands and the options available with each command, see the Cisco IOS Configuration Fundamentals Command Reference Guide.

# Configuring Bridge-Domain Virtual IP Interface

```
enable
configure terminal
[no] interface BD-VIF interface-number
  [ [no] vrf forwarding vrf-name]
  [ [no] mac address mac-address]
  [ [no] ip address ip-address mask]
  [ [no] ipv6 address {X:X:X:X::X link-local| X:X:X:X::X/prefix [anycast | eui-64] |
autoconfig [default]}]

exit
```

To delete BD-VIF interface, use the 'no' form of the command.

# Associating VIF Interface with a Bridge Domain

```
enable
configure terminal
bridge-domain bridge-domain number
[no] member BD-VIF interface-number
exit
```

To dissociate the VIF interface, use the 'no' form of the command.

# Verifying Bridge-Domain Virtual IP Interface

All existing show commands for interface and IP interface can be used for the BD-VIF interface.

show interface bd-vif *bd-vif-id*

show ip interface bd-vif *bd-vif-id*

show bd-vif interfaces in fman-fp

show pla sof inter fp ac brief | i BD_VIF

# Example Configuration Bridge-Domain Virtual IP Interface

```
Detail sample:

interface Port-channel1
mtu 9000
no ip address
 !Ethernet service endpoint one per neutron network
service instance 1756 ethernet
  description 4e8e5957-649f-477b-9e5b-f1f75b21c03c
  encapsulation dot1q 1756
  rewrite ingress tag pop 1 symmetric
  bridge-domain 1756
!
interface BD-VIF5001
no shutdown
vrf forwarding vrf5001
ip address 10.0.0.1 255.255.255.0
interface BD-VIF5002
no shutdown
vrf forwarding vrf5002
ip address 10.0.0.2 255.255.255.0

bridge-domain 1756
member Port-channel1 service-instance 1756
member bd-vif5001
member bd-vif5002
```

# Configuring Flexible NetFlow over a Bridge Domain Virtual IP Interface

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password, if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** *type number*<br>**Example:**<br>`Device (config)# interface BD-VIF 100` | Specifies an interface and enters interface configuration mode. Enter the BD-VIF number. |
| **Step 4** | {**ip** \| **ipv6**}**flow monitor** *monitor-name* [**sampler** *sampler-name*] {**input** \| **output**}<br>**Example:** | Enables a Flexible NetFlow flow monitor for IP traffic that the router is receiving or transmitting on the interface. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-if)# ip flow monitor FLOW-MONITOR-1 input` | |
| **Step 5** | **exit**<br>**Example:**<br>`Device(config-if)# exit` | Exits interface configuration mode and returns to privileged EXEC mode. |

# Examples: Flexible NetFlow over a Bridge Domain Virtual IP Interface

The following is a sample output for the **show platform hardware qfp active interface if-name** command showing the QFP information and flow direction for flow monitors. The table below provides the key to the CLI output.

| Configuration | Output |
|---|---|
| ip flow monitor <monitor-name> input | IPV4_INPUT_FNF_FIRST<br>IPV4_INPUT_FNF_FINAL |
| ip flow monitor <monitor-name> output | IPV4_BDI_OUTPUT_FNF_FINAL |
| ipv6 flow monitor <monitor-name> input | IPV6_INPUT_FNF_FIRST<br>IPV6_INPUT_FNF_FINAL |
| ipv6 flow monitor <monitor-name> output | IPV6_BDI_OUTPUT_FNF_FINAL |

```
Device# show run interface bd-vif2
Building configuration...

Current configuration: 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
ipv6 flow monitor test2 output
ipv6 address 2001:DB8::1/32
end

Device# show platform hardware qfp active interface if-name BD-VIF 2
General interface information
  Interface Name: BD-VIF2
  Interface state: VALID
  Platform interface handle: 20
  QFP interface handle: 17
  Rx uidb: 262138
  Tx uidb: 262127
  Channel: 0
Interface Relationships

BGPPA/QPPB interface configuration information
  Ingress: BGPPA/QPPB not configured. flags: 0000
  Egress: BGPPA not configured. flags: 0000
```

```
ipv4_input enabled.
ipv4_output enabled.
ipv6_input enabled.
ipv6_output enabled.
layer2_input enabled.
layer2_output enabled.
ess_ac_input enabled.

Features Bound to Interface:
2 GIC FIA state
66 PUNT INJECT DB
70 cpp_l2bd_svr
43 icmp_svr
45 ipfrag_svr
46 ipreass_svr
47 ipv6reass_svr
44 icmp6_svr
58 stile
Protocol 0 - ipv4_input
FIA handle - CP:0x55a7f59df038 DP:0x3fff1000
  IPV4_INPUT_DST_LOOKUP_ISSUE (M)
  IPV4_INPUT_ARL_SANITY (M)
  IPV4_INPUT_SRC_LOOKUP_ISSUE
  IPV4_INPUT_DST_LOOKUP_CONSUME (M)
  IPV4_INPUT_SRC_LOOKUP_CONSUME
  IPV4_INPUT_FOR_US_MARTIAN (M)
  IPV4_INPUT_STILE_LEGACY
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_LOOKUP_PROCESS (M)
  IPV4_INPUT_FNF_FINAL
  IPV4_INPUT_IPOPTIONS_PROCESS (M)
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x55a7f59df0d8 DP:0x3ffeff00
  IPV4_VFR_REFRAG (M)
  IPV4_OUTPUT_SRC_LOOKUP_ISSUE
  IPV4_OUTPUT_L2_REWRITE (M)
  IPV4_OUTPUT_SRC_LOOKUP_CONSUME
  IPV4_OUTPUT_STILE_LEGACY
  IPV4_OUTPUT_FRAG (M)
  IPV4_BDI_OUTPUT_FNF_FINAL.
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
Protocol 6 - ipv6_input
FIA handle - CP:0x55a7f59dee58 DP:0x3fff4300
  IPV6_INPUT_SANITY_CHECK (M)
  IPV6_INPUT_DST_LOOKUP_ISSUE (M)
  IPV6_INPUT_SRC_LOOKUP_ISSUE
  IPV6_INPUT_ARL (M)
  IPV6_INPUT_DST_LOOKUP_CONT (M)
  IPV6_INPUT_SRC_LOOKUP_CONT
  IPV6_INPUT_DST_LOOKUP_CONSUME (M)
  IPV6_INPUT_SRC_LOOKUP_CONSUME
  IPV6_INPUT_STILE_LEGACY
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FOR_US (M)
  IPV6_INPUT_LOOKUP_PROCESS (M)
  IPV6_INPUT_FNF_FINAL
  IPV6_INPUT_LINK_LOCAL_CHECK (M)
  IPV6_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 7 - ipv6_output
```

```
FIA handle - CP:0x55a7f59dee08 DP:0x3fff4b80
  IPV6_VFR_REFRAG (M)
  IPV6_OUTPUT_SRC_LOOKUP_ISSUE
  IPV6_OUTPUT_SRC_LOOKUP_CONT
  IPV6_OUTPUT_SRC_LOOKUP_CONSUME
  IPV6_OUTPUT_L2_REWRITE (M)
  IPV6_OUTPUT_STILE_LEGACY
  IPV6_OUTPUT_FRAG (M)
  IPV6_BDI_OUTPUT_FNF_FINAL
  BDI_VLAN_TAG_ATTACH_AND_LAYER2_LOOKUP_GOTO
  LAYER2_BRIDGE
  BDI_OUTPUT_GOTO_OUTPUT_FEATURE
  IPV6_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

The following is a sample out of the **show flow monitor** [[**name**] [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] command showing the cache output in record format.

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record

Cache type:  Normal
Cache size:  1000
Current entries:  4
High Watermark:  4
Flows added:  101
Flows aged:  97
- Active timeout (1800 secs) 3
- Inactive timeout  (15 secs) 94
- Event aged  0
- Watermark aged  0
- Emergency aged
IPV4 DESTINATION ADDRESS:
198.51.100.1 0
ipv4 source address: 10.10.11.1
trns source port: 25
trns destination port: 25
counter bytes: 72840
counter packets: 1821
IPV4 DESTINATION ADDRESS: 198.51.100.2
ipv4 source address: 10.10.10.2
trns source port: 20
trns destination port: 20
counter bytes: 3913860
counter packets: 7326
IPV4 DESTINATION ADDRESS: 198.51.100.200
ipv4 source address: 192.168.67.6
trns source port: 0
trns destination port: 3073
counter bytes: 51072
counter packets: 1824


Device# show flow monitor name FLOW-MONITOR-2 cache format record

Cache type:  Normal
Cache size: 1000
Current entries: 2
High Watermark: 3
Flows added: 95
Flows aged: 93
- Active timeout (1800 secs) 0
- Inactive timeout (15 secs) 93
- Event aged 0
- Watermark aged 0
```

```
- Emergency aged 0
IPV6 DESTINATION ADDRESS: 2001:DB8:0:ABCD::1
ipv6 source address: 2001:DB8:0:ABCD::2
trns source port: 33572
trns destination port: 23
counter bytes: 19140
counter packets: 349
IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address: 2001:DB8::A8AA:BBFF:FEBB

trns source port: 521
trns destination port: 521
counter bytes: 92
counter packets: 1
```

The following is a sample out of the **show flow interface** command showing the flow status for an interface.

```
Device# show flow interface BD-VIF2001

Interface GigabitEthernet0/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Input
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on

Device# show flow interface BD-VIF2002

Interface GigabitEthernet1/0/0
FNF: monitor: FLOW-MONITOR-1
direction: Output
traffic(ip): on
FNF: monitor: FLOW-MONITOR-2
direction:    Input traffic(ipv6): on
```

The following is a sample output of the **show platform hardware qfp active interface if-name** | **in FNF** command showing the QFP information and flow direction for flow monitors in Flexible NetFlow configuration. The table below provides the key to the CLI output.

| Configuration | Output |
|---|---|
| ip flow monitor <monitor-name> input | IPV4_INPUT_FNF_FIRST<br>IPV4_INPUT_FNF_FINAL |
| ip flow monitor <monitor-name> output | IPV4_BDI_OUTPUT_FNF_FINAL |
| ipv6 flow monitor <monitor-name> input | IPV6_INPUT_FNF_FIRST<br>IPV6_INPUT_FNF_FINAL |
| ipv6 flow monitor <monitor-name> output | IPV6_BDI_OUTPUT_FNF_FINAL |

```
Device# show run interface bd-vif2
Building configuration...

Current configuration : 227 bytes
!
interface BD-VIF2
vrf forwarding vrf1
ip flow monitor test1 input
ip flow monitor test1 output
ip address 10.11.11.11 255.255.255.0
ipv6 flow monitor test2 input
```

```
ipv6 flow monitor test2 output
ipv6 address 2001::8/64
end
 Device# show platform hardware qfp active interface if-name BD-VIF 2  | in FNF
  IPV4_INPUT_FNF_FIRST
  IPV4_INPUT_FNF_FINAL
  IPV4_BDI_OUTPUT_FNF_FINAL.
  IPV6_INPUT_FNF_FIRST
  IPV6_INPUT_FNF_FINAL
  IPV6_BDI_OUTPUT_FNF_FINAL
```

The **clear flow monitor name** *monitor-name* [**cache** [**force-export**] | **force-export** | **statistics**] command clears a Flexible NetFlow flow monitor, flow monitor cache, or flow monitor statistics, and can be used to force the export of the data in the flow monitor cache.

For more details on configuring Flexible NetFlow, see the Flexible NetFlow Configuration Guide, Cisco IOS XE 17.

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Configuring Ethernet Virtual Connections on the Cisco ASR 1000 Series Aggregation Services Routers | Carrier Ethernet Configuration Guide |
| EVC Quality of Service | http://www.cisco.com/en/US/docs/ios/ios_xe/qos/configuration/guide/qos_evc_xe.html |

### MIBs

| MIB | MIBs Link |
|---|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | https://www.cisco.com/c/en_in/support/index.html |

# Feature Information for Configuring Bridge Domain Interfaces

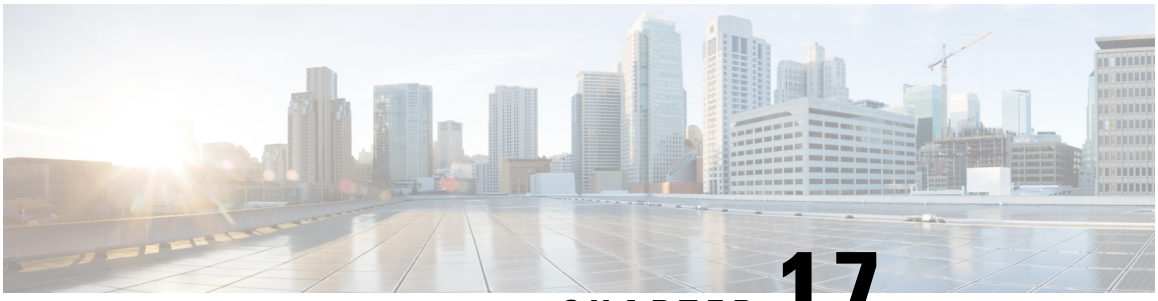
The following table lists the features in this module and provides links to specific configuration information.

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

**Note** The table below lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

*Table 23: Feature Information for Configuring Bridge Domain Interfaces*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Configuring Bridge Domain Interface | Cisco IOS XE Cupertino 17.7.1a | This feature was introduced on the Cisco 1000 Series ISR devices. |
| Bridge-Domain Virtual IP Interface | Cisco IOS XE Cupertino 17.7.1a | This feature was introduced on the Cisco 1000 Series ISR devices.<br>The Bridge-Domain Virtual IP Interface (VIF) now connects multiple Bridge Domain Interfaces (BDI) with a single BD instance so that each IP subnet within an L2 network can be associated with a single VRF. |
| Flexible NetFlow (FNF) on Bridge-Domain Virtual IP Interface (BD-VIF) | Cisco IOS XE Cupertino 17.7.1a | This feature was introduced on the Cisco 1000 Series ISR devices. The following command was introduced:<br>**{ip \| ipv6} flow monitor** *monitor-name* **[sampler** *sampler-name***] {input \| output}** |



CHAPTER 17

# Configuring VDSL2 and ADSL2/22 Plus for Cisco C1100 Series ISRs

VDSL2 and ADSL2/2+ Cisco C1100 Series Integrated Services Router provide highly reliable WAN connections for remote sites. These interfaces offer cost-effective virtualized WAN connections in both point-to-point and point-to-multipoint designs.

Organization needs high speed digital data transmission to operate between their data equipment and central office, usually located at the telecom service provider premises. The Cisco multimode VDSL2 and ADSL1/2/2+ provides 1-port (2-pair) multimode VDSL2 and ADSL2+ WAN connectivity. This connectivity in combination with Cisco C1100 Series Integrated Service Routers, provides high-speed digital data transmission between customer premises equipment (CPE) and the central office.

This capability enables service providers and resellers to offer additional services, such as business-class security, voice, video, and data; differentiated classes of service (QoS), and managed network access over existing telephony infrastructure. These value-added features, along with the flexible manageability and reliability of Cisco IOS Software, provide the mission-critical networking features that businesses expect.

The following table describes the VDSL2 and ADSL2/2+ Variants:

| Product Number | Description |
|---|---|
| C1117-4P - Annex A | 1-port (2-pair) VDSL2/ADSL2+ over POTS<br>• VDSL2 over POTS Band Plans<br>• VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a<br>• Vectoring<br>• ADSL1/2/2+ Annex A, ADSL2 Annex L, non-optimized ADSL2/2+ Annex M |
| C1117-4PM - Annex M | 1-port (2-pair) VDSL2/ADSL2+ over POTS with Annex M<br>• VDSL2 over POTS Band Plans<br>• VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a |

| Product Number | Description |
|---|---|
| | • Vectoring<br>• Optimized ADSL2/2+ Annex M<br>• ADSL/ADSL2/2+ Annex A |
| C1116-4P - Annex B/J | 1-port (1-pair) VDSL2/ADSL2+ over ISDN<br>• ADSL1/2/2+ Annex B, non-optimized ADSL2/2+ Annex J<br>• VDSL2 over ISDN Band Plans (8a to 17a) with Vectoring |

For more information on DSLAM interoperability, refer to the Cisco Multimode VDSL2 and ADSL2/2 Network Interface Module Datasheet.


- DSL Feature Specifications, on page 210
- Configuring DSL, on page 211
- Features Supported in xDSL , on page 215
- Show and Debug Commands, on page 229
- Sample Configurations, on page 247


# DSL Feature Specifications

***Table 24: DSL Feature Specifications***

| | |
|---|---|
| Multimode DSL (VDSL2 and ADSL2/2+) | • Broadcom chipset<br>• One RJ-14 VDSL2 interface<br>• Independent module firmware subpackage loading<br>• Dying gasp<br>• Support for double-ended line testing (DELT) diagnostics mode |

*Table 25: VDSL2 Feature Specifications*

| | |
|---|---|
| VDSL2 | • ITU G.993.2 (VDSL2) and ITU G.993.5 (VDSL2)<br>• 997 and 998 band plans<br>• VDSL2 profiles: 8a, 8b, 8c, 8d, 12a, 12b, and 17a<br>• Vectoring<br>• U0 band support (25 to 276 kHz)<br>• Ethernet packet transfer mode (PTM) based only on IEEE 802.3ah 64/65 octet encapsulation |

*Table 26: ADSL2/2+ Feature Specifications*

| | |
|---|---|
| ADSL2/2+ | • ADSL over POTS with Annex A and Annex B ITU G. 992.1 (ADSL), G.992.3 (ADSL2), and G.992.5 (ADSL2+)<br>• ADSL over POTS with Annex M (extended upstream bandwidth) G.992.3 (ADSL2) and G.992.5 (ADSL2+)<br>• G.994.1 ITU G.hs<br>• Reach-extended ADSL2 (G.922.3) Annex L for increased performance on loop lengths greater than 16,000 feet from central office<br>• T1.413 ANSI ADSL DMT issue 2 compliance<br>• DSL Forum TR-067, and TR-100 conformity<br>• Impulse noise protection (INP) and extended INP<br>• Downstream power backoff (DPBO)<br>• Asynchronous transfer mode (ATM) only<br>• Maximum 8 PVCs per interface |

# Configuring DSL

Cisco C1100 Series Integrated Services Routers (ISRs) support asymmetric digital subscriber line (ADSL) 1/2/2+ and very high speed digital subscriber line 2 (VDSL2) transmission modes, also called multimode.

## Configuring ADSL

Perform the below mentioned steps to configure a DSL controller.

# Configuring Auto Mode

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`router> enable` | Enables privileged EXEC mode. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **controller VDSL** *slot/subslot/port*<br>**Example:**<br>`router(config-controller)# controller vdsl 0/3/0` | Enters configuration mode for the VDSL controller. |
| **Step 4** | **operating mode** *auto*<br>**Example:**<br>`router(config-controller)# operating mode auto` | Configures the auto operating mode, which is the default configuration. |
| **Step 5** | **end**<br>**Example:**<br>`router(config-controller)# end` | Exits controller configuration mode. |

# Configuring ADSL1 and ADSL2/2+ plus Annex A and Annex M Mode

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`router> enable` | Enables privileged EXEC mode. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **controller VDSL** *slot/subslot/port*<br>**Example:**<br>`router(config-controller)# controller vdsl 0/3/0` | Enters configuration mode for the VDSL controller. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **operating mode** {*adsl1* \| *adsl2 annex a* \| *annex m* \| *adsl2+ annex a* \| *annex m]*}<br>**Example:**<br>`router(config-controller)# operating mode adsl2+ annex m` | Configures the operating mode.<br>• ADSL1—Configures operation in ITU G.992.1 Annex A full-rate mode.<br>• ADSL2—Configures operation in ADSL2 operating mode-ITU G.992.3 Annex A, Annex L, and Annex M. If an Annex operating mode is not chosen, Annex A, Annex L, and Annex M are enabled. The final mode is decided by negotiation with the DSL access multiplexer (DSLAM).<br>• ADSL2+—Configures operation in ADSL2+ mode-ITU G.992.5 Annex A and AnnexM. If an Annex A operating mode is not chosen, both Annex and Annex M is enabled. The final mode is decided by negotiation with DSLAM.<br>• Annex A and M—(Optional) If the annex option is not specified, both Annex A and Annex M are enabled. The final mode is decided by negotiation with the Digital Synchronous Line Access Multiplexer (DSLAM). |
| **Step 5** | **end**<br>**Example:**<br>`router(config-controller)# end` | Exits controller configuration mode. |

# Configuring VDSL2

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`router> enable` | Enables privileged EXEC mode. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`router# configure terminal` | Enters global configuration mode. |
| **Step 3** | **controller VDSL** *slot/subslot/port*<br>**Example:** | Enters configuration mode for the VDSL controller. |

| | Command or Action | Purpose |
|---|---|---|
| | `router(config-controller)# controller vdsl 0/3/0` | |
| **Step 4** | **operating mode** *mode*<br>**Example:**<br>`router(config-controller)# operating mode vdsl2` | Configures the operating mode. The operating mode is VDSL2. Enables 8a through 17a profile. |
| **Step 5** | **end**<br>**Example:**<br>`router(config-controller)# end` | Exits controller configuration mode. |

# Examples of DSL Interface Configuration

In Cisco IOS XE, ATM PVCs can be configured under ATM sub-interfaces only. PVC configuration is not allowed under the main ATM interface. You can configure 8 point to point sub-interfaces either with one PVC configured under each point to point sub-interface or single multi-point sub-interface.

You do not need to configure the **tx-ring-limit** command in the Cisco C1100 Series Integrated Services Routers, if you are migrating from classic Cisco IOS and using**tx-ring-limit** command to reduce the latency. Because the DSL modules buffers have been fine tuned for the optimal performance and latency.

The following example shows how to configure ATM interface:

```
interface ATM0/3/0
 no ip address
 no atm oversubscribe
 no atm enable-ilmi-trap
 no shut


interface ATM0/3/0.1 point-to-point
 ip address 192.0.2.1 255.255.255.0
 no atm enable-ilmi-trap
 pvc 1/77
 vbr-rt 400 400
```

The following example shows how to configure Ethernet interface.

```
interface Ethernet0/3/0
 ip address 192.0.2.1 255.255.255.0
 load-interval 30
 no negotiation auto
```

If the trained mode is VDSL2 or VDSL2+, the TC mode should be in Packet Transfer Mode (PTM). In this case, the PTM Ethernet interface is in the **up** state. All other upper layer parameters such as PPP, IP, and so on should be configured under the Ethernet interface. If the trained mode is ADSL, ADSL2, or ADSL2+, the TC mode should be ATM and all the upper layer parameters should be configured under the ATM Permanent Virtual Circuit (PVC). If you change the operating mode between ADSL and VDSL, you need not to reboot the router in order to activate the corresponding Ethernet or ATM interfaces. In case of PTM mode, check with your ISP if they are expecting Dot1q tag configuration on the CPE. ISP should provide Dot1q tag value.

```
Router(config)#interface Ethernet0.835

Router(config-subif)#encapsulation dot1Q 835

Router(config-subif)#pppoe-client dial-pool-member 1
```

# Features Supported in xDSL

## ATM Conditional Debug Support

Most ATM debugging commands are implemented either at the system level or at the interface level. The ATM Conditional Debug Support feature allows debugging to be limited specifically to an ATM interface, to a virtual channel identifier (VCI), or to a virtual path identifier/virtual channel identifier (VPI/VCI) pair, through use of the debug condition interface command.

For more information on configuring ATM conditional debug support feature, see the ATM Conditional Debug Support document.

## ATM OAM Loopback Mode Detection

The Loopback Mode Detection Through OAM feature allows you to enable automatic detection of when a peer ATM interface is in loopback mode. When loopback is detected on an interface where end-to-end F5 Operation, Administration, and Maintenance (OAM) is enabled, the impacted permanent virtual circuit (PVC) is moved to a DOWN state, and traffic is suspended. When the loopback condition in the peer ATM interface is removed, the PVC is moved back to an UP state.

For more information on configuring ATM OAM Loopback Mode Detection, see the Loopback Mode Detection through OAM document.

## ATM Oversubscription for DSL

The ATM Oversubscription for DSL feature enables users to improve network utilization of otherwise underutilized shared networks by leveraging statistical multiplexing on ATM networks. Instead of supporting only unconditional reservation of network bandwidth to VBR PVCs, the Router offers PVC oversubscription to statistically guarantee bandwidth to VBR PVCs.

In Cisco IOS XE Release 3.14.0S or later, the ATM Oversubscription feature enables you to specify the amount of oversubscription (oversubscription factor) equal to twice the line rate. Following are the features of oversubscription:

- Oversubscription is allowed on VBR-rt and VBR-nrt.
- Under no over subscription condition, PVCs can be configured up to line rate. For example, if the line rate is 1000 Kbps. The SCR or PCR of a VBR PVC cannot be more than 1000 Kbps if there are no other PVCs. If there is a CBR PVC with PCR of 500Kbps, then the maximum SCR or PCR allowed on the VBR PVC is 500 Kbps.
- When over-subscription is enabled, multiple VBR-rt or VBR-nrt PVCs are allowed to be configured even if the sum of their SCRs exceeds the actual bandwidth available over the physical line. Suppose oversubscription is enabled and over subscription factor of 2 is set for a line rate of 1000k sum of SCRs of VBR-rt and VBR-nrt can be less than or equal to 2000k, this is excluding CBR PVCs bandwidth.

- If the user configures VBR-rt or VBR-nrt more than the configured oversubscription factor then PVC will be configured for the bandwidth available. If there is no oversubscription bandwidth left then VC will be downgraded to UBR. For example for line rate of 1000k, with oversubscription factor 2: PVC1 is vbr-rt 400k 400k, PVC2 is vbr-nrt 1600k 1600k and PVC3 is vbr-rt 500k 500k. In this case the PVC1 and PVC2 will be configured to given pcr and scr, PVC3 will be downgraded to UBR class.
- If there is no bandwidth left, then some PVCs may be downgraded to UBR class.
- PCR & SCR of VBR PVC can never exceed the line rate even if there is enough available bandwidth for the configured PCR and SCR.

Oversubscription of the ATM interfaces is enabled by default and is subject to infinite oversubscription factor which is not supported on DSL NIM. User must enable oversubscription factor.

The following configuration enables the oversubscription 2. The only oversubscription factor supported is 2.

```
Router(config)#interface atm 0/3/0
Router(config-if)#atm oversubscription factor 2
Router(config-if)#exit
```

To disable oversubscription of the interface, use the no atm oversubscribe command.

For example, the following configuration disables oversubscription of the ATM 0/1/0 interface:

```
Router(config)#interface atm 0/3/0
Router(config-if)#no atm oversubscribe
Router(config-if)#exit
```

**Example**:

Below is the example for the sum of pvc rates less than the line rate of 1561kbps.

```
Router#show atm pvc
      VCD /                 Peak Av/Min Burst
Interface Name VPI VCI Type Encaps SC Kbps Kbps Cells St

0/3/0.1 2     0 32 PVC SNAP CBR 300 UP
                  (C) CBR 300
0/3/0.2 3     0 33 PVC SNAP CBR 100 UP
                  (C) CBR 100
0/3/0.3 4     0 34 PVC SNAP VBR 400 200 10 UP
                  (C) VBR 400 200 10
0/3/0.4 5     0 35 PVC SNAP VBR 600 300 10 UP
                  (C) VBR 600 300 10
0/3/0.5 6     0 36 PVC SNAP VBR 300 150 10 UP
                  (C) VBR 300 150 10
0/3/0.6 7     0 37 PVC SNAP VBR 700 450 10 UP
                  (C) VBR 700 450 10
0/3/0.7 8     0 38 PVC SNAP UBR 1561 UP
                  (C) UBR 0
0/3/0.8 1     0 39 PVC SNAP UBR 1000 UP
                  (C) UBR 1000
```

When line rate gets downgraded to 294 kbps, CBR and VBR PVC rates gets adjusted dynamically as below.

```
Router#show atm pvc

       VCD /                 Peak Av/Min Burst
Interface Name VPI VCI Type Encaps SC Kbps Kbps Cells St
```

```
0/3/0.1 2     0 32 PVC SNAP CBR 294 UP
                  (C) CBR 300
0/3/0.2 3     0 33 PVC SNAP UBR 294 UP
                  (C) CBR 100
0/3/0.3 4     0 34 PVC SNAP VBR 294 200 10 UP
                  (C) VBR 400 200 10
0/3/0.4 5     0 35 PVC SNAP VBR 294 294 1 UP
                  (C) VBR 600 300 10
0/3/0.5 6     0 36 PVC SNAP VBR 94 94 1 UP
                  (C) VBR 300 150 10
0/3/0.6 7     0 37 PVC SNAP UBR 294 UP
                  (C) VBR 700 450 10
0/3/0.7 8     0 38 PVC SNAP UBR 294 UP
                  (C) UBR 0
0/3/0.8 1     0 39 PVC SNAP UBR 294 UP
                  (C) UBR 1000
```

# ATM Routed Bridge Encapsulation (RBE)Concept

ATM routed bridge encapsulation (RBE) is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN.

For more information on configuring ATM RBE, see the Providing Connectivity Using ATM Routed Bridge Encapsulation over PVCs document.

# Default Route on a PPP Virtual Access Interface

If a Virtual-Template (VT) interface is configured to obtain its IP address by IPCP, the dynamically created Virtual-Access (VA) interface gets the IP address after PPP negotiation. Since the Virtual-access is created dynamically, we cannot configure mappings on the dynamic interface. Also, there is no way to configure a static route through the virtual-access interface; we need to insert a default route via the next-hop address for the virtual-access and this is achieved using "ppp ipcp route default".

For more information on the usage of the command, see the ppp ipcp default route command document.

# Dynamic Bandwidth Change for ATM PVCs

The ATM Dynamic Bandwidth for ATM PVCs over DSL feature provides the ability to configure Cisco IOS-XE software to automatically adjust PVC bandwidth in response to changes in the total available interface bandwidth. This feature eliminates the manual intervention every time DSL line rate changes, and allows the available bandwidth to be used effectively at all times.

It is recommended to enable ATM Dynamic Bandwidth feature on ATM interfaces. For more information on enabling the ATM Dynamic Bandwidth feature, refer the section "Enabling ATM Dynamic Bandwidth" .

**Note**

- When there is a change in line condition or DSL line flaps, ATM interface Bandwidth gets updated after line condition is stable. PVC Service Class bandwidth and Multilink Bundle bandwidth (if MLPPP is configured) gets adjusted dynamically. As a result, traffic flows according to the adjusted bundle bandwidth.
- When "bandwidth x" is configured under dialer and there is a change in line condition or DSL line flaps, ATM interface Bandwidth gets updated after line condition is stable. PVC Service Class bandwidth gets adjusted dynamically, but Multilink Bundle bandwidth (if MLPPP is configured) does not get updated dynamically because of fixed dialer bandwidth configuration. Because of this, throughput might not be achieved as expected. It is recommended not to configure "bandwidth x" under dialer interface for MLP ATM configurations to be in sync with ATM interface/Service Class bandwidth.

## Enabling ATM Dynamic Bandwidth

By default ATM dynamic bandwidth feature is enabled. If ATM dynamic bandwidth is disabled, perform the below steps to enable the feature:

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int atm0/3/0
Router(config-if)#atm bandwidth dynamic
Router(config-if)#end
Router#
```

**Sample configuration:**

```
!
interface ATM0/3/0
 no ip address
 load-interval 30
 no atm enable-ilmi-trap
!
```

Show atm pvc output with atm dynamic bandwidth enabled.

Example 1:

```
Router#show atm pvc
        VCD /               Peak Av/Min Burst
Interface Name VPI VCI Type Encaps SC Kbps Kbps Cells St
0/1/0.1 1 8 37 PVC MUX UBR 1045 UP
                  (C) UBR 0
Router#
```

Example 2:

```
Router#show atm pvc
      VCD /                 Peak Av/Min Burst
Interface Name VPI VCI Type Encaps SC Kbps Kbps Cells St
0/3/0.1 2 0 32 PVC SNAP CBR 294 UP
                   (C) CBR 300
```

**Note** (C) is the configured rates.

In example 2, CBR PVC was configured with PCR as 300 kbps. Due to line rate change, PCR rate has dynamically changed to 294 kbps.

## Disabling ATM Dynamic Bandwidth

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int atm0/3/0
Router(config-if)#no atm bandwidth dynamic
Router(config-if)#end
Router#
Router#sh run int atm0/3/0
Building configuration...

Current configuration : 110 bytes
!
interface ATM0/3/0
 no ip address
 load-interval 30
 no atm bandwidth dynamic
 no atm enable-ilmi-trap
end

Router#
```

Show atm pvc output with atm dynamic bandwidth feature disabled:

```
Router#show atm pvc | sec 0/3/0
0/1/0.1 1 8 37 PVC MUX UBR 1045 UP
Router#
```

## How the ATM Dynamic Bandwidth Feature Works

When the total available bandwidth on a DSL interface changes, all of the PVCs configured under the ATM sub-interface(s) are re-created.

If necessary and applicable for a particular PVC based on its service class, new values are applied for the following parameters when PVCs are re-created:

- PCR—peak cell rate
- SCR—sustainable cell rate

The following steps are performed by the Cisco IOS-XE software to determine what value should be assigned to a parameter when a PVC is re-created in response to a change in total available bandwidth:

- A value is calculated for the parameter. The calculation takes into account the configured value for the parameter, the active value for the parameter (if it is different from the configured value), and the change in total available bandwidth.
- The calculated value is compared to the configured value of the parameter and to the maximum available cell rate, and a new value is determined. The new value is applied when the PVC is re-created.

The following sections describe how the new parameter values are determined when a PVC is re-created for supported QoS classes:

### CBR PVCs

When the total available bandwidth changes, PVCs configured with CBR service class are recreated as follows:

- If the configured PCR value is less than the calculated PCR value, the PVC is recreated with the configured PCR value.
- If the configured PCR value is greater than the calculated PCR value, the PVC is recreated with the calculated value with no change in class.
- If there is no bandwidth left for the CBR PVC, then CBR PVCs will be downgraded to UBR class with a PCR value equal to the maximum available rate.

### VBR PVCs

When the total available bandwidth changes, PVCs configured with VBR service class are re-created as follows:

- If the configured PCR value is less than the calculated PCR value, the PVC is recreated with the configured PCR value.
- If the configured PCR value is greater than the calculated PCR value, the PVC is recreated with a new PCR value. The new PCR value will be the lower of the following values:
  - The calculated PCR value
  - The maximum available cell rate
- If the configured SCR value is less than the calculated PCR value, the PVC is re-created with the configured SCR value.
- If the configured SCR value is greater than the calculated PCR value, the PVC is recreated with a new SCR value. The new SCR value will be the lower of the following values:
  - The calculated PCR value
  - The maximum available cell rate

### UBR PVCs

When the total available bandwidth changes, PVCs configured with UBR service class are re-created as follows:

- If the PCR configuration is set to the default, the PVC is re-created with a PCR value equal to the new line rate.
- If the configured PCR value is less than the calculated PCR value, the PVC is re-created with the configured PCR value.
- If the configured PCR value is greater than the calculated PCR value, the PVC is recreated with a new PCR value. The new PCR value will be the lower of the following values:
  - The calculated PCR value

- New line rate

**Example:**

Below is the example for the sum of pvc rates less than the line rate of 1561kbps.

```
Router#show atm pvc
     VCD /                  Peak Av/Min Burst
Interface Name VPI VCI Type Encaps SC Kbps Kbps Cells St

0/3/0.1 2    0 32 PVC SNAP CBR 300 UP
                 (C) CBR 300
0/3/0.2 3    0 33 PVC SNAP CBR 100 UP
                 (C) CBR 100
0/3/0.3 4    0 34 PVC SNAP VBR 400 200 10 UP
                 (C) VBR 400 200 10
0/3/0.4 5    0 35 PVC SNAP VBR 600 300 10 UP
                 (C) VBR 600 300 10
0/3/0.5 6    0 36 PVC SNAP VBR 300 150 10 UP
                 (C) VBR 300 150 10
0/3/0.6 7    0 37 PVC SNAP VBR 700 450 10 UP
                 (C) VBR 700 450 10
0/3/0.7 8    0 38 PVC SNAP UBR 1561 UP
                 (C) UBR 0
0/3/0.8 1    0 39 PVC SNAP UBR 1000 UP
                  (C) UBR 1000
```

When line rate gets downgraded to 687kbps, CBR and VBR PVC rates gets adjusted dynamically as below.

```
Router#show atm pvc
VCD / Peak Av/Min Burst
Interface Name VPI VCI Type Encaps SC Kbps Kbps Cells St

0/3/0.1 2     0 32 PVC SNAP CBR 300 UP
                   (C) CBR 300
0/3/0.2 3     0 33 PVC SNAP CBR 100 UP
                   (C) CBR 100
0/3/0.3 4     0 34 PVC SNAP VBR 287 200 10 UP
                   (C) VBR 400 200 10
0/3/0.4 5     0 35 PVC SNAP VBR 87 87 1 UP
                   (C) VBR 600 300 10
0/3/0.5 6     0 36 PVC SNAP UBR 687 UP
                   (C) VBR 300 150 10
0/3/0.6 7     0 37 PVC SNAP UBR 687 UP
                   (C) VBR 700 450 10
0/3/0.7 8     0 38 PVC SNAP UBR 687 UP
                   (C) UBR 0
0/3/0.8 1     0 39 PVC SNAP UBR 687 UP
                   (C) UBR 1000
```

# Upgrading the Firmware on DSL Interface

To upgrade the firmware on a DSL interface, perform these steps:

### Before you begin

When you boot the router in packages.conf mode with the Cisco IOS XE image (super package) during the installation period, you can upgrade or downgrade the firmware without reloading the router.

If you do not boot the router in packages.conf mode with the Cisco IOS XE image, you must follow the prerequisites given below, before proceeding with the firmware upgrade:

- Copy the firmware subpackage into bootflash:/mydir.
- Type the **request platform software package expand file** command *boot flash:/mydir/<IOS-XE image>* to expand the super package.
- Type the **reload** command to load the module with the new firmware
- Boot the router with *packages.conf*.
- Copy the firmware subpackage to the folder *bootflash:mydir/*.
- Issue **request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>* .
- Reload the hardware module subslot to boot the module with the new firmware.
- Verify that the module is booted up with the new firmware using the **show platform software subslot 0/3 module firmware** command.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | copy Cisco IOS XE image into bootflash: **mydir**.<br>**Example:**<br>`Router# mkdir bootflash:mydir` | Creates a directory to save the expanded software image.<br>You can use the same name as the image to name the directory. |
| **Step 2** | **request platform software package expand file** *bootflash:/mydir /<IOS-XE image* to expand super package.<br>**Example:**<br>`Router# request platform software package expand file bootflash:/mydir/c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin` | Expands the platform software package to super package. |
| **Step 3** | **reload**.<br>**Example:**<br>`Router# reload`<br>`rommon >` | Enables ROMMON mode, which allows the software in the super package file to be activated. |
| **Step 4** | **boot bootflash:mydir/ /packages.conf**.<br>**Example:**<br>`rommon 1 > boot bootflash:mydir/packages.conf` | Boots the super package by specifying the path and name of the provisioning file: packages.conf. |
| **Step 5** | **copy** firmware subpackage to the folder **bootflash:mydir/**.<br>**Example:**<br>`Router#copy bootflash:c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin` | Copies the firmware subpackage into bootflash:mydir. |

| | Command or Action | Purpose |
|---|---|---|
| | `bootflash:mydir/` | |
| **Step 6** | **request platform software package install** *rp 0 file bootflash:/mydir/<firmware subpackage>.*<br>**Example:**<br>`Router#`**`request platform software package install rp 0 file`**<br>`bootflash:mydir/c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin` | Installs the software package. |
| **Step 7** | **hw-module subslot x/y reload** to boot the module with the new firmware.<br>**Example:**<br>`Router#`**`hw-module subslot 0/3 reload`** | Reloads the hardware module subslot and boots the module with the new firmware. |
| **Step 8** | **show platform software subslot 0/3 module firmware** to verify that the module is booted up with the new firmware.<br>**Example:**<br>`Router#` **`show platform software subslot 0/3 module firmware`**<br>`Pe` | Displays the version of the newly installed firmware. |

The following example shows how to perform firmware upgrade in a router module:

```
Routermkdir bootflash:mydir
Create directory filename [mydir]?
Created dir bootflash:/mydir
Router#c
Router#copy bootflash:c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin bootflash:mydir/
Destination filename [mydir/c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCC 425288648 bytes copied in 44.826 secs (9487544 bytes/sec)
Router#
Router#
Router#dir bootflash:mydir
Directory of bootflash:/mydir/
632738 -rw- 425288648 Dec 12 2014 09:16:42 +00:00
c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin
7451738112 bytes total (474025984 bytes free)
Router#

Router#request platform software package
expand file bootflash:/mydir/c1100-universalk9.03.14.00.S.155-1.S-std.SPA.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router#reload
```

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

[OK]
Proceed with reload? [confirm]
Rom image verified correctly

System Bootstrap, Version C900-1100-20170915-SDR52-Micron-Toshiba, DEVELOPMENT SOFTWARE
Copyright (c) 1994-2017 by cisco Systems, Inc.

Current image running: Boot ROM1

Last reset cause: LocalSoft
C1111-8PLTEEAWR platform with 4194304 Kbytes of main memory


rommon 1  boot bootflash:mydir/packages.conf

File size is 0x000028f1 Located mydir/packages.conf Image size 10481 inode num 632741, bks
 cnt 3 blk size 8*512 # File size is 0x150ae3cc Located mydir/
c1100-universalk9.03.14.00.S.155-1.S-std. SPA.pkg Image size 353035212 inode num 356929,
bks cnt 86191 blk size 8*512
###################################################################
################################################################### Boot image size =
353035212 (0x150ae3cc) bytes Package header rev 1 structure detected Calculating SHA-1
hash...done validate_package: SHA-1 hash: calculated
8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3 expected
8e966678:8afb08f4:8a88bb8f:fe591121:8bddf4b3 RSA Signed RELEASE Image Signature Verification
 Successful. Package Load Test Latency : 3799 msec Image validated Dec 12 09:28:50.338 R0/0:
 %FLASH_CHECK-3-DISK_QUOTA: Flash disk quota exceeded [free space is 61864 kB] - Please
clean up files on bootflash.

Technical Support: http://www.cisco.com/techsupport Copyright (c) 1986-2014 by Cisco Systems,
 Inc. Compiled Thu 20-Nov-14 18:28 by mcpre Cisco IOS-XE software, Copyright (c) 2005-2014
 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. 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:

Router>
Router>en
Password:

Router#
Router show controller vdsl 0/3/0
Controller VDSL 0/3/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xA3A3
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
```

```
Modem Vendor Country:   0xB500                    0xB500
Serial Number Near:                C1117-4P16.6.201707
Serial Number Far:
Modem Version Near:     16.6.20170704:13462
Modem Version Far:      0xa3a3

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.992.5 (ADSL2+) Annex A

TC Mode:                ATM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running

Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.14L.04
Modem PHY Version:      A2pv6F039t.d26d

Line 0:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     disabled                disabled
SRA count:               0                       0
Bit swap:                enabled                 enabled
Bit swap count:          0                       325
Line Attenuation:         1.0 dB                  3.2 dB
Signal Attenuation:       1.9 dB                  2.7 dB
Noise Margin:            12.5 dB                 11.4 dB
Attainable Rate:        27580 kbits/s            1257 kbits/s
Actual Power:            6.3 dBm                12.0 dBm
Total FECC:             0                        0
Total ES:               0                        0
Total SES:              0                        0
Total LOSS:             0                        0
Total UAS:              81                       81
Total LPRS:             0                        0
Total LOFS:             0                        0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):              NA           25004            NA              1111
SRA Previous Speed:        NA               0            NA                 0
Previous Speed:            NA               0            NA                 0
Total Cells:               NA       120724290            NA           5356209
User Cells:                NA               0            NA                 0
Reed-Solomon EC:           NA               0            NA                 0
CRC Errors:                NA               0            NA                 0
Header Errors:             NA               0            NA                 0
Interleave (ms):           NA            7.00            NA              5.41
Actual INP:                NA            1.29            NA              1.56

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin


Router#
Router#
```

```
Router# copy bootflash: c1100-firmware_c1100_vadsl2017-07-07_23.01.SSA.pkg
bootflash:mydir/ Destination filename
[mydir/c1100-firmware_c1100_vadsl2017-07-07_23.01.SSA.pkg]?
Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC 6640604 bytes copied in 1.365 secs (4864911
bytes/sec)
Router#

Router#request platform software package install rp 0 file
bootflash: c1100-firmware_c1100_vadsl2017-07-07_23.01_.SSA.pkg

--- Starting local lock acquisition on R0 --- Finished local lock acquisition on R
--- Starting file path checking --- Finished file path checking --- Starting image file
verification

--- Checking image file names Locating image files and validating name syntax Found Verifying
image file locations Inspecting image file types Processing image file constraints Creating
candidate provisioning file Finished image file verification --- Starting candidate package
set construction --- Verifying existing software set Processing candidate provisioning
file Constructing working set for candidate package set Constructing working set for running
package set Checking command output Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete Finished candidate package
set construction --- Starting ISSU compatiblity verficiation --- Verifying image type
compatibility Checking IPC compatibility with running software Checking candidate package
set infrastructure compatibility Checking infrastructure compatibility with running software
Checking package specific compatibility Finished ISSU compatiblity verficiation --- Starting
impact testing --- Checking operational impact of change Finished impact testing ---
Starting list of software package changes --- Old files list: Removed
c1100-firmware_c1100_vadsl2017-07-07_23.01_.SSA.pkg New files list: Added
c1100-firmware_c1100_vadsl2017-07-07_23.01_.SSA _39n.SSA.pkg Finished list of software
package changes --- Starting commit of software changes --- Updating provisioning rollback
files Creating pending provisioning file Committing provisioning file Finished commit of
software changes --- Starting analysis of software changes --- Finished analysis of software
changes --- Starting update running software --- Blocking peer synchronization of operating
information Creating the command set placeholder directory Finding latest command set
Finding latest command shortlist lookup file Finding latest command shortlist file
Router#

Router#
Router#show platform software subslot 0/3 module firmware

Avg Load info
-------------------------------------------
1.83 1.78 1.44 3/45 607
Kernel distribution info
-------------------------------------------
Linux version 3.4.11-rt19 (sapanwar@blr-atg-001) (gcc version 4.6.2 (Buildroot 2011.11) )
#3 SMP PREEMPT Fri Nov 7 09:26:19 IST 2014
Module firmware versions
-------------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039t.d24o_rc1
Boot Loader: Secondry
-------------------------------------------
Version: 1.1
Modem Up time
-------------------------------------------
0D 0H 25M 38S
Router#
```

# IP to ATM CoS, Per-VC WFQ and CBWFQ QoS: PPPoE QoS Markings of .1P Bits in S (AOL)

IP to ATM CoS support for a single ATM VC allows network managers to use existing features, such as committed access rate (CAR) or policy-based routing (PBR), to classify and mark different IP traffic by modifying the IP Precedence field in the IP version 4 (IPv4) packet header. Subsequently, Weighted Random Early Detection (WRED) or distributed WRED (DWRED) can be configured on a per-VC basis so that the IP traffic is subject to different drop probabilities (and therefore priorities) as IP traffic coming into a router competes for bandwidth on a particular VC.

For more information, see the Configuring IP to ATM CoS document.

# Low Latency Queueing

Low Latency Queuing (LLQ) allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic. The **priority** command is used to allow delay-sensitive data to be dequeued and sent first. LLQ enables use of a single priority queue within which individual classes of traffic can be placed. For more details on configuring LLQ, see the following documents:

Low Latency Queueing with Priority Percentage Support

Configuring Low Latency Queueing

# Modular QoS CLI (MQC) Unconditional Packet Discard

The Modular QoS CLI (MQC) Unconditional Packet Discard feature allows customers to classify traffic matching certain criteria and then configure the system to unconditionally discard any packets matching that criteria. The Modular QoS CLI (MQC) Unconditional Packet Discard feature is configured using the Modular Quality of Service Command-Line Interface (MQC) feature. Packets are unconditionally discarded by using the new **drop** command within the MQC.

For more information on configuring Modular QOS CLI unconditional packet discard feature, see the Modular QoS CLI Unconditional Packet Discard document.

# MQC Policy Map Support on Configured VC Range ATM

The Modular Quality of Service Command Line Interface (MQC) Policy Map support on Configured VC Range ATM feature extends the functionality for policy maps on a single ATM VC to the ATM VC range.

For more information on configuring MQC Policy Map Support on Configured VC Range ATM, see the MQC Policy Map on Configured VC Range ATM document.

# Multilink PPP (MLPPP) bundling

This feature describes how to configure Multilink PPP over broadband interfaces. Configuring Multilink PPP over broadband includes configuring Multilink PPP over ATM (MLPoA), Multilink PPP over Ethernet (MLPoE), Multilink PPP over Ethernet over ATM (MLPoEoA), and so on.

For more information on Multilink PPP bundles and to configure Multilink PPP minimum links, Bundling and Multilink PPP support on multiple VC's , see the following documents:

Configuring Multilink PPP Connections for Broadband and Serial Topologies

ATM Multilink PPP Support on Multiple VCs

# PPPoE Enhancement with RFC 4638

The PPP over Ethernet Client feature provides PPP over Ethernet (PPPoE) client support on routers on customer premises.

For more information on configuring PPP over Ethernet feature, see the PPP over Ethernet Client document.

# PPPoEoA over ATM AAL5Mux

The PPPoEoA over ATM AAL5MUX feature enables PPP over Ethernet (PPPoE) over ATM adaptation layer 5 (AAL5)-multiplexed permanent virtual circuits (PVCs), reducing logical link control (LLC) and Subnetwork Access Protocol (SNAP) encapsulation bandwidth usage and thereby improving bandwidth usage for the PVC.

For more information on configuring PPPoEoA over ATm AAL5MUX feature, see How to Configure PPPoEoA over ATM AAL5MUX at PPPoEoA over ATM AAL5Mux.

# PPP Over ATM (IETF-Compliant)

PPP over ATM enables a high-capacity central site router with an ATM interface to terminate multiple remote PPP connections. PPP over ATM provides security validation per user, IP address pooling, and service selection capability.

For more information on configuring PPP over ATM for different encapsulation types, see the following documents:

Providing Protocol Support for Broadband Access Aggregation of PPP over ATM Sessions

Configuring PPP over ATM with NAT

# PPPoE Specification Conformance with PADT Message

The PPP over Ethernet Client feature provides PPP over Ethernet (PPPoE) client support on routers on customer premises.

For more information on configuring PPP over Ethernet feature, see the PPP over Ethernet Client document.

# QoS on Dialer

QOS on dialer interfaces feature provides support for Point-to-Point Protocol over Ethernet (PPPoE) and Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) configurations on dialer interfaces. The feature provides support for Modular QoS CLI (MQC)-based queuing and shaping that supports per-customer quality of service (QoS). For more details on configuring QOS on dialer, see the Shaping on Dialer Interfaces document.

# QoS: PPPoE QoS Markings of .1P Bits

The 802.1P CoS Bit Set for PPP and PPPoE Control Frames feature provides the ability to set user priority bits in the IEEE 802.1Q tagged frame to allow traffic prioritization. This capability enables a way to provide best effort quality of service (QoS) or class of service (CoS) at layer 2 without requiring reservation setup.

For more information on configuring PPPoE QOS Markings of 802.1P bits feature, see the 802.1P CoS Bit Set for PPP and PPPoE Control Frames document.

# RBE Client Side Encapsulation with QoS

The RBE client side encapsulation with QoS feature provides secure connectivity to an ATM bridged network in which previously a broadband access server would not forward Address Resolution Protocol (ARP) requests or perform proxy ARP, and would respond to ARPs for its own IP address only. This feature combines RBE with QoS policy-based routing to provide security to the entire network. RBE was developed to address known issues with RFC1483 bridging such as broadcast storms and security.

For more information on configuring ATM RBE with QOS, see the following documents:

RBE Client Side Encapsulation with QoS and the Command References

RBE Client Side Encapsulation with QoS

# VC Bundling

APP License is required to support this feature on this module in Cisco IOS XE.

```
Router(config)#license boot level appxk9
```

ATM VC bundle management allows you to define an ATM VC bundle and add VCs to it. You can configure multiple Permanent Virtual Circuits (PVC) that have different QoS characteristics between two end devices. Each VC of a bundle has its own ATM traffic class and ATM traffic parameters. You can apply attributes and characteristics to discrete VC bundle members, or you can apply them collectively at the bundle level.

For more details on configuring VC Bundling, see the Configuring ATM document.

# Show and Debug Commands

Verifies that the configuration is set properly.

```
Router#show controller vdsl 0/3/0
Controller VDSL 0/3/0 is UP

Daemon Status:          UP

                        XTU-R (DS)              XTU-C (US)
Chip Vendor ID:         'BDCM'                   'BDCM'
Chip Vendor Specific:   0x0000                   0xA3A3
Chip Vendor Country:    0xB500                   0xB500
Modem Vendor ID:        'CSCO'                   'BDCM'
Modem Vendor Specific:  0x4602                   0x0000
Modem Vendor Country:   0xB500                   0xB500
Serial Number Near:                C1117-4P16.6.201707
Serial Number Far:
Modem Version Near:     16.6.20170704:13462
```

```
Modem Version Far:      0xa3a3

Modem Status:           TC Sync (Showtime!)
DSL Config Mode:        AUTO
Trained Mode:           G.992.5 (ADSL2+) Annex A

TC Mode:                ATM
Selftest Result:        0x00
DELT configuration:     disabled
DELT state:             not running

Failed full inits:      0
Short inits:            0
Failed short inits:     0

Modem FW  Version:      4.14L.04
Modem PHY Version:      A2pv6F039t.d26d

Line 0:

                        XTU-R (DS)              XTU-C (US)
Trellis:                 ON                      ON
SRA:                     disabled                disabled
SRA count:               0                       0
Bit swap:                enabled                 enabled
Bit swap count:          0                       100
Line Attenuation:         1.0 dB                  3.2 dB
Signal Attenuation:       1.9 dB                  2.6 dB
Noise Margin:            12.4 dB                 11.2 dB
Attainable Rate:        27576 kbits/s            1253 kbits/s
Actual Power:            6.3 dBm                 12.0 dBm
Total FECC:             0                        0
Total ES:               0                        0
Total SES:              0                        0
Total LOSS:             0                        0
Total UAS:              81                       81
Total LPRS:             0                        0
Total LOFS:             0                        0
Total LOLS:             0                        0


                  DS Channel1     DS Channel0   US Channel1       US Channel0
Speed (kbps):              NA           25004            NA              1111
SRA Previous Speed:        NA               0            NA                 0
Previous Speed:            NA               0            NA                 0
Total Cells:               NA        37914565            NA           1674506
User Cells:                NA               0            NA                 0
Reed-Solomon EC:           NA               0            NA                 0
CRC Errors:                NA               0            NA                 0
Header Errors:             NA               0            NA                 0
Interleave (ms):           NA            7.00            NA              5.41
Actual INP:                NA            1.29            NA              1.56

Training Log :  Stopped
Training Log Filename : flash:vdsllog.bin


Router#show platform software subslot 0/3 module firmware

Avg Load info
-----------------------------------------
2.00 1.88 1.19 1/46 598

Kernel distribution info
-----------------------------------------
```

```
Linux version 3.4.11-rt19 (pavrao@bgl-ads-1863) (gcc version 4.6.2 (Buildroot 2011.11) )
#3 SMP PREEMPT Tue Jun 27 18:47:55 IST 2017

Module firmware versions
----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039t.d26d

Boot Loader: Secondry
----------------------------------------
Version: 1.1

Modem Up time
----------------------------------------
0D 0H 13M 47S


Router#show platform software subslot 0/3 module status
Process and Memory
-------------------------------------
Mem: 43020K used, 76596K free, 0K shrd, 3200K buff, 9668K cached
CPU:   0% usr   4% sys   0% nic  95% idle   0% io   0% irq   0% sirq
Load average: 2.00 1.90 1.24 1/46 602
  PID  PPID USER     STAT   VSZ %MEM CPU %CPU COMMAND
  518   322 admin    S     6092   5%   0   0% dslmgmt
  538   537 admin    S     6092   5%   0   0% dslmgmt
  537   518 admin    S     6092   5%   0   0% dslmgmt
  516   322 admin    S     4056   3%   1   0% tr64c -m 0
  323   322 admin    S     3948   3%   1   0% ssk
  521   519 admin    S     3932   3%   1   0% consoled
  322     1 admin    S     3596   3%   1   0% /bin/smd
  312   311 admin    S     2976   2%   0   0% /bin/swmdk
  311   310 admin    S     2976   2%   0   0% /bin/swmdk
  313   311 admin    S     2976   2%   0   0% /bin/swmdk
  310     1 admin    S     2976   2%   0   0% /bin/swmdk
  602   601 admin    R     1680   1%   0   0% /usr/bin/top -b -n 1 -d 30
    1     0 admin    S     1676   1%   0   0% init
  519     1 admin    S     1676   1%   0   0% -/bin/sh -l -c consoled
  601   538 admin    S     1672   1%   0   0% sh -c /usr/bin/top -b -n 1 -d 30
  363   322 admin    S     1552   1%   0   0% dhcpd
  517   322 admin    S     1480   1%   0   0% dsldiagd
  326   322 admin    S     1432   1%   0   0% dnsproxy
  511     2 admin    SW       0   0%   1   0% [dsl0]
  241     2 admin    SW       0   0%   0   0% [bcmsw_rx]
  145     2 admin    SW       0   0%   1   0% [mtdblock0]
  260     2 admin    SW       0   0%   1   0% [bcmsw_timer]
  206     2 admin    SW       0   0%   1   0% [bcmFlwStatsTask]
    5     2 admin    SW       0   0%   0   0% [kworker/u:0]
    9     2 admin    SW       0   0%   1   0% [ksoftirqd/1]
   10     2 admin    SW       0   0%   0   0% [kworker/0:1]
    8     2 admin    SW       0   0%   1   0% [kworker/1:0]
  156     2 admin    SW<      0   0%   0   0% [linkwatch]
   50     2 admin    SW       0   0%   1   0% [bdi-default]
   69     2 admin    DW       0   0%   1   0% [skbFreeTask]
   87     2 admin    SWN      0   0%   1   0% [kswapd0]
   88     2 admin    SW       0   0%   1   0% [fsnotify_mark]
    7     2 admin    SW       0   0%   1   0% [migration/1]
  152     2 admin    SW       0   0%   1   0% [kworker/1:1]
  329     2 admin    DW       0   0%   0   0% [Avs65_Task]
  160     2 admin    SW<      0   0%   0   0% [deferwq]
   11     2 admin    SW<      0   0%   1   0% [khelper]
   12     2 admin    SW       0   0%   1   0% [kworker/u:1]
   48     2 admin    SW       0   0%   0   0% [sync_supers]
  261     2 admin    SW       0   0%   1   0% [bcmsw]
   52     2 admin    SW<      0   0%   1   0% [kblockd]
```

```
    2     0 admin    SW       0   0%   1   0% [kthreadd]
    3     2 admin    SW       0   0%   0   0% [ksoftirqd/0]
    4     2 admin    SW       0   0%   0   0% [kworker/0:0]
   89     2 admin    SW<      0   0%   1   0% [crypto]
    6     2 admin    SW       0   0%   0   0% [migration/0]

Processors utilization
---------------------------------------
Linux 3.4.11-rt19 ((none))      01/01/70        _mips_  (2 CPU)

00:14:47     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
00:14:47     all    0.13    0.00    1.42    0.00    0.00    0.17    0.00    0.00   98.28
00:14:47       0    0.13    0.00    1.52    0.00    0.00    0.28    0.00    0.00   98.07
00:14:47       1    0.13    0.00    1.32    0.00    0.00    0.06    0.00    0.00   98.49
Interrupts
---------------------------------------
           CPU0       CPU1
  0:       8608       9201   BCM63xx  IPI
  7:     881960     881466   BCM63xx  timer
  9:          0          0  BCM63xx_no_unmask  brcm_9
 10:       1780          0  BCM63xx_no_unmask  brcm_10
 13:          0        717  BCM63xx_no_unmask  serial
 21:          0          0  BCM63xx_no_unmask  brcm_21
 22:          0          0  BCM63xx_no_unmask  brcm_22
 31:      33832          0  BCM63xx_no_unmask  dsl
 34:          0          0  BCM63xx_no_unmask  brcm_34
 35:          0          0  BCM63xx_no_unmask  brcm_35
 39:          0          0  BCM63xx_no_unmask  brcm_39
 89:          0          0  BCM63xx_no_unmask  brcm_89
 91:          0          0  BCM63xx_no_unmask  brcm_91
ERR:          0
System status
---------------------------------------
cpu  237 0 2521 174333 0 0 305 0 0 0
cpu0 118 0 1350 86981 0 0 249 0 0 0
cpu1 118 0 1170 87352 0 0 55 0 0 0
intr 1817730 17926 0 0 0 0 0 0 1763474 0 0 1781 0 0 717 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
33832 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0
ctxt 616258

btime 0

processes 609

procs_running 1

procs_blocked 0

softirq 2174222 0 1762914 3274 270 0 0 32104 349576 0 26084

KLM Module status

---------------------------------------

iptable_mangle 1168 0 - Live 0xc0371000

iptable_filter 848 0 - Live 0xc036a000

ip_tables 11528 2 iptable_mangle,iptable_filter, Live 0xc0361000

xt_multiport 1446 0 - Live 0xc0357000
```

```
xt_mark 813 0 - Live 0xc0350000

xt_mac 739 0 - Live 0xc034a000

xt_DSCP 1819 0 - Live 0xc0344000

xt_dscp 1187 0 - Live 0xc033d000

pwrmngtd 8147 0 - Live 0xc0336000 (P)

bcmvlan 90718 0 - Live 0xc0312000 (P)

p8021ag 5891 0 - Live 0xc02e8000 (P)

bcmarl 6338 0 - Live 0xc02df000 (P)

nciTMSkmod 306764 0 - Live 0xc0288000 (P)

bcm_enet 199999 1 pwrmngtd, Live 0xc01ec000

adsldd 458747 0 - Live 0xc0120000 (P)

bcmxtmcfg 75415 1 adsldd, Live 0xc009b000 (P)

pktflow 85993 2 bcmarl,bcm_enet, Live 0xc0067000 (P)

bcm_bpm 9827 0 [permanent], Live 0xc0045000 (P)

bcm_ingqos 8159 0 - Live 0xc003a000 (P)

chipinfo 1325 0 - Live 0xc0031000 (P)

System Memory status

--------------------------------------

MemTotal:         119616 kB

MemFree:           76496 kB

Buffers:            3220 kB

Cached:             9732 kB
SwapCached:            0 kB
Active:             5300 kB
Inactive:           9572 kB
Active(anon):       1924 kB
Inactive(anon):        0 kB
Active(file):       3376 kB
Inactive(file):     9572 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:          1976 kB
Mapped:             2764 kB
Shmem:                 0 kB
Slab:              26208 kB
SReclaimable:        556 kB
SUnreclaim:        25652 kB
KernelStack:         752 kB
PageTables:          252 kB
```

```
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:       59808 kB
Committed_AS:       4888 kB
VmallocTotal:    1032116 kB
VmallocUsed:        1544 kB
VmallocChunk:    1028200 kB
```

# Module Specific Show Commands

| Command | Purpose |
|---|---|
| **show platform software subslot** *slot*/*subslot* **module firmware** | Displays firmware version, CFE version, build label of both module (base board). |
| **show platform software subslot** *slot*/*subslot* **module status** | Displays CPU utilization, memory utilization, firmware status, and so on. |
| **show platform hardware subslot** *slot*/*subslot* **module device help** | Displays device information specific to the module (for example, Phy, Non-Interface Registers). |
| **show platform hardware subslot** *slot*/*subslot* **module host-if status** | Displays configuration and status for the host interface port(s) (that is, ports connected to the backplane switch) of baseboard. |
| **show platform hardware subslot** *slot*/*subslot* **module host-if statistics** | Displays link statistics for the host interface port(s) (that is, ports connected to the backplane switch). |
| **show platform hardware subslot** *slot*/*subslot* **module interface** *interface name* **status** | Displays status, configuration and IID for specified user-visible interface. |
| **show platform hardware subslot** *slot*/*subslot* **module interface** *interface name* **statistics** | Displays link statistics including FC info for specified user-visible interface. |

```
Router#show platform software subslot 0/3 module firmwareAvg Load info
-----------------------------------------
2.00 1.88 1.19 1/46 598

Kernel distribution info
-----------------------------------------
Linux version 3.4.11-rt19 (pavrao@bgl-ads-1863) (gcc version 4.6.2 (Buildroot 2011.11) )
#3 SMP PREEMPT Tue Jun 27 18:47:55 IST 2017

Module firmware versions
-----------------------------------------
Modem Fw Version: 4.14L.04
Modem Phy Version: A2pv6F039t.d26d

Boot Loader: Secondry
-----------------------------------------
Version: 1.1

Modem Up time
-----------------------------------------
```

```
0D 0H 13M 47S


Router#show platform software subslot 0/3 module status
Process and Memory
-------------------------------------
Mem: 43020K used, 76596K free, 0K shrd, 3200K buff, 9668K cached
CPU:   0% usr   4% sys   0% nic  95% idle   0% io   0% irq   0% sirq
Load average: 2.00 1.90 1.24 1/46 602
  PID  PPID USER     STAT   VSZ %MEM CPU %CPU COMMAND
  518   322 admin    S     6092   5%   0   0% dslmgmt
  538   537 admin    S     6092   5%   0   0% dslmgmt
  537   518 admin    S     6092   5%   0   0% dslmgmt
  516   322 admin    S     4056   3%   1   0% tr64c -m 0
  323   322 admin    S     3948   3%   1   0% ssk
  521   519 admin    S     3932   3%   1   0% consoled
  322     1 admin    S     3596   3%   1   0% /bin/smd
  312   311 admin    S     2976   2%   0   0% /bin/swmdk
  311   310 admin    S     2976   2%   0   0% /bin/swmdk
  313   311 admin    S     2976   2%   0   0% /bin/swmdk
  310     1 admin    S     2976   2%   0   0% /bin/swmdk
  602   601 admin    R     1680   1%   0   0% /usr/bin/top -b -n 1 -d 30
    1     0 admin    S     1676   1%   0   0% init
  519     1 admin    S     1676   1%   0   0% -/bin/sh -l -c consoled
  601   538 admin    S     1672   1%   0   0% sh -c /usr/bin/top -b -n 1 -d 30
  363   322 admin    S     1552   1%   0   0% dhcpd
  517   322 admin    S     1480   1%   0   0% dsldiagd
  326   322 admin    S     1432   1%   0   0% dnsproxy
  511     2 admin    SW       0   0%   1   0% [dsl0]
  241     2 admin    SW       0   0%   0   0% [bcmsw_rx]
  145     2 admin    SW       0   0%   1   0% [mtdblock0]
  260     2 admin    SW       0   0%   1   0% [bcmsw_timer]
  206     2 admin    SW       0   0%   1   0% [bcmFlwStatsTask]
    5     2 admin    SW       0   0%   0   0% [kworker/u:0]
    9     2 admin    SW       0   0%   1   0% [ksoftirqd/1]
   10     2 admin    SW       0   0%   0   0% [kworker/0:1]
    8     2 admin    SW       0   0%   1   0% [kworker/1:0]
  156     2 admin    SW<      0   0%   0   0% [linkwatch]
   50     2 admin    SW       0   0%   1   0% [bdi-default]
   69     2 admin    DW       0   0%   1   0% [skbFreeTask]
   87     2 admin    SWN      0   0%   1   0% [kswapd0]
   88     2 admin    SW       0   0%   1   0% [fsnotify_mark]
    7     2 admin    SW       0   0%   1   0% [migration/1]
  152     2 admin    SW       0   0%   1   0% [kworker/1:1]
  329     2 admin    DW       0   0%   0   0% [Avs65_Task]
  160     2 admin    SW<      0   0%   0   0% [deferwq]
   11     2 admin    SW<      0   0%   1   0% [khelper]
   12     2 admin    SW       0   0%   1   0% [kworker/u:1]
   48     2 admin    SW       0   0%   0   0% [sync_supers]
  261     2 admin    SW       0   0%   1   0% [bcmsw]
   52     2 admin    SW<      0   0%   1   0% [kblockd]
    2     0 admin    SW       0   0%   1   0% [kthreadd]
    3     2 admin    SW       0   0%   0   0% [ksoftirqd/0]
    4     2 admin    SW       0   0%   0   0% [kworker/0:0]
   89     2 admin    SW<      0   0%   1   0% [crypto]
    6     2 admin    SW       0   0%   0   0% [migration/0]

Processors utilization
-------------------------------------
Linux 3.4.11-rt19 ((none))      01/01/70        _mips_  (2 CPU)

00:14:47     CPU    %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest   %idle
00:14:47     all    0.13    0.00    1.42    0.00    0.00    0.17    0.00    0.00   98.28
00:14:47       0    0.13    0.00    1.52    0.00    0.00    0.28    0.00    0.00   98.07
```

```
00:14:47       1    0.13    0.00    1.32    0.00    0.00    0.06    0.00    0.00   98.49
Interrupts
---------------------------------------
           CPU0       CPU1
  0:       8608       9201   BCM63xx  IPI
  7:     881960     881466   BCM63xx  timer
  9:          0          0  BCM63xx_no_unmask  brcm_9
 10:       1780          0  BCM63xx_no_unmask  brcm_10
 13:          0        717  BCM63xx_no_unmask  serial
 21:          0          0  BCM63xx_no_unmask  brcm_21
 22:          0          0  BCM63xx_no_unmask  brcm_22
 31:      33832          0  BCM63xx_no_unmask  dsl
 34:          0          0  BCM63xx_no_unmask  brcm_34
 35:          0          0  BCM63xx_no_unmask  brcm_35
 39:          0          0  BCM63xx_no_unmask  brcm_39
 89:          0          0  BCM63xx_no_unmask  brcm_89
 91:          0          0  BCM63xx_no_unmask  brcm_91
ERR:          0
System status
---------------------------------------
cpu  237 0 2521 174333 0 0 305 0 0 0
cpu0 118 0 1350 86981 0 0 249 0 0 0
cpu1 118 0 1170 87352 0 0 55 0 0 0
intr 1817730 17926 0 0 0 0 0 0 1763474 0 0 1781 0 0 717 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
33832 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0
ctxt 616258

btime 0

processes 609

procs_running 1

procs_blocked 0

softirq 2174222 0 1762914 3274 270 0 0 32104 349576 0 26084

KLM Module status

---------------------------------------

iptable_mangle 1168 0 - Live 0xc0371000

iptable_filter 848 0 - Live 0xc036a000

ip_tables 11528 2 iptable_mangle,iptable_filter, Live 0xc0361000

xt_multiport 1446 0 - Live 0xc0357000

xt_mark 813 0 - Live 0xc0350000

xt_mac 739 0 - Live 0xc034a000

xt_DSCP 1819 0 - Live 0xc0344000

xt_dscp 1187 0 - Live 0xc033d000

pwrmngtd 8147 0 - Live 0xc0336000 (P)

bcmvlan 90718 0 - Live 0xc0312000 (P)

p8021ag 5891 0 - Live 0xc02e8000 (P)
```

```
bcmarl 6338 0 - Live 0xc02df000 (P)

nciTMSkmod 306764 0 - Live 0xc0288000 (P)

bcm_enet 199999 1 pwrmngtd, Live 0xc01ec000

adsldd 458747 0 - Live 0xc0120000 (P)

bcmxtmcfg 75415 1 adsldd, Live 0xc009b000 (P)

pktflow 85993 2 bcmarl,bcm_enet, Live 0xc0067000 (P)

bcm_bpm 9827 0 [permanent], Live 0xc0045000 (P)

bcm_ingqos 8159 0 - Live 0xc003a000 (P)

chipinfo 1325 0 - Live 0xc0031000 (P)

System Memory status

--------------------------------------

MemTotal:         119616 kB

MemFree:           76496 kB

Buffers:            3220 kB

Cached:             9732 kB
SwapCached:            0 kB
Active:             5300 kB
Inactive:           9572 kB
Active(anon):       1924 kB
Inactive(anon):        0 kB
Active(file):       3376 kB
Inactive(file):     9572 kB
Unevictable:           0 kB
Mlocked:               0 kB
SwapTotal:             0 kB
SwapFree:              0 kB
Dirty:                 0 kB
Writeback:             0 kB
AnonPages:          1976 kB
Mapped:             2764 kB
Shmem:                 0 kB
Slab:              26208 kB
SReclaimable:        556 kB
SUnreclaim:        25652 kB
KernelStack:         752 kB
PageTables:          252 kB
NFS_Unstable:          0 kB
Bounce:                0 kB
WritebackTmp:          0 kB
CommitLimit:       59808 kB
Committed_AS:       4888 kB
VmallocTotal:    1032116 kB
VmallocUsed:        1544 kB
VmallocChunk:    1028200 kB


Router#show platform hardware subslot 0/3 module interface ethernet 0/3/0 statistics
Mode: PTM IID : 1
```

```
Queue Stats LP HP
Throttles 0 0
Enables 0 0
Throttles Ref 0 0
Enables Ref 55 55
Throttled 0 0
Tx Packets 14 0
Tx Bytes 6046 0
Tx Q Drops 0 0
Rx Packets 0 NA
Rx Bytes 0 NA
Rx Q Drops 0 NA
Max Q Depth 400 400
Q Depth 0 0
XON Q Depth 25 25
XOFF Q Depth 35 35

End of XDSL Interface Statistics
```

```
Router#show platform hardware subslot 0/3 module interface atm 0/3/0 statistics
Mode: ATM IID:3 PVC:8/37
==========================================

Queue Stats LP HP
Throttles 0 0
Enables 0 0
Throttles Ref 0 0
Enables Ref 1543 1543
Throttled 0 0
Tx Packets 7306 0
Tx Bytes 277628 0
Tx Q Drops 0 0
Rx Packets 0 NA
Rx Bytes 0 NA
Rx Q Drops 0 NA
Max Q Depth 400 400
Q Depth 0 0
XON Q Depth 96 96
XOFF Q Depth 100 100

End of XDSL Interface Statistics
```

```
Router#show platform hardware subslot 0/3 module device help
help The current information
conn Conn mgr details
rp RP details
rgmii BCM switch port RGMII details
mips BCM switch port MIPS details
steering Steering driver details
dma BCM switch and xtm DMA details
```

```
Router#show platform hardware subslot 0/3 module device conn
Connection Manager Statistics
Total number of packets used by NGIO is: 1 (2 Kbytes)
Processing statistics, processed: 427
Queue depth: current: 0 max: 5
handler (ms): min/avg/max: 0/0/0
NGIO (ms): min/avg/max: 0/0/10
statistics per invocation: avg: 1 max: 6
Corrupted packet Overrun: errors 0
Corrupted packet Underrun errors: 0
packet out of memory errors: 0
```

```
          local remote
        pkts in pkts out errors   pkts in pkts out errors
Control Point: 0: Last update was 280 ms ago
SAP     7: 0 0 0 0 0 0
SAP     6: 0 0 0 0 0 0
SAP     5: 0 0 0 0 0 0
SAP     4: 0 0 0 0 0 0
SAP     3: 0 0 0 0 0 0
SAP     2: 14 85 0 68 13 0
SAP     1: 12 873 0 872 12 0
SAP     0: 402 328 0 326 401 0
Total : 428 1286 0 1266 426 0
Heartbeats Local Remote
State: HB_INACTIVE HB_ACTIVE
   in 184 28
   out 28 184
  acks in 28 183
  acks out 184 28
   lost 0 0
  resets 0 0
Grand Total: 428 1286 0 1266 426 0
```

```
Router#show platform hardware subslot 0/3 module device rp
Reliable Protocol Statistics
link 0 packets in 435
link 0 packets out 1346
link 0 acks in 1342
link 0 acks out 435
link 0 retries 2
link 0 timeouts 0
link 0 delete errors 0
link 0 errors 0
link 0 transmit errors 0
link 0 revision errors 0
link 0 duplicates 0
link 0 out of sequence 0
link 0 out of window 0
link 0 current queue depth 0
link 0 max queue depth 14
link 0 processed 435
link 0 delivered 435
link 0 minimum latency(ms) 0
link 0 maximum latency(ms) 120
link 0 average latency(ms) 3
```

```
Router#show platform hardware subslot 0/3 module device rgmii
RGMII Tx Stats
----------------------------------------
1762802 tx_octets_lo, 0 tx_octets_hi
0 tx_drop_pkts, 273 tx_qos_pkts
11 tx_bcast_pkts, 272 tx_mcast_pkts
14152 tx_ucast_pkts, 0 tx_col
0 tx_single_col, 0 tx_multi_col
0 tx_defer, 0 tx_late_col
0 tx_excess_col, 0 tx_framein_disc
0 tx_pause_pkts, 102618 tx_qos_octets_lo
0 tx_qos_octets_hi
RGMII Rx Stats
----------------------------------------
7103314 rx_octets_lo, 0 rx_octets_hi
0 rx_undersize_pkts, 0 rx_pause_pkts
0 rx_oversize_pkts, 0 rx_jabber
0 rx_align_err, 0 rx_fcs_err
```

```
7103314 rx_good_octets_lo, 0 rx_good_octets_hi
0 rx_drop_pkts, 14092 rx_ucast_pkts
0 rx_mcast_pkts, 2 rx_bcast_pkts
0 rx_fragments, 0 rx_excess_frame_disc
0 rx_symbol_err, 9 rx_qos_pkts
4055 rx_qos_octets_lo, 0 rx_qos_octets_hi


Router#show platform hardware subslot 0/3 module device dma
BCMSW DAM info
-------------------------------------
== dma controller registers ==
controller config: 00000003
ch: config:int stat:int mask
rx:00000001:00000000:00000007
tx:00000000:00000007:00000000

== sram contents ==
ch: bd base: status:current bd content
rx:078ec000:0000000b:08402000:07b37060
tx:07ae2000:0000004a:003c6110:05e96002

== MIPS and MISC registers ==
CP0 cause: 00000000
CP0 status: 10008d01
XTM Rx DMA info
-------------------------------------

Ch 0, NumRxBds: 776, HeadIdx: 1, TailIdx: 1, AssignedBds: 776
DMA cfg: 0x00000001, intstat: 0x00000000, intmask: 0x00000007

Ch 1, NumRxBds: 16, HeadIdx: 1, TailIdx: 1, AssignedBds: 16
DMA cfg: 0x00000001, intstat: 0x00000000, intmask: 0x00000007
XTM Tx Bonding DMA info
-------------------------------------
No Bonding Information
XTM Tx DMA info
-------------------------------------

Ch 0, NumTxBds: 400, HeadIdx: 3, TailIdx: 3, FreeBds: 400
BD RingOffset: 0x00000003, Word1: 0x01bd60f3

Ch 1, NumTxBds: 400, HeadIdx: 0, TailIdx: 0, FreeBds: 400
BD RingOffset: 0x00000000, Word1: 0x00000000


Router#show platform hardware subslot 0/3 module device mips
MIPS Tx Stats
-----------------------------------------
7112517 tx_octets_lo, 0 tx_octets_hi
0 tx_drop_pkts, 11 tx_qos_pkts
2 tx_bcast_pkts, 0 tx_mcast_pkts
14161 tx_ucast_pkts, 0 tx_col
0 tx_single_col, 0 tx_multi_col
0 tx_defer, 0 tx_late_col
0 tx_excess_col, 0 tx_framein_disc
0 tx_pause_pkts, 4997 tx_qos_octets_lo
0 tx_qos_octets_hi
MIPS Rx Stats
-----------------------------------------
1780378 rx_octets_lo, 0 rx_octets_hi
0 rx_undersize_pkts, 0 rx_pause_pkts
0 rx_oversize_pkts, 0 rx_jabber
0 rx_align_err, 0 rx_fcs_err
1780378 rx_good_octets_lo, 0 rx_good_octets_hi
```

```
0 rx_drop_pkts, 14223 rx_ucast_pkts
272 rx_mcast_pkts, 12 rx_bcast_pkts
0 rx_fragments, 0 rx_excess_frame_disc
0 rx_symbol_err, 273 rx_qos_pkts
102618 rx_qos_octets_lo, 0 rx_qos_octets_hi


Router#show platform hardware subslot 0/3 module device steering
Steering drv Data path stats
Mode: PTM, IID:1
25 low_watermark, 35 high_watermark
0 FcDrops
----Egress path----
Tx Priority queue :0
11 RxPkts, 4711 RxBytes, 11 TxPkts, 4711 TxBytes, 0 RxDroppedPkts, 0 RxDroppedBytes
0 TxDroppedPkts, 0 TxDroppedBytes
Tx Priority queue :1
0 RxPkts, 0 RxBytes, 0 TxPkts, 0 TxBytes, 0 RxDroppedPkts, 0 RxDroppedBytes
0 TxDroppedPkts, 0 TxDroppedBytes
----Ingress path----
0 RxPkts, 0 RxBytes
0 RxDroppedPkts, 0 RxDroppedBytes
0 TxPkts, 0 TxBytes
0 TxDroppedPkts, 0 TxDroppedBytes
Steering drv Control path stats
1973 pkt2Linux, 225957 pktBytes2Linux
0 pktDrops, 0 pktCpDrops


Router#show platform hardware subslot 0/3 module host-if statistics
Data path counters
Mode: PTM IID : 1 Module Datapath Enabled

----- Egress path -----
Enet counters
   14795 RxPkts, 7187018 RxBytes, 0 RxErrs, 0 RxDropped
Steering counters
 Tx Priority queue :0
   13 RxPkts, 5601 RxBytes, 0 RxDroppedPkts
   13 TxPkts, 5601 TxBytes, 0 TxDroppedPkts
Tx Priority queue :1
   0 RxPkts, 0 RxBytes, 0 RxDroppedPkts
   0 TxPkts, 0 TxBytes, 0 TxDroppedPkts
NGIO Flow Control Msgs
   LP XON 51 XOFF 0, HP XON 51 XOFF 0, DroppedFCMsgs 0
   Low Watermark 25 High Watermark 35
XTM counters
   5 TxPkts, 2225 TxBytes, 0 TxErrs, 0 TxDropped

----- Ingress path -----
XTM counters
   0 RxPkts, 0 RxBytes, 0 RxErrs, 0 RxDropped
Steering counters
   0 RxPkts, 0 RxBytes, 0 RxDroppedPkts
   0 TxPkts, 0 TxBytes, 0 TxDroppedPkts
Enet counters
   15162 TxPkts, 2119357 TxBytes, 0 TxErrs, 0 TxDropped
Steering drv Control path stats
 2531 pkt2Linux, 289693 pktBytes2Linux
 0 pktDrops, 0 pktCpDrops


Router#show platform hardware subslot 0/3 module host-if status
Host Module L2 info:
CP_MAC: 30.f7.0d.55.40.ac
```

```
FFP_DP_MAC: 30.f7.0d.55.40.a9
FFP_FC_MAC: 30.f7.0d.55.40.a9
Module_MAC: d0.72.dc.93.f5.4b
CP VLAN ID: 2351
FFP DP VLAN ID: 2350
FFP HP1 VLAN ID: 2350
FFP HP2 VLAN ID: 2350
FC VLAN ID: 2350
Max CP MTU : 2048
```

```
Router#show platforrm hardware subslot 0/3 module interface ethernet 0/3/0 status
PTM Interface IID:1
Channel Status:ENABLE

-------End of XDSL Interface Status----------
```

**Other useful CLIs for debugging issues related to packet flow:**

- **show platform hardware backplaneswitch-manager rp active ffp statistics**
- **show platform hardware backplaneswitch-manager rp active subslot** *subslot* **GE0 statistics**
- **Show platform hardware qfp act infra bqs queue out default interface** *interface name*
- **show platform hardware qfp active interface if-name** *interface name*
- **show platform hardware qfp active interface if-name** *interface name* **statistics**
- **show platform hardware qfp active statistics drop**
- **show platform hardware qfp active interface statistics clear**

# Packet Flow Specific to ATM PVC Related Show and Debug Commands

```
Router#show platform software atm F0 pvc
Forwarding Manager ATM PVC Information
Interface VCD ID Ing-ID Eg-ID VC State AOM ID
ATM0/3/0.1 1 0x1004010 0 0 0x1248 378
```

```
Router#show platform hardware qfp active infrastructure bqs interface-string
ATM0/3/0.1.1.1004010 hierarchy detail
Interface: ATM0/3/0.1.1.1004010 QFP: 0.0 if_h: 33 Num Queues/Schedules: 5
Queue specifics:
Index 0 (Queue ID:0x448, Name: ATM0/3/0.1.1.1004010)
PARQ Software Control Info:
(cache) queue id: 0x00000448, wred: 0xe79955d0, qlimit (pkts ): 64
parent_sid: 0x91, debug_name: ATM0/3/0.1.1.1004010
sw_flags: 0x08000011, sw_state: 0x00000c01, port_uidb: 65503
orig_min : 0 , min: 0
min_qos : 0 , min_dflt: 0
orig_max : 0 , max: 0
max_qos : 0 , max_dflt: 0
share : 1
plevel : 0, priority: 65535
defer_obj_refcnt: 0
ifm_h: 36, qos_h: 0x00000000, parent_obj_h: 0x00000024
ifh 33 queue_type 0(NONE)
qm_obj: 0x00007f81b81c9fa0
subdevice_id : 0
```

```
Statistics:
tail drops (bytes): 0 , (packets): 0
total enqs (bytes): 103686 , (packets): 6098
queue_depth (pkts ): 0
Schedule specifics:
Index 0 (SID:0x91, Name: ATM0/3/0.1.1.1004010)
PARQ Software Control Info:
sid: 0x91, parent_sid: 0x90
evfc_fc_id: 0x5200, fc_sid: 0xfffff
obj_id: 0x24, parent_obj_id: 0x20, debug_name: ATM0/3/0.1.1.1004010
num_entries (active): 1, num_children (max): 1
presize_hint: 0
sw_flags: 0x0842002a, sw_state: 0x00000801
orig_min : 0 , min: 0
min_qos : 0 , min_dflt: 1045000
orig_max : 0 , max: 1045000
max_qos : 0 , max_dflt: 1045000
share : 1
plevel: 0, service_fragment: False, port_uidb: 65503
priority: 0, defer_obj_refcnt: 0
ifm_h: 36, qos_h: 0x00000000, parent_obj_h: 0x00000020
ifh 33 queue_type 0(NONE)
qm_obj: 0x00007f81b81ca0f0
subdevice_id : 0
REM Schedule Info:
Cntl=0x0 (FC_Enabled) Aggregate State=0x0 (XON XON XON)
HP2, priority level 1. Enforced State=XON (XON)
Bytes Left=2147483647, Paks Left=2147483647
Rvd Flow-On Msgs=0, Rvd Flow-Off Msgs=0
Rvd Refresh Msgs=370, Refresh xon_mismatch=0 xoff_mismatch=0
HP1, priority level 2. Enforced State=XON (XON XON)
Bytes Left=0, Paks Left=0
Rvd Flow-On Msgs=0, Rvd Flow-Off Msgs=0
Rvd Refresh Msgs=0, Refresh xon_mismatch=0 xoff_mismatch=0
LP, normal priority. Enforced State=XON (XON XON XON)
Bytes Left=2147483647, Paks Left=2147483647
Rvd Flow-On Msgs=0, Rvd Flow-Off Msgs=0
Rvd Refresh Msgs=370, Refresh xon_mismatch=0 xoff_mismatch=0
Schedule specifics:
Index 1 (SID:0x90, Name: ATM0/3/0 UBR COS)
PARQ Software Control Info:
sid: 0x90, parent_sid: 0x7f
evfc_fc_id: 0xffff, fc_sid: 0xfffff
obj_id: 0x20, parent_obj_id: 0x1c, debug_name: ATM0/3/0 UBR COS
num_entries (active): 1, num_children (max): 1
presize_hint: 0
sw_flags: 0x08520022, sw_state: 0x00000801
orig_min : 0 , min: 0
min_qos : 0 , min_dflt: 0
orig_max : 0 , max: 0
max_qos : 0 , max_dflt: 0
share : 1
plevel: 0, service_fragment: False, port_uidb: 65504
priority: 0, defer_obj_refcnt: 0
ifm_h: 32, qos_h: 0x00000000, parent_obj_h: 0x0000001c
ifh 0 queue_type 0(NONE)
qm_obj: 0x00007f81b81caa20
subdevice_id : 0
Schedule specifics:
Index 2 (SID:0x7f, Name: ATM0/3/0)
PARQ Software Control Info:
sid: 0x7f, parent_sid: 0x7c
evfc_fc_id: 0x5100, fc_sid: 0xfffff
obj_id: 0x1c, parent_obj_id: 0x17, debug_name: ATM0/3/0
```

```
num_entries (active): 2, num_children (max): 2
presize_hint: 0
sw_flags: 0x0842002a, sw_state: 0x00000801
orig_min : 0 , min: 1097000
min_qos : 0 , min_dflt: 1097000
orig_max : 0 , max: 1097000
max_qos : 0 , max_dflt: 1097000
share : 1
plevel: 0, service_fragment: False, port_uidb: 65525
priority: 0, defer_obj_refcnt: 0
ifm_h: 28, qos_h: 0x00000000, parent_obj_h: 0x00000017
ifh 11 queue_type 0(NONE)
qm_obj: 0x00007f81b81cb0b0
subdevice_id : 0
REM Schedule Info:
Cntl=0x0 (FC_Enabled) Aggregate State=0x0 (XON XON XON)
HP2, priority level 1. Enforced State=XON (XON)
Bytes Left=0, Paks Left=0
Rvd Flow-On Msgs=0, Rvd Flow-Off Msgs=0
Rvd Refresh Msgs=0, Refresh xon_mismatch=0 xoff_mismatch=0
HP1, priority level 2. Enforced State=XON (XON XON)
Bytes Left=0, Paks Left=0
Rvd Flow-On Msgs=0, Rvd Flow-Off Msgs=0
Rvd Refresh Msgs=0, Refresh xon_mismatch=0 xoff_mismatch=0
LP, normal priority. Enforced State=XON (XON XON XON)
Bytes Left=0, Paks Left=0
Rvd Flow-On Msgs=0, Rvd Flow-Off Msgs=0
Rvd Refresh Msgs=0, Refresh xon_mismatch=0 xoff_mismatch=0
Schedule specifics:
Index 3 (SID:0x7c, Name: Licensed Shaper)
PARQ Software Control Info:
sid: 0x7c, parent_sid: 0x0
evfc_fc_id: 0xffff, fc_sid: 0xfffff
obj_id: 0x17, parent_obj_id: 0x0, debug_name: Licensed Shaper
num_entries (active): 5, num_children (max): 5
presize_hint: 2
sw_flags: 0x0802208a, sw_state: 0x00000001
orig_min : 0 , min: 400000000
min_qos : 0 , min_dflt: 400000000
orig_max : 0 , max: 400000000
max_qos : 0 , max_dflt: 400000000
share : 1
plevel: 0, service_fragment: False, port_uidb: 0
priority: 0, defer_obj_refcnt: 0
ifm_h: 23, qos_h: 0x00000000, parent_obj_h: 0x00000000
ifh 0 queue_type 0(NONE)
qm_obj: 0x00007f81b81cbf20
subdevice_id : 0
```

- **show platform hardware qfp active interface platform ATM0/3/0.1.1.1004010 path**
- **show platform hardware qfp active interface if-name atm0/3/0.1 statistics**

# Collecting DSL Training Logs

Perform the following steps to collect the DSL training logs:

```
Router#debug vdsl controller 0/3/0 training log
VDSL Controller VDSL 0/3/0 - Training debugging is on
```

Perform the following steps to stop collecting the training logs:

```
Router#no debug vdsl controller 0/3/0 training log
[VDSL_DIAG_LOG] recvd 158991 bytes, written 158991 bytes
[VDSL_DIAG_LOG]: File written sucessfully..
VDSL Controller VDSL 0/3/0 - Training debugging is off
Router#
```

By default training log is collected in the file, **flash:vdsllog.bin**_*slot-subslot*.

**Example**:

```
Router#sh controller vdsl 0/3/0
Controller VDSL 0/3/0 is UP
Daemon Status: UP

         XTU-R (DS) XTU-C (US)
Chip Vendor ID: 'BDCM' 'BDCM'
Chip Vendor Specific: 0x0000 0x544D
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'CSCO' 'BDCM'
Modem Vendor Specific: 0x4602 0x544D
Modem Vendor Country: 0xB500 0xB500
Serial Number Near: FOC18426DR9 4351/K9 15.5(201412
Serial Number Far:
Modem Version Near: 15.5(20141202:161930
Modem Version Far: 0x544d

Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.5 (ADSL2+) Annex A

TC Mode: ATM

Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running

Failed full inits: 0
Short inits: 0
Failed short inits: 0

Modem FW Version: 4.14L.04
Modem PHY Version: A2pv6F039h.d24o_rc1

Line 0:
        XTU-R (DS) XTU-C (US)
Trellis: ON ON
SRA: disabled disabled
SRA count: 0 0
Bit swap: enabled enabled
Bit swap count: 669 383
Line Attenuation: 3.5 dB 1.7 dB
Signal Attenuation: 3.1 dB 0.0 dB
Noise Margin: 9.4 dB 5.9 dB
Attainable Rate: 15912 kbits/s 1379 kbits/s
Actual Power: 18.0 dBm 12.2 dBm
Total FECC: 176 176
Total ES: 43 0
Total SES: 0 0
Total LOSS: 0 0
Total UAS: 50 50
Total LPRS: 0 0
Total LOFS: 0 0
```

```
Total LOLS: 0 0

        DS Channel1 DS Channel0 US Channel1 US Channel0
Speed (kbps): NA 13073 NA 1045
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 0 NA 0
Total Cells: NA 1479777783 NA 2179031143
User Cells: NA 388927 NA 6870
Reed-Solomon EC: NA 176 NA 176
CRC Errors: NA 47 NA 0
Header Errors: NA 335 NA 0
Interleave (ms): NA 1.99 NA 1.94
Actual INP: NA 0.15 NA 0.77

Training Log : Stopped
Training Log Filename : flash:vdsllog_0-1.bin
```

User can modify the file in which training logs be stored before starting the training log collection procedure by configuring **training log filename flash:***user-filename*.

**Example:**

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

Router(config)#controller vdsl 0/3/0

Router(config-controller)#training log filename flash:mytraininglog_file

Router(config-controller)#exit

Router#show controller vdsl 0/3/0
Controller VDSL 0/3/0 is UP
Daemon Status: UP
XTU-R (DS) XTU-C (US)
Chip Vendor ID: 'BDCM' 'BDCM'
Chip Vendor Specific: 0x0000 0x544D
Chip Vendor Country: 0xB500 0xB500
Modem Vendor ID: 'CSCO' 'BDCM'
Modem Vendor Specific: 0x4602 0x544D
Modem Vendor Country: 0xB500 0xB500
Serial Number Near: FOC18426DR9 4351/K9 15.5(201412
Serial Number Far:
Modem Version Near: 15.5(20141202:161930
Modem Version Far: 0x544d

Modem Status: TC Sync (Showtime!)
DSL Config Mode: AUTO
Trained Mode: G.992.5 (ADSL2+) Annex A

TC Mode: ATM
Selftest Result: 0x00
DELT configuration: disabled
DELT state: not running

Failed full inits: 0
Short inits: 0
Failed short inits: 0

Modem FW Version: 4.14L.04
Modem PHY Version: A2pv6F039h.d24o_rc1

Line 0:

        XTU-R (DS) XTU-C (US)
```

```
Trellis: ON ON
SRA: disabled disabled
SRA count: 0 0
Bit swap: enabled enabled
Bit swap count: 669 383
Line Attenuation: 3.5 dB 1.7 dB
Signal Attenuation: 3.1 dB 0.0 dB
Noise Margin: 8.8 dB 5.9 dB
Attainable Rate: 15464 kbits/s 1379 kbits/s
Actual Power: 18.0 dBm 12.2 dBm
Total FECC: 176 176
Total ES: 43 0
Total SES: 0 0
Total LOSS: 0 0
Total UAS: 50 50
Total LPRS: 0 0
Total LOFS: 0 0
Total LOLS: 0 0

        DS Channel1 DS Channel0 US Channel1 US Channel0
Speed (kbps): NA 13073 NA 1045
SRA Previous Speed: NA 0 NA 0
Previous Speed: NA 0 NA 0
Total Cells: NA 1484200375 NA 2179384795
User Cells: NA 388991 NA 6938
Reed-Solomon EC: NA 176 NA 176
CRC Errors: NA 47 NA 0
Header Errors: NA 335 NA 0
Interleave (ms): NA 1.99 NA 1.94
Actual INP: NA 0.15 NA 0.77

Training Log : Stopped
Training Log Filename : flash:mytraininglog_file
```

# Sample Configurations

## Sample MLPPP Configurations and Show Commands

```
!
interface Ethernet0/3/0
no ip address
load-interval 30
no negotiation auto
pppoe enable
pppoe-client dial-pool-number 2
!
!
interface Dialer2
bandwidth 55000
ip address negotiated
encapsulation ppp
load-interval 30
dialer pool 1
dialer-group 1
ppp authentication chap
ppp chap hostname cisco
ppp multilink
ppp multilink endpoint string mlpp
!
```

```
Router#show pppoe session
    1 client sessions
Uniq ID PPPoE RemMAC Port VT VA State
N/A 268 a44c.119d.d671 Et0/3/0 Di2 Vi2 UP
    c067.af94.c2a8 UP
Router#


Router#show ppp multilink active
Virtual-Access3
Bundle name: cisco1/mlpp/cisco/mlpp
Remote Username: cisco1
Remote Endpoint Discriminator: [1] mlpp
Local Username: cisco
Local Endpoint Discriminator: [1] mlpp
Bundle up for 05:40:46, total bandwidth 89000, load 196/255
Receive buffer limit 24384 bytes, frag timeout 1000 ms
Bundle is Distributed
Dialer interface is Dialer1
  0/0 fragments/bytes in reassembly list
  0 lost fragments, 0 reordered
  0/0 discarded fragments/bytes, 0 lost received
  0xD received sequence, 0xC2AE3 sent sequence
Platform Specific Multilink PPP info
  NOTE: internal keyword not applicable on this platform
  Interleaving: Disabled, Fragmentation: Disabled
Member links: 2 (max 16, min not set)
  Vi1, since 05:40:46, 206250 weight, 1496 frag size
  Vi2, since 05:40:41, 127500 weight, 1496 frag size


Router#show platform hardware qfp active feature mlp client bundle Virtual-Access3
Bundle Interface: Virtual-Access3
Bundle State: Up
Platform Interface Handle: 35
QFP Interface Handle: 26
QFP Interface uIDB Handle: Rx 65510, Tx 65510
Shadow Base: 0x020E19D0, Size: 1160
Num Links: 2, Next Link: 2, Enabled Links Mask: 0x0003
Tx Channel: 0x32, Tx Queue ID: 0x451, Tx Flow Control SID: 0x9f
Max Frags: 0x0, Lost Fragment Timeout: 1000
Max Frag Size: 65535, Frag Delay: 30
RX Class Buffer Size: 24384
MRRU: 1524, Peer MRRU: 1524
Bundle Bandwidth: 89000 kbps
RX Classes: 1, TX Classes: 1
Bundle Flags: 0x00000011, RX DP Flags: 0x04, TX DP Flags: 0x20
Outstanding datapath proxy requests:
  Bundle Create: 0, Update: 0, Remove: 0
  Links Add: 0, Delete: 0
Member Link Interfaces:
 Interface: EVSI20
  Platform Interface Handle: 20
  QFP Interface Handle: 17
  QFP Interface uIDB Handle: Rx 65519, Tx 65519
  Shadow Base: 0x02075CA0, Size: 218
  TX Chan: 52, P1 Queue ID: 1107, P2 Queue ID: 0
  Link Bandwidth: 55000 kbps, Link Weight: 206250, Link Qlimit: 2286
  Link Optimal Frag Size: 1496, Max Frag Size: 65535
  Rewrite Len w/ PID: 2 Rewrite Len w/o PID: 0
  Rewrite String: 00, 3d
  Outstanding datapath proxy requests:
  Links Add: 0, Update: 0, Delete: 0
 Interface: EVSI21
```

```
  Platform Interface Handle: 21
  QFP Interface Handle: 18
  QFP Interface uIDB Handle: Rx 65518, Tx 65518
  Shadow Base: 0x01D48550, Size: 218
  TX Chan: 51, P1 Queue ID: 1109, P2 Queue ID: 0
  Link Bandwidth: 34000 kbps, Link Weight: 127500, Link Qlimit: 2286
  Link Optimal Frag Size: 1496, Max Frag Size: 65535
  Rewrite Len w/ PID: 2 Rewrite Len w/o PID: 0
  Rewrite String: 00, 3d
  Outstanding datapath proxy requests:
   Links Add: 0, Update: 0, Delete: 0
```

```
Router#show platform hardware qfp active feature mlp datapath bundle Virtual-Access3 detail
QFP: 0.0 - Bundle Rx Interface: Virtual-Access3, State: UP
 Rx Bundle uIDB: 65510
  Num Links: 2, Num Classes: 1, MRRU: 1524
  Defined Links: 0x0003, Enabled Links: 0x0003
  Config Flags: 0x04 (EVSI, MCMP: Disabled, Strict Seq Check: Enabled)
  Buffer Limit: 24384 bytes per class, Lost Frag Timeout: 1000 ms
  Stats Non-MLP Encapped Rx: 0 packets
    Meta Packet Drop: 0, Attn Sync Drop: 0
    No Buffer: 0, Invalid Class: 0
    Hit Buffer Limit: 0, Rx Pkt Exceeds MRRU: 0
    Lost Frag Timeout: 0
 Reassembly QID: 0x000003F8, Qlimit: 2000, Qdepth: 0
 Bundle SB: 0x33445150, SB Size: 144
Rx Classes:
 Class: 0
  Expected Seq Number: 0x00000D, In Order/In Sync Links: 0x0003/0x0003
  Stats Rx Buffered: 0/0 fragments/bytes
    Rx Fragmented: 0 fragments
    Rx Unfragmented: 13 packets
    Rx Post Reassembly: 13 packets
    Rx Discarded: 0/0 fragments/bytes
    Rx NULL Frags: 0, Rx Lost: 0
    Rx Out of Order: 0, Rx Rcv'd Lost: 0
  Reorder/Reassembly Stats:
    Reassembly Packet: 0/0 fragments/bytes
    Staged Packets: 0 (S1-empty,S2-empty)
    Inflight Packets: 0
  Class SB: 0x3334D910, SB Size: 272
Rx Member Links:
 Member Link Interface: EVSI20, State: UP
  Rx Link uIDB: 65519, Link ID: 0, Link Mask: 0x0001
   Config Flags: 0x01 (EVSI)
    Class Link Buffered Fragments
     0      0
    Link SB: 0x33470430, SB Size: 32
  Member Link Interface: EVSI21, State: UP
    Rx Link uIDB: 65518, Link ID: 1, Link Mask: 0x0002
      Config Flags: 0x01 (EVSI)
      Class Link Buffered Fragments
       0     0
     Link SB: 0x33470410, SB Size: 32
QFP: 0.0 - Bundle Tx Interface: Virtual-Access3, State: UP
 Tx Bundle uIDB: 65510
  Num Links: 2, Num Classes: 1, Peer MRRU: 1524
  Member Links Defined: 0x0003 Enabled: 0x0003 Congested(HP/LP): 0x0000/0x0000
  Bundle Equal Cost Frag Size: 1496
  Config Flags: 0x20 (EVSI, MCMP: Disabled, MCMP Encap Seq: No,
    Interleave: Disabled, Fragmentation: Disabled
    NCP MLP Encaped: Yes, NCP Tx Link ID: 0)
    EVSI First Member Link Encap Type: 1, EVSI L2 Overhead: 20
  Bundle Flow Control SID: 0x9F, SID Update In Prog: No, Bundle Flags: 0x01
```

```
    Flow Control Timer: Stopped, Xoff Timer Tics: 0, Check Interval: 4572
    MLP FC: Xon, SW FC: Full-Xon, HW FC: Full-Xon
    HW FC Full Xoff Events: 6410, HW FC LP Xoff Events: 0
   Bundle Load Cycle ID (HP/LP): 0/2594, Next Tx Link ID (HP/LP): 0/1
 Link Link Queue Cycle ID Cycle Tx Bytes Queue Depth
  ID Weight Limit HP/LP HP/LP HP(agg)/LP
  0 206250 9 0/2594 0/98444 0/0
  1 127500 9 0/2594 0/98314 0/0
 Stats Non-MLP Encapped Tx: 2 packets
     Non-MLP Priority Interleaved: 0 packets
     Tx Drop: 0, Tx ESS Packet Drop: 0
     Invalid Class: 0
   Bundle SB: 0x34F6C800, SB Size: 256
 Tx Classes:
  Class: 0
    Next Send Seq Number: 0x976A97
    Stats Tx Pre Frag Packets: 127363735 packets
       Tx Fragmented: 0 fragments
       Tx Unfragmented: 127363735 packets
       Tx Frag Interleaved: 0 fragments
       Tx Unfrag Interleaved: 0 packets
    Class SB: 0x3334DD20, SB Size: 64
Tx Member Links:
  Member Link Interface: EVSI20, Parent: Ethernet0/3/0, State: UP
   Tx Link uIDB: 65519, Link ID: 0, Link Mask: 0x0001
     Config Flags: 0x01 (EVSI)
     EVSI Parent Encap Type: 1, EVSI L2 Overhead: 20
     Link Weight: 206250, Frag Size: 1496
     P1 Tx QID: 0x00000453, Qdepth: 0
     P2 Tx QID: 0x00000000, Qdepth: 0
     Default Tx QID: 0x00000452, Qdepth: 0
L2 Rewrite String: 003D
      Rewrite length w/ PID: 2, Length w/o PID: 0
   Link SB: 0x34FAB0C0, SB Size: 144
 Member Link Interface: EVSI21, Parent: Ethernet0/3/0, State: UP
   Tx Link uIDB: 65518, Link ID: 1, Link Mask: 0x0002
     Config Flags: 0x01 (EVSI)
     EVSI Parent Encap Type: 1, EVSI L2 Overhead: 20
     Link Weight: 127500, Frag Size: 1496
     P1 Tx QID: 0x00000455, Qdepth: 0
     P2 Tx QID: 0x00000000, Qdepth: 0
     Default Tx QID: 0x00000454, Qdepth: 0
     L2 Rewrite String: 003D
        Rewrite length w/ PID: 2, Length w/o PID: 0
     Link SB: 0x34FAB030, SB Size: 144
```

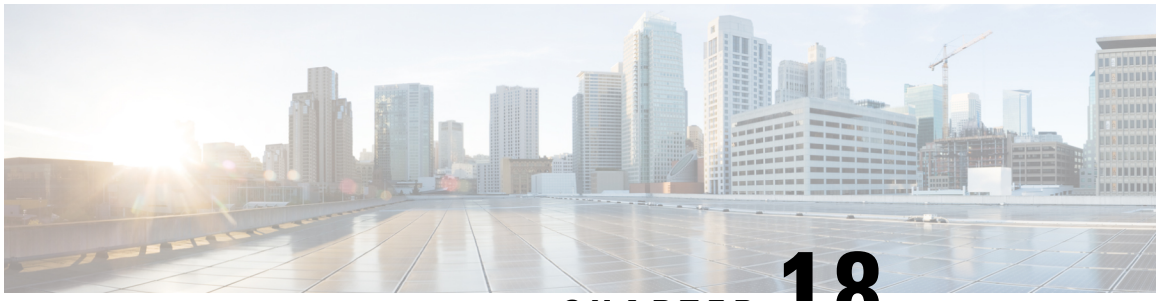
# Sample PPPoA Configuration

```
interface ATM0/2/0.1 point-to-point
 ip unnumbered Loopback0
 no atm enable-ilmi-trap
 pvc 71/200
  oam-pvc 0
  encapsulation aal5mux ppp dialer
  dialer pool-member 151
!
interface Dialer151
 ip address negotiated
 encapsulation ppp
 load-interval 30
 dialer pool 151
 ppp chap hostname BBIP45687587@adslmax.bt.com
```

```
 ppp chap password 0 cisco1
!
dialer-list 1 protocol ip permit
!
```

# Sample PPPoEoA Configuration

```
interface ATM0/1/0
 no ip address
 no atm enable-ilmi-trap
!
interface ATM0/1/0.10 point-to-point
 no atm enable-ilmi-trap
 cdp enable
 pvc 22/62
  ubr 1045
  encapsulation aal5mux pppoe-client
  pppoe-client dial-pool-number 120
 !
!
interface Dialer120
 mtu 1492
 ip address negotiated
 ip nat outside
  encapsulation ppp
 load-interval 30
 dialer pool 120
 dialer-group 1
 ppp mtu adaptive
 ppp chap hostname test@cisco.com
 ppp chap password 0 cisco
 ppp ipcp address required
 ppp link reorders
 !
```



CHAPTER 18

# Cisco LTE/5G on Cisco 1000 Series Integrated Services Router

This chapter provides an overview of the software features and configuration information for Cisco LTE/5G on the Cisco 1000 Series Integrated Services Router (ISR).

For information on Cisco 3G/4G LTE and LTEA Omnidirectional Dipole Antenna (LTE-ANTM-SMA-D), see the Cisco 4G LTEA, 4G LTE, and 3G LTE-ANTM-SMA-D section.

For more information on Cisco LTE/5G SKUs, faceplates, and LED descriptions, see the Cisco 1000 Series Integrated Services Router (ISR) Hardware Installation Guide.


- Finding Feature Information, on page 253
- Overview of Cisco LTE/5G , on page 254
- Prerequisites for Configuring Cisco LTE/5G, on page 256
- Restrictions for Configuring Cisco LTE/5G , on page 256
- Features not Supported in Cisco LTE/5G, on page 256
- Cisco LTE/5G Features, on page 257
- Configuring Cisco LTE/5G, on page 267
- Configuring Cellular Modem Link Recovery , on page 296
- Verifying the Cellular Modem Link Recovery Configuration , on page 298
- Configuration Examples for 3G and 4G Serviceability Enhancement, on page 300
- Configuration Examples for LTE/5G, on page 301
- Upgrading the Modem Firmware, on page 310
- SNMP MIBs, on page 313
- Troubleshooting, on page 315
- Additional References, on page 322


## Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

# Overview of Cisco LTE/5G

Cisco LTE/5G supports the following modes:

- **4G LTE** —4G LTE mobile specification provides multi-megabit bandwidth, more efficient radio network, latency reduction, and improved mobility. LTE solutions target new cellular networks. These networks initially support up to 300 Mb/s peak rates in the downlink and up to 50 Mb/s peak rates in the uplink. The throughput of these networks is higher than the existing 3G networks.
- **3G Evolution High-Speed Packet Access (HSPA/HSPA+)** —HSPA is a UMTS-based 3G network. It supports High-Speed Downlink Packet Access (HSDPA) and High-Speed Uplink Packet Access (HSUPA) data for improved download and upload speeds. Evolution High-Speed Packet Access (HSPA+) supports Multiple Input/Multiple Output (MIMO) antenna capability.

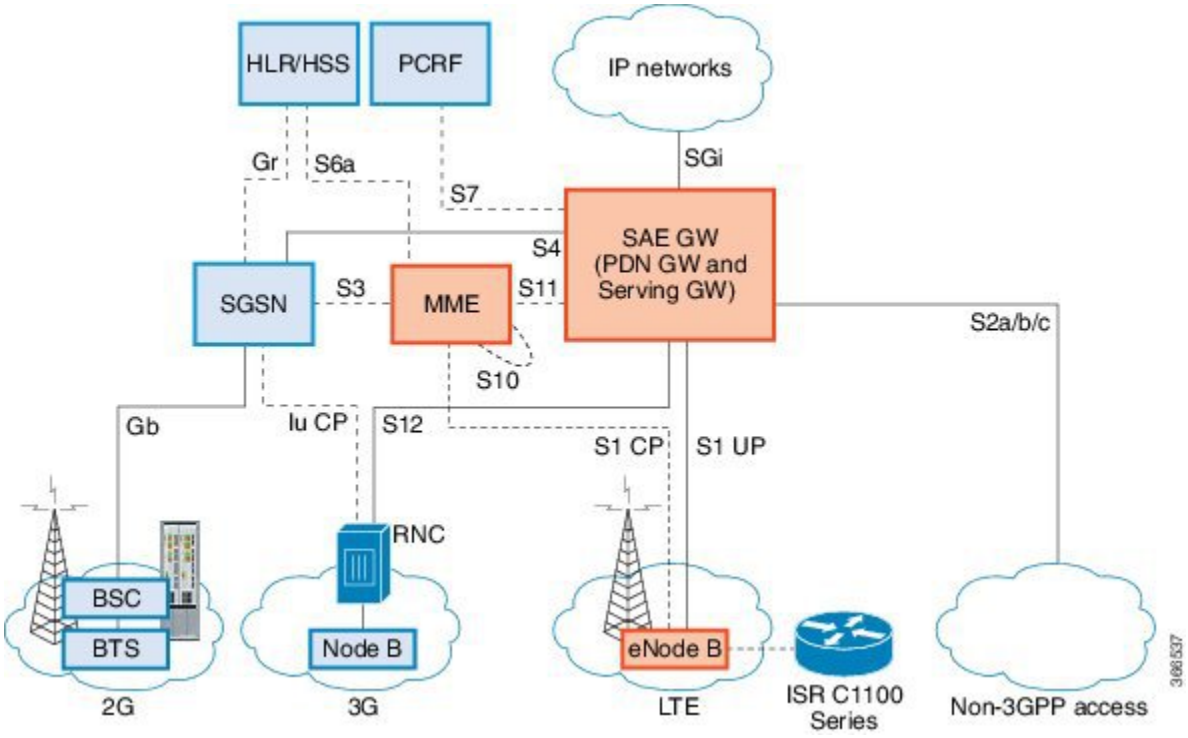
The following table describes the Cisco 4G LTE Cat 6 SKUs:

***Table 27: Cisco 4G LTE Cat 6 SKUs***

| Region Theaters | Cisco LTE Advanced 3.0 LTEEA SKU (European Union, North America) | Cisco LTE Advanced 3.0 LTELA SKUs (Latin America, Asia-Pacific) |
|---|---|---|
| Bands | LTE bands 1-5, 7, 12, 13, 20, 25, 26, 29, 30, and 41<br>FDD LTE 700 MHz (band 12), 700 MHz (band 29), 800 MHz (band 20), 850 MHz (band 5 CLR), 850 MHz (band 26 Low), 900 MHz (band 8), 1800 MHz (band 3), 1900 MHz (band 2), 1900 MHz (PCS band 25), 1700 MHz and 2100 MHz (band 4 AWS), 2100 MHz (band 1), 2300 MHz (band 30), or 2600 MHz (band 7)<br>TDD LTE 2500 MHz (band 41)<br>Carrier aggregation band combinations:<br>1+8; 2+(2,5,12,13,29); 3+(7,20); 4+(4,5,12,13,29); 7+(7,20); 12+30, 5+30, and 41+41 | LTE bands 1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, and 41<br>FDD LTE 700 MHz (band 28), 850 MHz (band 5 CLR), 850 MHz (bands 18 and 19 Low), 900 MHz (band 8), 1500 MHz (band 21), 1800 MHz (band 3), 2100 MHz (band 1), or 2600 MHz (band 7)<br>TDD LTE 1900 MHz (band 39), 2300 MHz (band 40), 2500 MHz (band 41), or 2600 MHz (band 38)<br>Carrier aggregation band combinations:<br>1+(8,18,19,21); 3+(5,7,19,28); 7+(5,7,28); 19+21, 38+38, 39+39,40+40, and 41+41 |

The following figure explains the 4G LTE packet core network architecture.

*Figure 2: 4G LTE Packet Core Network Architecture*




| | |
|---|---|
| Gateways | The Serving Gateway (SGW) routes and forwards user data packets, while also acting as the mobility anchor for the user plane, and is the anchor for mobility between LTE and other 3GPP technologies. The Packet Data Network (PDN) Gateway (PGW) provides connectivity from the User Equipment (UE) to external packet data networks by being the point of exit and entry of traffic for the UE.<br>A UE may have simultaneous connectivity with more than one PGW for accessing multiple PDNs. The PGW performs policy enforcement, packet filtering for each user, charging support, lawful interception, and packet screening. Another key role of the PGW is to act as the anchor for mobility between 3GPP and non-3GPP technologies such as WiMAX and 3GPP2 (CDMA 1X and EvDO).<br>The System Architecture Evolution GW (SAE GW) is the entity that covers the PGW and SGW functionality in the Evolved Packet Core (EPC). |
| RNC | The Radio Network Controller (RNC) is responsible for controlling the Radio Access Network (RAN) that are connected to it. The RNC carries out radio resource management and some of the mobility management functions and is the point where encryption is done before user data is sent to and from the mobile. The RNC connects to the Circuit-Switched Core Network through the Media Gateway (MGW). |
| BTS | Base Transceiver Station. |
| BSC | Base Station Controller. |
| SGSN | Service GPRS Support Node. |

# Prerequisites for Configuring Cisco LTE/5G

- If the signal is not good at the router, use the Cisco offered antenna accessories and extension cables to place the antenna away from router in a better coverage area.
- You must have LTE/5G network coverage where your router is physically placed. For a complete list of supported carriers.
- You must subscribe to a service plan with a wireless service provider and obtain a Subscriber Identity Module (SIM) card. Only micro SIM is supported.
- You must install the SIM card before configuring the LTE/5G on Cisco C1100 series router.
- The standalone antenna that supports GPS capabilities must be installed for the GPS feature to work. See the Cisco 4G Indoor/Outdoor Active GPS Antenna (GPS-ACT-ANTM-SMA) document for installation information.

# Restrictions for Configuring Cisco LTE/5G

- Currently, cellular networks support only user initiated bearer establishment.
- Due to the shared nature of wireless communications, the experienced throughput varies depending on the number of active users or congestion in a given network.
- Cellular networks have higher latency compared to wired networks. Latency rates depend on the technology and carrier. Latency also depends on the signal conditions and can be higher because of network congestion.
- CDMA-EVDO, CDMA-1xRTT, and GPRS technology modes are not supported.
- Any restrictions that are part of the terms of service from your carrier.
- SMS—Only one text message up to 160 characters to one recipient at a time is supported. Larger texts are automatically truncated to the proper size before being sent.
- It is strongly recommended that you configure SNMP V3 with authentication/privacy.

# Features not Supported in Cisco LTE/5G

The following features are not supported on Cisco LTE/5G C1100 Series ISR, when compared to Classic IOS:

- TTY support or Line
- Chat script/dialer string
- External Dialer
- DM log output to USB flash is not supported.

# Cisco LTE/5G Features

Cisco LTE/5G supports the following major features:

- Global Positioning System (GPS) and National Marine Electronics Association (NMEA) streaming.
- Short Message Service (SMS)
- 3G/4G Simple Network Management Protocol (SNMP) MIB
- SIM lock and unlock capabilities
- Dual SIM
- Auto SIM
- NeMo
- Public Land Mobile Network (PLMN) selection
- IPv6
- Multiple PDN
- LTE Link Recovery

The following sections explains the Cisco LTE/5G features:

## 4G GPS and NMEA

Active GPS is supported on the SubMiniature version A (SMA) port. Active GPS antenna is supported only in the standalone mode. An Active GPS antenna includes a built-in Low-Noise Amplifier that provides sufficient gain to overcome coaxial cable losses while providing the proper signal level to the GPS receiver. Active GPS antennae require power from the GPS receiver SMA port to operate. See the Example: Connecting to a Server Hosting a GPS Application, on page 258 for more information.

National Marine Electronics Association (NMEA) streams GPS data either from a LTE/5G through a virtual COM port and a TCP/IP Ethernet connection to any marine device (such as a Windows-based PC) that runs a commercially available GPS-based application.

The following GPS and NMEA features are supported on the Cisco LTE/5G:

- GPS standalone mode (satellite-based GPS)
- Cisco IOS CLI display coordinates.
- External application displays router map location
- Objects in the CISCO-WAN-3G-MIB supports GPS and NMEA features
- The Cisco LTE/5G only supports NMEA over IP and uses show commands in the platform

**Note** Assisted GPS mode is not supported.

For instructions on setting up the GPS antenna, see the Cisco 4G Indoor/Outdoor Active GPS Antenna (GPS-ACT-ANTM-SMA) document.

## Example: Connecting to a Server Hosting a GPS Application

You can feed the NMEA data to a remote server that hosts the GPS application. The server can be connected to the router either directly using an Ethernet cable or through a LAN or WAN network. If the application supports serial port, run a serial port emulation program to create a virtual serial port over the LAN or WAN connection.

**Note** Microsoft Streets & Trips is a licensed software that you can download from the Microsoft website.

To connect a Cisco LTE/5G through IP to a PC running Microsoft Streets & Trips, perform the following steps:

1. Connect the PC to the router using an Ethernet cable.
2. Ensure that the PC and router can ping.
3. Launch the serial port redirector on the PC.
4. Create a virtual serial port that connects to the NMEA port on the router.
5. Launch **Microsoft Streets & Trips** on your PC.
6. Select the GPS Menu.
7. Click Start Tracking.
8. If you have acquired a location fix from the **show cellular 0/2/0 gps** command output on the router, the current location is plotted on the graph, and a reddish brown dotted cursor with a circle around it is seen on the map.

**Note** If you have not acquired a location fix, the Microsoft application times out and disconnects.

# Dual SIM Card

SIM card primary slot is selected when router boots up or when NIM reloads. The default slot is 0. If SIM card is not present in the primary slot, select the alternative slot if SIM card is present.

```
controller cellular 0/2/0
lte sim primary slot <slot#>
```

If the active SIM card loses connectivity to the network a failover to the alternative SIM card slot occurs.

By default the failover timer is two minutes. The failover timer can be set from 1 to 7 minutes.

```
controller cellular 0/2/0
lte failovertimer <3-7>
```

You can also manually switch the SIM slot via the command line interface.

```
cellular 0/2/0 lte sim activate slot <0-1>
```

# Auto SIM

The Auto SIM feature detects the SIM and loads the corresponding firmware. For example, if a Verizon SIM is detected, the modem loads the Verizon firmware. If you switch the SIM to an ATT SIM, the modem will load ATT firmware.

When Auto-SIM is enabled, it is said to be in Auto-SIM mode and when disabled, it is known as Manual mode. In Auto-SIM mode, the modem selects the right carrier firmware from the list of firmware's available. When in manual mode, you can select the firmware manually. Modem resets every time you make a config change from Auto-SIM enabled to disabled or vice-versa.

**Note** Auto SIM is always enabled by default.

## Enable Auto SIM

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters configuration mode. |
| **Step 2** | **Cellular** *slots/sub-slots/interface* **lte firmware-activate** *firmware-index*<br>**Example:**<br>`Router(config)# Cellular 0/2/0 lte firmware-activate 1` | Activates the firmware index.<br>**Note** For the LTE/5G, the *unit* argument identifies the slot, subslot, and the interface separated by slashes (0/2/0). |

## Example: List the firmware when Auto-SIM is Enabled

```
Device# show cellular 0/2/0
firmware          Idx Carrier      FwVersion      PriVersion   Status
 1   ATT          192.0.2.1        002.035_000  Inactive
 2   GENERIC      192.0.2.2        002.035_000  Active
 3   ROGERS       192.0.2.3        001.012_000  Inactive
 4   SPRINT       192.0.2.4        002.012_000  Inactive
 5   VERIZON      192.0.2.5        002.042_000  Inactive

Firmware Activation mode  =  AUTO
```

## Disable Auto SIM

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters configuration mode. |
| **Step 2** | **controller cellular** *slots/sub-slots/interface*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Specifies the controller interface. |
| **Step 3** | **no lte firmware auto-sim**<br>**Example:**<br>`Router(config-if)# no lte firmware auto-sim` | Disable auto SIM. |

# Example: List the firmware when Auto-SIM is Disabled

```
Device# show cellular 0/2/0 firmware
 Idx Carrier      FwVersion    PriVersion   Status
 1   ATT          192.0.2.1  002.035_000  Active
 2   GENERIC      192.0.2.2  002.035_000  Inactive
 3   ROGERS       192.0.2.3  001.012_000  Inactive
 4   SPRINT       192.0.2.4  002.012_000  Inactive
 5   VERIZON      192.0.2.5  002.042_000  Inactive


Firmware Activation mode  =  Manual
```

# Using a SIM Card

Cisco LTE/5G needs an active SIM card provided by a service provider. The SIM cards are usually provided in an unlocked state so that it can be used without a Personal Identification Number (PIN). If the SIM is unlocked, it can be inserted into a LTE/5G and used without an authorization code.

The SIM can be initially locked with a PIN code (4 to 8 digits s long) defined by the service provider. Contact your service provider for the PIN code.

The SIM-Lock feature allows a SIM to be locked or unlocked with a PIN code so that it is used only in an authorized device. Perform the SIM lock and unlock procedures using the Cisco IOS CLI through a console or Telnet/SSH to the ISR.

After the SIM is locked, it cannot initiate a call unless authentication is done using the same PIN. Authentication is done automatically by Cisco IOS through configuration of the PIN. This mandatory configuration for automatic SIM authentication is done using the Cisco IOS CLI as part of the router startup configuration.

After the Cisco IOS configuration is in place, the ISR can initiate an LTE connection. The ISR uses the configured PIN to authenticate prior to the LTE connection. If the Cisco IOS PIN configuration is missing or if the PIN is incorrect, the SIM authentication will fail and the connection will not be initiated.

If the locked SIM is moved to a different ISR or to another device, or if the LTE/5G in which the locked SIM resides is moved to a different LTE/5G slot in the same ISR, the ISR configuration should be changed. The configuration is associated with the cellular controller that is specific to an ISR LTE/5G slot number. This will ensure that the SIM card will not be used in any unauthorized device, or, if there are multiple LTE/5G in a single ISR, that the appropriate PIN is applied to each LTE/5G SIM. An authentication command (with the same PIN used to lock the SIM) must be defined on the new device or on the new cellular controller slot to successfully initiate the LTE connection.

The following procedures are used to configure a SIM:

**Caution** It is very important to use the correct PIN after it is configured. The SIM card will be blocked if the wrong PIN is entered three consecutive times on a locked SIM during authentication or when trying to unlock a locked SIM. You can unblock a blocked SIM card using the PUK code. Contact your service provider for the PUK code. Use the **cellular** <*slot*> **lte sim unblock** <*PUK code*> <*new PIN code*> command to unblock the SIM.

## Changing the PIN

Ensure to enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cellular** *slots subslots interface* **lte sim change-pin** *current-pin new-pin*<br>**Example:**<br>`Router# cellular 0/2/0 lte sim lock 1111 1234` | Locks or unlocks the SIM card using a PIN code.<br>**Note** Locks or unlocks the SIM card using a PIN code. *pin*—A code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card.<br>**Note** SIM should be in locked state when the PIN is being changed. |

## Locking and Unlocking a SIM Card Using a PIN

Perform this task to lock or unlock a SIM card given by your service provider. Make sure you enter the correct PIN, the SIM card gets blocked if the wrong PIN is entered three consecutive times.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cellular** *unit* **lte sim** {**lock** \| **unlock**} *pin*<br>**Example:**<br>`Router# cellular 0/2/0 lte sim lock 1111` | Locks or unlocks the SIM card using a PIN code.<br>**Note** *pin*—A code (4 to 8 digits long) provided by your service provider to lock or unlock the SIM card. |

## Configure CHV1 for Unencrypted Level 0

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cellular** *slots subslots interface* **lte sim lte sim authenticate 0 pin**<br>**Example:**<br>`Router# controller cellular 0/0/0` | Enters the cellular controller configuration mode<br>Use either of these commands:**lte sim authenticate 0 pin**<br>or **lte sim authenticate 0 pin slot {0 \| 1}** |

# Configure CHV1 for Unencrypted Level7

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode. When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command.

**Note** After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration. A SIM should be locked for SIM authentication to work.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **service password-encryption**<br>**Example:**<br>`Router (config)# service password-encryption` | Enables password encryption. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | *username* **privilege** *var password pin*<br>**Example:**<br>`Router (config)# username SIM privilege 0 password 1111` | **Note** Creates username and password.<br>name - specifies the username.*pin*—A 4 to 8 digits PIN code. |
| **Step 3** | **do show run \| i name**<br>**Example:**<br>`Device(config)# do show run \| i SIM` | Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user "SIM" in the example shown). Copy the scrambled password for use in Step 6 (as the PIN). |
| **Step 4** | *username* **privilege 0** *password pin*<br>**Example:**<br>`Device(config)# controller cellular 0/0/0` | Enters the cellular controller configuration mode. |
| **Step 5** | **lte sim authenticate 7***pin* OR**lte sim authenticate 7 pin slot {0 \| 1}**<br>**Example:**<br>`Device(config-controller)# lte sim authenticate 7 055A575E70` | Authenticates the SIM CHV1 code by using the encrypted keyword 7 and the scrambled PIN from Step 4. ThePIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call.<br>**Note** The slot keyword and its options are available only on platforms that supports Dual-SIM feature. |
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-controller)# exit` | (Optional) Exits the cellular controller configuration mode. |
| **Step 7** | **no username***name*<br>**Example:**<br>`Device(config-controller)# no username SIM` | (Optional) Removes the username and password created in Step 3 |
| **Step 8** | **no service password-encryption***name*<br>**Example:**<br>`Device(config-controller)# no service password-encryption` | (Optional) Removes the username and password created in Step 3 |

# Configure CHV1 for Unencrypted Level7

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode. When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command.

**Note** After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration. A SIM should be locked for SIM authentication to work.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **service password-encryption**<br>**Example:**<br>`Router (config)# service password-encryption` | Enables password encryption. |
| **Step 2** | *username* **privilege** *var password pin*<br>**Example:**<br>`Router (config)# username SIM privilege 0 password 1111` | **Note** Creates username and password.<br>name - specifies the username.*pin*—A 4 to 8 digits PIN code. |
| **Step 3** | **do show run \| i name**<br>**Example:**<br>`Device(config)# do show run \| i SIM` | Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user "SIM" in the example shown). Copy the scrambled password for use in Step 6 (as the PIN). |
| **Step 4** | *username* **privilege 0** *password pin*<br>**Example:**<br>`Device(config)# controller cellular 0/0/0` | Enters the cellular controller configuration mode. |
| **Step 5** | **lte sim authenticate 7***pin* OR**lte sim authenticate 7 pin slot {0 \| 1}**<br>**Example:**<br>`Device(config-controller)# lte sim authenticate 7 055A575E70` | Authenticates the SIM CHV1 code by using the encrypted keyword 7 and the scrambled PIN from Step 4. ThePIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call.<br>**Note** The slot keyword and its options are available only on platforms that supports Dual-SIM feature. |

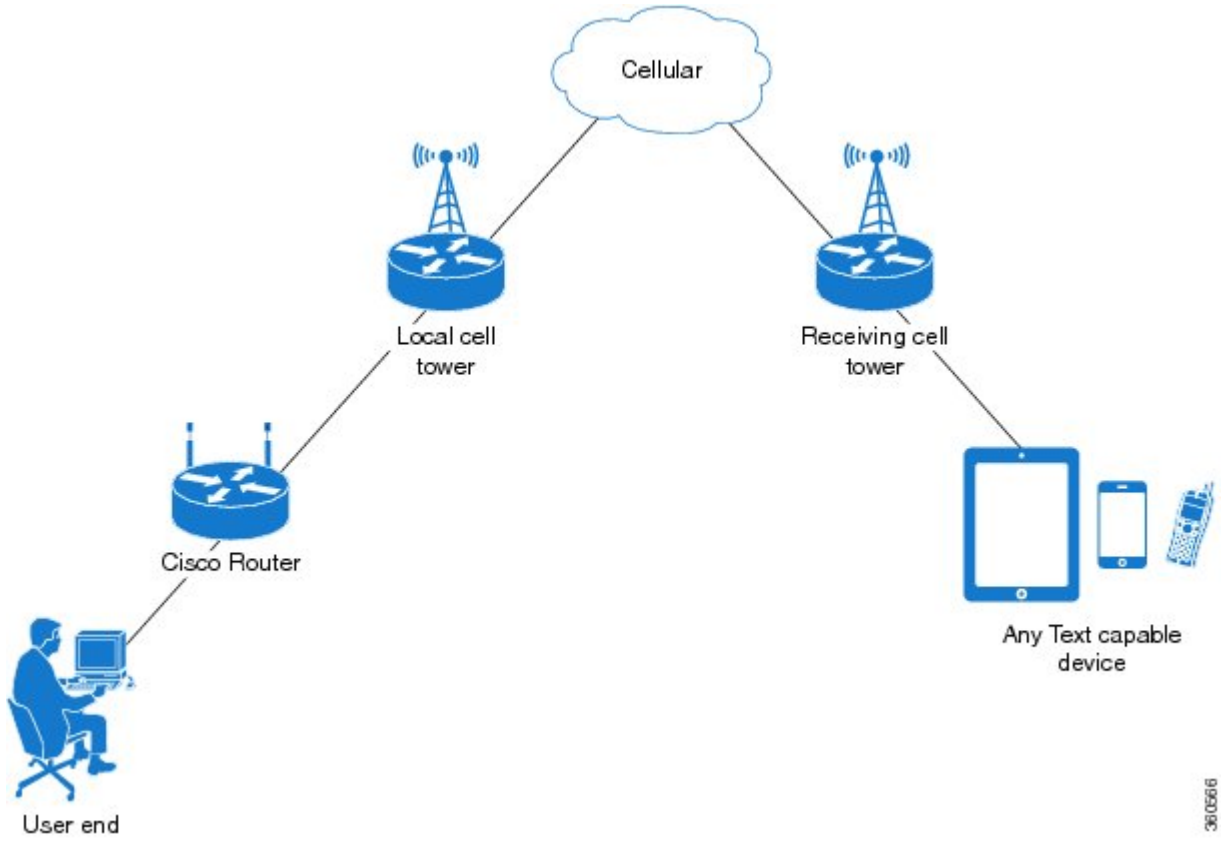
| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | **exit**<br>**Example:**<br>`Device(config-controller)# exit` | (Optional) Exits the cellular controller configuration mode. |
| **Step 7** | **no username***name*<br>**Example:**<br>`Device(config-controller)# no username SIM` | (Optional) Removes the username and password created in Step 3 |
| **Step 8** | **no service password-encryption***name*<br>**Example:**<br>`Device(config-controller)# no service password-encryption` | (Optional) Removes the username and password created in Step 3 |

# Short Message Service (SMS) Capabilities

Cisco LTE/5G support receiving, transmitting, archiving, and deleting of SMS messages. This support includes the ability to view up to 25 received texts, and archive more messages in a custom file location. SMS is supported on multiple carriers. Cisco LTE/5G also have the capability to revert from LTE SMS to 3G and 2G SMS technology if necessary.

A sending device behind a Cisco LTE/5G transmits an SMS text message over the 4G cellular link through cellular towers until it the message reaches the recipient's router, which then notifies the recipient device, such as a cell phone. The receiving device uses the same process to return a reply to the sending device. The following figure describes the flow from a mobile device to a sending device. For SMS transmission to work, end users must have a text-capable device, and optionally, a text plan. If end users do not have a text plan, standard SMS rates apply to their text transmissions.

*Figure 3: SMS Network*




# Data Account Provisioning

One or more modem data profiles can be created to provision a modem on a LTE/5G SKU. An active wireless account with a service provider with one or more (dual) SIM cards must be installed. The modem data profile is pre-configured on the modem.

The following tasks are used to verify the signal strength and service availability of the modem and to create, modify, and delete modem data profiles:

## IP Multimedia Subsystem Profiles

IP Multimedia Subsystem (IMS) profiles establish a session, and are a part of the modem configuration and are stored in the modem's NVRAM. An IMS network is an access-independent and standard-based IP connectivity service that enables different types of multimedia services to end users using common Internet-based protocols.

# LTE/5G LEDs

The following table describes the LED behavior in LTE/5G.

*Table 28: LTE/5G LED Indicators*

| LED | Color/Bar and Description | |
|---|---|---|
| LTE SIM(0) & SIM(1) | Green (Solid) | Modem up, SIM installed and active |
| | Green Blink | LTE data activity |
| | Off | Modem not up; or modem up and no SIM |
| | Amber (Solid) | Modem up, SIM installed but not active |
| RSSI - Uses Bars for LED Indication | Four Bar | High RSSI >= -69dBm |
| | Three Bar | Medium RSSI, -89dBm <> -70dBm |
| | Two Bar | Low RSSI, -99dBm <> -90dBm |
| | One Bar | RSSI <= -100dBm |
| | 0 or No Bar | No Service |
| SERVICE - Uses Color Indication | Green(solid) | LTE signal present (RSSI LEDs will be Green) |
| | Amber(solid) | 2G/3G signal present (RSSI LEDs will be Amber) |
| | No Color | No service detected. |
| GPS | Green (Solid) | GPS coordinates are obtained. |
| | Off | GPS is disabled, GPS is enabled without GPS mode and NMEA configuration, or GPS is acquiring |

# Configuring Cisco LTE/5G

For LTE/5G, the numbering for slot 0, module 0, and port 0 is 0/2/0 for all commands.

## Verifying Modem Signal Strength and Service Availability

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show cellular** *unit* **network**<br>**Example:**<br>`Router# show cellular 0/2/0 network` | Displays information about the carrier network, cell site, and available service. |
| **Step 2** | **show cellular** *unit* **radio**<br>**Example:**<br>`Router# show cellular 0/2/0 radio` | Shows the radio signal strength.<br>**Note** The RSSI should be better than –90 dBm for steady and reliable connection. |
| **Step 3** | **show cellular** *unit* **profile**<br>**Example:**<br>`Router# show cellular 0/2/0 profile` | Shows information about the modem data profiles created. |
| **Step 4** | **show cellular** *unit* **security**<br>**Example:**<br>`Router# show cellular 0/2/0 security` | Shows the security information for the modem, such as SIM and modem lock status. |
| **Step 5** | **show cellular** *unit* **all**<br>**Example:**<br>`Router# show cellular 0/2/0 all` | Shows consolidated information about the modem, profiles created, radio signal strength, network security, and so on. |

# Guidelines for Creating, Modifying, or Deleting Modem Data Profiles

Customized profiles (Access Point Name (APN) in mobile networks) can be created and used on Cisco LTE/5G SKU's. Maximum number of profiles that can be created are 16.

Cisco SKU's shipping with specific carrier provisioning file (Can be found in Carrier label under "show cellular <slot> hardware"), default profiles are already populated and can be deployed readily.

In all other cases where profile configurations are not available, separate profiles should be created with required parameters.

You can create multiple profiles on Cisco LTE/5G. The following are the default internet profile numbers for the modems:

| Modem | Profile Number |
|---|---|
| EM7430 | Profile 1 |
| EM7455 (Verizon or Sprint) | Both Profile 1 and Profile 3 |
| EM7455 (AT&T or other SP's) | Profile 1 |

Follow these guidelines when you configure a data profile using EXEC mode or Config mode :

- You do not have to make any profile-related changes if your modem comes with a data profile, for instance, AT&T, Sprint and Verizon.
- If any profile parameter changes are required for a connection type, the changes will likely be carried out in the default profiles.
- To configure different profile types and use them for a different connection, you can create separate profiles with different parameters (for instance, APN names). Note that only one profile is active at a given time.
- Use the **show cellular <unit> profile** command to view the data profile. An asterisk(*) symbol is displayed against the data profile. Double asterisk(**) symbol is displayed against the attach profile.
- The data profile is used to set up a data call. If you want to use a different profile, that profile needs to be made the default one. Use the **lte sim data-profile** *number* command to change the default profile under **controller cellular 0/2/0**.

## Creating, Modifying, or Deleting Data Profiles Using EXEC Mode

Customized profiles (Access Point Name (APN) in mobile networks) can be created and used on Cisco LTE/5G SKU's. Maximum number of profiles that can be created are 16.

Cisco SKU's shipping with specific carrier provisioning file (can be found in carrier label under **show cellular** *slot* **hardware**, default profiles are already populated and can be deployed readily.

**Note** For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cellular** *unit* **lte profile** *[***create** \| **delete***]* *profile-number [apn [authentication [username password [bearer-type]]]]*<br>**Example:**<br>`Router# cellular 0/2/0 lte profile create 2 apn.com pap username pwd ipv4` | Creates, modifies, or deletes a modem data profile in the privileged EXEC mode.<br>• The *profile-number* argument specifies the profile number created for the modem.<br>• (Optional) The *apn* argument specifies an Access Point Name (APN). An APN is provided by your service provider. Only a single APN can be specified for a single profile.<br>• (Optional) The *authentication* parameter specifies the authentication type used. Acceptable parameters are **chap**, **none** (no authentication), **pap**, and **pap_chap** (PAP or CHAP authentication).<br>• (Optional) The *username* and *password* arguments are given by a service provider. These are mandatory when an |

| | Command or Action | Purpose |
|---|---|---|
| | | authentication type other than **none** is used.<br>• (Optional) The *PDN* type parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: **ipv4 ipv6** and **ipv4v6** (IPv4 and IPv6).<br>The **show cellular** *slot* profile displays configured profile list.<br>**Note** Single asterisk(*) displayed against data profile.<br>Double asterisk(**) displayed against attached profile. |

### Example

```
router# show cellular 0/2/0 profile
Profile 1 = INACTIVE **
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
Authentication = None

Profile 2 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None

Profile 3 = ACTIVE*
--------
PDP Type = IPv4v6
PDP address = 192.0.2.1
PDP IPV6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64  Scope: Global
Access Point Name (APN) = VZWINTERNET
Authentication = None
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.2
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
```

**Note** If data and attach profile bindings need modification, use the **controller cellular** slot.

```
router(config-controller)# lte sim data-profile 3 attach-profile 2 slot unit


Device #show cellular 0/2/0 profile
Profile 1 = INACTIVE
--------------------------------------------------
```

```
PDP Type = IPv4v6
Access Point Name (APN) = test
Authentication = None

Profile 2 = INACTIVE **
--------
PDP Type = IPv4
Access Point Name (APN) = internet
Authentication = PAP or CHAP
Username =  user@solution.com
Password =  cisco

Profile 3 = INACTIVE*
--------
PDP Type = IPv4v6
Access Point Name (APN) = basic
Authentication = None

  * - Default profile
 ** - LTE attach profile
Configured default profile for active SIM 0 is profile 2.
```

## Creating, Modifying, or Deleting Data Profiles in Configuration Mode

**Note** For the LTE/5G NIM, the *unit* argument identifies the router slot, WIC slot, and port separated by slashes (0/1/0).

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **profile id***id* **apn** *apn name [***authentication** *[username password ]***pdn-type** *[pdn type][***slot***slot-number*\| *no-overwrite]]]]*<br>**Example:**<br>`Router(config-controller)# profile id 1 apn apn_internet authentication none pdn-type ipv4 slot 0` | Configures a cellular profile in the configuration mode.<br>• The *id* argument specifies the profile number created for the modem. The maximum number of profiles that can be created for each modem are given as follows:<br>  • EM7455 – Up to 16 profiles<br>  • EM7430 – Up to 16 profiles<br>• (Optional) The *apn* argument specifies an Access Point Name (APN) in the profile. An APN is provided by your service provider. Only a single APN can be specified in a single profile.<br>• (Optional) The *authentication* parameter specifies the authentication type used. Acceptable parameters are **chap**, **none** (no |

| | Command or Action | Purpose |
|---|---|---|
| | | authentication), **pap**, and **pap_chap** (PAP or CHAP authentication).<br>• (Optional) The *username* and *password* arguments are provided by a service provider. These are mandatory when an authentication type is used other than none.<br>• (Optional) The *PDN-type* parameter specifies the type of packet data session established with mobile network using this profile. Acceptable parameters are: **ipv4**, **ipv6** and **ipv4v6**.<br>• (Optional) The *slot-number* parameter specifies the slot number. By default, the slot-number is the current active slot-number, if not specified.<br>• (Optional) *No-overwrite* action to be taken when a profile already exists in modem for the profile id. If there is a profile already exists in the modem for this profile id and no-overwrite option is specified, this configuration will not overwrite existing profile. Default is *overwrite*. |

## Configuration Examples

The following example shows how to change a default profile on LTE/5G:

```
router(config-controller)# lte sim data-profile 2 attach-profile 1 slot <unit>
```

The following example shows the output of the **show cellular** command for Verizon network service:

```
router# show cellular 0/2/0 profile
Profile 1 = INACTIVE **
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
Authentication = None

Profile 2 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None

Profile 3 = ACTIVE*
--------
PDP Type = IPv4v6
PDP address = 192.0.2.1
PDP IPV6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64  Scope: Global
Access Point Name (APN) = VZWINTERNET
```

```
Authentication = None
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.3
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF

Profile 4 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwapp
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzw800
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = CISCO.GW4.VZWENTP
Authentication = None

  * - Default profile
 ** - LTE attach profile
```

# Configuration Example

### Example Configuration under Controller Cellular

```
router(config-controller)# profile id 1 apn apn_internet authentication none pdn-type ipv4
 no-overwrite
```

### Controller Cellular Running Configuration

```
Router #show running-config controller cellular <slot>
Building configuration...

Current configuration : 330 bytes
!
controller Cellular 0/2/0
profile id 1 apn apn_internet authentication none pdn-type ipv4 no-overwrite
end
```

```
 ** This will override exec mode profile configuration
 ** If for a profile ID, configuration CLI exists, exec mode configuration cannot be
performed.
 Router #show cellular <slot> profile 5
Profile 5 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = apn_old
Authentication = None

TSN1#cellular <slot> lte profile create 5 apn_new
 Warning: You are attempting to create Profile 5
 Profile 5 was configured through controller configuration 'profile id <profile #>'
 Please execute command under controller configuration using '[no] profile id <profile #>'
 for profile 5 to create
 Profile 5 NOT written to modem
```

```
** As part of this enhancement, any attach and/or data profile changes will immediately
trigger a connection reset and take effect. Below warning message will be displayed.

Warning: You are attempting to modify the data/attach profile.
Connection will be reset
```

## Configure Radio Band Selection

This feature allow users to configure and lock down the modem to a specific RF band, or set of bands. The preference can be set to be equal to, or a sub-set of the capability supported by the modem/carrier combination.

The following examples show the controller configuration commands.

:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **conf t**<br>**Example:**<br>`Device# conf t`<br>`Enter configuration commands, one per line.  End with CNTL/Z.` | |
| **Step 2** | **controllercellular***interface-number*<br>**Example:**<br>`Device(config)# controller cellular 0/2/0` | |
| **Step 3** | **lte modem band-select indices umts3g***indices* **lte4g***indices* [**nr5g***indices*] **slot***slot #*<br>**Example:**<br>`Device(config-controller)# lte modem band-select indices umts3g 24 lte4g 48 nr5g 40 slot 0` | |

### Example

```
router#show cellular 0/2/0 radio ?
  band     Show Radio band settings
  history  Show Radio history in graph format
  |        Output modifiers
  <cr>     <cr>

router#show cell 0/2/0 radio band
LTE bands supported by modem:
- Bands 1 2 3 4 5 7 8 12 13 14 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66 71.
LTE band Preference settings for the active sim(slot 0):
- Bands 1 2 3 4 5 7 8 12 13 14 18 19 20 25 26 28 29 30 32 34 38 39 40 41 42 43 46 48 66 71.
```

```
NR5G bands supported by modem:
- Bands 1 2 3 5 7 8 12 20 25 28 38 40 41 48 66 71 77 78 79.
NR5G band Preference settings for the active sim(slot 0):
- Bands 1 2 3 5 7 8 12 20 25 28 38 40 41 48 66 71 77 78 79.

3G bands supported by modem:
Index: <none>
3G band Preference settings for the active sim(slot 0):
Index: <none>

=========================================

Band index reference list:

For LTE and 5G, indices 1-128 correspond to bands 1-128.

For 3G, indices 1-64 maps to the 3G bands mentioned against each above.
```

## Multiple PDN Contexts

This feature enables router to connect to multiple (currently two) packet data networks. This allows users to enable different features independently on each PDN. For instance, the first PDN can be used for public Internet access and the second one for VPN connectivity; each PDN has its own set of IP addresses and QoS characteristics.

During the initialization of the router, two cellular interfaces corresponding to the two PDNs are created:

cellular 0/2/0 and cellular 0/2/1

These interfaces can be viewed as two logical interfaces using the same radio resources.

The interface cellular 0/2/0 is referred as the first PDN, and cellular 0/2/1 as the second PDN.

To bring up the two PDNs, configuration needs to be applied on both the cellular interfaces in order to make two simultaneous data calls. The next step is to associate the data-bearer profile with its corresponding cellular interface or PDN. It is sufficient to associate the profile for just the first PDN under the controller cellular configuration. Note that the second PDN assumes a profile that is just one above the profile used for the first PDN. For example, if the first PDN uses profile 1, the second PDN uses profile 2 automatically when the call is initiated for the second one.

After the interesting traffic is routed through these cellular interfaces, data calls are initiated and each interface is assigned its own IP and DNS addresses provided by the cellular network.

**Note** Both PDNs share radio resources. Therefore, any throughput measurement needs to take into account the aggregate throughput on both PDNs, instead of just one.

**Note** For Verizon cellular network, the second PDN uses profile #6 automatically, when the call is initiated for the second data connection.

### Configuration Examples

The following example shows how to configure multiple PDN on Cisco LTE/5G SKU:

```
interface Cellular0/2/0
ip address negotiated
 dialer in-band
 dialer idle-timeout 0
 dialer-group 1
 ipv6 enable
 pulse-time 1
!
interface Cellular0/2/1
ip address negotiated
dialer in-band
dialer idle-timeout 0
dialer-group 1
ipv6 enable
pulse-time 1
! dialer-list 1 protocol ipv6 permit
!

ip route 192.0.2.1 255.255.255.0 Cellular0/2/0
ip route 192.0.2.2 255.255.255.255 Cellular0/2/1
!
```

The following show commands can be used to verify the status of the multiple PDN calls:

```
Router#sh cellular 0/2/0 profile
Profile 1 = ACTIVE* **
--------
PDP Type = IPv4v6
PDP address = 192.0.2.1
PDP IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF/64  Scope: Global
Access Point Name (APN) = broadband
Authentication = None
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.3
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF

.
.
.

Profile 16 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = CHAP
Username: ipv4v6
Password: xxxxxx

  * - Default profile
 ** - LTE attach profile

Configured default profile for active SIM 0 is profile 1.

Router# sh cellular 0/2/0 connection
Profile 1, Packet Session Status = ACTIVE
        Cellular0/2/0:
        Data Packets Transmitted = 9 ,  Received = 9
        Data Transmitted = 900 bytes, Received = 900 bytes
        IP address = 192.0.2.1
        IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF/64  Scope: Global
        Primary DNS address = 192.0.2.2
        Secondary DNS address = 192.0.2.3
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
```

```
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
Profile 2, Packet Session Status = ACTIVE
        Cellular0/2/1:
        Data Packets Transmitted = 7 ,  Received = 2
        Data Transmitted = 700 bytes, Received = 176 bytes
        IP address = 192.0.2.4
        IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF/64  Scope: Global
        Primary DNS address = 171.70.168.183
        Secondary DNS address = 192.0.2.5
        Primary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
        Secondary DNS IPV6 address = 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
.
.
.
Profile 16, Packet Session Status = INACTIVE

Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.0.2.1       YES manual up                    up
GigabitEthernet0/0/1   unassigned      YES unset  administratively down down
GigabitEthernet0/1/0   unassigned      YES unset  administratively down down
GigabitEthernet0/1/1   unassigned      YES unset  administratively down down
GigabitEthernet0/1/2   unassigned      YES unset  administratively down down
GigabitEthernet0/1/3   unassigned      YES u
nset  administratively down down
GigabitEthernet0/1/4   unassigned      YES unset  administratively down down
GigabitEthernet0/1/5   unassigned      YES unset  administratively down down
GigabitEthernet0/1/6   unassigned      YES unset  administratively down down
GigabitEthernet0/1/7   unassigned      YES unset  administratively down down
Wl0/1/8                unassigned      YES unset  administratively down down
Cellular0/2/0          192.0.2.2      YES IPCP   up                    up
Cellular0/2/1          192.0.2.3    YES IPCP   up                    up
Vlan1                  unassigned      YES manual up                    down

Router#
Router# show ip dns view
DNS View default parameters:
DNS Resolver settings:
  Domain lookup is enabled
  Default domain name:
  Domain search list:
  Domain name-servers:
    192.0.2.1
    2001:4860:4860::8888
    192.0.2.2
    2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF
    192.0.2.3
    8.8.8.8
DNS Server settings:
  Forwarding of queries is enabled
  Forwarder addresses: DNS View default parameters: DNS Resolver settings:
Domain lookup is enabled Default domain name: Domain search list: Domain name-servers:
192.0.2.1
192.0.2.2
192.0.2.3
DNS Server settings:
Forwarding of queries is enabled
Forwarder addresses:
Router#
```

# Configuring a SIM for Data Calls

## Locking and Unlocking a SIM Card Using a PIN Code

Perform this task to lock or unlock a SIM card given by your service provider.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code. Using the PUK code, you can unblock the SIM card.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cellular** *unit* **lte sim** {**lock** \| **unlock**} *pin*<br>**Example:**<br>`Router# cellular 0/2/0 lte sim lock 1111` | Locks or unlocks the SIM card using a PIN code.<br>• *pin*—A code (4 to 8 digits long) provided by your carrier to lock or unlock the SIM card. |

## Changing the PIN Code

Perform this task to change the PIN code of a SIM.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **cellular** *unit* **lte sim change-pin** *pin new-pin*<br>**Example:**<br>`Router# cellular 0/2/0 lte sim change-pin 1111 1234` | Changes the assigned PIN code. SIM should be in locked state when the PIN is being changed. |

## Verifying the Security Information of a Modem

Perform this task to verify the security information of a modem.

**Note** For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show cellular** *unit* **security**<br>**Example:**<br>`Router# show cellular 0/2/0 security` | Shows the security information of the modem, including the SIM lock status. |

## Configuring Automatic Authentication for a Locked SIM

An unencrypted PIN can be configured to activate the Card Holder Verification (CHV1) code that authenticates a modem.

The SIM card gets blocked if the wrong PIN is entered three consecutive times. Make sure you enter the correct PIN the SIM is configured with. If your SIM card gets blocked, contact your service provider for a PUK code.

Follow these procedures when using an unencrypted Level 0 PIN to configure CHV1. For instructions on how to configure CHV1 using an encrypted Level 7 PIN, see the Configuring an Encrypted PIN for a SIM, on page 280.

A SIM should be locked for SIM authentication to work. To verify the SIM's status, use the **show cellular** *unit* **security** command.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller cellular** *unit*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters the cellular controller configuration mode. |
| **Step 3** | **lte sim authenticate 0** *pin* | Authenticates the SIM CHV1 code by using an unencrypted (**0**) keyword and PIN. This PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call. |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** This command is valid only when an unencrypted PIN is used. To configure CHV1 code using an encrypted PIN, see the Configuring an Encrypted PIN for a SIM, on page 280. |

## Configuring an Encrypted PIN for a SIM

To configure an encrypted PIN, the scrambled value of the PIN must be obtained. To get the scrambled Level 7 PIN and to configure the SIM CHV1 code for verification using this encrypted PIN, enter the following commands in the EXEC mode.

**Note** When obtaining the encrypted PIN for a SIM, a username and password are created by configuring password encryption, defining the username and associated password, copying the resulting scrambled password, and using this scrambled password in the SIM authentication command. After the scrambled PIN has been obtained and used in SIM authentication, the username created can be deleted from the Cisco IOS configuration.

**Note** A SIM should be locked for SIM authentication to work. To verify the SIM's status, use the **show cellular** <*unit*> **security** command.

**Note** For the 4G LTE SKU, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **service password-encryption**<br>**Example:**<br>`Router(config)# service password-encryption` | Enables password encryption. |
| **Step 3** | **username** *name* **privilege 0 password** *pin*<br>**Example:** | Creates username and password.<br>• *name*—Specifies the username. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config)# username SIM privilege 0 password 1111` | • *pin*—Specifies the four- to eight-digit PIN code. |
| **Step 4** | **do show run** \| **i** *name*<br>**Example:**<br>`Router(config)# do show run \| i SIM` | Shows the username configuration line with the encrypted level 7 PIN for the username created in Step 3 (user "SIM" in the example shown).<br>Copy the scrambled password for use in Step 6 (as the PIN). |
| **Step 5** | **controller cellular** *unit*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters the cellular controller configuration mode. |
| **Step 6** | **lte sim authenticate** {**0** \| **7**} *pin* | Authenticates the SIM CHV1 code by using the encrypted keyword **7** and the scrambled PIN from Step 4. The PIN is sent to the modem for authentication with each subsequent LTE connection. If authentication passes based on the configured PIN, the data call is allowed. If authentication fails, the modem does not initiate the data call. |
| **Step 7** | **exit**<br>**Example:**<br>`Router(config-controller)# exit` | (Optional) Exits the cellular controller configuration mode. |
| **Step 8** | **no username** *name*<br>**Example:**<br>`Router(config)# no username SIM` | (Optional) Removes the username and password created in Step 3. |
| **Step 9** | **no service password-encryption**<br>**Example:**<br>`Router(config)# no service password-encryption` | (Optional) Disables password encryption. |

## Applying a Modem Profile in a SIM Configuration

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:** | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# configure terminal` | |
| **Step 2** | **controller cellular** *unit*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters the cellular controller configuration mode. |
| **Step 3** | **lte sim data-profile** *number* **attach-profile** *number* | Applies the configured profile number to the SIM and its slot number. The default (primary) slot is 0.<br>The **attach profile** is the profile used by the modem to attach to the LTE network.<br>The **data profile** is the profile used to send and receive data over the cellular network. |

# Data Call Setup

To set up a data call, use the following procedures:

## Configuring the Cellular Interface

To configure the cellular interface, enter the following commands starting in EXEC mode.

For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

If a tunnel interface is configured with **ip unnumbered cellular 0/2/0**, it is necessary to configure the actual static IP address under the cellular interface, in place of **ip address negotiated**.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface cellular** unit<br>**Example:**<br>`Router(config)# interface cellular 0/2/0` | Specifies the cellular interface. |
| **Step 3** | **ip address negotiated**<br>**Example:**<br>`Router(config-if)# ip address negotiated` | Specifies that the IP address for a particular interface is dynamically obtained. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **dialer in-band**<br>**Example:**<br>`Router(config-if)# dialer in-band` | Enables DDR and configures the specified serial interface to use in-band dialing. |
| **Step 5** | **dialer-group** group-number<br>**Example:**<br>`Router(config-if)# dialer-group 1` | Specifies the number of the dialer access group to which the specific interface belongs. |
| **Step 6** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Enters the global configuration mode. |
| **Step 7** | **ip route** *network-number network-mask* {*ip-address* \| *interface*} [*administrative distance*] [**name** *name*]<br>**Example:**<br>`Router(config)# ip route 209.165.200.225 255.255.255.224 cellular 0/2/0` | Establishes a floating static route with the configured administrative distance through the specified interface.<br>**Note** A higher administrative distance should be configured for the route through the backup interface so that it is used only when the primary interface is down. |
| **Step 8** | **dialer-list** dialer-group **protocol** protocol-name {**permit** \| **deny** \| **list** *access-list-number* \| **access-group**}<br>**Example:**<br>`Router(config)# dialer-list 1 protocol ip list 1` | Creates a dialer list for traffic of interest and permits access to an entire protocol. |

## Configuring DDR

To configure DDR for the cellular interface, enter the following commands starting in EXEC mode.

**Note** For the LTE/5G, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:** | Enters global configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# configure terminal` | |
| **Step 2** | **interface cellular** *unit*<br>**Example:**<br>`Router(config)# interface cellular 0/2/0` | Specifies the cellular interface. |
| **Step 3** | **ip address negotiated**<br>**Example:**<br>`Router(config-if)# ip address negotiated` | Specifies that the IP address for a particular interface is dynamically obtained. |
| **Step 4** | **dialer in-band**<br>**Example:**<br>`Router(config-if)# dialer in-band` | Enables DDR and configures the specified serial interface to use in-band dialing. |
| **Step 5** | **ip address negotiated**<br>**Example:**<br>`Router(config-if)# ip address negotiated` | Specifies that the IP address for a particular interface is dynamically obtained. |
| **Step 6** | **dialer idle-timeout** *seconds*<br>**Example:**<br>`Router(config-if)# dialer idle-timeout 30` | Specifies the duration of idle time, in seconds, after which a line has no outbound traffic. “0” second means no idle timeout. The default idle timeout is 120 seconds if there is no idle timer specified. |
| **Step 7** | dialer-group group-number<br>**Example:**<br>`Router(config-if)# dialer-group 1` | Specifies the number of the dialer access group to which the specific interface belongs. |
| **Step 8** | **exit**<br>**Example:**<br>`Router(config-if)# exit` | Enters the global configuration mode. |
| **Step 9** | dialer-list dialer-group protocol protocol-name {permit \| deny \| list *access-list-number* \| access-group}<br>**Example:**<br>`Router(config)# dialer-list 1 protocol ip list 1` | Creates a dialer list for traffic of interest and permits access to an entire protocol. |
| **Step 10** | access-list access-list-number permit *ip*-source-address | Defines traffic of interest. |

| | Command or Action | Purpose |
|---|---|---|
| | **Example:**<br>`Router(config)# access-list 1 permit any` | |

# Enabling 4G GPS and NMEA Data Streaming

GPS NMEA data streaming to external NMEA 2.0-compliant GPS plotter applications can be enabled on Cisco LTE/5G.

**Note** For the LTE/5G, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | configure terminal<br>**Example:**<br>`Router# configure terminal` | Enters the configuration mode. |
| **Step 2** | controller cellular *unit*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters the controller cellular configuration mode. |
| **Step 3** | lte gps enable<br>**Example:**<br>`Router(config-controller)# lte gps enable` | (Optional) GPS is enabled by default. Use this command to enable the GPS feature if GPS has been disabled for any reason. |
| **Step 4** | lte gps mode standalone<br>**Example:**<br>`Router(config-controller)# lte gps mode standalone` | Enables the standalone GPS mode. |
| **Step 5** | lte gps nmea {ip \| udp [*source address*][*destination address*][*destination port*] }<br>**Example:**<br>`Router(config-controller)# lte gps nmea ip`<br>or<br>`Router(config-controller)# lte gps nmea` | Enables NMEA. Cisco 4G LTE Advanced support only IP NMEA. Therefore, the IP interface and serial interface options are unavailable. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 6** | test cellular *unit* modem-power-cycle<br>**Example:**<br>`Router# test cellular 0/2/0 modem-power-cycle` | GPS can take effect only after modem power cycle. |
| **Step 7** | end<br>**Example:**<br>`Router(config-controller)# end` | Exits the controller configuration mode and returns to the privileged EXEC mode. |
| **Step 8** | show cellular *unit* gps<br>**Example:**<br>`Router# show cellular 0/2/0 gps`<br><br>`GPS Info`<br>`-------------`<br>`GPS Feature: enabled`<br>`GPS Mode Configured: standalone`<br>`GPS Port Selected: Dedicated GPS port`<br>`GPS Status: GPS coordinates acquired`<br>`Last Location Fix Error: Offline [0x0]`<br>`Latitude: 38 Deg 11 Min 22.1939 Sec North`<br>`Longitude: 96 Deg 40 Min 48.7066 Sec West`<br>`Timestamp (GMT): Thu Jun 29 07:13:42 2017`<br><br>`Fix type index: 0, Height: 318 m`<br>`Satellite Info`<br>`----------------`<br>`Satellite #3, elevation 62, azimuth 282, SNR 53`<br>`.`<br>`.`<br>`.`<br>`Satellite #28, elevation 0, azimuth 0, SNR 0`<br>`Router#` | Displays a summary of the following GPS data:<br>• GPS state information (GPS disabled, GPS acquiring, GPS enabled)<br>• GPS mode configured (standalone)<br>• GPS location and timestamp information<br>• GPS satellite information<br>• GPS feature (enabled or disabled)<br>• GPS port selected (Dedicated GPS and GPS port with voltage-no-bias) |
| **Step 9** | show cellular *unit* gps detail<br>**Example:**<br>`Router# show cellular 0 gps detail`<br>`GPS Info`<br>`-------------`<br>`GPS Feature: enabled`<br>`GPS Mode Configured: standalone`<br>`GPS Port Selected: Dedicated GPS port`<br>`GPS Status: GPS coordinates acquired`<br>`Last Location Fix Error: Offline [0x0]`<br>`Latitude: 38 Deg 11 Min 22.1939 Sec North`<br>`Longitude: 96 Deg 40 Min 48.7066 Sec West`<br>`Timestamp (GMT): Thu Jun 29 07:13:42 2017`<br>`Fix type index: 0, Height: 0 m`<br>`HDOP: , GPS Mode Used: not configured`<br><br>`Satellite Info`<br>`----------------`<br>`Satellite #3, elevation 0, azimuth 0, SNR 53` | Displays detailed GPS data. |

| | Command or Action | Purpose |
|---|---|---|
| | .<br>.<br>.<br>Satellite #9, elevation 0, azimuth 0, SNR 0<br>Router# | |

# Configuring 4G SMS Messaging

**Note** For the LTE/5G, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/2/0).

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | configure terminal<br>**Example:**<br>`Router# configure terminal` | Enters the configuration mode. |
| **Step 2** | controller cellular *unit*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters the controller cellular configuration mode. |
| **Step 3** | lte sms archive path *FTP-URL*<br>**Example:**<br>`Router(config-controller)# lte sms archive path ftp://username:password@172.25.211.175/SMS-LTE` | Specifies an FTP server folder path to send all the incoming and outgoing SMS messages. After the folder path is identified, it is appended automatically with outbox and inbox folders for the path to which SMS messages are sent and received, for example:<br>`ftp://172.25.211.175/SMS-LTE/outbox`<br>`ftp://172.25.211.175/SMS-LTE/inbox` |
| **Step 4** | cellular *unit* lte sms view { all \| *ID* \| summary }<br>**Example:**<br>`Router# cellular 0/2/0 lte sms view summary`<br><br>`ID FROM YY/MM/DD HR:MN:SC SIZE CONTENT`<br>`0 4442235525 12/05/29 10:50:13 137 Your entry last month has...`<br>`2 5553337777 13/08/01 10:24:56 5 First`<br>`3 5553337777 13/08/01 10:25:02 6 Second` | Displays the message contents of incoming texts received by a modem.<br>• **all**—Displays the message contents of up to 255 incoming text messages received by the modem.<br>• *ID*—Displays the message contents for a specified ID (0-255) of an incoming text message.<br>• **summary**—Displays a summary of the incoming text messages received by the modem. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | end<br>**Example:**<br>`Router# end` | Exits the configuration mode and returns to the privileged EXEC mode. |
| **Step 6** | show cellular *unit* sms<br>**Example:**<br>`Router#  show cellular 0/2/0 sms`<br>`Incoming Message Information`<br>`----------`<br>`SMS stored in modem = 20`<br>`SMS archived since booting up = 0`<br>`Total SMS deleted since booting up = 0`<br>`Storage records allocated = 25`<br>`Storage records used = 20`<br>`Number of callbacks triggered by SMS = 0`<br>`Number of successful archive since booting up = 0`<br>`Number of failed archive since booting up = 0`<br><br>`Outgoing Message Information`<br>`----------`<br>`Total SMS sent successfully = 0`<br>`Total SMS send failure = 0`<br>`Number of outgoing SMS pending = 0`<br>`Number of successful archive since booting up = 0`<br>`Number of failed archive since booting up = 0`<br>`Last Outgoing SMS Status = SUCCESS`<br>`Copy-to-SIM Status = 0x0`<br>`Send-to-Network Status = 0x0`<br>`Report-Outgoing-Message-Number:`<br>`Reference Number = 0`<br>`Result Code = 0x0`<br>`Diag Code = 0x0 0x0 0x0 0x0 0x0`<br><br>`SMS Archive URL = ftp://lab:lab@1.3.150.1/outbox` | Displays all the information in the text messages sent and received. Message information includes text messages sent successfully, received, archived, and messages pending to be sent. LTE-specific information on errors in case of a FAILED attempt may also be displayed. |
| **Step 7** | cellular *unit* lte sms send *number*<br>**Example:**<br>`Router# cellular 0/2/0 lte sms send 15554443333 <sms text>` | Enables a user to send a LTE/5G band SMS message to other valid recipients, provided they have a text message plan. The *number* argument is the telephone number of the SMS message recipient.<br>**Note** 10-digit or 11-digit (phone) numbers are the proper numerical format for sending a text. For example, ########## or 1##########. Seven digits are not supported. |
| **Step 8** | cellular *unit* lte sms delete [ all \| *id* ]<br>**Example:** | (Optional) Deletes one message ID or all of the stored messages from memory. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router# cellular 0/2/0 lte sms delete [ all \| id ]` | |

# Configuring Modem DM Log Collection

Diagnostic Monitor (DM) Log is a modem's feature that captures data transactions between the modem and the network over the radio frequency interface. This feature is a useful tool for troubleshooting 3G and 4G data connectivity or performance issues.

Once a DM log file is captured, diagnostic software tools, such as Sierra Wireless SwiLog and Qualcomm QXDM, can be used to decode the DM log file to understand the issues. A member of Cisco TAC can help with decoding the DM log files.

To configure DM log collection, enter the following commands, starting in privileged EXEC mode.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller cellular** *slot*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters cellular controller configuration mode. |
| **Step 3** | **lte modem dm-log** {**autoshop** {**link-down** \| **timer** *time*} \| **enable** \| **filesize** *size* \| **filter** } **bootflash:***file* \| **flash:***file*} **rotation** \| **size** *log-size*}<br>**Example:**<br>`Router(config-controller)# lte modem dm-log enable` | Configures DM logging for LTE modem.<br>• **autostop**—Automatically stops DM log capturing based on:<br>**link-down**—cellular interface link down event<br>**timer***timer*—amount of time in minutes<br>• **enable**—Starts DM log capturing.<br>• **filesize** *size*—Specifies the maximum log file size, in MB for each DM log file before creating another DM log file. Range is from 1 to 64. Default is 20.<br>• **filter** *location***:***filename*—Specifies the DM log filter to use from the following locations:<br>—bootflash:*file*<br>—flash:*file* |

| | Command or Action | Purpose |
|---|---|---|
| | | **Note** Bootflash and flash are the only valid locationsto store the DM log filter file.<br><br>**Note** If the DM log filter file is not specified, the generic filter file, which comes with the router will be used.<br><br>**Note** The DM log filter file needs to be in .sqf format.<br><br>• **rotation**—Enables continuous DM log capturing by replacing the oldest DM log files with the latest.<br><br>• **size** *log-size*—Specifies the maximum total size in MB of all DM log files that can be allowed in the bootflash or flash before modem stops capturing DM log files. If rotation is enabled, the oldest DM files is replaced with the latest DM file to meet this size configuration. |
| **Step 4** | **end**<br>**Example:**<br><br>`Router(config-controller)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **show cellular** *unit* **logs dm-log**<br>**Example:**<br><br>`Router# show cellular 0/2/0 logs dm-log`<br>`Integrated DM logging is on`<br>`output path = Utility Flash`<br>`filter = MC74xx generic -`<br>`v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf`<br>`maximum log size = 0`<br>`maximum file size = 0`<br>`log rotation = disabled`<br><br>`33 packets sent to the modem, 4663 bytes,`<br>`0 errors`<br>`28521 packets received from the modem,`<br>`13500758 bytes, 0 input drops`<br>`28521 packets stored in utility flash,`<br>`13500758 bytes`<br><br>`current file size = 13500758`<br>`current log size = 13500758`<br>`total log size = 13500758`<br>`Utility Flash DM log files = (1) files` | (Optional) Displays DM log configuration and statistics. |

# Example

The following example shows how to:

- Specifies the maximum size of all DM log files that can be stored in bootflash or flash to 512 MB
- Specifies the maximum size of each DM log file to 32 MB
- Uses MC7xxx_GPS_Log.sqf DM log filter in the flash
- Enable rotation
- Enables DM log capturing

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log filesize 512

Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log filesize 32
```

The following example shows how to specify the filter file for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log filter flash:MC7xxx_GPS_Log.sqf
```

The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log rotation
```

The following example shows how to specify the maximum log size for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log enable
```

The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# end
```

The following example shows how to specify the maximum log size for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# lte modem dm-log size 1024
```

The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/2/0
Router(config-controller)# end
```

The following example shows what was configured on the router for DM log feature:

```
Router#show running-config | section controller
controller Cellular 0/2/0
 lte modem dm-log filter flash:MC7xxx_GPS_Log.sqf
 lte modem dm-log size 512
 lte modem dm-log filesize 32
 lte modem dm-log rotation
 lte modem dm-log enable
 lte modem dm-log size 1024
```

The following displays DM log configuration and statistics

```
Router#show cellular 0/2/0 logs dm-log
Integrated DM logging is on
output path = Utility Flash
filter = flash:MC7xxx_GPS_Log.sqf
maximum log size = 536870912
```

```
maximum file size = 33554432
log rotation = enabled

32 packets sent to the modem, 3879 bytes, 0 errors
158324 packets received from the modem, 75971279 bytes, 0 input drops
158324 packets stored in utility flash, 75971279 bytes

current file size = 8863042
current log size = 75971279
total log size = 75971279
Utility Flash DM log files =  (3) files
end
```

The following shows the DM log files created:

```
Router#dir flash:dmlog*
Directory of bootflash:/dmlog*

Directory of bootflash:/

   27  -rw-    33554069   Jun 7 2018 18:08:46 -08:00  dmlog-slot2-20180607-180628.bin
   28  -rw-    33554168   Jun 7 2018 18:11:25 -08:00  dmlog-slot2-20180607-180846.bin
   29  -rw-    14188544   Jun 7 2018 18:12:37 -08:00  dmlog-slot2-20180607-181125.bin
2885718016 bytes total (521891840 bytes free)
lte modem dm-log size 1024
```

The following shows hot to disable/stop DM log capturing:

```
Router(config)#controller cellular 0/2/0
Router(config-controller)#no lte modem dm-log enable
Router(config-controller)#end
```

# Enabling Modem Crashdump Collection

Modem crashdump collection is useful in debugging firmware crash. To collect crash data, the modem has to be pre-configured so that it will stay in memdump mode after a crash. Memdump mode is a special boot-and-hold mode for the memdump utility to collect crash data.

For earlier releases, the crashdump collection required the PC to be connected to the router using a USB cable or a special RJ45-USB cable on a non-HSPA+7 3G module.

As part of the 3G and 4G serviceability enhancement, the crashdump collection utility is integrated into Cisco IOS.

To enable modem crashdump collection, perform the following steps.

**Note** The integrated modem crashdump collection feature is supported only on 3G HSPA and LTE/5G based SKUs.

### Before you begin

Ensure that the following prerequisites are met before attempting to enable crashdump logging:

- The modem needs to be provisioned for modem crashdump collection. Contact Cisco TAC for details.
- The modem should be in crash state. Run tests that will result in modem firmware crash. A “MODEM_DOWN” message on the router console or syslog is indicative of modem firmware crash.

**Note** After the modem firmware crashes, the modem is available for crashdump log collection only. Data calls cannot be made.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | test { cell-cwan } *unit* modem-crashdump { on *location* \| off }<br>**Example:**<br>`Router# test cell-host 0/2/0 modem-crashdump on local_uf` | Enables or disables modem crashdump collection.<br>• **cell-host**<br>—Keyword for fixed platform.<br>• **cell-cwan**<br>— Keyword for LTE on a modular inside platform.<br>• *unit*<br>—For LTE module, this is the router slot, module slot, and port separated by slashes (for example, 0/2/0). For fixed platform, this is the number 0.<br>• **on**<br>Enables crashdump log collection.<br>• *location*<br>—Specifies the destination URL where the modem crashdump logs will be stored.<br>• **off**<br>—Disables crashdump log collection. |

# Displaying Modem Log Error and Dump Information

As part of the 3G serviceability enhancement, commands strings (**at!err** and **at!gcdump**) can be sent to the modem using Cisco IOS CLI rather than setting up a reverse telnet session to the cellular modem to obtain log error and dump information.

To obtain log error and dump information, perform the following steps.

**Note** The modem log error and dump collection feature is supported only on 3G SKUs.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **show cellular** *unit* **log error**<br>**Example:**<br>`Router# show cellular 0/2/0 log error` | Shows modem log error and dump information. |
| **Step 2** | **test cellular** *unit* **modem-error-clear**<br>**Example:**<br>`Router# test cellular 0/2/0 modem-error-clear` | (Optional) Clears out the error and dump registers. By default, error and dump registers are not cleared out after a read. This command changes the operation so that registers are cleared once they are read. As a result, the AT command strings are changed to "**at!errclr=–1**" for CDMA and "**at!err=0**" for GSM modems. |

# Verifying the LTE/5G Router Information

You can verify the configuration by using the following show commands:

### show version

```
Router#show version
Cisco IOS XE Software, Version BLD_V166_THROTTLE_LATEST_20170622_080605_V16_6_0_237
Cisco IOS Software [Everest], ISR Software (ARMV8EB_LINUX_IOSD-UNIVERSALK9_IAS-M),
Experimental Version 16.6.20170622:072729
[v166_throttle-/scratch/mcpre/BLD-BLD_V166_THROTTLE_LATEST_20170622_080605 108]
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Thu 22-Jun-17 03:39 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2017 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 2 hours, 16 minutes
Uptime for this control processor is 2 hours, 18 minutes
System returned to ROM by Reload Command
System image file is
"bootflash:c1100-universalk9_ias.BLD_V166_THROTTLE_LATEST_20170622_080605_V16_6_0_237.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.



Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot
--------------------------------------------------------------------------------

Technology Package License Information:

------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------

cisco C1111-8PLTEAW (1RU) processor with 1464691K/6147K bytes of memory.
Processor board ID FGL21071SK4
1 Virtual Ethernet interface
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6598655K bytes of flash memory at bootflash:.
978928K bytes of USB flash at usb0:.
0K bytes of WebUI ODM Files at webui:.
```

## show platform

```
router# show platform
Chassis type: C1111-8PLTELAWN

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C1111-8PLTELAWN     ok                    00:04:56
 0/0      C1111-2x1GE         ok                    00:02:41
 0/1      C1111-ES-8          ok                    00:02:40
 0/2      C1111-LTE           ok                    00:02:41
 0/3      ISR-AP1100AC-N      ok                    00:02:41
R0        C1111-8PLTELAWN     ok, active            00:04:56
F0        C1111-8PLTELAWN     ok, active            00:04:56
P0        PWR-12V             ok                    00:04:30

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         17100501            16.6(1r)RC3
R0        17100501            16.6(1r)RC3
F0        17100501            16.6(1r)RC3
```

### show interfaces

```
router#sh interface cellular 0/2/0
Cellular0/2/0 is up, line protocol is up
  Hardware is LTE Adv CAT6 - Europe/North America Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/
  Internet address is 192.0.2.1/32
  MTU 1500 bytes, BW 50000 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, loopback not set
  Keepalive not supported
  DTR is pulsed for 1 seconds on reset
  Last input never, output 00:00:42, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     5 packets input, 460 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     21 packets output, 1692 bytes, 0 underruns
     0 output errors, 0 collisions, 8 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
router#
```

# Configuring Cellular Modem Link Recovery

The cellular modem link recovery feature is disabled by default and it is recommended to enable the link recovery feature.

To enable or disable the cellular modem link recovery feature, if required, perform the following steps:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **controller cellular** *unit*<br>**Example:**<br>`Router(config)# controller cellular 0/2/0` | Enters cellular controller configuration mode. |
| **Step 3** | {**lte**} **modem link-recovery disable** \| **no lte** \| **modem link-recoverydisable**}<br>**Example:**<br>`Router(config-controller)# lte modem link-recovery disable` | Enables or disables the cellular modem link recovery feature.<br>Enables or disables the cellular modem link recovery feature. |

| | Command or Action | Purpose |
|---|---|---|
| | Router(config-controller)# no lte modem link-recovery disable<br><br>Device#show run \| sec controller Cellular 0/2/0<br>controller Cellular 0/2/0<br>lte modem link-recovery rssi onset-threshold -110<br>lte modem link-recovery monitor-timer 20<br>lte modem link-recovery wait-timer 10<br>lte modem link-recovery debounce-count 6<br><br>Example:<br>Device#configure terminal<br>Device(config)#controller Cellular 0/2/0<br>Device(config-controller)#lte modem link-recovery<br>monitor-timer 30<br>Device(config-controller)#lte modem wait-timer 15<br>Device(config-controller)#lte modem debounce-count 8<br>Device(config-controller)#lte modem rssi onset-threshold -100 | Once we enable link-recovery, the default Cisco recommended values for link-recovery parameters are populated.<br>We can change the values of link-recovery parameters from the default Cisco recommended values, by using cli for each parameter like in example.<br>**Note** Changing the default recommended cisco values is not advised as it will impact ideal performance of link-recovery feature. |
| **Step 4** | **end**<br>**Example:**<br>Router(config)# end | Exits the configuration mode and returns to the privileged EXEC mode. |

# Cellular Modem Link Recovery Parameters

There are four configurable parameters to adjust the behavior of cellular link recovery. The default values optimized for the best performance of the feature and changing it is not recommended unless advised by Cisco.

The following table explains the link recovery parameters.:

***Table 29: Link Recovery Parameters***

| Parameter | Description |
|---|---|
| **rssi onset-threshold** | This parameter defines the RSSI value below which the link recovery feature triggers additional scrutiny to look for potential issues and take action if needed. The range of this parameter can be set from -90 dBm to -125 dBm. The recommended and default value is -110 dBm. |

| Parameter | Description |
|---|---|
| **monitor-timer** | This parameter determines how often link recovery looks for potential issues. The default value for this parameter is 20 seconds meaning that link recovery feature will be triggered every 20 seconds and look at certain parameters to determine if there is a potential issue. You can configure the monitor-timer range between 20 to 60 seconds. Increasing the monitor timer value above 20 seconds will increase the response time of the feature. |
| **wait-timer and debounce-count** | The wait-timer parameter is used in conjunction with the debounce-count parameter to perform more frequent, additional checks, once the link recovery feature has identified a potential issue that needs to be recovered from, with a modem power-cycle. The default value for wait-timer is 10 seconds and the default value for debounce- count is 6. With this setting, once link recovery has identified an inoperative modem state, it performs additional checks every 10 seconds, up to 6 times, to determine if the issue has been resolved without a modem power-cycle. Reducing the debounce-count and the wait-timer makes faster link recovery, while reducing them may increase the time for recovery. The configurable range for wait-timer is 5-60 seconds. The configurable range for debounce-count is 6-20 seconds. |

# Verifying the Cellular Modem Link Recovery Configuration

To determine if the cellular modem link recovery is enabled, use the **show controller cellularunit** command. In this example, the cellular modem link recovery feature related information is highlighted.

```
Router# show controller cellular 0/2/0Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
--------------------------
SIM 0 is present
SIM 1 is not present
```

```
SIM 0 is active SIM

Module Reload Statistics
------------------------
Soft OIR reloads = 0
Hard OIR reloads = 0
------------------------

Modem Management Statistics
---------------------------
Modem resets = 1
Modem timeouts = 0
Link recovery is ON

Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6

Link recovery count is 0
```

When the cellular modem link recovery occurs and modem is power cycled, you can see the %CELLWAN-2-MODEM_DOWN message on the console logs and additionally there is a %CELLWAN-2-LINK_RECOVERY message which indicates that action has been taken by the cellular modem link recovery feature.

Whenever the cellular modem link recovery has occurred, it updates the Modem timeouts counter under the Modem Management Statistics section of the show controller cellular unit command output. Modem parameters at the last timeout section has information that helps to identify the cause of the issue that triggered link recovery

In the following example log, the messages, modem time out counter, and modem parameters at the last time out are highlighted.

***Jul 19 17:15:18.980 PDT: %CELLWAN-2-LINK_RECOVERY: Cellular0/1/0: Cellular Modem has been power cycled**

```
Device#show controller Cellular 0/2/0
Interface Cellular0/2/0
LTE Module - Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS unit 2

Cellular Modem Configuration
============================
Modem is recognized as valid
Power save mode is OFF
manufacture id =  0x00001199     product id = 0x000068C0
Sierra Wireless unknown modem
Modem Uplink Speed = 50000 kbit.
Modem Downlink Speed = 300000 kbit.

GPS Feature = enabled
GPS Status =  NMEA Disabled
GPS Mode = not configured

Cellular Dual SIM details:
--------------------------
SIM 0 is present
SIM 1 is not present
SIM 0 is active SIM

Module Reload Statistics
------------------------
```

```
Soft OIR reloads = 0
Hard OIR reloads = 0
------------------------
 Modem Management Statistics
--------------------------
Modem resets = 1
Modem user initiated resets = 0
Modem user initiated power-cycles = 0
Modem timeouts = 1
Modem parameters at the last timeout:
         LTE first time attach State was No
         Radio Interface Technology Mode was AUTO
         Operating Mode was Online
         RSSI was -0 dBm
         Packet switch domain status was Not Attached
         Registration state(EMM) was Not Registered
         Downlink traffic was not present
Link recovery is ON
Registration check is ON
RSSI threshold value is -110 dBm
Monitor Timer value is 20 seconds
Wait Timer value is 10 seconds
Debounce Count value is 6
```

# Configuration Examples for 3G and 4G Serviceability Enhancement

## Example: Sample Output for the show cellular logs dm-log Command

The following shows a sample output of the **show cellular logs dm-log** command:

```
Router# show cellular 0/2/0 logs dm-log
Integrated DM logging is on
filter = generic
maximum log size = 67108864
maximum file size = 20971520
log rotation = disabled
7 packets sent to the modem, 3232 bytes, 0 errors
75 packets received from the modem, 57123 bytes, 0 input drops
75 packets stored in file system, 57123 bytes, 0 errors, 0 aborts
2 max rcv queue size
current file size = 57123
current log size = 57123
total log size = 57123
DM log files: (1 files)
```

## Example: Sample Output for the show cellular logs modem-crashdump Command

The following shows a sample output of the **show cellular logs modem-crashdump** command:

```
Router# show cellular 0/2/0 logs modem-crashdump
```

```
Modem crashdump logging: off
Progress = 100%
Last known State = Getting memory chunks
Total consecutive NAKs = 0
Number of retries = 0
Memory Region Info:
1: Full SDRAM [Base:0x0, Length:0x2000000]
2: MDSP RAM A region [Base:0x91000000, Length:0x8000]
3: MDSP RAM B region [Base:0x91200000, Length:0x8000]
4: MDSP RAM C region [Base:0x91400000, Length:0xC000]
5: MDSP Register region [Base:0x91C00000, Length:0x28]
6: ADSP RAM A region [Base:0x70000000, Length:0x10000]
7: ADSP RAM B region [Base:0x70200000, Length:0x10000]
8: ADSP RAM C region [Base:0x70400000, Length:0xC000]
9: ADSP RAM I region [Base:0x70800000, Length:0x18000]
10: CMM Script [Base:0x6A350, Length:0x310]
Router#
```

# Configuration Examples for LTE/5G

## Example: Basic Cellular Interface Configuration: Cisco LTE/5G

The following example shows how to configure the cellular interface to be used as a primary and is configured as the default route:

```
Router# show running-config
interface Cellular 0/2/0
ip address negotiated
dialer in-band
dialer-group 1
ip route 172.22.1.10 255.255.255.255 cellular 0/2/0
dialer-list 1 protocol ip permit
```

## Configuration Examples for Cisco LTE/5G

The following example shows how to configure Cisco LTE/5G:

```
Router# show running-config
Building configuration...
Current configuration : 2991 bytes
!
! Last configuration change at 21:31:48 UTC Mon May 18 2015
!
version 15.5
service timestamps debug datetime msec
service timestamps log datetime msec
service internal
no platform punt-keepalive disable-kernel-core
platform shell
!
hostname C1111-LTEEA
!
boot-start-marker
!
!
!
```

```
logging buffered 10000000
no logging console
enable password lab
!
no aaa new-model
!
!
!
!
!
!
!
subscriber templating
!
multilink bundle-name authenticated
icense udi pid ISR4321/K9 sn FDO181701PZ
!
spanning-tree extend system-id
!
!
redundancy
 mode none
!
!
!
!
controller Cellular 0/2/0
 lte sim data-profile 16 attach-profile 16
 lte gps mode standalone
 lte gps nmea
 lte modem link-recovery disable

 interface GigabitEthernet0/0/1
 ip address 192.0.2.1 255.255.255.0
 ip nat outside

 negotiation auto
!
interface Cellular0/2/0
 ip address negotiated
 ip nat outside
 dialer in-band
 dialer idle-timeout 0
 dialer watch-group 1
 dialer-group 1
 pulse-time 1
!
interface Cellular0/2/1
 no ip address
 shutdown
 dialer in-band
 pulse-time 1
!
!
interface Vlan1
 no ip address
!
no ip nat service dns tcp
no ip nat service dns udp
ip nat inside source list 1 interface Cellular0/2/0 overload
ip forward-protocol nd
ip http server
no ip http secure-server
ip http max-connections 16
```

```
ip tftp source-interface GigabitEthernet0/0/1
ip dns server
ip route 192.0.2.2 192.0.2.3 Cellular0/2/0
ip route 223.255.254.0 255.255.255.0 1.3.0.1
!
!
access-list 1 permit 192.0.2.5 255.255.255.255
dialer watch-list 1 ip 192.0.2.6 255.255.255.255
dialer-list 1 protocol ip permit
!
snmp-server community public RO
snmp-server community private RW
snmp-server community lab RW
snmp-server host 192.0.2.1 public
snmp-server manager
control-plane
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line aux 0
 exec-timeout 0 0
 stopbits 1
line vty 0 4
 login
 transport input all
!
!
end
```

# Cellular Back-off: Example

The following example shows how to configure the cellular back-off feature to stop continuous session activation requests back to the router:

```
Router#show cell 0/2/0 all
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
.
.
.
Profile 16, Packet Session Status = INACTIVE
Router#
Router#show cell 0/2/0 c n
Current System Time = Sun Jan 6 0:8:37 1980
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network = 123 456
Mobile Country Code (MCC) = 123
Mobile Network Code (MNC) = 456
Packet switch domain(PS) state = Attached
LTE Carrier Aggregation state = Deconfigured
Registration state(EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1801
Cell ID = 768001
Network MTU is not Available
Router#
Router#ping 192.0.2.1
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.192.187.254, timeout is 2 seconds:

*Dec 20 23:22:28.025: %CELLWAN-6-CELLULAR_BACKOFF_START: Cellular0/2/0: Cellular back-off
has started on PDN 0....
Success rate is 0 percent (0/5)
Router#

Router#ping 192.0.2.2
Type escape sequence to abort.
RouterSending 5, 100-byte ICMP Echos to 192.0.2.2, timeout is 2 seconds
.
.
.
Router#show cell 0/2/0
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
Router Call end mode = 3GPP
Router Session disconnect reason type = 3GPP specification defined(6)
Session disconnect reason = Option unsubscribed(33)
Enforcing cellular interface back-off
Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE
Router#
Router#show cell 0/2/0 cn
Sending 5, 100-byte ICMP Echos to 192.0.2.2, timeout is 2 seconds:
Router.....
Success rate is 0 percent (0/5)
Router#
Router#ping 192.0.2.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.5, timeout is 2 seconds:
Router.....
Success rate is 0 percent (0/5)
Router#show cell 0/2/0 cping 192.0.2.6  Type escape sequence to abort.
RouterSending 5, 100-byte ICMP Echos to 192.0.2.6 , timeout is 2 seconds:
Router.....
RouterSuccess rate is 0 percent (0/5)
Router#ping 192.0.2.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.6 , timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Router#ping 192.0.2.6
Router#sh cell 0/2/0 c
Profile 1, Packet Session Status = INACTIVE
Profile 2, Packet Session Status = INACTIVE
Profile 3, Packet Session Status = INACTIVE
RouterCall end mode = 3GPP
RouterSession disconnect reason type = 3GPP specification defined(6)
RouterSession disconnect reason = Option unsubscribed(33)
RouterEnforcing cellular interface back-off
 Period of back-off = 1 minute(s)
Profile 4, Packet Session Status = INACTIVE
...
Profile 16, Packet Session Status = INACTIVE
Profile 4, Packet Session Status = INACTIVE
Profile 5, Packet Session Status = INACTIVE
.
.
.
```

```
Profile 16, Packet Session Status = INACTIVE
```

# Example: GRE Tunnel over Cellular Interface Configuration

The following example shows how to configure the static IP address when a GRE tunnel interface is configured with **ip address unnumbered** *cellular interface*:

**Note** The GRE tunnel configuration is supported only if the service providers provide a public IP address on the LTE interface.

**Note** For service providers using a private IP address, the point-to-point static GRE tunnel cannot be set up with a private IP address at one end and a public IP address on the other end.

```
interface Tunnel2
ip unnumbered <internal LAN interface GE0/0 etc.>
tunnel source Cellular0/2/0
tunnel destination a.b.c.d
interface Cellular0/2/0
ip address negotiated
no ip mroute-cache
dialer in-band
dialer-group 1
```

# Example: LTE/5G as Backup with NAT and IPSec

The following example shows how to configure the LTE/5G on the router as backup with NAT and IPsec:

The receive and transmit speeds cannot be configured. The actual throughput depends on the cellular network service.

For service providers using a private IP address, use the **crypto ipsec transform-set esp** command (that is, esp-aes esp-sha256-hmac...).

```
ip dhcp excluded-address 10.4.0.254
!
ip dhcp pool lan-pool
   network 10.4.0.0 255.255.0.0
   dns-server 10.4.0.254
   default-router 10.4.0.254
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
crypto isakmp key  address a.b.c.d
!
!
crypto ipsec transform-set  ah-sha-hmac esp-3des
!
crypto map gsm1 10 ipsec-isakmp
 set peer a.b.c.d
```

```
 set transform-set
 match address 103
!
interface ATM0/2/0
 no ip address
 ip virtual-reassembly
 load-interval 30
 no atm ilmi-keepalive
 dsl operating-mode auto
!
interface ATM0/2/0.1 point-to-point
 backup interface Cellular0/2/0
ip address negotiated
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
load-interval 30
dialer pool 2
dialer-group 2
ppp authentication chap callin
ppp chap hostname cisco@dsl.com
ppp chap password 0 cisco
ppp ipcp dns request
crypto map gsm1

 ip nat outside
 ip virtual-reassembly
 no snmp trap link-status
 pvc 0/35
  pppoe-client dial-pool-number 2
 !
!
interface Cellular0/2/0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly
no ip mroute-cache
 dialer in-band
 dialer idle-timeout 0
dialer-group 1
 crypto map gsm1
!
interface Vlan1
 description used as default gateway address for DHCP clients
 ip address 10.4.0.254 255.255.0.0
 ip nat inside
 ip virtual-reassembly
!
ip local policy route-map track-primary-if
ip route 0.0.0.0 0.0.0.0 Dialer2 track 234
ip route 0.0.0.0 0.0.0.0 Cellular0/3/0 254
!
!
ip nat inside source route-map nat2cell interface Cellular0/2/0 overload
ip nat inside source route-map nat2dsl overload
!
ip sla 1
 icmp-echo 2.2.2.2 source
 timeout 1000
 frequency 2
ip sla schedule 1 life forever start-time now
access-list 1 permit any
access-list 101 deny ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
```

```
access-list 101 permit ip 10.4.0.0 0.0.255.255 any
access-list 102 permit icmp any host 2.2.2.2
access-list 103 permit ip 10.4.0.0 0.0.255.255 10.0.0.0 0.255.255.255
dialer-list 1 protocol ip list 1
dialer-list 2 protocol ip permit
!
!
route-map track-primary-if permit 10
 match ip address 102
!
route-map nat2dsl permit 10
 match ip address 101
!
route-map nat2cell permit 10
 match ip address 101
 match interface Cellular0/2/0
!
exec-timeout 0 0
login
 modem InOut
```

# Example: SIM Configuration

## Locking the SIM Card

The following example shows how to lock the SIM. The italicized text in this configuration example is used to indicate comments and are not be seen when a normal console output is viewed.

```
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!
Router# cellular 0/2/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 19:35:28.339: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 19:35:59.967: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state.!
```

## Unlocking the SIM Card

The following example shows how to unlock the SIM. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
```

```
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state.!
Router# cellular 0/2/0 lte sim unlock 1111
!!!WARNING: SIM will be unlocked with pin=1111(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!
```

## Automatic SIM Authentication

The following example shows how to configure automatic SIM authentication. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# show cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router# !! SIM is in unlocked state.!Router# cellular 0/2/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 21:22:34.555: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:23:06.495: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router# !! SIM is in locked state. SIM needs to be in locked state for SIM authentication
to ! work.!Router#
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# controller cellular 0/2/0
Router(config-controller)# lte sim authenticate 0 1111
CHV1 configured and sent to modem for verification
Router(config-controller)# end
Router#
Apr 26 21:23:50.571: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! SIM is now in locked state but it can be used for connectivity since authentication
 is ! good. Authentication can be saved in the router configuration so that when you boot
up ! the router with the same locked SIM, connection can be established with the correct !
 Cisco IOS configuration.!
```

## Changing the PIN Code

The following example shows how to change the assigned PIN code. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! SIM is in unlocked state.!Router#
Router# cellular 0/2/0 lte sim lock 1111
!!!WARNING: SIM will be locked with pin=1111(4).
Do not enter new PIN to lock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Apr 26 21:58:11.903: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:58:43.775: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#!! SIM is in locked state. SIM needs to be in locked state to change its PIN.!Router#
Router# cellular 0/2/0 lte sim change-pin 1111 0000
!!!WARNING: SIM PIN will be changed from:1111(4) to:0000(4)
Call will be disconnected. If old PIN is entered incorrectly in 3 attempt(s), SIM will be
blocked!!!
Are you sure you want to proceed?[confirm]
Resetting modem, please wait...
CHV1 code change has been completed. Please enter the new PIN in controller configuration
for verfication
Router#
Apr 26 21:59:16.735: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
Apr 26 21:59:48.387: %CELLWAN-2-MODEM_UP: Modem in NIM slot 0/2 is now UP
Router#
Router#
Router# sh cellular 0/2/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = Locked
SIM User Operation Required = Enter CHV1
Number of CHV1 Retries remaining = 3
Router#!! SIM stays in locked state, as expected, but with new PIN.!Router# cellular 0/2/0
 lte sim unlock 0000
!!!WARNING: SIM will be unlocked with pin=0000(4).
Do not enter new PIN to unlock SIM. Enter PIN that the SIM is configured with.
Call will be disconnected!!!
Are you sure you want to proceed?[confirm]
Router#
Router# show cellular 0/2/0 security
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! Unlock with new PIN is successful. Hence, changing PIN was successful.!
```

## Configuring an Encrypted PIN

The following example shows how to configure automatic SIM authentication using an encrypted PIN. The italicized text throughout this configuration example is used to indicate comments and will not be seen when a normal console output is viewed.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# service password-encryption
Router(config)# username SIM privilege 0 password 1111
Router(config)# do sh run | i SIM
username SIM privilege 0 password 7 055A575E70.!! Copy the encrypted level 7 PIN. Use this
 scrambled PIN in the SIM authentication ! command.!

Router(config)# controller cellular 0/2/0
Router(config-controller)# lte sim authenticate 7 055A575E70
CHV1 configured and sent to modem for verification
Router(config-controller)# exit
Router(config)# no username SIM
Router(config)# end
May 14 20:20:52.603: %SYS-5-CONFIG_I: Configured from console by console
```

# Upgrading the Modem Firmware

The following table describes the Sierra Wireless modems that are supported on Cisco LTE/5G. The firmware for the modem is upgradable using Cisco IOS commands. The firmware is a Crossword Express (cwe) file and can be downloaded from the wireless software download page on Cisco.com.

**Note** Firmware upgrade is supported on utility flash.

Use only Cisco certified firmware. Using a firmware version not certified by Cisco may impact the wireless service provider network adversely.

**Caution** Do not disconnect power or switch the router off during the firmware upgrade process. This may result in permanent modem failure.

**Note** Firmware downgrade is not supported.

***Table 30: Modem SKUs***

| SKU | Modem | Firmware | Release |
|---|---|---|---|
| EHWIC-4G-LTE-A | MC7700 | MC7700 | Cisco 16.6.1 or Later |

# Upgrading the Modem Firmware Manually With CLI

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Go to the Cisco Wireless WAN software download website at: http://software.cisco.com/download/navigator.html | Provides access to Cisco Wireless WAN software downloads page to select the firmware for Cisco LTE/5G.<br>**Note** This website is only available to registered Cisco.com users. |
| **Step 2** | On the Cisco Wireless WAN software page, go to **Products** -> **Cisco Interfaces and Modules** -> **Cisco High-Speed WAN interface Cards** and select your product from the list of available cards. | Select your product for firmware upgrade. |
| **Step 3** | Select and download the appropriate firmware. | Download the modem firmware file to flash memory on the router. |
| **Step 4** | **terminal monitor**<br>**Example:**<br>`Router# terminal monitor` | Enables the logging console in privileged EXEC mode. |
| **Step 5** | **microcode reload cellular** pa-bay slot **modem-provision** [**flash**:<firmware_directory_name>]<br>**Example:**<br>Router# microcode reload cellular 0 2 modem-provision bootflash:/<firmware directory> | Initiates the firmware upgrade process.<br>• pa-bay—Use 0 for LTE/5G.<br>• slot—For LTE/5G, slot number, 0 to 3, where the LTE/5G is plugged in.<br>• For remote download, you can transfer this using the wireless link from Cisco.com onto flash. |
| **Step 6** | **show cellular** *0/2/0* **hardware**<br>**Example:**<br>`Router# show cellular 0 hardware`<br>`Modem Firmware built = 2016/06/30 10:54:05`<br>`Hardware Version = 1.0`<br>`Device Model ID: EM7455` | Verifies the firmware upgrade process. |

## EM74xx Manual Modem Firmware Upgrade: Example

```
Router#  sh cellu 0/2/0 hardware
Modem Firmware Version = SWI9X30C_02.20.03.00
Modem Firmware built = 2016/06/30 10:54:05
Hardware Version = 1.0
Device Model ID: EM7455
```

```
International Mobile Subscriber Identity (IMSI) = <imsi>
International Mobile Equipment Identity (IMEI) = <imei>
Integrated Circuit Card ID (ICCID) = <iccid>
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Modem Online
Current Modem Temperature = 44 deg C
PRI SKU ID = 1102526, PRI version = 002.020_000, Carrier = AT&T
OEM PRI version = 006
Router#cd fw_22_vzw
Router#dir
Directory of bootflash:/fw_22_vzw/

227586  -rw-         64389490  Jun 30 2000 10:21:29 +00:00  74XX_02.20.03.22.cwe
227587  -rw-            16951  Jun 30 2000 10:22:10 +00:00
7455_02.20.03.22_Verizon_002.026_000.nvu

6816092160 bytes total (5965422592 bytes free)
Router#cd
Router#microcode reload cellular 0 2 modem-provision bootflash:/fw_22_vzw/
Reload microcode? [confirm]
Log status of firmware download in router flash?[confirm]
Firmware download status will be logged in bootflash:fwlogfile
Microcode Reload Process launched for cwan slot/bay =0/2; hw type=0x102download option = 0

Router#Success !! send FW Upgrade command to card

*****************************************************
 The interface will be Shut Down for Firmware Upgrade
 This will terminate any active data connections.
*****************************************************
*************************
 Modem will be upgraded!
 Upgrade process will take up to 15 minutes. During
 this time the modem will be unusable.
 Please do not remove power or reload the router during
 the upgrade process.
*************************
*Jul  6 10:19:34.701: %LINK-5-CHANGED: Interface Cellular0/2/0, changed state to
administratively down
*Jul  6 10:19:34.701: %LINK-5-CHANGED: Interface Cellular0/2/1, changed state to
administratively down
----------------------------
FIRMWARE INFO BEFORE UPGRADE:
Modem Device ID: EM7455     MODEM F/W Boot Version: SWI9X30C_02.20.03.00
Modem F/W App Version: SWI9X30C_02.20.03.00     Modem SKU ID: 1102526
Modem Package Identifier:      Modem Carrier String: 4
Modem PRI Ver: 000.006     Modem Carrier Name: ATT
Modem Carrier Revision: 002.020_000
----------------------------
FW_UPGRADE: Modem needs CWE, PRI
*Jul  6 10:19:57.978: %CELLWAN-2-MODEM_DOWN: Modem in NIM slot 0/2 is DOWN
FW_UPGRADE: Upgrade begin at Thu Jul  6 10:20:01 2000
FW_UPGRADE: Upgrade end at Thu Jul  6 10:21:14 2000
FW_UPGRADE: Firmware upgrade success.....
FW_UPGRADE: Waiting for modem to become online
----------------------------
FIRMWARE INFO AFTER UPGRADE:
Modem Device ID: EM7455     MODEM F/W Boot Version: SWI9X30C_02.20.03.22
Modem F/W App Version: SWI9X30C_02.20.03.22     Modem SKU ID: 1102526
Modem Package Identifier:      Modem Carrier String: 5
Modem PRI Ver: 000.006     Modem Carrier Name: VERIZON
Modem Carrier Revision: 002.026_000
----------------------------
```

```
F/W Upgrade: Firmware Upgrade has Completed Successfully
*Jul  6 10:21:55.275: %CELLWAN-2-MODEM_RADIO: Cellular0/2/0 Modem radio has been turned on
*Jul  6 10:21:57.276: %LINK-3-UPDOWN: Interface Cellular0/2/0, changed state to down
*Jul  6 10:21:57.277: %LINK-3-UPDOWN: Interface Cellular0/2/1, changed state to down
Router#
Router#  sh cellu 0/2/0 hardware
Modem Firmware Version = SWI9X30C_02.20.03.22
Modem Firmware built = 2016/10/11 16:03:14
Hardware Version = 1.0
Device Model ID: EM7455
International Mobile Subscriber Identity (IMSI) =<imsi>
International Mobile Equipment Identity (IMEI) = <imei>
Integrated Circuit Card ID (ICCID) = <iccid>
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) = <msisdn>
Modem Status = Modem Online
Current Modem Temperature = 0 deg C
PRI SKU ID = 1102526, PRI version = 002.026_000, Carrier = Verizon
OEM PRI version = 006
```

## Configuring dm-log to Utility Flash: Example

```
Router(config)#controller cellular 0/2/0
Router(config-controller)#lte modem dm-log enable
Router(config-controller)#
*May 8 17:57:09.905: %SYS-5-CONFIG_I: Configured from console by console
Router#
Router#sh cell 0/2/0 log dm-log
Integrated DM logging is on
output path = Utility Flash
filter = bootflash:v11026_Generic_GPS.sqf
maximum log size = 0
maximum file size = 0
log rotation = disabled

32 packets sent to the modem, 4021 bytes, 0 errors
23668 packets received from the modem, 11131720 bytes, 0 input drops
23668 packets stored in utility flash, 11131720 bytes

current file size = 11131720
current log size = 11131720
total log size = 11131720
Utility Flash DM log files: (1) files
```

# SNMP MIBs

**Note** It is recommended that you configure SNMP V3 with authentication/privacy when implementing SNMP SET operation.

The following Simple Management Network Protocol (SNMP) MIBs are supported on Cisco LTE/5G:

- IF-MIB
- ENTITY-MIB
- CISCO-WAN-3G-MIB

- CISCO-WAN-CELL-EXT-MIB

For the CISCO-WAN-3G-MIB, the following tables and sub-tables are supported for 3G and LTE technologies:

- ciscoWan3gMIB(661)
- ciscoWan3gMIBNotifs(0)
- ciscoWan3gMIBObjects(1)
- c3gWanCommonTable(1)
- c3gWanGsm(3)
- c3gGsmIdentityTable(1)
- c3gGsmNetworkTable(2)
- c3gGsmPdpProfile(3)
- c3gGsmPdpProfileTable(1)
- c3gGsmPacketSessionTable(2)
- c3gGsmRadio(4)
- c3gGsmRadioTable(1)
- c3gGsmSecurity(5)
- c3gGsmSecurityTable(1)

For the CISCO-WAN-CELL-EXT-MIB, the following tables and sub-tables are supported for LTE technology only:

- ciscoWanCellExtMIB(817)
- ciscoWanCellExtMIBNotifs(0)
- ciscoWanCellExtMIBObjects(1)
- ciscoWanCellExtLte(1)
- cwceLteRadio(1)
- cwceLteProfile(2)

You can download the MIBs from the Cisco MIB Locator at http://www.cisco.com/go/mibs.

# SNMP LTE/5G Configuration: Example

The following example describes how to configure 3G 4G MIB trap on the router:

```
controller Cellular 0/2/0
 lte event rssi onset mib-trap All-lte
 lte event rssi onset threshold -100
 lte event rssi abate mib-trap All-lte
 lte event rssi abate threshold -90
 lte event temperature onset mib-trap
 lte event temperature onset threshold 55
 lte event temperature abate mib-trap
```

```
lte event temperature abate threshold 50
lte event modem-state mib-trap all
lte event service mib-trap
lte event network mib-trap
lte event connection-status mib-trap All-lte
lte event rsrp onset mib-trap All-lte
lte event rsrp onset threshold -85
lte event rsrp abate mib-trap All-lte
lte event rsrp abate threshold -80
lte event rsrq onset mib-trap All-lte
lte event rsrq onset threshold -8
lte event rsrq abate mib-trap All-lte
lte event rsrq abate threshold -6
```

The following example describes how to configure SNMP capability on the router:

```
snmp-server group neomobilityTeam v3 auth notify 3gView
snmp-server view 3gView ciscoWan3gMIB included
snmp-server community neomobility-test RW snmp-server community public RW
snmp-server enable traps c3g
snmp server enable traps LTE
snmp-server host 172.19.153.53 neomobility c3g snmp-server host 172.19.152.77 public c3g
snmp-server host 172.19.152.77 public udp-port 6059
```

The following example describes how to configure an external host device to communicate with the router through SNMP:

```
setenv SR_MGR_CONF_DIR /users/<userid>/mibtest
setenv SR_UTIL_COMMUNITY neomobility-test
setenv SR_UTIL_SNMP_VERSION -v2c
setenv SR_TRAP_TEST_PORT 6059
```

# Troubleshooting

This section provides the essential information and resources available for troubleshooting the Cisco LTE/5G feature.

## Verifying Data Call Setup

To verify the data call setup, follow these steps:

1. After you create a modem data profile using the cellular profile create command and configuring DDR on the cellular interface, send a ping from the router to a host across the wireless network.
2. If the ping fails, debug the failure by using the following debug and show commands:
3. **debug chat**
4. **debug modem**
5. **debug dialer**
6. **show cellular all**
7. **show controller cell***0/2/0*
8. **show interface cellular**
9. **show running-config**

10. **show ip route**
11. **show platform**
12. Save the output from these commands and contact your system administrator.

# Checking Signal Strength

If the Received Signal Strength Indication (RSSI) level is very low (for example, if it is less than –110 dBm), follow these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Check the antenna connection. Make sure the TNC connector is correctly threaded and tightened. | |
| **Step 2** | If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved. | |
| **Step 3** | Contact your wireless service provider to verify if there is service availability in your area. | |

# Verifying Service Availability

The following is a sample output for the **show cellular all** command for a scenario where the antenna is disconnected and a modem data profile has not been created.

```
Router# show cellular 0/2/0 all
Hardware Information
====================
Modem Firmware Version = SWI9X30C_02.20.03.00
Modem Firmware built = 2016/06/30 10:54:05
Hardware Version = 1.0
Device Model ID: EM7455
International Mobile Subscriber Identity (IMSI) = 123456000031546
International Mobile Equipment Identity (IMEI) = 356129070052334
Integrated Circuit Card ID (ICCID) = 8949001508130031546
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Modem Online
Current Modem Temperature = 42 deg C
PRI SKU ID = 1102526, PRI version = 002.017_000, Carrier = Generic
OEM PRI version = 002

Profile Information
====================

Profile 1 = ACTIVE* **
--------
PDP Type = IPv4v6
PDP address = 29.29.29.196
PDP IPV6 address = 2001:2678:2680:5FD7:DDE7:70E1:DC07:CCB7/64  Scope: Global
```

```
Access Point Name (APN) = broadband
Authentication = None
        Primary DNS address = 8.0.0.8
        Secondary DNS address = 8.8.4.4
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844

Profile 2 = ACTIVE
--------
PDP Type = IPv4v6
PDP address = 21.21.21.206
PDP IPV6 address = 2001:567A:567A:1480:5DD6:18D1:BD63:49DA/64  Scope: Global
Access Point Name (APN) = basic
Authentication = None
        Primary DNS address = 171.70.168.183
        Secondary DNS address = 8.8.8.8
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844

Profile 3 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mpdn
Authentication = None

Profile 4 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = None

Profile 5 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = cisco.gw4.vzwentp
Authentication = None

Profile 6 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de1
Authentication = None

Profile 7 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de2
Authentication = None

Profile 8 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = None

Profile 9 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mpdndt-qos
Authentication = None

Profile 10 = INACTIVE
--------
PDP Type = IPv4
```

```
Access Point Name (APN) = mobility-de2
Authentication = None

Profile 11 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = None

Profile 12 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = wfqos
Authentication = CHAP
Username: ipv4v6
Password:

Profile 13 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = CHAP
Username: ipv4v6
Password:

Profile 14 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = mobility-de2
Authentication = CHAP
Username: ipv4v6
Password:

Profile 15 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = aaaauth
Authentication = CHAP
Username: ipv4v6
Password:

Profile 16 = INACTIVE
--------
PDP Type = IPv4
Access Point Name (APN) = broadband
Authentication = CHAP
Username: ipv4v6
Password:

  * - Default profile
 ** - LTE attach profile


Configured default profile for active SIM 0 is profile 1.


Data Connection Information
===========================
Profile 1, Packet Session Status = ACTIVE
        Cellular0/2/0:
        Data Packets Transmitted = 198 ,  Received = 209
        Data Transmitted = 14410 bytes, Received = 24882 bytes
        IP address = 29.29.29.196
        IPV6 address = 2001:2678:2680:5FD7:DDE7:70E1:DC07:CCB7/64  Scope: Global
```

```
        Primary DNS address = 8.0.0.8
        Secondary DNS address = 8.8.4.4
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844
Profile 2, Packet Session Status = ACTIVE
        Cellular0/2/1:
        Data Packets Transmitted = 12 ,  Received = 13
        Data Transmitted = 1200 bytes, Received = 1144 bytes
        IP address = 21.21.21.206
        IPV6 address = 2001:567A:567A:1480:5DD6:18D1:BD63:49DA/64  Scope: Global
        Primary DNS address = 171.70.168.183
        Secondary DNS address = 8.8.8.8
        Primary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8888
        Secondary DNS IPV6 address = 2001:4860:4860:0:0:0:0:8844
Profile 3, Packet Session Status = INACTIVE
Profile 4, Packet Session Status = INACTIVE
Profile 5, Packet Session Status = INACTIVE
Profile 6, Packet Session Status = INACTIVE
Profile 7, Packet Session Status = INACTIVE
Profile 8, Packet Session Status = INACTIVE
Profile 9, Packet Session Status = INACTIVE
Profile 10, Packet Session Status = INACTIVE
Profile 11, Packet Session Status = INACTIVE
Profile 12, Packet Session Status = INACTIVE
Profile 13, Packet Session Status = INACTIVE
Profile 14, Packet Session Status = INACTIVE
Profile 15, Packet Session Status = INACTIVE
Profile 16, Packet Session Status = INACTIVE

Network Information
==================
Current System Time = Tue Jan 8 23:24:22 1980
 --More--
*Jun 19 06:13:14.665: %IOSXE_OIR-6-INSSPA: SPA inserted in sCurrent Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Roaming
Network Selection Mode = Automatic
Network = 123 456
Mobile Country Code (MCC) = 123
Mobile Network Code (MNC) = 456
Packet switch domain(PS) state = Attached
LTE Carrier Aggregation state = Deconfigured
Registration state(EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1801
Cell ID = 768001
Network MTU is not Available

Radio Information
=================
Radio power mode = online
LTE Rx Channel Number =  2000
LTE Tx Channel Number =  20000
LTE Band =  4
LTE Bandwidth = 10 MHz
Current RSSI = -71 dBm
Current RSRP = -95 dBm
Current RSRQ = -7 dB
Current SNR = 26.4  dB
Physical Cell Id = 12
Number of nearby cells = 1
Idx      PCI (Physical Cell Id)
--------------------------------
1             12
```

```
Radio Access Technology(RAT) Preference = LTE
Radio Access Technology(RAT) Selected = LTE

Modem Security Information
==========================
Active SIM = 0
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

Cellular Firmware List
==========================
 Idx Carrier      FwVersion    PriVersion   Status
 1   ATT          02.20.03.00  002.019_000  Inactive
 2   GENERIC      02.20.03.00  002.017_000  Active
 3   SPRINT       02.20.03.22  002.020_000  Inactive
 4   TELSTRA      02.20.03.00  002.018_000  Inactive
 5   VERIZON      02.20.03.22  002.026_000  Inactive

Firmware Activation mode : AUTO

GPS Information
==========================

GPS Info
-------------
GPS Feature: enabled
GPS Mode Configured: not configured
GPS Status: NMEA Disabled

SMS Information
===============
Incoming Message Information
----------------------------
SMS stored in modem = 0
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 0
Number of callbacks triggered by SMS = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0

Outgoing Message Information
----------------------------
Total SMS sent successfully = 0
Total SMS send failure = 0
Number of outgoing SMS pending = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Last Outgoing SMS Status = SUCCESS
Copy-to-SIM Status =     0x0
Send-to-Network Status = 0x0
Report-Outgoing-Message-Number:
  Reference Number =     0
  Result Code =          0x0
  Diag Code =            0x0 0x0 0x0 0x0 0x0

SMS Archive URL =

Error Information
=================
```

```
This command is not supported on 4G modems.


Modem Crashdump Information
===========================
Modem crashdump logging: off
```

# Successful Call Setup

The following is a sample output when a call is set up. It shows a received IP address from the network. Call setup is successful and data path is open.

```
debug dialer
debug cellular 0/2/0 messages callcontrol
```

# Modem Troubleshooting Using Integrated Modem DM Logging

As part of the 3G and 4G serviceability enhancement in Cisco IOS Release 15.2(4)M2 and Cisco IOS Release 15.3(1)T, DM log collection has been integrated into Cisco IOS, eliminating the need for an external PC and simplifying the DM log collection process. The lte modem dm-log command can be used in controller cellular configuration mode to configure integrated DM logging to monitor traffic on the modem. See the Cisco 3G and 4G Serviceability Enhancement User Guide for more information on configuring Integrated DM Logging parameters.

# Modem Settings for North America and Carriers Operating on 700 MHz Band

For LTE-EA deployments in North America and for carriers operating in the 700 MHz band, the following changes to the modem settings are required to prevent long network attach times.

The output of show cellular x/x/x all command shows the following:

- Current RSSI is –125 dBM
- LTE Technology Preference = No preference specified (AUTO)

The following sections explain useful commands for changing modem settings:

## Changing Modem Settings

To change the modem settings to force the modem to scan different technologies, use the following Cisco IOS command:

```
Router# cellular 0/2/0 lte technology ?
auto  Automatic LTE Technology Selection
  lte   LTE
  umts  UMTS
```

## Electronic Serial Number (ESN)

The ESN number is located directly on the modem label in hexadecimal notation. It can also be retrieved using the Cisco IOS CLI using the show cellular *slot/port/module* **hardware** command.

The sample output below shows the ESN number:

```
Hardware Information
====================
Electronic Serial Number (ESN) = 0x603c9854 [09603971156]
Electronic Serial Number (ESN) = <specific ESN in hexadecimal> [specific ESN in decimal]
```

# Additional References

### Related Documents

| Related Topic | Document Title |
|---|---|
| Hardware Overview and Installation | • *Cisco 4G-LTE Wireless WAN EHWIC*<br>http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/EHWIC-4G-LTEH<br>• *Cisco Fourth-Generation LTE Network Interface Module Installation Guide*<br>http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/hardware/installation/guide/4GLTENIM |
| Supported Cisco antennas and cables | • *Installing Cisco Interface Cards in Cisco Access Routers*<br>http://www.cisco.com/en/US/docs/routers/access/interfaces/ic/hardware/installation/guide/inst_ic.html<br>• *Cisco 4G/3G Omnidirectional Dipole Antenna (4G-LTE-ANTM-D)*<br>http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/4G3G_ant.html<br>• *Cisco 4G Indoor Ceiling-Mount Omnidirectional Antenna (4G-ANTM-OM-CM)*<br>http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/antcm4gin.html<br>• *Cisco Outdoor Omnidirectional Antenna for 2G/3G/4G Cellular (ANT-4G-OMNI-OUT-N)*<br>http://www.cisco.com/en/US/docs/routers/connectedgrid/antennas/installing/Outdoor_Omni_for_2G_3G_4G<br>• *Cisco Integrated 4G Low-Profile Outdoor Saucer Antenna (ANT-4G-SR-OUT-TNC)*<br>http://www.cisco.com/en/US/docs/routers/connectedgrid/antennas/installing/4G_LowProfile_Outdoor_Sauce<br>• *Cisco Single-Port Antenna Stand for Multiband TNC Male-Terminated Portable Antenna (Cisco 4G-AE*<br>http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/4Gantex15-10r.html<br>• *Cisco 4G Lightning Arrestor (4G-ACC-OUT-LA)*<br>http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/4Glar.html<br>• *Lightning Arrestor for the Cisco 1240 Connected Grid Router*<br>http://www.cisco.com/en/US/docs/routers/connectedgrid/lightning_arrestor/Lightning_Arrestor_for_the_Cisc<br>Cisco 4G Indoor/Outdoor Active GPS Antenna (GPS-ACT-ANTM-SMA) |

| Related Topic | Document Title |
|---|---|
| Datasheet | • Modules data sheets for ISR4k<br>http://www.cisco.com/c/en/us/products/routers/4000-series-integrated-services-routers-isr/datasheet-listir<br>• LTE datasheet<br>http://www.cisco.com/en/US/docs/routers/access/wireless/hardware/notes/4Gantex15-10r.html<br>http://www.cisco.com/c/en/us/td/docs/routers/access/4400/roadmap/isr4400roadmap.html |

### MIBs

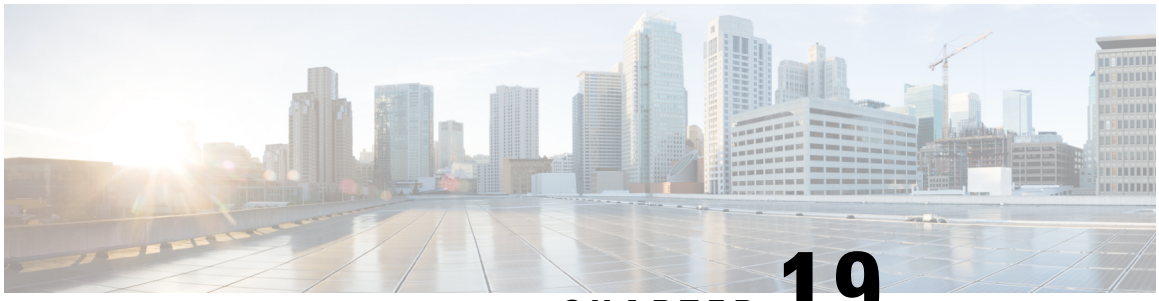
| MIB | MIBs Link |
|---|---|
| • IF-MIB<br>• CISCO-ENTITY-VENDORTYPE-OID-MIB<br>• CISCO-WAN-3G-MIB | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

### RFCs

| RFC | Title |
|---|---|
| RFC 3025 | Mobile IP Vendor/Organization-Specific Extensions |

### Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |



CHAPTER 19

# Configuring Ethernet Switch Ports

This chapter contains the following sections:


- Configuring VLANs, on page 325
- Configuring VTP, on page 326
- Configuring 802.1x Authentication, on page 327
- Configuring Spanning Tree Protocol, on page 328
- Configuring MAC Address Table Manipulation, on page 330
- Configuring Switch Port Analyzer, on page 330
- Configuring IGMP Snooping, on page 331
- Configuring LACP, on page 332
- Configuring HSRP , on page 339
- Configuring VRRP , on page 340


## Configuring VLANs

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

**Note** Internal VLANs cannot be configured. By default, these are the VLAN IDs from 2350 - 2449. Use the **show vlan internal usage** command to check for the range of internal VLANS.

Example: VLAN configuration

```
Router# configure terminal
 Router(config)# vlan 1
```

```
Router(config)# vlan 2
Router(config)# interface vlan 1
Router(config-if)# ip address 192.0.2.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface vlan 2
Router(config-if)# ip address 192.0.2.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface gigabitethernet 0/1/0
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 1
Router(config-if)# interface gigabitethernet 0/1/1
Router(config-if)# switchport access vlan 2
Router(config-if)# exit
```

# Configuring VTP

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

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

You should understand the following concepts for configuring VTP.

- VTP domain: A VTP domain (also called a VLAN management domain) consists of one switch or several interconnected switches or switch stacks under the same administrative responsibility sharing the same VTP domain name. A switch can be in only one VTP domain. You make global VLAN configuration changes for the domain.
- VTP server: In VTP server mode, you can create, modify, and delete VLANs, and specify other configuration parameters (such as the VTP version) for the entire VTP domain. VTP Version 3 should be configured on each switch manually including the VTP server and client. VTP servers advertise their VLAN configurations to other switches in the same VTP domain and synchronize their VLAN configurations with other switches based on advertisements received over trunk links.VTP server is the default mode.
- VTP client: A VTP client behaves like a VTP server and transmits and receives VTP updates on its trunks, but you cannot create, change, or delete VLANs on a VTP client. VLANs are configured on another switch in the domain that is in server mode.
- VTP transparent: VTP transparent switches do not participate in VTP. A VTP transparent switch does not advertise its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements. However, in VTP version 2 or version 3, transparent switches do forward VTP advertisements that they receive from other switches through their trunk interfaces. You can create, modify, and delete VLANs on a switch in VTP transparent mode.
- VTP pruning is not supported.

For detailed information on VTP, see the following web link:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/geshwic_cfg.html#wp1046901

Example: Configuring VTP

The following example shows how to configure the switch as a VTP server:

```
Router# configure terminal
Router(config)# vtp mode server
Router(config)# vtp domain Lab_Network
Router(config)# exit
```

The following example shows how to configure the switch as a VTP client:

```
Router# configure terminal
Router(config)# vtp domain Lab_Network
Router(config)# vtp mode client
Router(config)# exit
```

The following example shows how to configure the switch as VTP transparent:

```
Router# configure terminal
Router(config)# vtp mode transparent
Router(config)# exit
```

# Configuring 802.1x Authentication

IEEE 802.1x port-based authentication defines a client-server-based access control and authentication protocol to prevent unauthorized clients from connecting to a LAN through publicly accessible ports.The authentication server authenticates each client connected to a switch port before allowing access to any switch or LAN services. Until the client is authenticated, IEEE 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL), Cisco Discovery Protocol (CDP), and Spanning Tree Protocol (STP) traffic through the port to which the client is connected. After authentication, normal traffic passes through the port.

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

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

responsible for encapsulating and decapsulating the EAP frames and interacting with the authentication server.

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

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

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

This example shows how to configure Cisco 1100 series router as 802.1x authenticator:

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

# Configuring Spanning Tree Protocol

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

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

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

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

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

For detailed configuration information on STP see the following link:

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

Example: Spanning Tree Protocol Configuration

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

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

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

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

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

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

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

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

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

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

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

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

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

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

# Configuring MAC Address Table Manipulation

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

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

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

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

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

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

Example: MAC Address Table Manipulation

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

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

The following example shows setting the aging timer.

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

# Configuring Switch Port Analyzer

Cisco 1100 Series ISRs support local SPAN only, and upto one SPAN session. You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

Only traffic that enters or leaves source ports or traffic that enters or leaves source can be monitored by using SPAN; traffic routed to a source cannot be monitored. For example, if incoming traffic is being monitored,

traffic that gets routed from another source cannot be monitored; however, traffic that is received on the source and routed to another can be monitored.

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

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

Example: SPAN Configuration

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

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

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

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

The following example shows how to remove gigabit ethernet as a SPAN source for SPAN session 1:

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

# Configuring IGMP Snooping

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

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

Use the **[no] ip igmp snooping enable** command to configure IGMP Snooping on Cisco 1100 Series ISRs.

By default, IGMP snooping is globally enabled in Cisco 1100 Series ISRs.

# Configuring LACP

## 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 portchannel 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 4 for C1100TG and 1 to 2 for C1131. This port-channel interface number corresponds to the one specified with the channel-group interface configuration command.

## 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.

## Auto-LAG

globally and is enabled on all port interfaces. The auto-LAG applies to a switch only when it is enabled globally.

On enabling auto-LAG globally, the following scenarios are possible:

- All port interfaces participate in creation of auto EtherChannels provided the partner port interfaces have EtherChannel configured on them. For more information, see the "The supported auto-LAG configurations between the actor and partner devices" table below.

- Ports that are already part of manual EtherChannels cannot participate in creation of auto EtherChannels.
- When auto-LAG is disabled on a port interface that is already a part of an auto created EtherChannel, the port interface will unbundle from the auto EtherChannel.
- The following table shows the supported auto-LAG configurations between the actor and partner devices:

***Table 31: The supported auto-LAG configurations between the actor and partner devices***

| Actor/Partner | Active | Passive | Auto |
|---|---|---|---|
| Active | Yes | Yes | Yes |
| Passive | Yes | No | Yes |
| Auto | Yes | Yes | Yes |

On disabling auto-LAG globally, all auto created Etherchannels become manual EtherChannels.

You cannot add any configurations in an existing auto created EtherChannel. To add, you should first convert it into a manual EtherChannel by executing the **port-channel** <*channel-number*> **persistent**.

# 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 C1100TG and C1131 EtherChannels.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface***interface-id*<br>**Example:**<br>For C1100TG<br>`Device(config)# interface gigabitethernet0/2/x`<br>**Example:**<br>For C1131<br>`Device(config)# interface gigabitethernet0/1/x` | Specifies a physical port and enters interface configuration mode.<br>Valid interfaces are physical ports.<br>For a LACP EtherChannel, you can configure up to 4 Ethernet active ports and 4 standby ports (for both C1100TG and C1131) of the same type. Up to 4 ports can be active, and up to 4 ports can be in standby mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **switchportmode** {**access** \| **trunk**<br>**Example:**<br>`Device(config-if)# switchport mode access` | Assigns all ports as static-access ports in the same VLAN, or configure them as trunks.<br>If you configure the port as a static-access port,assign it to only one VLAN. The range is 1 to 4094. |
| **Step 5** | **switchportaccessvlan** *vlan-id*<br>**Example:**<br>`Device(config-if)# switchport access vlan 22` | (Optional) If you configure the port as a static-access port, assign it to only one VLAN. The range is 1 to 4094. |
| **Step 6** | **channel-group** *channel-group-number* **mode** {**on**} \| {**active** \| **passive**}<br>**Example:**<br>`Device(config-if)# channel-group 5 modeauto` | Assigns the port to a channel group and specifies the LACP mode.<br>For mode, select one of these keywords:<br>• **on** —Forces the port to channel without LACP. In the on mode, an EtherChannel exists only when a port-group in the on mode is connected to another port group in the on mode.<br>• **active**—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.<br>• • **passive** —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. |
| **Step 7** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |

In the above table, the port-channel interface is created implicitly through the "channel-group" command. An alternate way is to create the port-channel interface explicitly with the following steps:

**Procedure**

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

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interfaceport-channel**<br>**Example:**<br>`Device(config)#interface portchannel [interface-number]` | Creates the port-channel interface that by default, creates the Layer 3 interface. |
| **Step 4** | **switchportinterface**<br>**Example:**<br>`Device(config-if)#switchport` | Assigns switch port-channel interface to layer 2 switching interface. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | 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 |
|---|---|---|
| **Step 1** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 2** | **port-channelswportload-balance**<br>**Example:**<br>For C1100TG<br>`Device(config)# port-channel swport load-balance src-mac` | Select one of these load-distribution methods:<br>**a.** dst-ip—Specifies destination-host IP address.<br>**b.** dst-mac—Specifies the destination-host MAC address of the incoming packet.<br>**c.** dst-mixed-ip-port—Specifies the host IP address and TCP/UDP port.<br>**d.** dst-port—Specifies the destination TCP/UDP port.<br>**e.** src-dst-ip—Specifies the source and destination host IP address.<br>**f.** src-dst-mac—Specifies the source and destination host MAC address. |

| | Command or Action | Purpose |
|---|---|---|
| | | **g.** src-dst-mixed-ip-port—Specifies the source and destination host IP address and TCP/UDP port.<br>**h.** src-dst-port—Specifies the source and destination TCP/UDP port.<br>**i.** src-ip—Specifies the source host IP address.<br>**j.** src-mac—Specifies the source MAC address of the incoming packet.<br>**k.** src-mixed-ip-port—Specifies the source host IP address and TCP/UDP port.<br>**l.** src-port—Specifies the source TCP/UDP port. |
| **Step 3** | **end**<br>**Example:**<br>`Device(config)# end` | 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 |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interfaceport-channel** *channel-number*<br>**Example:**<br>`Device(config)# interface port-channel 2` | Enters interface configuration mode for a port-channel.<br>For channel-number, the range is 1 to 4 for C1100TG and 1 to 2 for C1131. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **port-channelmin-links***min-links-number*<br>**Example:**<br>`Device(config-if)# port-channel min-links 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>For min-links-number, the range is 1 to 4 for C1100TG and 1 to 2 for C1131. |
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | 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 |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **interface** {**gigabitethernet**} *slot/subslot/port*<br>**Example:**<br>For C1100TG<br>`Device(config)# interface gigabitEthernet 0/2/x`<br>**Example:**<br>For C1131<br>`Device(config)# interface gigabitEthernet 0/1/x` | Configures an interface and enters interface configuration mode. |
| **Step 4** | **lacprate** {**normal** \| **fast**}<br>**Example:**<br>`Device(config-if)# lacp rate fast` | Configures the rate at which LACP control packets are received by an LACP-supported interface. To reset the timeout rate to its default, use the **no lacp rate** command. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 6** | **showlacpinternal**<br>**Example:**<br>`Device# show lacp internal`<br>`Device# show lacp counters` | Verifies your configuration. |

# Configuring Auto-LAG Globally

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode. Enter your password if prompted. |
| **Step 2** | **configureterminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | [**no**] **port-channelswportauto**<br>**Example:**<br>`Device(config)# port-channel swport auto` | Enables the auto-LAG feature on a switch globally. Use the no form of this command to disable the auto-LAG feature on the switch globally.<br>**Note** By default, the auto-LAG feature is enabled on the port |
| **Step 4** | **end**<br>**Example:**<br>`Device(config)# end` | Returns to privileged EXEC mode. |
| **Step 5** | **showetherchannelswportauto**<br>**Example:**<br>`Device# show etherchannel swport auto` | Displays that EtherChannel is created automatically. |

# Configuring HSRP

**Note** HSRP is supported only on the SVI interface.

The Hot Standby Router Protocol (HSRP) is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. HSRP routes IP traffic without relying on the availability of any single router. It enables a set of router interfaces to work together to present the appearance of a single virtual router or default gateway to the hosts on a LAN. When HSRP is configured on a network or segment, it provides a virtual Media Access Control (MAC) address and an IP address that is shared among a group of configured routers. HSRP allows two or more HSRP-configured routers to use the MAC address and IP network address of a virtual router. The virtual router does not exist; it represents the common target for routers that are configured to provide backup to each other. One of the routers is selected to be the active router and another to be the standby router, which assumes control of the group MAC address and IP address should the designated active router fail.

HSRP uses a priority mechanism to determine which HSRP configured device is to be the default active device. To configure a device as the active device, you assign it a priority that is higher than the priority of all the other HSRP-configured devices. The default priority is 100, so if you configure just one device to have a higher priority, that device will be the default active device. In case of ties, the primary IP addresses are compared, and the higher IP address has priority. If you do not use the standby preempt interface configuration command in the configuration for a router, that router will not become the active router, even if its priority is higher than all other routers.

For more information about configuring HSRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-hsrp.html

Example: Configuring HSRP

In this example, Router A is configured to be the active device for group 1 and standby device for group 2. Device B is configured as the active device for group 2 and standby device for group 1.

```
RouterA# configure terminal
RouterA(config)# interface vlan 2
RouterA(config-if)# ip address 10.1.0.21 255.255.0.0
RouterA(config-if)# standby 1 priority 110
RouterA(config-if)# standby 1 preempt
RouterA(config-if)# standby 1 ip 10.1.0.3
RouterA(config-if)# standby 2 priority 95
RouterA(config-if)# standby 2 preempt
RouterA(config-if)# standby 2 ip 10.1.0.4
RouterA(config-if)# end

RouterB# configure terminal
RouterB(config)# interface vlan 2
RouterB(config-if)# ip address 10.1.0.22 255.255.0.0
RouterB(config-if)# standby 1 priority 105
RouterB(config-if)# standby 1 preempt
RouterB(config-if)# standby 1 ip 10.1.0.3
RouterB(config-if)# standby 2 priority 110
RouterB(config-if)# standby 2 preempt
RouterB(config-if)# standby 2 ip 10.1.0.4
```

# Configuring VRRP

The Virtual Router Redundancy Protocol (VRRP) is an election protocol that dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing several routers on a multiaccess link to utilize the same virtual IP address. A VRRP router is configured to run the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, one router is elected as the primary virtual router, with the other routers acting as backups in case the primary virtual router fails.

An important aspect of the VRRP is VRRP router priority. Priority determines the role that each VRRP router plays and what happens if the primary virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the physical interface, this router will function as a primary virtual router. Priority also determines if a VRRP router functions as a virtual router backup and the order of ascendancy to becoming a primary virtual router if the primary virtual router fails. You can configure the priority of each virtual router backup using the vrrp priority command.

By default, a preemptive scheme is enabled whereby a higher priority virtual router backup that becomes available takes over for the virtual router backup that was elected to become primary virtual router. You can disable this preemptive scheme using the no vrrp preempt command. If preemption is disabled, the virtual router backup that is elected to become virtual router primary remains the primary until the original primary virtual router recovers and becomes primary again.

The primary virtual router sends VRRP advertisements to other VRRP routers in the same group. The advertisements communicate the priority and state of the primary virtual router. The VRRP advertisements are encapsulated in IP packets and sent to the IP Version 4 multicast address assigned to the VRRP group. The advertisements are sent every second by default; the interval is configurable.

For more information on VRRP, see the following link:

http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-mt/fhp-15-mt-book/fhp-vrrp.html

Example: Configuring VRRP

In the following example, Router A and Router B each belong to two VRRP groups, group1 and group 5. In this configuration, each group has the following properties:

Group 1:

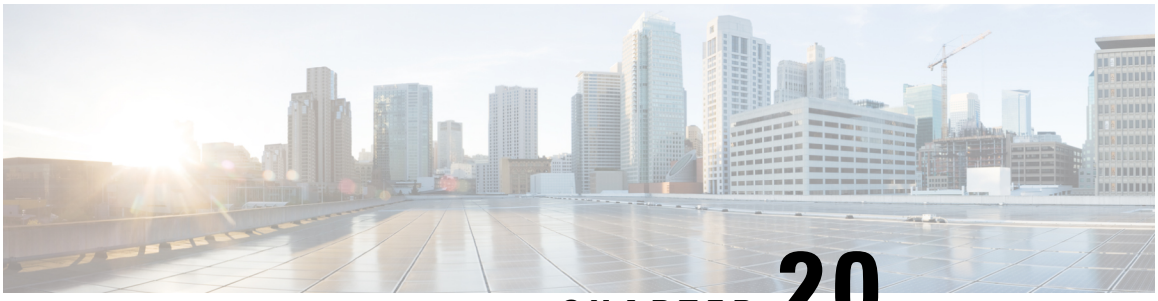
- Virtual IP address is 10.1.0.10.
- Router A will become the primary for this group with priority 120.
- Advertising interval is 3 seconds.
- Preemption is enabled.

Group 5:

- Router B will become the primary for this group with priority 200.
- Advertising interval is 30 seconds.
- Preemption is enabled.

```
RouterA(config)# interface vlan 2
RouterA(config-if)# ip address 10.1.0.2 255.0.0.0
RouterA(config-if)# vrrp 1 priority 120
RouterA(config-if)# vrrp 1 authentication cisco
```

```
RouterA(config-if)# vrrp 1 timers advertise 3
RouterA(config-if)# vrrp 1 timers learn
RouterA(config-if)# vrrp 1 ip 10.1.0.10
RouterA(config-if)# vrrp 5 priority 100
RouterA(config-if)# vrrp 5 timers advertise 30
RouterA(config-if)# vrrp 5 timers learn
RouterA(config-if)# vrrp 5 ip 10.1.0.50
RouterA(config-if)# no shutdown
RouterA(config-if)# end
RouterB(config)# interface vlan 2
RouterB(config-if)# ip address 10.1.0.1 255.0.0.0
RouterB(config-if)# vrrp 1 priority 100
RouterB(config-if)# vrrp 1 authentication cisco
RouterB(config-if)# vrrp 1 timers advertise 3
RouterB(config-if)# vrrp 1 timers learn
RouterB(config-if)# vrrp 1 ip 10.1.0.10
RouterB(config-if)# vrrp 5 priority 200
RouterB(config-if)# vrrp 5 timers advertise 30
RouterB(config-if)# vrrp 5 timers learn
RouterB(config-if)# vrrp 5 ip 10.1.0.50
RouterB(config-if)# no shutdown
RouterB(config-if)# end
```



CHAPTER 20

# Slot and Subslot Configuration

This chapter contains the following sections:


- Configuring the Interfaces, on page 343


# Configuring the Interfaces

The following sections describe how to configure interfaces and also provide examples of configuring the router interfaces:

## Configuring the Interfaces: Example

The following example shows the **interface gigabitEthernet** command being used to add the interface and set the IP address. **0/0/0** is the slot/subslot/port. The ports are numbered 0 to 3.

```
Router# show running-config interface gigabitEthernet 0/0/0
Building configuration...
Current configuration : 71 bytes
!
interface gigabitEthernet0/0/0
no ip address
negotiation auto
end

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/0
```

## Viewing a List of All Interfaces: Example

In this example, **show interfaces summary** command is used to display all the interfaces:

```
Router# show interfaces summary
    *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ       IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
```

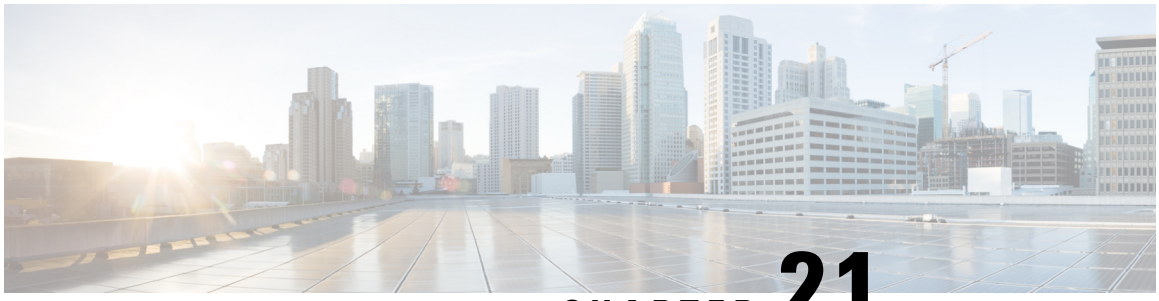
```
------------------------------------------------------------------------------------------------------------------
* GigabitEthernet0/0/0           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/0/1           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/0           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/1           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/2           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/3           0         0         0         0         0         0
  0         0         0

  Interface                   IHQ       IQD       OHQ       OQD       RXBS       RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------------
* GigabitEthernet0/1/4           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/5           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/6           0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/1/7           0         0         0         0         0         0
  0         0         0
* Wl0/1/8                        0         0         0         0         0         0
  0         0         0
* Cellular0/2/0                  0         0         0         0         0         0
  0         0         0
  Cellular0/2/1                  0         0         0         0         0         0
  0         0         0
* Loopback3                      0         0         0         0         0         0
  0         0         0
* Loopback50                     0         0         0         0         0         0
  0         0         0
* Loopback100                    0         0         0         0         0         0
  0         0         0
* Loopback544534                 0         0         0         0         0         0
  0         0         0
```

# Viewing Information About an Interface: Example

The following example shows how to display a brief summary of an interface's IP information and status, including the virtual interface bundle information, by using the **show ip interface brief** command:

```
Router# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   192.168.1.46    YES NVRAM  up                    up
GigabitEthernet0/0/1   192.0.2.1      YES NVRAM  up                   up
GigabitEthernet0/1/0   unassigned      YES unset  up                    up
GigabitEthernet0/1/1   unassigned      YES unset  up                    up
GigabitEthernet0/1/2   unassigned      YES unset  up                    up
GigabitEthernet0/1/3   unassigned      YES unset  up                    up
GigabitEthernet0/1/4   unassigned      YES unset  up                    up
GigabitEthernet0/1/5   unassigned      YES unset  up                    up
GigabitEthernet0/1/6   unassigned      YES unset  up                    up
GigabitEthernet0/1/7   unassigned      YES unset  up                    up
Wl0/1/8                unassigned      YES unset  up                    up
Cellular0/2/0          unassigned      YES NVRAM  up                    up
Cellular0/2/1          unassigned      YES NVRAM  administratively down down
Loopback3              unassigned      YES unset  up                    up
Loopback50             192.0.2.2        YES NVRAM  up                     up
Loopback100            unassigned      YES unset  up                    up
```

```
Loopback544534         unassigned      YES unset  up                    up
Loopback32432532       unassigned      YES unset  up                    up
Port-channel2          unassigned      YES unset  down                  down
Vlan1                  10.10.10.1      YES NVRAM  up                    up
```



CHAPTER 21

# Online Insertion and Removal

Online insertion and removal (OIR) enables you to replace faulty modules without affecting system operation. There is only soft OIR,which is done via CLI.


- Soft OIR Procedures, on page 347
- Manage OIR for Pluggable LTE Modules, on page 347


## Soft OIR Procedures

The following describes the soft OIR procedures:

```
Router# hw-module subslot 0/0 start
client#
*Oct 26 21:50:22.272: %IOSXE_OIR-6-SOFT_STARTSPA: SPA(C1111-2x1GE) restarted in subslot 0/0
client#
*Oct 26 21:50:28.553: %SPA_OIR-6-ONLINECARD: SPA (C1111-2x1GE) online in subslot 0/0

Router# hw-module subslot 0/0 stop
Proceed with stop of module? [confirm]

*Oct 26 21:50:15.498: %SPA_OIR-6-OFFLINECARD: SPA (C1111-2x1GE) offline in subslot 0/0
*Oct 26 21:50:15.499: %IOSXE_OIR-6-SOFT_STOPSPA: SPA(C1111-2x1GE) stopped in subslot 0/0,
interfaces disabled

Router# hw-module subslot 0/0 reload
Proceed with reload of module? [confirm]
Router#
*Nov  6 17:23:58.176: %IOSXE_OIR-6-SOFT_RELOADSPA: SPA(C1111-2x1GE) reloaded on subslot 0/0
*Nov  6 17:23:58.179: %SPA_OIR-6-OFFLINECARD: SPA (C1111-2x1GE) offline in subslot 0/0
*Nov  6 17:24:09.320: %SPA_OIR-6-ONLINECARD: SPA (C1111-2x1GE) online in subslot 0/0
```

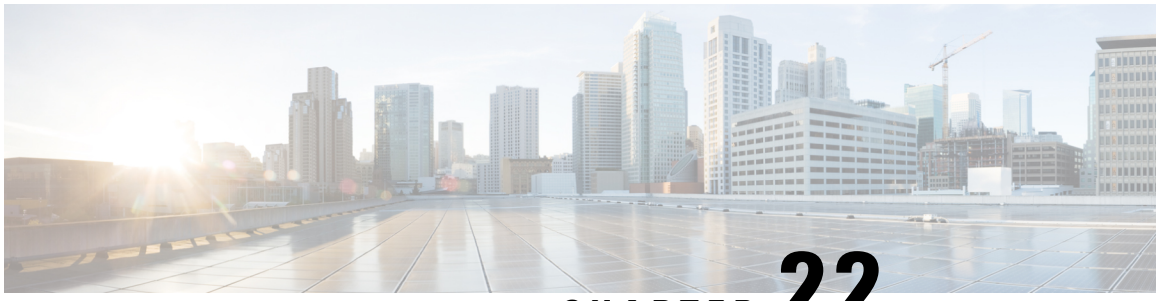
## Manage OIR for Pluggable LTE Modules

To replace a faulty pluggable module, or to swap a module when the system is in operation, use the following CLI:

**hw-module subslot** <*subslot*> **stop**

Wait for the module to power off and then remove the module. Insert another pluggable LTE module into the slot, which is automatically detected, powers-up, and is authenticated.

```
Router# hw-module subslot 0/2 stop
Proceed with stop of module? [confirm]

Router#
*Oct 26 21:50:15.498: %SPA_OIR-6-OFFLINECARD: SPA (C1111-2x1GE) offline in subslot 0/2
*Oct 26 21:50:15.499: %IOSXE_OIR-6-SOFT_STOPSPA: SPA(C1111-2x1GE) stopped in subslot 0/2,
interfaces disabled
```



CHAPTER 22

# Cisco Multimode G.SHDSL EFM-ATM in Cisco ISR 1000 Series Routers

G.SHDSL is the technology that allows devices to send and receive high-speed symmetrical data streams over a single pair of copper wires at rates between 192 kbps and 15.36 Mbps. This document describes how to configure Cisco G.SHDSL Ethernet in the first mile (EFM) and Asynchronous Transfer Mode (ATM). Cisco G.SHDSL EFM/ATM Network Interface Module (NIM) connects Cisco ISR 1000 Series Routers with central office Digital Subscriber Line Access Multiplexers (DSLAMs) and provides up to four lines of G.SHDSL (ITU-T 991.2) connectivity.


- Connecting Cisco G.SHDSL EFM or ATM to the Network, on page 349
- Cisco G.SHDSL EFM or ATM, on page 349
- Configuring Cisco G.SHDSL EFM or ATM in CPE/CO Mode, on page 350
- Configuring NIM-4SHDSL-EA as CPE, on page 350
- Configuring Bonding on CPE, on page 350
- Additional References, on page 351


## Connecting Cisco G.SHDSL EFM or ATM to the Network

For connecting Cisco G.SHDSL EFM/ATM NIMs to a network, see the section about connecting an interface card to a network in Connecting DSL WAN Interface Cards.

## Cisco G.SHDSL EFM or ATM

Cisco G.SHDSL EFM/ATM NIM support up to four pairs of digital subscriber lines (DSL). The DSL pairs are bundled in groups and configured in the Cisco IOS command-line interface (CLI) by using the dsl-group command. Selecting the mode (ATM or EFM) is done by using the mode command.

The NIM supports the following features:

- You can configure up to 4 DSL groups.
- Auto mode is supported only on one DSL group. For instance, DSL group 0.
- In ATM mode, the NIM supports maximum throughput of 22.7Mbps; each line supports 5704kbps.
- In EFM mode, the NIM supports maximum throughput of 61.4Mbps; each line supports maximum of 15Mbps with 128-TCPAM.

- In EFM mode, you can configure a DSL group with any one of the lines in 2-wire non-bonding mode or with multiple lines in bonding mode.
- Depending on the mode (ATM or EFM), the corresponding interface (ATM or EFM) is automatically created.

# Configuring Cisco G.SHDSL EFM or ATM in CPE/CO Mode

You can configure the NIM in termination mode (either in CPE or CO). NIM in CO mode supports only limited features:

# Configuring NIM-4SHDSL-EA as CPE

This section describes the following topics:

The following example shows how to configure Termination CPE.

**Note** The default termination is CPE.

```
Router# conf t
Router(config)# controller shdsl 0/1/0
Router(config-controller)# termination cpe
```

# Configuring Bonding on CPE

To ensure a successful bonding group in the ATM mode configuration, confirm that the central office (CO) network equipment that is connected with the Cisco NIM-4SHDSL-EA is also configured with the same bonding group type.

The following example shows how to configure an ATM M-pair bonding on CPE:

```
Router(config)# controller shdsl 0/1/0 Router(config-controller)# termination cpe
Router(config-controller)# mode atm
Router(config-controller)# dsl-group 0 pairs 0-3 m-pair
Router(config-controller-dsl-group)#
M-pair mode should be either one of these:
o  0-1
o  0-2
o  0-3
o  2-3
The following example shows how to configure an EFM bonding on  CPE:
Router(config)# controller shdsl 0/1/0 Router(config-controller)# termination cpe
Router(config-controller)# mode efm
Router(config-controller)# dsl-group 0 pairs 0 efm-bond
Router(config-controller-dsl-group)#
```

# Verify the Configuration

The following example shows the output of a 2-wire configuration in ATM mode:

```
Router# show controllers shdsL 0/1/0
Controller SHDSL 0/1/0 is UP
Hardware is NIM-4SHDSL-EA, on slot 0,bay 0 Capabilities: EFM: 2-wire, EFM-Bond, Annex A,
B, F & G
ATM: 2-wire, Mpair, Annex A, B, F & G CPE termination
Configured Mode: ATM cdb=0x7F7ED60CF480
...
...
...
ATM Stats:
ATM-TC Tx: data cells: 0, Idle/Unassigned: 0 ATM-TC Rx: data cells: 0, uncorr HEC: 0
ATM-TC Rx: OCD: 0, LCD start: 0, LCD end: 0
Group 1 is not configured Group 2 is not configured
```

# Additional References

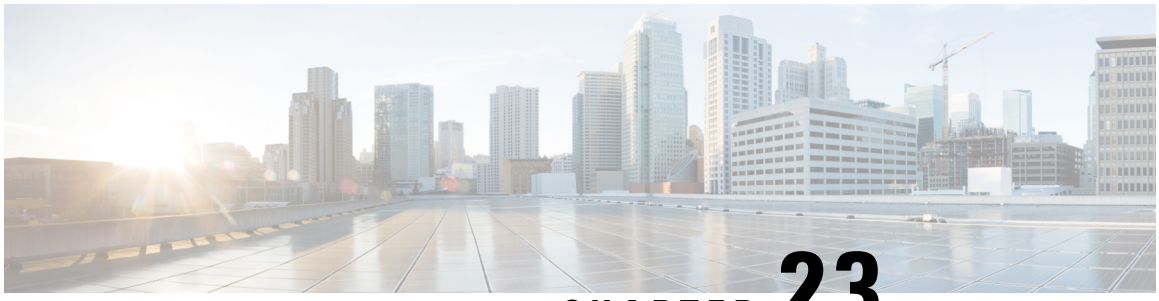
The following sections provide references related to the power efficiency management feature.

### MIBs

| MIBs | MIBs Link |
|---|---|
| CISCO-ENTITY-FRU-CONTROL-MIB | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator at: http://www.cisco.com/go/mibs.<br>Also see the "MIB Specifications Guide for the Cisco 1100 Series Integrated Service Routers". |

# Technical Assistance

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



CHAPTER 23

# Configuring SFP Auto-Failover

This chapter contains the following sections:


- Enabling Auto-Detect, on page 353


# Enabling Auto-Detect

When the media-type is not configured, the Auto-Detect feature is enabled by default. The Auto-Detect feature automatically detects the media that is connected and links up. If both the media are connected, whichever media comes up first is linked. By default, the media-type on FPGE ports is set to auto-select. User can overwrite the media-type configuration to either RJ-45 or SFP using the **media-type rj45/sfp** command under the FPGE interface. The media type configuration also falls back to "Auto-select" mode when the **no media-type** command is configured. You can use the **no media-type** command in interface configuration mode to enable the Auto-Detect feature.

## Configuring Auto-Detect

The Auto-Detect feature is enabled by default on the Front Panel Gige Ports. Auto-Failure is enabled by default when auto-select is enabled. To configure the Auto-Detect, perform these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface gigabitethernet** {**slot** \| **bay** \| **port**}<br>**Example:**<br>`Router(config)# interface gigabitethernet 0/0/0` | Enters interface configuration mode. |
| **Step 3** | **media-type auto-select**<br>**Example:** | Auto-select mode uses whichever connector is attached. The options are: |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-if)# media-type auto-select` | • **rj45**—Uses RJ45 connector.<br>• **sfp**—Uses SFP connector.<br>• **auto-select** |
| **Step 4** | **End**<br>**Example:**<br>`Router(config-if)#end` | Exits configuration mode. |

### Examples

The following example shows the default configuration and the show running configuration does not show any media type when the no media-type is selected.

```
Router(config)# show running interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 71 bytes
!
interface GigabitEthernet0/0/0
 no ip address
 negotiation auto
end
```

# Configuring the Primary and Secondary Media

When the router receives an indication that the primary media is down, the secondary failover media is enabled. After the switchover, the media does not switch back to primary media when the primary media is restored. You need to use either **shut** or **no shut** command or reload the module to switch the media-type back to primary(preferred) media.

To assign the primary or secondary failover media on the GE-SFP port, perform these steps:

### Procedure

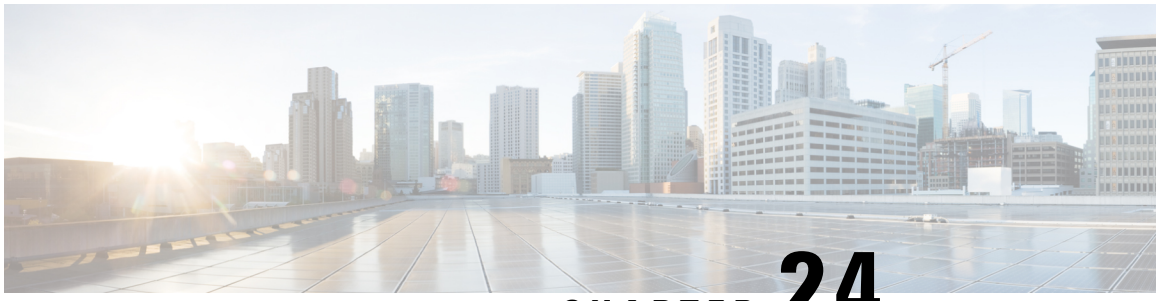
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface gigabitethernet** {**slot** \| **bay** \| **port**}<br>**Example:**<br>`Router(config)# interface gigabitethernet slot/bay/port` | Enters interface configuration mode. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 3** | **media-type rj45 autofailover**<br>**Example:**<br>`Router(config-if)# media-type rj45 autofailover` | Configures the port with rj45 as the primary media for automatic failover. |
| **Step 4** | **End**<br>**Example:**<br>`Router(config-if)#end` | Exits configuration mode. |

### Examples

The following example shows the primary configuration.

```
Router(config)# show running interface gigabitethernet 0/0/0
Building configuration...

Current configuration : 102 bytes
!
interface GigabitEthernet0/0/0
 no ip address
 media-type rj45 auto-failover
 negotiation auto
end
```



CHAPTER 24

# Configuring Cellular IPv6 Address

This chapter contains the following sections:


- Cellular IPv6 Address, on page 357


# Cellular IPv6 Address

IPv6 addresses are represented as a series of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x. Following are two examples of IPv6 addresses:

- 2001:DB8:FFFF:0000:0000:0000:0001
- 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF

IPv6 addresses commonly contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the beginning, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The table below lists compressed IPv6 address formats.

An IPv6 address prefix, in the format ipv6-prefix/prefix-length, can be used to represent bit-wise contiguous blocks of the entire address space. The ipv6-prefix must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons. The prefix length is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). For example, 2001:DB8::1/64 is a valid IPv6 prefix.

# IPv6 Unicast Routing

An IPv6 unicast address is an identifier for a single interface, on a single node. A packet that is sent to a unicast address is delivered to the interface identified by that address.

Cisco 1100 Series supports the following address types:

## Link-Lock Address

A link-local address is an IPv6 unicast address that can be automatically configured on any interface using the link-local prefix FE80::/10 (1111 1110 10) and the interface identifier in the modified EUI-64 format. An link-local address is automatically configured on the cellular interface when an IPv6 address is enabled.

After the data call is established, the link-local address on the celluar interface is updated with the host generated link-local address that consists of the link-local prefix FF80::/10 (1111 1110 10) and the auto-generated

interface identifier from the USB hardware address. The figure below shows the structure of a link-local address.

## Global Address

A global IPv6 unicast address is defined by a global routing prefix, a subnet ID, and an interface ID. The routing prefix is obtained from the PGW. The Interface Identifier is automatically generated from the USB hardware address using the interface identifier in the modified EUI-64 format. The USB hardware address changes after the router reloads.

## Configuring Cellular IPv6 Address

To configure the cellular IPv6 address, perform these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **interface Cellular** {**type** \| **number**}<br>**Example:**<br>`Router(config)# interface cellular 0/1/0` | Specifies the cellular interface. |
| **Step 3** | ip address negotiated<br>**Example:**<br>`Router(config-if)# ipv6 address negotiated` | Specifies that the IP address for a particular interface is dynamically obtained. |
| **Step 4** | load-interval ***seonds***<br>**Example:**<br>`Router(config-if)# load-interval 30` | Specifies the length of time for which data is used to compute load statistics. |
| **Step 5** | dialer in-band<br>**Example:**<br>`Router(config-if)# dialer in-band` | Enables DDR and configures the specified serial interface to use in-band dialing. |
| **Step 6** | dialer idle-timeout ***seonds***<br>**Example:**<br>`Router(config-if)# dialer idle-timeout 0` | Specifies the dialer idle timeout period. |
| **Step 7** | dialer string **string**<br>**Example:**<br>`Router(config-if)# dialer string lte` | Specifies the number or string to dial. |

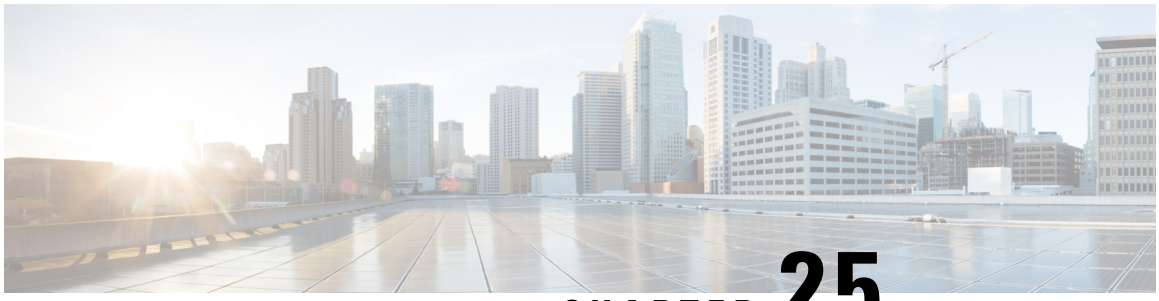
| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | dialer-group**group-number**<br>**Example:**<br>`Router(config-if)# dialer-group 1` | Specifies the number of the dialer access group to which the specific interface belongs. |
| **Step 9** | no peer default ip address<br>**Example:**<br>`Router(config-if)# no peer default ip address` | Removes the default address from your configuration. |
| **Step 10** | ipv6 address autoconfig<br>**Example:**<br>`Router(config-if)# ipv6 address autoconfig` | Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface. |
| **Step 11** | async mode interactive<br>**Example:**<br>`Router(config-if)# async mode interactive` | Please provide the inputs? |
| **Step 12** | routing dynamic<br>**Example:**<br>`Router(config-if)#routing dynamic` | Enables the router to pass routing updates to other routers through an interface. |
| **Step 13** | **dialer-listdialer-groupprotocolprotocol-name** {**permit** \|deny\|**list** \|*access-list-number* \| *access-group* }<br>**Example:**<br>`Router(config)# dialer-list 1 protocol ipv6 permit` | Defines a dial-on-demand routing (DDR) dialer list for dialing by protocol or by a combination of a protocol and a previously defined access list. |
| **Step 14** | **ipv6 route** *ipv6-prefix/prefix-length 128*<br>**Example:**<br>`Router(config)#ipv6 route 2001:1234:1234::3/128 Cellular0/1/0` | |
| **Step 15** | **End**<br>**Example:**<br>`Router(config-if)#end` | Exits to global configuration mode. |

### Examples

The following example shows the Cellular IPv6 configuration .

Configuring Cellular IPv6 Address

```
Router(config)# interface Cellular0/0/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic
!
interface Cellular0/1/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer-group 1
no peer default ip address
ipv6 address autoconfig
async mode interactive
routing dynamic

dialer-list 1 protocol ipv6 permit
ipv6 route 2001:1234:1234::/64 Cellular0/1/0
ipv6 route 2001:4321:4321::5/128 Cellular0/1/1
```



CHAPTER 25

# Dying Gasp Through SNMP, Syslog, and Ethernet OAM

Dying Gasp—One of the following unrecoverable condition occurs:

- System reload
- Interface shutdown
- Power failure—supported on specific platforms

This type of condition is vendor specific. An Ethernet Operations, Administration, and Maintenance (OAM) notification about the condition may be sent immediately.


- Prerequisites for Dying Gasp Support, on page 361
- Restrictions for Dying Gasp Support, on page 361
- Information About Dying Gasp Through SNMP, Syslog and Ethernet OAM, on page 362
- How to Configure Dying Gasp Through SNMP, Syslog and Ethernet OAM, on page 362
- Configuration Examples for Dying Gasp Through SNMP, Syslog and Ethernet OAM, on page 363
- Feature Information for Dying Gasp Support, on page 364


## Prerequisites for Dying Gasp Support

You must enable Ethernet OAM before configuring Simple Network Management Protocol (SNMP) for dying gasp feature. For more information, see Enabling Ethernet OAM on an Interface.

## Restrictions for Dying Gasp Support

- The dying gasp feature is not supported if you remove the power supply unit (PSU) from the system.
- SNMP trap is sent only on power failure or removal of power supply cable on selected platforms.
- The dying gasp support feature cannot be configured using CLI. To configure hosts using SNMP, refer to the SNMP host configuration examples below.
- In the case of system reload or interface shutdown on the Cisco 4000 Series ISRs and Cisco 1100 Series ISRs running Cisco IOS-XE Everest Release 16.6.2, dying gasp packets are sent to peer routers. However, the system state is not captured in the system logs (syslogs) or SNMP traps.

# Information About Dying Gasp Through SNMP, Syslog and Ethernet OAM

## Dying Gasp

One of the OAM features as defined by IEEE 802.3ah is Remote Failure Indication, which helps in detecting faults in Ethernet connectivity that are caused by slowly deteriorating quality. Ethernet OAM provides a mechanism for an OAM entity to convey these failure conditions to its peer via specific flags in the OAM PDU. One of the failure condition method to communicate is Dying Gasp, which indicates that an unrecoverable condition has occurred; for example, when an interface is shut down. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously.

# How to Configure Dying Gasp Through SNMP, Syslog and Ethernet OAM

## Dying Gasp Trap Support for Different SNMP Server Host/Port Configurations

**Note** You can configure up to five different SNMP server host/port configurations.

### Environmental Settings on the Network Management Server

```
setenv SR_TRAP_TEST_PORT=UDP port
setenv SR_UTIL_COMMUNITY=public
setenv SR_UTIL_SNMP_VERSION=v2c
setenv SR_MGR_CONF_DIR=Path to the executable snmpinfo.DAT file
```

The following example shows SNMP trap configuration on the host:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#
Router(config)# snmp-server host 172.31.255.254 vrf Mgmt-intf version 2c public udp-port
6264
Router(config)#
Router(config)# ^Z
Router#
```

After performing a power cycle, the following output is displayed on the router console:

```
Router#
System Bootstrap, Version 16.6(2r), RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1994-2017  by cisco Systems, Inc.
Current image running: Boot ROM0
Last reset cause: LocalSoft
C1111-8PLTELA platform with 4194304 Kbytes of main memory
rommon 1 >

======================================
Dying Gasp Trap Received for the Power failure event:
------------------------------------------------------
  Trap on the Host
++++++++++++++

snmp-server host = 192.0.2.1 (nms1-lnx)  and SR_TRAP_TEST_PORT=6264
/auto/sw/packages/snmpr/15.4.1.9/bin> /auto/sw/packages/snmpr/15.4.1.9/bin/traprcv
Waiting for traps.
Received SNMPv2c Trap:
Community: public
From: 192.0.2.2
snmpTrapOID.0 = ciscoMgmt.305.1.3.5.0.2
ciscoMgmt.305.1.3.6 = Dying Gasp - Shutdown due to power loss
```

# Message Displayed on the Peer Router on Receiving Dying Gasp Notification

```
001689: *May 30 14:16:47.746 IST: %ETHERNET_OAM-6-RFI: The client on interface Gi0/0/0 has
 received a remote failure indication from its remote peer(failure reason = remote client
power failure action = )
```

# Displaying SNMP Configuration for Receiving Dying Gasp Notification

Use the show running-config command to display the SNMP configuration for receiving dying gasp notification:

```
Router# show running-config | i snmp
snmp-server community public RW
snmp-server host 192.0.2.1 vrf Mgmt-intf version 2c public udp-port 6264
Router#
```

# Configuration Examples for Dying Gasp Through SNMP, Syslog and Ethernet OAM

## Example: Configuring SNMP Community Strings on a Router

Setting up the community access string to permit access to the SNMP:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server community public RW
Router(config)# exit
```

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

# Example: Configuring SNMP-Server Host Details on the Router Console

Specifying the recipient of a SNMP notification operation:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host X.X.X.XXX vrf mgmt-intf version 2c public udp-port 9800
Router(config)# exit
```

For more information on command syntax and examples, refer to the Cisco IOS Network Management Command Reference.

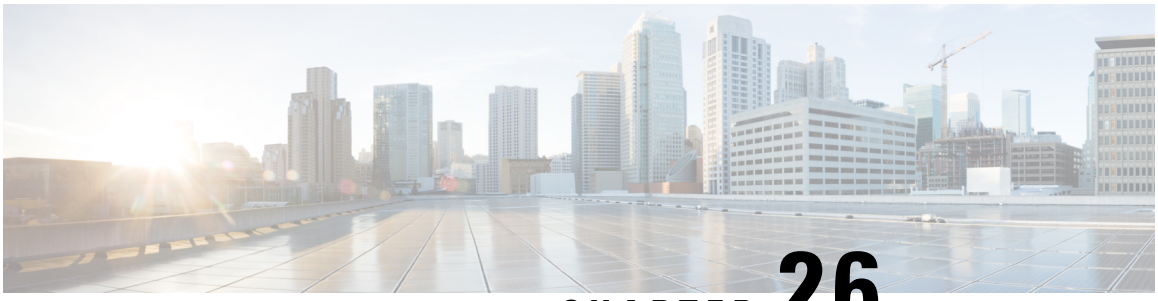
# Feature Information for Dying Gasp Support

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

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

***Table 32: Feature Information for Dying Gasp Support***

| Feature Name | Releases | Feature Information for |
|---|---|---|
| Dying Gasp | Cisco IOS XE Release 16.6.2 | Ethernet OAM provides a mechanism for an OAM entity to convey failure conditions to its peer via specific flags in the OAM PDU. One of the failure condition method to communicate is Dying Gasp, which indicates that an unrecoverable condition has occurred; for example, when an interface is shut down. This type of condition is vendor specific. A notification about the condition may be sent immediately and continuously. |



CHAPTER 26

# Cisco Umbrella Integration

The Cisco Umbrella Integration feature enables cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the Cisco 1000 Series Integrated Services Routers (ISRs). The security administrator configures policies on the Cisco Umbrella portal to either allow or deny traffic towards the fully qualified domain name (FQDN). Cisco 1000 Series ISR acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Cisco Umbrella portal.


- Feature Information for Cisco Umbrella Integration , on page 365
- Prerequisites for Cisco Umbrella Integration, on page 366
- Restrictions for Cisco Umbrella Integration , on page 366
- Cloud-based Security Service Using Cisco Umbrella Integration, on page 367
- Encrypting the DNS Packet, on page 367
- Benefits of Cisco Umbrella Integration, on page 368
- How to Configure Cisco Umbrella Connector, on page 368
- Verify the Cisco Umbrella Connector Configuration, on page 370
- Show Commands, on page 371
- Clear Command, on page 371
- Troubleshoot the Cisco Umbrella Integration, on page 371
- Configuration Examples, on page 372
- Deploy the Cisco Umbrella Integration using Cisco Prime CLI Templates, on page 372
- Additional References for Cisco Umbrella Integration, on page 373


# Feature Information for Cisco Umbrella Integration

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

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

*Table 33: Feature Information for Cisco Umbrella Integration*

| Feature Name | Releases | Feature Information |
|---|---|---|
| Cisco Umbrella Integration | Cisco IOS XE Everest Release 16.6.1 | The Cisco Umbrella Integration feature enables cloud-based security service by inspecting the DNS query that is sent to the DNS server through Cisco 1000 Series Integrated Services Routers (ISR). The security administrator configures policies on the Umbrella cloud to either allow or deny traffic towards the fully qualified domain name (FQDN). |

# Prerequisites for Cisco Umbrella Integration

Before you configure the Cisco Umbrella Integration feature on the Cisco 1000 Series ISR, ensure that the following are met:

- The Cisco 1000 Series ISR has a security K9 license to enable Cisco Umbrella Integration.
- The Cisco 1000 Series ISR runs the Cisco IOS XE Everest 16.6.3 software image or later.
- Cisco Umbrella subscription license is available.
- The DNS traffic passed through the Cisco 1000 Series ISR.
- Communication for device registration to the Cisco Umbrella server is through HTTPS. This requires a root certificate to be installed on the router. To download this certificate directly from a link instead of pasting it in, you can find the certificate here: https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt

# Restrictions for Cisco Umbrella Integration

- If an application or host uses IP address directly instead of DNS to query domain names, policy enforcement is not applied.
- When the client is connected to a web proxy, the DNS query does not pass through the Cisco device. In this case, the connector does not detect any DNS request and the connection to the web server bypasses any policy from the Cisco Umbrella portal.
- When the Cisco Umbrella Integration policy blocks a DNS query, the client is redirected to a Cisco Umbrella block page. HTTPS servers provide these block pages and the IP address range of these block pages is defined by the Cisco Umbrella portal.
- User authentication and identity is not supported in this release.
- The type A, AAAA, and TXT queries are the only records that are redirected. Other types of query bypasses the connector. Cisco Umbrella Connector maintains a list of IP address that is known for malicious traffic. When the Cisco Umbrella roaming client detects the destination of packets to those addresses, it forwards those addresses to Cisco Umbrella cloud for further inspection.
- Only the IPv4 address of the host is conveyed in the EDNS option.

- A maximum of 64 local domains can be configured, and the allowed domain name length is 100 characters.

# Cloud-based Security Service Using Cisco Umbrella Integration

The Cisco Umbrella Integration feature provides cloud-based security service by inspecting the DNS query that is sent to the DNS server through Cisco 1000 Series ISRs. When a host initiates the traffic and sends a DNS query, the Cisco Umbrella Connector in Cisco 1000 Series ISR intercepts and inspects the DNS query. If the DNS query is for a local domain, it forwards the query without changing the DNS packet to the DNS server in the enterprise network. If it is for an external domain, it adds an Extended DNS (EDNS) record to the query and sends it to Cisco Umbrella Resolver. An EDNS record includes the device identifier information, organization ID and client IP. Based on this information, Cisco Umbrella Cloud applies different policies to the DNS query.

# Encrypting the DNS Packet

The DNS packet sent from the Cisco 1000 Series ISR to Cisco Umbrella Integration server must be encrypted if the EDNS information in the packet contains information such as user IDs, internal network IP addresses, and so on. When the DNS response is sent back from the DNS server, Cisco 1000 Series ISR decrypts the packet and forwards it to the host.

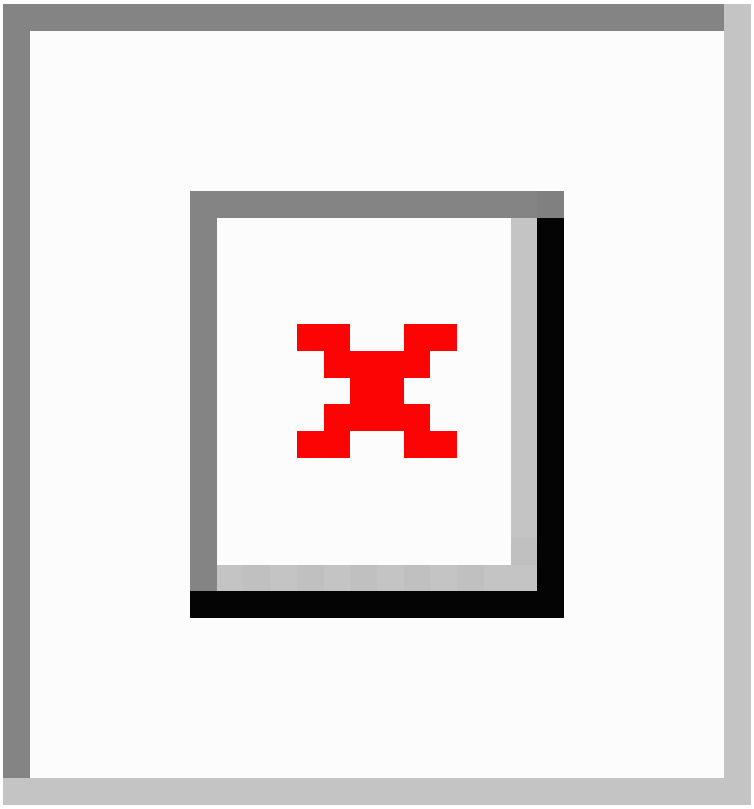
You can encrypt DNS packets only when the DNScrypt feature is enabled on the Cisco 1000 Series ISR.

Cisco 1000 Series ISR uses the following Anycast recursive Cisco Umbrella Integration servers:

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

The Figure 1 describes the Cisco Umbrella Integration topology.

*Figure 4: Cisco Umbrella Integration Topology*



# Benefits of Cisco Umbrella Integration

Cisco Umbrella Integration provides security and policy enforcement at DNS level. It enables the administrator to split the DNS traffic and directly send some of the desired DNS traffic to a specific DNS server (DNS server located within the enterprise network). This helps the administrator to bypass the Cisco Umbrella Integration.

# How to Configure Cisco Umbrella Connector

## Configure the Cisco Umbrella Connector

To configure Cisco Umbrella Connector:

- Get the API token from the Cisco Umbrella registration server.
- Have the root certificate establish the HTTPS connection with the Cisco Umbrella registration server. Import the root certificate of DigiCert given below into the device using the **crypto pki trustpool import terminal** command.

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

- Verify that the PEM import is successful. A message is displayed after importing the certificate.

This is the sample configuration:

```
enable
configure terminal
parameter-map type umbrella global
 token AABBA59A0BDE1485C912AFE472952641001EEECC

exit
```

# Register the Cisco Umbrella Tag

1. Configure the umbrella parameter map as shown in the previous section.
2. Configure **umbrella out** on the WAN interface:

   ```
   interface gigabitEthernet 0/0/0
    umbrella out
   ```

3. Configure **umbrella in** on the LAN interface:

   ```
   interface vlan20
    umbrella in mydevice_tag
   ```

**Note** For Cisco 1000 Series ISRs, the length of the hostname and umbrella tag should not exceed 49 characters.

4. After you configure **umbrella in** with a tag using the **umbrella in mydevice_tag** command, the Cisco 1000 Series ISR registers the tag to the Cisco Umbrella portal.

5. The Cisco 1000 Series ISR initiates the registration process by resolving *api.opendns.com*. You need to have a name server (*ip name-server x.x.x.x*) and domain lookup (*ip domain-lookup*) configured on Cisco 1000 Series ISR to successfully resolve the FQDN.

**Note** You should configure the **umbrella out** command before you configure **opendns in** command. Registration is successful only when the port 443 is in *open* state and allows the traffic to pass through the existing firewall.

# Configure Cisco 1000 Series ISR as a Pass-through Server

You can identify the traffic to be bypassed using domain names. In the Cisco 1000 Series ISR, you can define these domains in the form of regular expressions. If the DNS query that is intercepted by the Cisco 1000 Series ISR matches one of the configured regular expressions, then the query is bypassed to the specified DNS server without redirecting to the Cisco Umbrella cloud. This sample configuration shows how to define a regex parameter-map with a desired domain name and regular expressions:

```
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config)# pattern www.fisco.com
Device(config)# pattern .*engineering.fisco.*

Attach the regex param-map with the umbrella global configuration as shown below:

Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
```

# Verify the Cisco Umbrella Connector Configuration

Verify the Cisco Umbrella Connector configuration using the following commands:

# Show Commands

## Show Commands at FP Layer

## Show Commands at Cisco Packet Processor Layer

## Data Path Show Commands

# Clear Command

### clear platform hardware qfp active feature umbrella datapath stats

The **clear platform hardware qfp active feature umbrella datapath stats** command clears the Umbrella connector statistics in datapath.

```
Device# clear platform hardware qfp active feature umbrella datapath stats
Umbrella Connector Stats Cleared
```

# Troubleshoot the Cisco Umbrella Integration

Troubleshoot issues that are related to enabling Cisco Umbrella Integration feature using these commands:

- **debug umbrella device-registration**
- **debug umbrella config**
- **debug umbrella dnscrypt**

Depending on the OS, run either of these two commands from the client device:

- The **nslookup -type=txt debug.umbrella.com** command from the command prompt of the Windows machine
- The **nslookup -type=txt debug.umbrella.com** command from the terminal window or shell of the Linux machine

```
nslookup -type=txt debug.opendns.com 192.0.2.1
Server:         192.0.2.2
Address:        192.0.2.3

Non-authoritative answer:
debug.opendns.com       text = "server r6.mum1"
debug.opendns.com       text = "device 010A826AAABB6C3D"
debug.opendns.com       text = "organization id 1892929"
debug.opendns.com       text = "remoteip 172.16.0.1"
debug.opendns.com       text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com       text = "originid 119211936"
debug.opendns.com       text = "orgid 1892929"
```

```
debug.opendns.com       text = "orgflags 3"
debug.opendns.com       text = "actype 0"
debug.opendns.com       text = "bundle 365396"
debug.opendns.com       text = "source 172.31.255.254:36914"
debug.opendns.com       text = "dnscrypt enabled (713156774457306E)"
```

When you deploy the Cisco Umbrella Integration feature:

- If you use the multiple EDNS options, DNS packets containing EDNS (DNSSEC) will not pass through the device. For assistance, contact Cisco Technical Support.
- If the WAN interface is down for more than 30 minutes, the device may reload with an exception. Disable the DNScrypt to stop this exception. For assistance, contact Cisco Technical Support .

# Configuration Examples

This example shows how to enable Cisco Umbrella Integration on Cisco 1000 Series ISRs:

# Deploy the Cisco Umbrella Integration using Cisco Prime CLI Templates

You can use the Cisco Prime CLI templates to provision the Cisco Umbrella Integration deployment. The Cisco Prime CLI templates make provisioning Cisco Umbrella Integration deployment simple.

**Note** The Cisco Prime CLI templates is supported only on Cisco Prime version 3.1 or later.

To use the Cisco Prime CLI templates to provision the Cisco Umbrella Integration deployment, perform these steps:

**Procedure**

**Step 1** Download the Cisco Prime templates corresponding to the Cisco IOS XE version running on your system.

**Step 2** Unzip the file, if it is a zipped version.

**Step 3** From Cisco Prime Web UI, choose **Configuration** > **Templates** > **Features and Technologies**, and then select **CLI Templates** (User Defined).

**Step 4** Click **Import**.

**Step 5** Select the folder where you want to import the templates and click Select Templates and choose the templates that you just downloaded.

**Step 6** The following Cisco Umbrella Integration templates are available:

- Umbrella—Use this template to provision Umbrella Connector on Cisco 1000 Series ISR.

- Umbrella Cleanup—Use this template to remove previously configured Umbrella Connector on Cisco 1000 Series ISR.

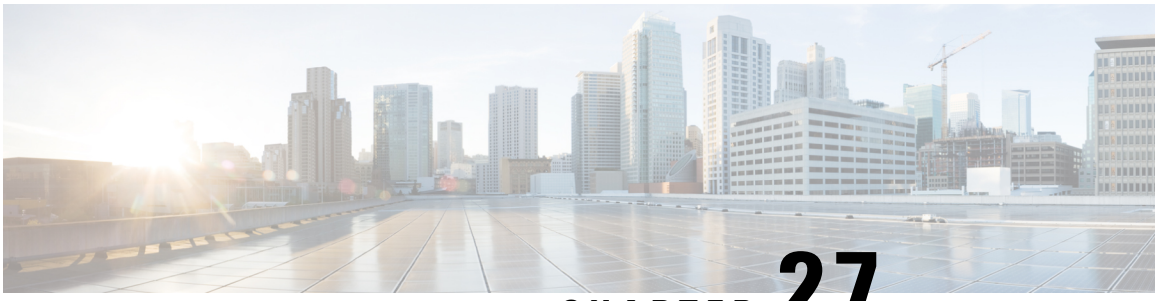
# Additional References for Cisco Umbrella Integration

### Related Documents

| Related Topic | Document Title |
|---|---|
| Security commands | • Cisco IOS Security Command Reference: Commands A to C<br>• Cisco IOS Security Command Reference: Commands D to L<br>• Cisco IOS Security Command Reference: Commands M to R<br>• Cisco IOS Security Command Reference: Commands S to Z |

### Technical Assistance

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



CHAPTER 27

# Wireless Device Overview

Wireless devices (commonly configured as access points ) provide a secure, affordable, and easy-to-use wireless LAN solution that combines mobility and flexibility with the enterprise-class features required by networking professionals. When configured as an access point, the wireless device serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless, uninterrupted access to the network.

With a management system based on Cisco IOS software, wireless devices are Wi-Fi CERTIFIED™, 802.11a-compliant, 802.11b-compliant, 802.11g-compliant, and 802.11n-compliant wireless LAN transceivers.

By adhering to the 802.11ac Wave 2 standard, the Cisco 1100 Series WLAN offers a data rate of up to 867 Mbps on the 5-GHz radio. This exceeds the data rates offered by access points that support the 802.11n standard. It also enables a total aggregate dual-radio data rate of up to 1 Gbps. This provides the necessary foundation for enterprise and service provider networks to stay ahead of the performance expectations and needs of their wireless users.

By leverage Cisco AP 1815i, the Cisco 1100 Series WLAN delivers industry-leading performance for highly secure and reliable wireless connections and provides a robust mobility end-user experience. For more detail specific information with Cisco Access point 1815i is available at: http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1815-series-access-points/datasheet-c78-738243.html.


- Wireless Connectivity for Cisco 1100 Series ISR, on page 375
- Module Managment, on page 376
- Access Points, on page 381
- Deploying Cisco Mobility Express, on page 386
- Configuring Cisco Mobility Express controller, on page 394
- Using internal DHCP server on Cisco Mobility Express , on page 405
- Configuring Cisco Mobility Express for Site Survey, on page 407
- Creating Wireless Networks , on page 411
- Managing Services with Cisco Mobility Express , on page 420
- Managing the Cisco Mobility Express Deployment , on page 425
- Primary AP Failover and Electing a New Primary , on page 427


# Wireless Connectivity for Cisco 1100 Series ISR

This module describes how to configure the WiFi card to the internal switch interface on the Cisco C1100 Integrated Services Routers (ISRs).

The WiFi card is connected to the internal switch interface, the *Wlan-GigabitEthernet* interface. The configuration of this interface is identical to the *GigabitEthernet 0/1/0* interface.

For Cisco 1111-8P Series of ISRs, it is always *Wlan-GigabitEthernet 0/1/8*; and for Cisco 1111-4P, 1116-4P, and 1117-4P Series of ISRs, is always *Wlan-GigabitEthernet 0/1/4*.

```
Router# show run int Wlan-GigabitEthernet 0/1/4
Building configuration...

Current configuration : 43 bytes
!
interface Wlan-GigabitEthernet0/1/4
end

Router#
```

# Module Managment

The router configures, manages, and controls the supported interfaces and modules using the module management facility built in its architecture. This new centralized module management facility provides a common way to control and monitor all the modules in the system regardless of their type and application.

## Slot and Subslots for WLAN

This section contains information on slots and subslots for WLAN. Slots specify the chassis slot number in your router and subslots specify the slot where the service modules are installed.

The table below describes the slot number for the Cisco 1100 Series ISR models.

***Table 34: Slot Numbers for Cisco 1100 Series ISR Models***

| Cisco 1100 Series SKU | WiFi Slot |
|---|---|
| C1111-8PWB | 0/2 |
| C1111-8PLTEEAWB | 0/3 |
| C1113-8PWE | 0/2 |
| C1113-8PMWE | 0/3 |
| C1113-8PLTEEAWE | 0/4 |
| C1111-4PWE | 0/2 |
| C1116-4PLTEEAWE | 0/4 |
| C1116-4PWE | 0/3 |
| C1117-4PLTEEAWE | 0/4 |
| C1117-4PWE | 0/3 |
| C1117-4PMLTEEAWE | 0/4 |

| Cisco 1100 Series SKU | WiFi Slot |
|---|---|
| C1117-4PMWE | 0/3 |

**Note**

- The WiFi slot is 0/2, if there is no 4G-LTE Advanced capability or no DSL configured.
- The WiFi slot is 0/3, if the model has either the 4G-LTE Advanced or VDSL/ADSL funtionalities.
- The WiFi slot is 0/4, if the model has both 4G-LTE Advanced or VDSL/ADSL funtionalities
- There will be no WiFi slot on the non-WiFi SKUs.

# Supported WiFi Cards

The supported WiFi card Product IDs (PIDs) are as follows:

- ISR-AP1100AC-A
- ISR-AP1100AC-B
- ISR-AP1100AC-H
- ISR-AP1100AC-D
- ISR-AP1100AC-E
- ISR-AP1100AC-F
- ISR-AP1100AC-N
- ISR-AP1100AC-R
- ISR-AP1100AC-Q
- ISR-AP1100AC-Z

```
Router#show platform

Chassis type: C1111-8PLTELAWN

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C1111-8PLTELAWN     ok                    00:04:56
 0/0      C1111-2x1GE         ok                    00:02:41
 0/1      C1111-ES-8          ok                    00:02:40
 0/2      C1111-LTE           ok                    00:02:41
 0/3      ISR-AP1100AC-N      ok                    00:02:41
R0        C1111-8PLTELAWN     ok, active            00:04:56
F0        C1111-8PLTELAWN     ok, active            00:04:56
P0        PWR-12V             ok                    00:04:30

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         17100501            16.6(1r)RC3
R0        17100501            16.6(1r)RC3
F0        17100501            16.6(1r)RC3
```

```
Router#
```

# Implementing Modules on Your Router

• Accessing Your Module Through a Console Connection, on page 378

## Accessing Your Module Through a Console Connection

Before you can access the modules, you must connect to the host router through the router console or through Telnet. After you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to your module. Open a session to your module using the **hw-module session** command in privileged EXEC mode on the router.

To establish a connection to the module, connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

Use the following configuration examples to establish a connection:

- The following example shows how to open a session from the router using the **hw-module session** command:

```
Router# hw-module session slot/card
Router# hw-module session 0/2 endpoint 0

Establishing session connect to subslot 0/2
```

- The following example shows how to exit a session from the router, by pressing **Ctrl-A** followed by **Ctrl-Q** on your keyboard:

```
type ^a^q
picocom v1.7

port is        : /dev/ttyS3
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
local echo is  : no
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : sz -vv
receive_cmd is : rz -vv
imap is        :
omap is        :
emap is        : crcrlf,delbs,

Terminal ready
```

## Deactivating a Module

A module can be removed from the router without first being deactivated. However, we recommend that you perform a graceful deactivation (or graceful power down) of the module before removing it. To perform a graceful deactivation, use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode.

**Note** When you are preparing for an OIR of a module, it is not necessary to independently shut down each of the interfaces before deactivating the module. The **hw-module subslot** *slot/subslot* **stop** command in EXEC mode automatically stops traffic on the interfaces and deactivates them along with the module in preparation for OIR. Similarly, you do not have to independently restart any of the interfaces on a module after OIR.

The following example shows how to use the **show facility-alarm status** command to verify if any critical alarm is generated when a module is removed from the system:

```
Device# show facility-alarm status
System Totals  Critical: 5  Major: 1  Minor: 0

Source                  Severity      Description [Index]
------                  --------      -------------------
Power Supply Bay 1      CRITICAL      Power Supply/FAN Module Missing [0]
GigabitEthernet0/0/0    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/1    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/2    CRITICAL      Physical Port Link Down [1]
GigabitEthernet0/0/3    CRITICAL      Physical Port Link Down [1]
xcvr container 0/0/0    INFO          Transceiver Missing [0]
xcvr container 0/0/1    INFO          Transceiver Missing [0]
xcvr container 0/0/2    INFO          Transceiver Missing [0]
xcvr container 0/0/3    INFO          Transceiver Missing [0]
V: 1.0v PCH R0/18       MAJOR         Volt Above Normal [3]
```

**Note** A critical alarm (Active Card Removed OIR Alarm) is generated even if a module is removed after performing graceful deactivation.

## Deactivating Modules and Interfaces in Different Command Modes

You can deactivate a module and its interfaces using the **hw-module subslot** command in one of the following modes:

- If you choose to deactivate your module and its interfaces by executing the **hw-module subslot** *slot/subslot* **shutdown unpowered** command in global configuration mode, you are able to change the configuration in such a way that no matter how many times the router is rebooted, the module does not boot. This command is useful when you need to shut down a module located in a remote location and ensure that it does not boot automatically when the router is rebooted.
- If you choose to use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode, you cause the module to gracefully shut down. The module is rebooted when the **hw-module subslot** *slot/subslot* **start** command is executed.

To deactivate a module and all of its interfaces before removing the module, use one of the following commands in global configuration mode.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **hw-module subslot** *slot/subslot* **shutdown unpowered**<br>**Example:**<br>`Router(config)# hw-module subslot 0/2 shutdown unpowered` | Deactivates the module located in the specified slot and subslot of the router, where:<br>• *slot*—Specifies the chassis slot number where the module is installed.<br>• *subslot*—Specifies the subslot number of the chassis where the module is installed.<br>• **shutdown**—Shuts down the specified module.<br>• **unpowered**—Removes all interfaces on the module from the running configuration and the module is powered off. |
| **Step 2** | **hw-module subslot** *slot/subslot* [**reload** \| **stop** \| **start**]<br>**Example:**<br>`Router# hw-module subslot 0/2 stop` | Deactivates the module in the specified slot and subslot, where:<br>• *slot*—Specifies the chassis slot number where the module is installed.<br>• *subslot*—Specifies the subslot number of the chassis where the module is installed.<br>• **reload**—Stops and restarts the specified module.<br>• **stop**—Removes all interfaces from the module and the module is powered off.<br>• **start**—Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and Input/Output Module daemon (IOMd) processes. |

## Reactivating a Module

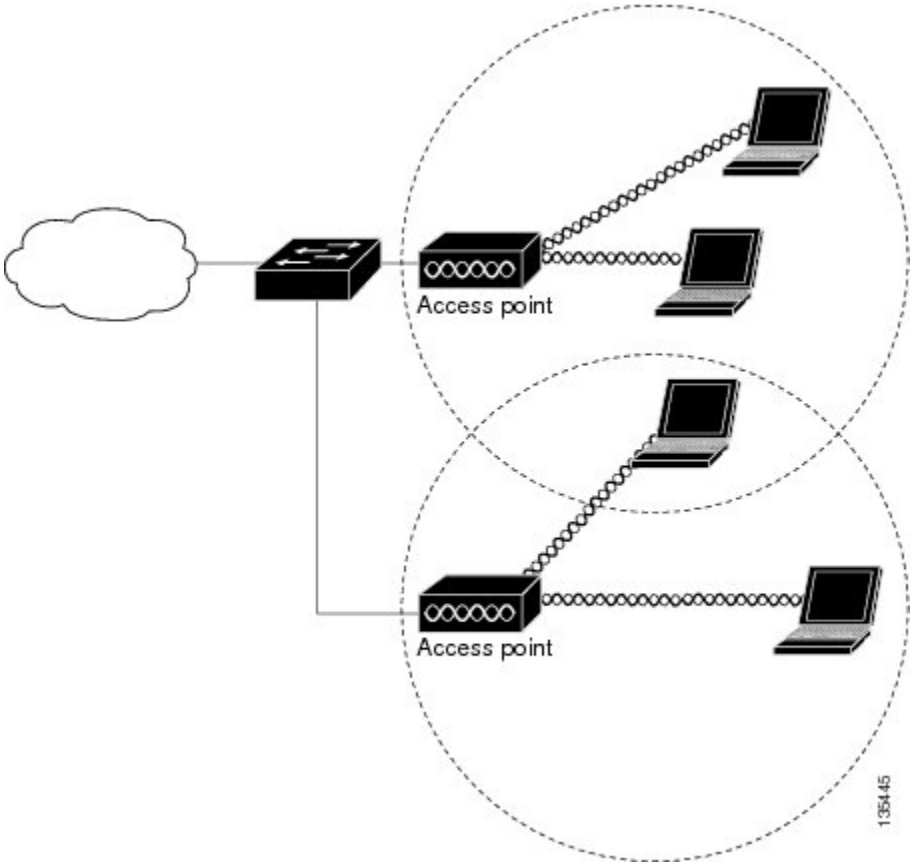
If, after deactivating a module using the **hw-module subslot** *slot/subslot* **stop** command, you want to reactivate it without performing an OIR, use one of the following commands (in privileged EXEC mode):

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

# Access Points

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. The figure below shows access points acting as root units on a wired LAN.

***Figure 5: Access Points as Root Units on a Wired LAN***




In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure below shows an access point in an all-wireless network.

## Configuring and Deploying the Access Point

This section describes how to connect the access point to a wireless LAN controller. The configuration process takes place on the controller. See the Cisco Wireless LAN Controller Configuration Guide for additional information.

# The Controller Discovery Process

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, inter-operable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

**Note** For additional information about the discovery process and CAPWAP, see the Cisco Wireless LAN Controller Software Configuration Guide. This document is available on Cisco.com.

**Note** CAPWAP support is provided in controller software release 8.5 or later. However, your controller must be running the release that supports Cisco 1100 Series access points.

**Note** You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

**Note** Make sure that the controller is set to the current time. If the controller is set to a time that has already passed, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- Layer 3 CAPWAP discovery—Can occur on different subnets than the access point and uses IP addresses and UDP packets.
- Locally stored controller IP address discovery—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the "Performing a Pre-Installation Configuration" section.

- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43" section.
- DNS discovery—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

## Deploying the Access Point on the Wireless Network

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Connect and power up the router. | |
| **Step 2** | Observe the wireless LAN LED (for LED descriptions, see "Checking the Access Point LED" section ). | |
| **Step 3** | Reconfigure the Cisco wireless LAN controller so that it is not the primary controller. | **Note** A primary Cisco wireless LAN controller should be used only for configuring access points and not in a working network. |

# Checking the Wireless LAN LED

**Note** It is expected that there will be small variations in the LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect.

The wireless LAN status LED indicates various conditions which are described in Table.

*Table 35: Wireless LAN LED*

| Message Type | LED State | Message Meanings |
|---|---|---|
| Boot loader status sequence | Blinking Green | DRAM memory test in progress |
| | | DRAM memory test OK |
| | | Board initialization in progress |
| | | Initializing FLASH file system |
| | | FLASH memory test OK |
| | | Initializing Ethernet |
| | | Ethernet OK |
| | | Starting the Cisco AP-OS operating system of the AP |
| | | Initialization successful |
| Association status | Chirping Green | Normal operating condition, but no wireless client associated |
| | Green | Normal operating condition with at least one wireless client association |
| Operating status | Blinking Amber | Software upgrade is in progress. |
| | Cycling through Green, Red, and Amber | Discovery/join process is in progress. |
| | Rapidly cycling through Red, Green, Amber, and off. | Access point location command invoked from controller web interface. |
| | Blinking Red | Ethernet link is not operational. |
| Boot loader warnings | Blinking Amber | Configuration recovery in progress (Mode button pushed for 2 to 3 seconds) |
| | Red | Ethernet failure or image recovery (Mode button pushed for 20 to 30 seconds) |
| | Blinking Green | Image recovery in progress (Mode button released) |

| Message Type | LED State | Message Meanings |
|---|---|---|
| Boot loader errors | Red | DRAM memory test failure |
| | Blinking Red and Amber | FLASH file system failure |
| | Blinking Red and off | One of the following:<br>• Environment variable failure<br>• Bad MAC address<br>• Ethernet failure during image recovery<br>• Boot environment failure<br>• No Cisco image file<br>• Boot failure |

# Miscellaneous Usage and Configuration Guidelines

Using the reset command you can reset the AP to the default factory-shipped configuration.

```
hw-module subslot x/y error-recovery password_reset
```

**Note** Since this is an IOS command, you must run this command on the Cisco 1100 router console, instead of the AP console.

The AP configuration files are cleared. This resets all configuration settings to factory defaults, including passwords, encryption keys, the IP address, and the SSID. However, the regulatory domain provisioning is not reset.

**Note** When you run the **hw-module subslot x/y error-recovery password_reset** command, the AP module automatically reloads to restore the configuration settings and enters the maintenance mode. In the maintenance mode, the AP module is on power on mode. When the module configuration reset is confirmed through the console or web UI, the **hw-module subslot x/x reload force** command reloads the AP and then quits the maintenance mode.

# Important Information for Controller-Based Deployments

Keep these guidelines in mind when you use the Cisco 1100 series access points:

- The access point can only communicate with Cisco wireless LAN controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.

- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

# Deploying Cisco Mobility Express

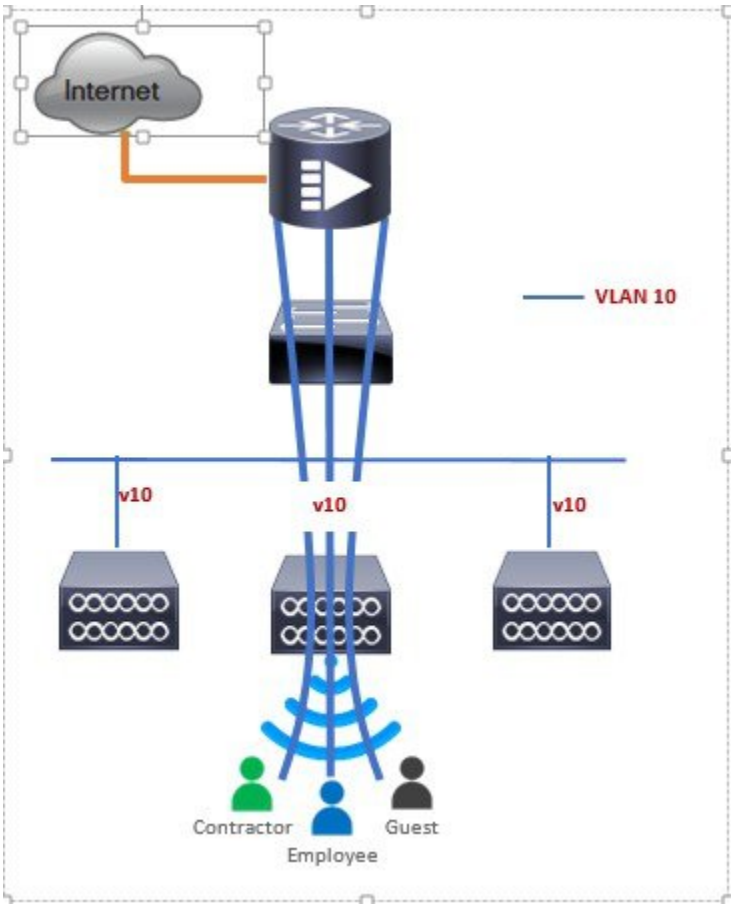
## Pre-Requisites for Deploying Mobility Express Solution

1. It is recommended not to have any other Cisco Wireless LAN Controllers; neither appliance nor virtual in the same network during set up or during daily operation of a Cisco Mobility Express network.
2. Decide on the first Access Point to be configured as a primary Access Point. This Access Point should be capable of supporting the Wireless LAN Controller function.
3. A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address. Starting AireOS® Release 8.4.100.0 or later, one can configure a DHCP server on the primary Access Point as well but this is typically used for Site Survey.

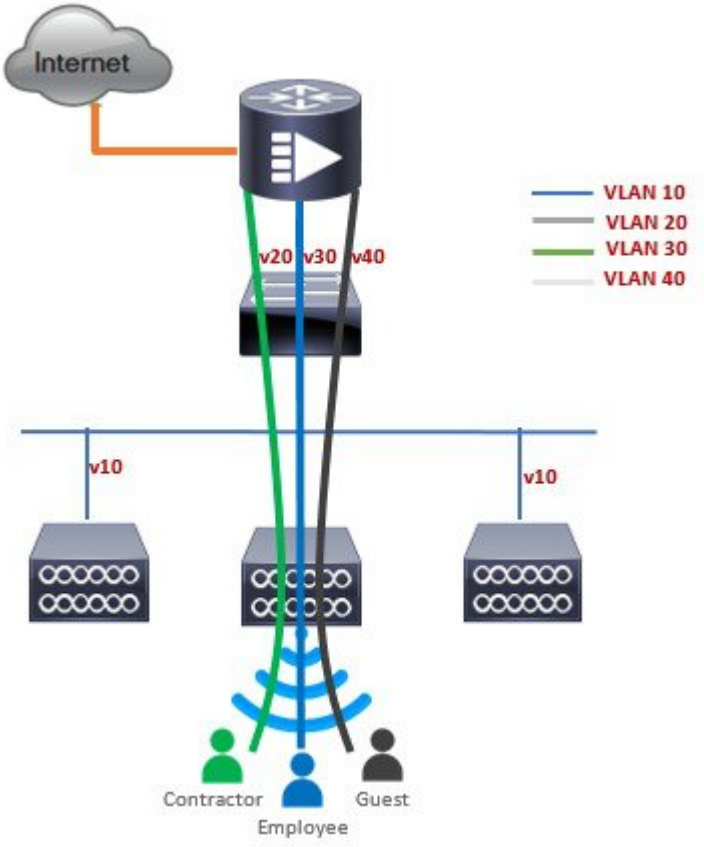
## Connecting Mobility Express Capable Access Point to the Network

Depending on the deployment, Mobility Express capable Access Points can be connected to an access port or a trunk port on the switch.

If Access Points and WLANs are all on the same network, Mobility Express capable Access Points can connect to an access port on the switch as shown below.




On Mobility Express, management traffic is untagged. If Access Points and WLANs are all on different VLANs, Mobility Express capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a deployment with Access Points and WLANs on different VLANs.




```
interface GigabitEthernet1/0/37
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

# Determining image on the Access Point

The Cisco 1100 Series ISR access points can either have CAPWAP image or the Cisco Mobility Express image which is capable of running the virtual Wireless LAN controller function on the Access Point.

To determine the image and capability of an Access Point, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Login to the Access Point CLI using a console and type **AP#show version** and check the full output of show version. The default login credentials are Username:**Cisco** and Password:**Cisco**. | |
| **Step 2** | If **show version** output does not display AP Image Type and AP Configuration parameters | `cisco ISR-AP1100AC-B ARMv7 Processor rev 5 (v7l) with 1016284/594068K bytes of` |

| | Command or Action | Purpose |
|---|---|---|
| | as highlighted below, it means that AP is running the CAPWAP image and a conversion to Cisco Mobility Express is required if you want to run the controller function on the Access Point. To convert from a CAPWAP Access Point to Mobility Express, go to Conversion section. | `memory.`<br>`Processor board ID`<br>`AP Running Image : 192.0.2.1`<br>`Primary Boot Image : 192.0.2.2`<br>`Backup Boot Image : 192.0.2.3`<br>`AP Image type : MOBILITY EXPRESS IMAGE`<br>`AP Configuration : MOBILITY EXPRESS CAPABLE`<br>`1 Gigabit Ethernet interfaces`<br>`2 802.11 Radios`<br>`Radio FW version :`<br>`e1c63a0bb171f78c5800c1478007abc1`<br>`NSS FW version : not available`<br><br>If the show version displays AP Image Type: MOBILITY EXPRESS IMAGE and AP Configuration: NOT MOBILITY EXPRESS CAPABLE , it means that even though the Access Point has the Cisco Mobility Express image, it is configured to run as a CAPWAP Access Point. In this case Access Point will not run the controller function and will not participate in the primary Election process upon failure of the active primary AP.<br><br>`cisco ISR-AP1100AC-B ARMv7 Processor rev 5 (v7l) with 1016284/754820K bytes of memory.`<br>`Processor board ID`<br>`AP Running Image : 192.0.2.1`<br>`Primary Boot Image : 192.0.2.2`<br>`Backup Boot Image : 192.0.2.3`<br>`AP Image type : MOBILITY EXPRESS IMAGE`<br>`AP Configuration : NOT MOBILITY EXPRESS CAPABLE`<br>`1 Gigabit Ethernet interfaces`<br>`2 802.11 Radios`<br>`Radio FW version :`<br>`e1c63a0bb171f78c5800c1478007abc1`<br>`NSS FW version : not available`<br><br>For this AP to run the controller function, AP Configuration has to be changed to MOBILITY EXPRESS CAPABLE . To change the AP Configuration, execute the following command from the AP CLI. AP#ap-type mobility-express tftp://<br><br>Access Point will reboot and after it comes up, it will be capable of running the controller function. You can check the output of show version again to confirm that AP Configuration has changed to MOBILITY EXPRESS CAPABLE .<br><br>If the show version displays AP Image Type: MOBILITY EXPRESS IMAGE and AP Configuration: MOBILITY EXPRESS |

| | Command or Action | Purpose |
|---|---|---|
| | | CAPABLE , it means that the Access Point has the Mobility Express image and is capable of running the controller function. For this scenario, the output of the show version is shown below:<br>`cisco ISR-AP1100AC-B ARMv7 Processor rev 5 (v7l) with 1016284/594068K bytes of memory.`<br>`Processor board ID`<br>`AP Running Image : 192.0.2.1`<br>`Primary Boot Image : 192.0.2.2`<br>`Backup Boot Image : 192.0.2.3`<br>`AP Image type : MOBILITY EXPRESS IMAGE`<br>`AP Configuration : MOBILITY EXPRESS CAPABLE`<br>`1 Gigabit Ethernet interfaces`<br>`2 802.11 Radios`<br>`Radio FW version : e1c63a0bb171f78c5800c1478007abc1`<br>`NSS FW version : not available` |

# Converting Access Point from CAPWAP to Cisco Mobility Express

One can convert an Access Point running CAPWAP to Cisco Mobility Express and vice versa.

Cisco Mobility Express support on 11ac Wave 2 Access Points is introduced in different AireOS releases and it is important to note that before an Access Point can be converted to Mobility Express, it must have the minimum AireOS CAPWAP image which supported Cisco Mobility Express capability for that Access Point. Given below is the minimum OS release for an Access Point which will support conversion from CAPWAP to Cisco Mobility Express.

| Access Point | Minimum AireOS Release with CAPWAP image |
|---|---|
| Cisco 1100 Series | Cisco IOS XE Everest 16.6.2 Release |

**Note** If the CAPWAP image on the Access Point is older than the minimum AireOS release capable of supporting Cisco Mobility Express, Access Point MUST first join a WLC running the minimum AireOS release or higher to upgrade its CAPWAP image. After the CAPWAP image of the AP has been upgraded, conversion of AP from CAPWAP to Mobility Express can be performed.

To perform a conversion on an Access Point running CAPWAP to Mobility Express, follow the procedure below:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Download the conversion image for the Access Point from cisco.com to the TFTP server. It is a tar file. Do not untar the file. The following | |

| | Command or Action | Purpose |
|---|---|---|
| | table lists the Cisco Mobility Express software for Cisco Wireless Release 8.4.100.0. | |
| **Step 2** | Login to the Access Point | |
| **Step 3** | Execute AP#show version on the Access Point CLI. From the show version output, you can determine the AP Image type and AP Configuration and can then proceed with the conversion | Case 1: If the AP Image type is MOBILITY EXPRESS IMAGE and AP configuration is NOT MOBILITY EXPRESS CAPABLE, enter the command below to change the AP Configuration to MOBILITY EXPRESS CAPABLE .<br>`AP#ap-type mobility-express`<br>Example:<br>`cisco ISR-AP1100AC-E ARMv7 Processor rev 5 (v7l) with 1016284/840700K bytes of memory.`<br>`Processor board ID`<br>`AP Running Image : 192.0.2.1`<br>`Primary Boot Image : 192.0.2.2`<br>`Backup Boot Image : 192.0.2.3`<br>`1 Gigabit Ethernet interfaces`<br>`2 802.11 Radios`<br>`Radio FW version : e1c63a0bb171f78c5800c1478007abc1`<br>`NSS FW version : not available`<br>`Router#ap-type mobility-express`<br>`Changing AP Type to Mobility Express`<br>`Writing reload timestamp (Wed May 24 17:17:53 UTC 2017) to disk`<br>`Router#[05/24/2017 17:17:54.4699] UBIFS: un-mount UBI device 0, volume 3`<br>`[05/24/2017 17:17:54.5199] UBIFS: background thread "ubifs_bgt0_3" stops`<br>`[05/24/2017 17:17:56.6099] reboot: Restart`<br>**Note** Since the Access Point has AP Image type: MOBILITY EXPRESS IMAGE, a new image will not be downloaded. After the command is executed, the Access Point will reboot and after it comes up, the AP Configuration will be changed to MOBILITY EXPRESS CAPABLE.<br>Case 2 : If the AP Image type and AP Configuration are not available, it means that the AP is running CAPWAP image. To do the conversion, execute the command below: |

| | Command or Action | Purpose |
|---|---|---|
| | | `Router#ap-type mobility-express tftp://<TFTP Server IP>/<path to tar file>`<br>Example:<br>`Router#ap-type mobility-express tftp://10.74.5.99/8.4CCO/ap1g5`<br>`Starting the ME image download...`<br>`It may take a few minutes to finish download.`<br>`If it is longer, please abort command, check network connection and try again`<br>`##########################################################`<br>`100.0%`<br>`Image transfer complete.`<br>`Image downloaded, writing to flash...`<br>`do CHECK_ME, part1 is active part`<br>`Image signing verify success.`<br>`upgrade.sh: btldr rel is 33 vs 33, does not need update`<br>`upgrade.sh: part to upgrade is part2`<br>`upgrade.sh: activate part2, set BOOT to part2`<br>`upgrade.sh: AP primary version: 8.4.100.0`<br>`Archive done.`<br>`[*10/11/2017 23:05:22.7599] AP Type changed: CAPWAP to ME. AP Mode changed to flexconnect. AP Rebooting...`<br>`[*10/11/2017 23:05:22.7699] AP Rebooting: Reset Request from Controller(AP Type Changed from CAPWAP to ME)`<br>`Writing reload timestamp (Wed Oct 11 23:05:22 UTC 2017) to disk`<br>`M-P2B#[10/11/2017 23:05:23.9699] UBIFS: un-mount UBI device 0, volume 3`<br>`[10/11/2017 23:05:24.0199] UBIFS: background thread "ubifs_bgt0_3" stops`<br>`The system is going down NOW!`<br>`Sent SIGKILL to all processes.1099]`<br>`Requesting system reboot99]`<br>`[10/11/2017 23:05:26.1099] reboot: Restarting`<br>**Note** After the image download is complete, it will be written to the flash followed by a reboot. After the AP comes up, AP Image type will be MOBILITY EXPRESS IMAGE and AP Configuration will MOBILITY EXPRESS CAPABLE . |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | If this is the first Access Point in the network, it will start the controller function and will broadcast the CiscoAirProvison SSID. | |

# Converting Access Point from Cisco Mobility Express to CAPWAP

There are typically two reasons why one would want to convert an Access Point running Mobility Express image to CAPWAP. There are as follows:

1. You want to keep the Access Point in a Mobility Express deployment but do not want the Access point to participate in the primary election process upon a failover of the primary AP.
2. You want to migrate one or more Access Points with Mobility Express to an appliance or vWLC based deployment.

1. If your reason to convert to CAPWAP is 1 above, follow the procedure below:
   a. Login to the Access Point CLI either through console or ssh and go to exec mode. If you are trying to convert the primary AP to CAPWAP, connecting a console will lead you to the controller CLI. To get to the AP CLI, type apciscochell at the controller prompt and login to the Access Point shell.
   b. Execute ap#ap-type capwap CLI. This will change the AP Configuration to NOT MOBILITY EXPRESS and the Access Point will no longer participate in the primary election process.

2. If your reason to convert to CAPWAP is 2 above, follow the procedure below:
   a. Login to the Access Point CLI either via console or ssh and go to exec mode.
   b. Execute the following CLI.

```
(Cisco Controller) >config ap unifiedmode <switch_name> <switch_ip_address>

<switch_name> and <switch_ip_address> is the name and IP address respectively of the
 WLC to which the APs need to be migrate.
```

**Note** The above command converts all connected Access Points with AP Configuration: MOBILITY EXPRESS CAPABLE to AP Configuration: NOT MOBILITY EXPRESS CAPABLE . When this command is issued, the APs are reloaded, and they come back up and look for the controller (switch_ip_address) to join.

# Configuring Cisco Mobility Express controller

## CLI Setup Wizard

To use the Setup Wizard from CLI, you must connect to the console port of the Access Point. The default parameters for the console ports are 9600 baud, eight data bits, one stop bit, and no parity. The console ports do not support hardware flow control.

After connecting to the console port on the Access Point, power up the Access Point. After a few minutes, Access Point will start the Controller.

To configure the Mobility Express controller, follow the steps as shown in the example below:

```
System Name [Cisco_2c:3a:40] (31 characters max): me-wlc
Enter Country Code list (enter 'help' for a list of countries) [US]:

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Note! Default NTP servers will be used

Management Interface IP Address: 192.0.2.1
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.0.2.2
Cleaning up Provisioning SSID
Create Management DHCP Scope? [yes][NO]: yes
DHCP Network : 192.0.2.1
DHCP Netmask : 255.255.255.0
Router IP: 40.40.40.1
Start DHCP IP address: 192.0.2.3
Stop DHCP IP address: 192.0.2.4
DomainName :
DNS Server : [OPENDNS][user DNS]
Create Employee Network? [YES][no]: YES
Employee Network Name (SSID)?: WestAutoBody-Employee
Employee VLAN Identifier? [MGMT][1-4095]: MGMT
Employee Network Security? [PSK][enterprise]: PSK
Employee PSK Passphrase (8-38 characters)?: Cisco123
Re-enter Employee PSK Passphrase: Cisco123
Create Guest Network? [yes][NO]: YES
Guest Network Name (SSID)?: WestAutoBody-Guest
Guest VLAN Identifier? [EMPLOYEE][1-4095]: EMPLOYEE
Guest Network Security? [WEB-CONSENT][psk]: WEB-CONSENT
Create Guest DHCP Scope? [yes][NO]: NO
Enable RF Parameter Optimization? [YES][no]: YES
Client Density [TYPICAL][Low][High]: TYPICAL
Traffic with Voice [NO][Yes]: Yes

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
Cleaning up Provisioning SSID
```

**Note** The Access Point will reboot and after it comes back up, login to the Mobility Express controller WebUI from the browser using https://<mangement_ip_address> Cisco Mobility Express controller uses a self-signed certificate for HTTPS. Therefore, all browsers display a warning message and asks whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the risk and proceed to access the Mobility Express Wireless LAN Controller login page.

# Over-the-Air Setup Wizard

Over-the-air is a simple and easy way to configure Mobility Express out of the box. Over-the-Air provisioning can be done using a WiFi enabled device or the Cisco Wireless app which can be downloaded from App Store for iOS devices and Play Store for Android Devices. The Cisco Wireless app provides a minimum set of configurable options to deploy Mobility Express in just a few minutes.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | When the LED on the Access Point chirps green, connect a WiFi enabled laptop to the CiscoAirProvision SSID. The default password is password. The laptop will get an IP address from subnet 192.168.1.0/24. | **Note** CiscoAirProvision SSID is broadcast at 2.4GHz. |
| **Step 2** | Open a web browser and browse to http://mobilityexpress.cisco. This will redirect to configuration wizard and the admin account page will appear. | |
| **Step 3** | Create an admin account on the controller by specifying the following parameters and then click on the Start button. | • Enter the admin username. Maximum up to 24 ASCII characters.<br>• Enter the password. Maximum up to 24 ASCII characters. When specifying a password, ensure that:<br>  • The password must contain characters from at least three of the following classes – lowercase letters, uppercase letters, digits, special characters.<br>  • No character in the password can be repeated more than three times consecutively.<br>  • The new password must not be the same as the associated username and the username reversed.<br>  • The password must not be cisco, ocsic, or any variants obtained by changing the capitalization of letters of the word Cisco. In addition, you cannot substitute 1, I, or ! for i, 0 for o, or $ for s. |
| **Step 4** | In the Set up Your Controller section, configure the following: | • Enter the System Name<br>• Select the Country from the drop-down list |

| | Command or Action | Purpose |
|---|---|---|
| | | • Date and Time should be auto-filled but one can manually configure it as well<br>• Select the Timezone from the drop-down list<br>• Enter the IP address of NTP Server if there is one available. If left blank, NTP Pools will be automatically configured<br>• Enter the Management IP Address of the controller<br>• Enter the Subnet Mask<br>• Enter the Default Gateway |
| **Step 5** | Disable Enable DHCP Server(Management Network) if an external DHCP server is being used. If internal DHCP server on the Mobility Express controller has to be used, specify the DHCP server related information. | |
| **Step 6** | Click Next. | |
| **Step 7** | In the Create Your Wireless Network, under Employee Network, configure the following: | • Enter the Network Name<br>• Select Security as WPA2 Personal or WPA2 Enterprise from the drop-down list<br>• If WPA2 Personal is selected, enter the Passphrase |
| **Step 8** | One can also enable RF Parameter Optimization and configure the following: | • Move the Client Density slider as needed<br>• From the Traffic Type, select Data or Data and Voice |
| **Step 9** | Click Next. | |

| | Command or Action | Purpose | |
|---|---|---|---|
| **Step 10** | Confirm the settings on the page and click on the Apply button. The Access Point will reboot and after it comes up, it will run the controller. | **Note** | The Access Point will reboot and after it comes back up, login to the Mobility Express controller WebUI from the browser using https:<management_ip_address>. Cisco Mobility Express controller uses a self-signed certificate for HTTPS. Therefore, all browsers display a warning message and asks whether you wish to proceed with an exception or not when the certificate is presented to the browser. Accept the risk and proceed to access the Mobility Express Wireless LAN Controller login page. |

# Network Plug and Play

## Introduction

The Cisco Network Plug and Play solution provides a simple, secure, unified, and integrated offering for enterprise network customers to ease new site rollouts for provisioning Cisco Mobility Express. The solution allows use of Cloud Redirection service, on-prem, or combination which provide a unified approach to provision enterprise networks comprised of Cisco Mobility Express, Cisco routers, switches, with a near zero touch deployment experience.

You can use the Cisco Network Plug and Play application to pre-provision the site and add Cisco Mobility Express capable access points to the site. This includes entering access point information and uploading a controller configuration file for virtual controller which will run on Mobility Express capable access points.

When an installer installs and powers up the Cisco Mobility Express capable access points, it auto-discovers the Cisco APIC-EM controller by using the DHCP, DNS or cloud redirection service. After the auto-discovery process is complete, the AP downloads the controller configuration file from local PnP server, or communicates with the cloud redirection service for direction to target PnP server.

## Pre-Requisites

- APIC-EM Release 1.4 with Cisco Network Plug and Play, virtually hosted in a Cisco UCS or equivalent server.
- Access Points–Cisco 802.11ac Wave 2 access points running Cisco Mobility Express software.
- Controller Configuration–Cisco Mobility Express controller configuration file to be uploaded on Network PnP.

## APIC-EM Discovery Options

1. DHCP server configured with option 43 to allow Cisco Mobility Express capable access points to auto-discover the APIC-EM controller (option 43 is not required if only testing cloud redirection). DHCP option 43 consists of a string value that is a configured DHCP server: option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"

**Note** 192.168.1.123 is the IP address of the APCI-EM Server

2. On–prem PnP server can be added to DNS using ‘pnpserver.yourlocal.domain’ If DHCP discovery fails to get the IP address of the APIC-EM controller, for example, because option 43 is not configured, the Cisco Plug and Play Agent falls back on a DNS lookup method. Based on the network domain name returned by the DHCP server, it constructs a fully qualified domain name (FQDN) for the APIC-EM controller, using the preset hostname pnpserver. For example, if the DHCP server returns the domain name " customer.com ", the Cisco Plug and Play IOS Agent constructs the FQDN "pnpserver.customer.com ". It then uses the local name server to resolve the IP address for this FQDN

Cloud redirection service requires a connection to the internet, and valid DNS server that can resolve ‘devicehelper.cisco.com’. The cloud redirection service redirect Cisco Mobility Express Access Point to APIC-EM.

## Configuring APIC-EM / Network PnP Server

### Site Pre-Provisioning Workflow

Cisco Network Plug and Play allows you to pre-provision and plan for new sites. When you create a new site, Cisco Network Plug and Play enables you to pre-provision Cisco Mobility Express access point(s) controller, configuration file, product ID, and product serial # for selected Access Points. This simplifies and accelerates the time that it takes to get a site fully functional.

To pre-provision a site on your network, perform these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Importing Cisco Mobility Express controller configuratio | |
| **Step 2** | Creating a Project | |
| **Step 3** | Adding Cisco Mobility Express capable Access Point to the Project and associating the controller config. | |

## Importing Cisco Mobility Express Configuration File to Network PnP

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Login to APIC-EM controller and navigate to Network Plug and Play > Configurations | |
| **Step 2** | Click on Upload to upload the controller configuration. | |
| **Step 3** | Select a controller configuration file from your local machine. | |

## Creating a Project

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Network Plug and Play > Projects. | |
| **Step 2** | Enter the name for the Project and click on the Add button. | |
| **Step 3** | Click on the Create button to create the Project. | |
| **Step 4** | | |

## Adding Cisco Mobility Express Capable Access Point to the Project and Associating the Controller Configuration

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Network Plug and Play > Projects. | |
| **Step 2** | Click on Add button under Project Devices. | |
| **Step 3** | In the Add Device window, enter the following: | • Device Name–Enter the device name; unique for each site<br>• Product ID–Select the Access Point device ID from the drop-down list<br>• Serial Number–Enter the Serial Number of the Mobility Express Access Point<br>• Config–You can either upload a new configuration or select the configuration file which was added earlier |
| **Step 4** | Click the Add button. | |

# APIC-EM Network Plug and Play Deployment Options with Cisco Mobility Express

There are two deployment options supported for deploying Cisco Mobility Express with Network Plug and Play.

## APIC-EM controller in Private Cloud

In this deployment option, there will be an On-Prem APIC-EM controller which can be discovered by Cisco Mobility Express Access Points using option 43 or DNS discovery.

***Figure 6: APIC-EM controller in Private Cloud flow***

Option 43 points to APIC-EM controller IP address. To configure DHCP scope with Option 43, it is important follow the format as shown below. In the example below, 192.168.1.123 is the IP address of APIC-EM controller .

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 43 ascii "5A1N;B2;K4;I192.168.1.123;J80"
```

To discover APIC-EM controller using the DNS discovery options, configure the DNS server and domain name on the DHCP scope.

```
ip dhcp pool pnp_device_pool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
domain-name cisco.com
dns-server 172.20.229.8
```

## Cloud Plug and Play Connect Redirect to APIC-EM Controller

Cloud re-direction service uses Cisco public hosted cloud to re-direct Cisco Mobility Express capable access points to APIC-EM controller. The minimal requirement is that the Mobility Express Access Points network have DHCP and DNS, and connectivity reachable to Cisco public cloud. There is no need to configure Option 43 on DHCP scope with this deployment option. A simple test would be to obtain DHCP address and ping 'devicehelper.cisco.com' from where the Mobility Express AP will be deployed.

***Figure 7: Cloud Plug and Play Device Redirect to APIC-EM controller flow***

## Cloud Plug and Play Device Redirect Provisioning Workflow

This section describes the steps to redirect Cisco Mobility Express Access Points to APIC-EM controller using Cloud Plug and Play Connect service.

To configure cloud Plug and Play connect redirect service, perform the following steps:

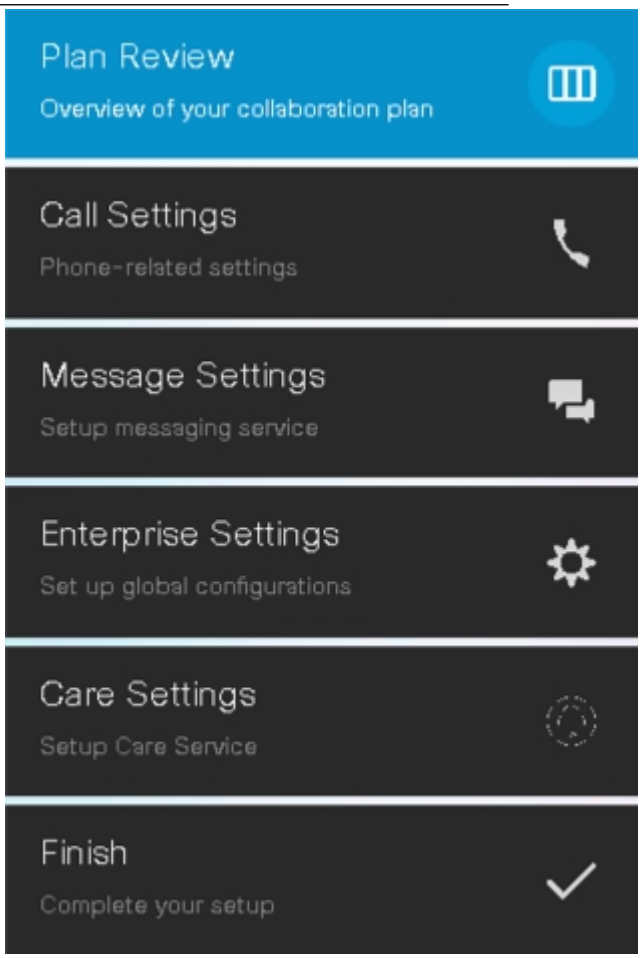
1. Obtain a Smart Account
2. Create APIC-EM Controller Profile

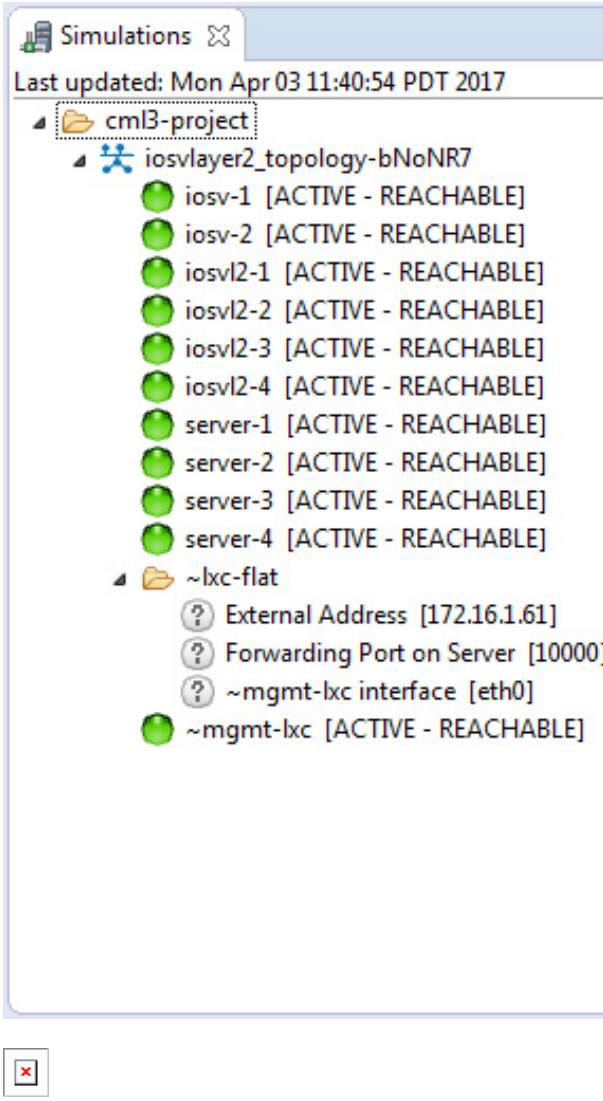
3. Adding Mobility Express capable Access Point to the Devices list
4. Associate Mobility Express capable Access Point to APIC-EM Controller profile

## Obtain a Smart Account

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Go to http://software.cisco.com | |
| **Step 2** | Request a Smart Account or Log In (existing Smart Account holders). | |
| **Step 3** | Click on Controller Profiles. Select a Virtual Account. If you do have one, create a Virtual Account first. | |
| **Step 4** | Click on the Add Profile to create a new controller profile. | |
| **Step 5** | Select Controller Type as PNP Server from the drop-down list and click on Next. | |
| **Step 6** | Enter the following and click Next. | • Profile Name<br>• Description<br>• Select IPv4 or IPv6, HTTP or HTTPS and enter the IP address if the PNP Server<br>**Note** If you select HTTPS, then you would have import a SSL certificate. Also, optionally one can enter information of the secondary controller. |

| | Command or Action | Purpose |
|---|---|---|
| | |  |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | Review the entries and click on Submit button to add the Controller Profile and finally click Done. |  |



## Create APIC-EM Controller Profile

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Go to http://software.cisco.com and login | |
| **Step 2** | Navigate to Provisioning > Plug and Play Connect | |
| **Step 3** | Click on Controller Profiles. Select a Virtual Account. If you do have one, create a Virtual Account first. | |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Click the Add Profile to create a new controller profile. | |
| **Step 5** | Select Controller Type as PNP Server from the drop-down list and click on Next. . | |
| **Step 6** | Enter the following and click Next. | • Profile Name<br>• Description<br>• Select IPv4 or IPv6, HTTP or HTTPS and enter the IP address if the PNP Server<br>**Note** If you select HTTPS, then you would have import a SSL certificate. Also, optionally one can enter information of the secondary controller. |
| **Step 7** | Review the entries and click on Submit button to add the Controller Profile and finally click Done. | |

*Adding Cisco Mobility Express capable Access Point to the Devices List*

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Provisioning > Plug and Play Connect. Click on Devices. | |
| **Step 2** | Click on Devices. Select a Virtual Account. If you do have one, create a Virtual Account first. | |
| **Step 3** | Click on Add Devices button to add a new device (Mobility Express Access Point). | |
| **Step 4** | Import a csv file with the Device info or select Enter Device info manually. Click Next. | |
| **Step 5** | Click on Identify Device button. The Identify Device window will pop up. Enter Serial Number, select Base PID, and Controller Profile(created earlier). Click on the Save button followed by Next button. | |
| **Step 6** | Review the entries and click on Submit button to add the Device. Finally, click Done. | |
| **Step 7** | Verify that the Device has been added and the status is Pending (Redirection). | |

## Connecting Cisco Mobility Access Points

To bring up a new Mobility Express site, make sure that Plug and Play service has been configured with Mobility Express Access Points with related controller configuration. If APIC-EM controller in Private Cloud deployment option is used, Option 43 or DNS discovery on DHCP scope must be configured. If Cloud Plug and Play Connect redirect to APIC-EM controller deployment option is used, make sure all the related configuration on Cloud Plug and Play Connect has also been done for successful redirect to APIC-EM controller.

Now, it is time to connect the Mobility Express Access Points at the site. One may connect one or more Access Points at a site. It is important to note that if multiple Mobility Express Access Points are connected at a site, primary Election will happen first and only after primary Access Point has been elected, it will initiate communication with the Network Plug and Play service and download the controller configuration file regardless of the deployment option. The other Access Points will not initiate communicate with the Network Plug and Play service. After the controller configuration file has been downloaded on the Access Point, it will reboot and after it comes up, it will run the controller. The rest of the Access Points at the site will join this primary Access Point as Subordinate Access Points.

# Using internal DHCP server on Cisco Mobility Express

## Creating a DHCP Scope

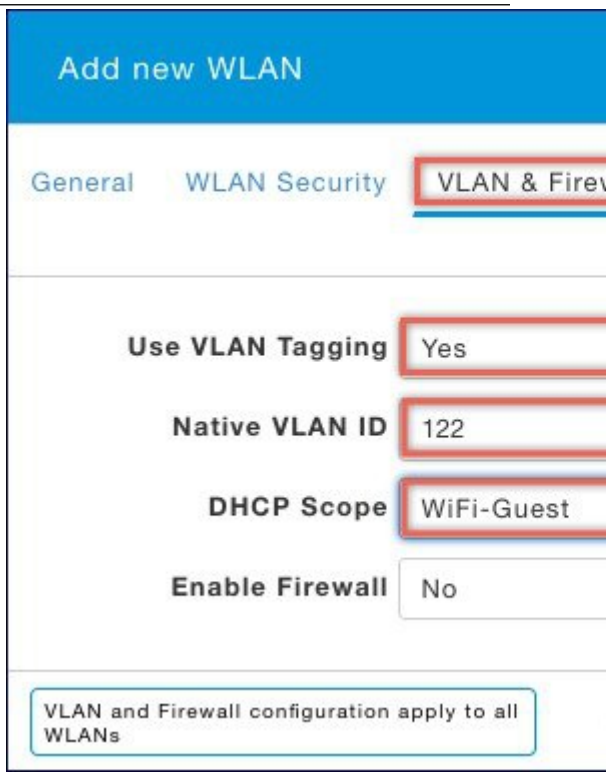
Internal DHCP server can be enabled and DHCP scope created during Day 0 from Setup Wizard as well as in Day 1 using the controller WebUI. Typically, one would create DHCP scopes in Day 1 if they want to associate the scopes with WLANs.

To create a scope and associate it to a WLAN using the controller WebUI, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > DHCP Server > Add new Pool . The Add DHCP Pool window will pop up. | |
| **Step 2** | On the Add DHCP Pool window. Enter the following fields: | • Enter the Pool Name for the WLAN<br>• Enable the Pool Status<br>• Enter the VLAN ID for the WLAN<br>• Enter the Lease Period for the DHCP clients. Default is 1 Day<br>• Enter the Network/Mask<br>• Enter the Start IP for the DHCP pool<br>• Enter the End IP for the DHCP pool<br>• Enter the Gateway IP for the DHCP pool |

| | Command or Action | Purpose |
|---|---|---|
| | | • Enter the Domain Name (Optional) for the DHCP pool<br>• For Name Servers, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated |
| **Step 3** | Click Apply. | |
| **Step 4** | After creating the scope, it is time to assign the VLAN mapped to the DHCP scope to the WLAN. To assign a VLAN to WLAN, navigate to Wireless Settings > WLANs . | |
| **Step 5** | If the WLAN does not exist, create a WLAN or if one does exist, edit the existing WLAN and click on the VLAN and Firewall tab. | |
| **Step 6** | On the VLAN and Firewall tab, configure the following: | • Select Yes for Use VLAN Tagging<br>• Enter the Native VLAN ID<br>• Select the DHCP Scope which was created previously for the WLAN. VLAN ID should be automatically populated after the DHCP scope is selected |

| | Command or Action | Purpose |
|---|---|---|
| | |  |
| **Step 7** | Click Apply. | |

# Configuring Cisco Mobility Express for Site Survey

Cisco 802.11ac Wave 2 access points are capable of running Cisco Mobility Express which a virtual wireless controller function embedded on an Access Point.

Cisco Mobility Express access point running the wireless controller function will also provide wireless connectivity to the clients. It also supports internal DHCP server which enables Access Point to be used for Site Survey.

## Introduction

Cisco 802.11ac Wave 2 access points are capable of running Cisco Mobility Express which a virtual wireless controller function embedded on an Access Point.

Cisco Mobility Express access point running the wireless controller function will also provide wireless connectivity to the clients. It also supports internal DHCP server which enables Access Point to be used for Site Survey.

# Configuring Mobility Express for Site Survey Using CLI

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Connect to the console of the Access Point. | |
| **Step 2** | Power up the Access Point using a power adapter or battery pack. | |
| **Step 3** | Wait for the Access Point to boot up completely such that it is running the Wireless Controller and is waiting to be configured. | |
| **Step 4** | Configure the Wireless Controller using the CLI Setup Wizard: | **Note** For Site Survey, a DHCP server is required and is supported on Cisco Mobility Express. DHCP Server configuration highlighted below is mandatory if you want to enable DHCP server on Cisco Mobility Express.<br><br>`Would you like to terminate autoinstall? [yes]:yes`<br>`Enter Administrative User Name (24 characters max):admin`<br>`Enter Administrative Password (3 to 24 characters max):Cisco123`<br>`Re-enter Administrative Password: Cisco123`<br>`System Name:[Cisco_3a:d2:b4] (31 characters max):me-wlc`<br>`Enter Country Code list(enter 'help' for a list of countries)[US]:US`<br>`Configure a NTP server now?[YES][no]:no`<br>`Configure the system time now?[YES][no]:yes`<br>`Enter the date in MM/DD/YY format:02/28/17`<br>`Enter the time in HH:MM:SS format:11:30:00`<br>`Enter timezone location index(enter 'help' for a list of timezones):5`<br>`Management Interface IP Address: 10.10.10.2`<br>`Management Interface Netmask: 255.255.255.0`<br>`Management Interface Default Router: 10.10.10.1`<br>`Create Management DHCP Scope?[yes][NO]:yes`<br>`DHCP Network: 10.10.10.0`<br>`DHCP Netmask: 255.255.255.0`<br>`Router IP: 10.10.10.1`<br>`Start DHCP IP address: 10.10.10.10`<br>`Stop DHCP IP address: 10.10.10.250`<br>`DomainName: mewlc.local`<br>`DNS Server:[OPENDNS][user DNS]OPENDNS`<br>`Create Employee Network?[YES][no]:yes` |

| | Command or Action | Purpose |
|---|---|---|
| | | `Employee Network Name(SSID)?:site_survey`<br>`Employee VLAN Identifier?[MGMT][1-4095]:MGMT`<br>`Employee Network Security?[PSK][enterprise]:PSK`<br>`Employee PSK Passphrase (8-38 characters)?: Cisco123`<br>`Re-enter Employee PSK Passphrase: Cisco123`<br>`Re-enter Employee PSK Passphrase: Cisco123`<br>`Create Guest Network? [yes][NO]:NO`<br>`Enable RF Parameter Optimization?[YES][no]:no`<br>`Configuration correct? If yes, system will save it and reset.[yes][NO]:yes` |
| **Step 5** | Wait for the Access Point to boot up completely. After the Wireless controller has started, log back in to the controller using administrative username or password configured during the initial setup wizard. | |
| **Step 6** | (Optional): During the CLI setup wizard, Employee Network Security was configured to PSK. This can be disabled for easy association of clients and also disable SSID broadcast to avoid unwanted clients from joining the SSID. To disable PSK and SSID broadcast, enter the following commands in the Controller CLI. | `(Cisco Controller)>config wlan disable 1`<br>`(Cisco Controller)>config wlan security wpa disable 1`<br>`(Cisco Controller)>config wlan broadcast-ssid disable wlan 1`<br>`(Cisco Controller)>config wlan enable 1`<br>`(Cisco Controller)>save config` |
| **Step 7** | To configure channel, TX power, and channel bandwidth for the radios, disable the radio first, make the changes and then re-enable it. | To change the 2.4GHz radio to channel 6, follow the steps below:<br>`(Cisco Controller)>config 802.11b disable <ap name>`<br>`(Cisco Controller)>config 802.11b channel <ap name> <ap name> 6`<br>`(Cisco Controller)>config 802.11b enable <ap name>`<br>To change the 2.4GHz radio Transmit Power to power level 3, follow the steps below:<br>`(Cisco Controller)>config 802.11b disable <ap name>`<br>`(Cisco Controller)>config 802.11b txPower <ap name> <ap name> 3`<br>`(Cisco Controller)>config 802.11b enable <ap name>`<br>To change the 5 GHz radio to channel 44, follow the steps below:<br>`(Cisco Controller)>config 802.11a disable <ap name>`<br>`(Cisco Controller)>config 802.11a channel <ap name> <ap name> 44`<br>`(Cisco Controller)>config 802.11a enable <ap name>` |

| | Command or Action | Purpose |
|---|---|---|
| | | To change the 5 GHz radio Transmit Power to level 5, follow the steps below:<br>`(Cisco Controller)>config 802.11a disable <ap name>`<br>`(Cisco Controller)>config 802.11a txPower <ap name> <ap name> 5`<br>`(Cisco Controller)>config 802.11a enable <ap name>`<br>To change the 5 GHz radio channel width to 40MHz, follow the steps below:<br>`(Cisco Controller)>config 802.11a disable <ap name>`<br>`(Cisco Controller)>config 802.11a chan_width <ap name> 40`<br>`(Cisco Controller)>config 802.11a enable <ap name>`<br>If access points are being used for Site Survey, please note the following with respect to the XOR radio.<br>**a.** Default operation state of XOR radio is 2.4GHz.<br>**b.** When the XOR (2.4 GHz) radio is configured to operate at 5GHz, 100MHz frequency separation is required from dedicated 5GHz radio.<br>**c.** When the XOR radio is configured to operate in 5GHz mode on an internal (I) Access Points, the Transmit power (tx) power will be fixed and cannot be modified.<br>**d.** One can configure the XOR radio on internal (I) Access Points from 2.4GHz to 5 and vice versa. On an external (E) Access Point, one must have an external antenna plugged into the DART connector prior to changing any configuration on the XOR radio.<br>**e.** To configure the XOR (2.4GHz) radio to operate at 5GHz on Access Points, follow the steps below:<br>`(Cisco Controller) >config 802.11-abgn disable ap`<br>`(Cisco Controller) >config 802.11-abgn role ap manual client-serving`<br>`(Cisco Controller) >config 802.11-abgn band ap ap 5GHz`<br>`(Cisco Controller) >config 802.11-abgn enable ap` |

| | Command or Action | Purpose |
|---|---|---|
| | | To configure the XOR radio operating at 5 GHz to channel 40, follow the steps below:<br>`(Cisco Controller) >config 802.11-abgn disable ap`<br>`(Cisco Controller) >config 802.11-abgn channel ap ap 40`<br>`(Cisco Controller) >config 802.11-abgn enable ap`<br>To configure the XOR radio operating at 5 GHz channel width to 40MHz, follow the steps below:<br>`(Cisco Controller) >config 802.11-abgn disable ap`<br>`(Cisco Controller) >config 802.11-abgn chan_width ap 40`<br>`(Cisco Controller) >config 802.11-abgn enable ap` |

# Creating Wireless Networks

Cisco Mobility Express solution supports a maximum of 16 WLANs. Each WLAN has a unique WLAN ID (1 through 16), a unique Profile Name, SSID, and can be assigned different security policies.

Access Points broadcast all active WLAN SSIDs and enforce the policies that you define for each WLAN.

You can configure WLANs with different service set identifiers (SSIDs) or with the same SSID. An SSID identifies the specific wireless network that you want the controller to access. Creating WLANs with the same SSID enables you to assign different Layer 2 security policies within the same wireless LAN. To distinguish among WLANs with the same SSID, you must create a unique profile name for each WLAN. WLANs with the same SSID must have unique Layer 2 security policies so that clients can make a WLAN selection based on information advertised in beacon and probe responses.

A number of WLAN Security options are supported on Cisco Mobility Express solution and are outlined below:

1. Open
2. WPA2 Personal
3. WPA2 Enterprise (External RADIUS, AP)

For Guest WLAN, a number of capabilities are supported:

1. CMX Guest Connect
2. WPA2 Personal
3. Captive Portal (AP)
4. Captive Portal (External Web Server)

# Creating Employee WLANs

## Creating Employee WLAN with WPA2 Personal

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up. | |
| **Step 2** | In the Add new WLAN window, on the General page, configure the following: | |
| **Step 3** | Click on the WLAN Security and configure the following: | |
| **Step 4** | Click Apply. | |

## Creating Employee WLAN using WPA2 Enterprise with External Radius Server

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up. | |
| **Step 2** | In the Add new WLAN window, on the General page configure the following: | |
| **Step 3** | Click on the WLAN Security and configure the following: | |
| **Step 4** | Add the Radius server and configure the following: | |
| **Step 5** | Click Apply. | |

## Creating Employee WLAN with WPA2 Enterprise and Authentication Server as AP

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up. | |

| | Command or Action | Purpose |
|---|---|---|
| **Step 2** | In the Add new WLAN window, on the General page configure the following: | • Enter the Profile Name.<br>• Enter the SSID. |
| **Step 3** | Click on the WLAN Security and configure the following: | • Select Security as WPA2 Enterprise.<br>• Select Authentication Server as AP.<br>**Note** AP is the primary AP running the controller function. In this use case, controller is the Authentication Server and therefore Local WLAN user account must exist to onboard the clients. |
| **Step 4** | Click the Apply. | |

## Creating Employee WLAN with WPA2 Enterprise/External RADIUS and MAC Filtering

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN. The Add new WLAN Window will pop up. | |
| **Step 2** | In the Add new WLAN window, on the General tab, configure the following: | • Enter the Profile Name<br>• Enter the SSID |
| **Step 3** | Click on the WLAN Security tab and configure the following: | • Enable MAC Filtering<br>• Select Security Type as WPA2 Enterprise<br>• Select Authentication Server as External RADIUS<br>• Select RADIUS Compatibility from the drop-down list<br>• Select MAC Delimiter from the drop-down list |
| **Step 4** | Add the Radius server and configure the following: | • Enter the Radius IP<br>• Enter the Radius Port<br>• Enter the Shared Secret<br>• Click on tick icon |

| | Command or Action | Purpose |
|---|---|---|
| **Step 5** | Click Apply. | |

# Creating Guest WLANs

Mobility Express controller can provide guest user access on WLANs which are specifically designated for use by guest users. To set this WLAN exclusively for guest user access, enable the Guest Network under the WLAN Security tab.

## Creating Guest WLAN with Captive Portal on CMX Connect

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up. | |
| **Step 2** | In the Add new WLAN window, on the General tab, configure the following: | • Enter the Profile Name<br>• Enter the SSID |
| **Step 3** | Enable the Guest Network under the WLAN Security tab. | |
| **Step 4** | Select Captive Portal as CMX Connect. | |
| **Step 5** | Enter Captive Portal URL. | **Note** Captive Portal URL must have the following format: https://yya7lc.cmxcisco.com/visitor/login where yya7lc is your Account ID. |
| **Step 6** | Click Apply. | **Note** Additional steps are required on CMX Cloud to create the Captive Portal, Site with Access Points and associating Captive Portal to the Site. |

## Creating Guest WLAN with Internal Splash Page

There is an internal splash page built into the Mobility Express controller which can be used to onboard the clients connecting to Guest WLANs. This internal splash page can also be customized by uploading a customized bundle. To upload a customized internal splash page, navigate to Wireless Settings > Guest WLANs. Select Page Type as Customized and click on the Upload button to upload a customized page bundle.

For internal splash page, Cisco Mobility Express supports multiple options for Access Type. They are as follows:

1. Local User Account
2. Web Consent

3. Email Address
4. RADIUS
5. WPA2 Personal

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up. | |
| **Step 2** | In the Add new WLAN window, on the General tab, configure the following: | • Enter the Profile Name<br>• Enter the SSID |
| **Step 3** | Enable the Guest Network under the WLAN Security tab. | |
| **Step 4** | Select Captive Portal as Internal Splash Page. | |
| **Step 5** | Select one of the following Access Type as needed: | • Local User Account–Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients.<br>• Web Consent–Splash Page will present the user to acknowledge before network access is granted.<br>• Email Address–Splash Page will present the user to enter the email address before network access is granted.<br>• RADIUS–Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select Access Type as RADIUS and enter the RADIUS server configuration.<br>• WPA2 Personal–This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select Access Type as WPA2 Personal and enter the Passphrase. |
| **Step 6** | Click Apply. | |

# Creating Guest WLAN with External Splash Page

An external splash page is one which resides on an external Web Server. Similar to the internal splash page, Cisco Mobility Express supports multiple options for Access Type with external splash page. They are as follows:

- Local User Account
- Web Consent
- Email Address
- RADIUS
- WPA2 Personal

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLANs and then click on Add new WLAN button. The Add new WLAN Window will pop up. | |
| **Step 2** | In the Add new WLAN window, on the General tab, configure the following: | • Enter the Profile Name<br>• Enter the SSID |
| **Step 3** | Enable the Guest Network under the WLAN Security tab. | |
| **Step 4** | Select Captive Portal as External Splash Page. | |
| **Step 5** | Select one of the following Access Type as needed: | • Local User Account–Splash Page will present the user to enter username and password which must be authenticated by the controller before network access is granted. Local WLAN users must be created on the controller to onboard the Guest clients.<br>• Web Consent–Splash Page will present the user to acknowledge before network access is granted.<br>• Email Address–Splash Page will present the user to enter the email address before network access is granted.<br>• RADIUS–Splash Page will present the user to enter username and password which must be authenticated by the RADIUS server before network access is granted. Select Access Type as RADIUS and enter the RADIUS server configuration. |

| | Command or Action | Purpose |
|---|---|---|
| | | • WPA2 Personal–This is an example of L2 + L3 (Web Consent). Layer 2 PSK security authentication will happen first followed by Splash Page which will present the user to acknowledge before network access is granted. Select Access Type as WPA2 Personal and enter the Passphrase. |
| **Step 6** | Click Apply | |

# Internal Splash Page for Web Authentication

Cisco Mobility Express supports a default internal guest portal that comes built-in and also a customized page, which can be imported by the user.

## Using Default Internal Guest Portal

To use the default Guest Portal Page or import a customized Guest Portal page, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > Guest WLANs. | |
| **Step 2** | Configure the following on the Guest WLAN page: | • Page Type–Select as Internal (Default).<br>• Preview–You can Preview the page by clicking on the Preview button.<br>• Display Cisco Logo–To hide the Cisco logo that appears in the top right corner of the default page, you can choose No. This field is set to Yes by default.<br>• Redirect URL After Login–To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters.<br>• Page Headline–To create your own headline on the login page, enter the desired text in this text box. You can enter up to 127 characters. The default headline is Welcome to the Cisco Wireless Network.<br>• Page Message–To create your own message on the login page, enter the desired text in this text box. You can enter |

| | Command or Action | Purpose |
|---|---|---|
| | | up to 2047 characters. The default message is Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work. |
| **Step 3** | Click Apply. | |

## Using Customized Internal Guest Portal

If a customized guest portal has to be presented to guest users, a sample page can be downloaded from cisco.com which can then be edited and imported to the Cisco Mobility Express controller. After the page has been edited and ready to be uploaded to the Cisco Mobility Express controller, follow the steps below.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > Guest WLANs. | |
| **Step 2** | Configure the following on the Guest WLAN page: | • Page Type–Select as Customized.<br>• Customized page Bundle–Click on the Upload button to upload the he customized page bundle to the Mobility Express controller.<br>• Preview–You can Preview the Guest portal by clicking on the Preview button.<br>• Redirect URL After Login–To have the guest users redirected to a particular URL (such as the URL for your company) after login, enter the desired URL in this text box. You can enter up to 254 characters. |
| **Step 3** | Click Apply. | |

# Managing WLAN Users

Cisco Mobility Express supports creation of local user accounts. These users can be authenticated for WLANs configured to use Security as WPA2 Enterprise with Authentication Server set to AP or Guest WLANs configured to use internal or external splash page with Access Type as Local User Account.

To create local user accounts, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLAN Users and then click on Add WLAN User button. | |
| **Step 2** | Navigate to Wireless Settings > WLAN Users and then click on Add WLAN User button. | • User Name–Enter the username<br>• Guest User–For Guest user, enable the Guest User checkbox<br>• Lifetime–For Guest User, define the user account validity. Default is 86400 seconds (or, 24 hours) from the time of its creation.<br>• WLAN Profile–Select the WLAN to which the user will connect<br>• Password–Enter the password for the user account<br>• Description–Additional details or comments for the user account<br>• Click on tickicon. |

# Adding MAC for Local MAC Filtering on WLANs

Cisco Mobility Express supports MAC Filtering on WLANs on controller as well as with external RADIUS. MAC addresses can be added to the controller and be either allowed or blocked. To add MAC addresses to the controller, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > WLAN Users and click on Local MAC Addresses. | |
| **Step 2** | Click Add MAC Address. | |
| **Step 3** | In the Add MAC Address window, configure the following: | • MAC Address–Enter the MAC Address of the device<br>• Description–Enter the description<br>• Type–Select whether this MAC has to be allowed or blocked<br>• Profile Name–Select the WLAN to which the user will connect |
| **Step 4** | Click Apply. | |

# Managing Services with Cisco Mobility Express

## Application Visibility and Control

Network Based Application Recognition (NBAR) provides application-aware control on a wireless network and enhances manageability and productivity. It also extends Cisco's Application Visibility and Control (AVC) as an end-to-end solution, which gives a complete visibility of applications in the network and allows the administrator to take some action on the same.

NBAR is a deep-packet inspection technology, which supports stateful L4 - L7 classification. The key use cases for NBAR are capacity planning, network usage base lining and better understanding of what applications are consuming bandwidth. Trending of application usage helps network admin improve quality of experience by protecting key applications from bandwidth-hungry applications when there is congestion on the network, capability to prioritize or de-prioritize, and drop certain application traffic. The AVC/NBAR2 engine interoperates with QoS settings on the specific WLAN.

## Enabling Application Visibility on WLAN

To configure Application Visibility on a WLAN, follow the procedure below:

**Procedure**

To enable Application Visibility on WLAN, navigate to Wireless Settings > WLANs. On the Add new WLAN or Edit WLAN window, click on the Traffic Shaping tab. To enable Application Visibility on this WLAN, select Enabled for Application Visibility Control.

## Enabling Application Control on WLAN

After Application Visibility has been enabled on the WLAN, one can add control for various applications. There are two way to add control for applications. One can either add control directly from the Applications widget on the Network Summary page or one can navigate to Monitoring > Applications and add control for applications as needed.

### Adding Application Control from Network Summary Page

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Add the Applications widget on the Network Summary Page. To add the Applications widget, click on the + icon on the right of the Network Summary banner. Select the Applications widget. The Applications widget will display the top 10 applications being browsed by the clients in the Mobility Express network. | |
| **Step 2** | Click on the application you wish to add control. The Add AVC Rule window will pop up. Select the Action. Action can be Mark, Drop or Rate Limit. For Mark, one can select DSCP | |

| | Command or Action | Purpose |
|---|---|---|
| | as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specific he DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application. | |
| **Step 3** | Select one or more AVC Profile/SSID combinations. | |
| **Step 4** | Click Apply. | |

### Adding Application Control from Applications Page

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Monitoring > Applications Page. | |
| **Step 2** | Click on the application you wish to add control. The Add AVC Rule window will pop up. Select the Action. Action can be Mark, Drop or Rate Limit. For Mark, one can select DSCP as Platinum, Gold, Silver, Bronze or Custom. If custom is selected, one has to specific he DSCP value. For Rate Limit, one can specify the Average Rate and Burst Rate for the application. | |
| **Step 3** | Select one or more AVC Profile/SSID combinations. | |
| **Step 4** | Click Apply. | |

# iOS Optimized WiFi Connectivity and Fast Lane

## Configuring Optimized WiFi Connectivity

802.11r enabled WLAN provides faster roaming for wireless client devices. It is desired that iOS devices running iOS 10 will be able to join a WLAN with 11r enabled for better roaming experience. However, if 11r is enabled on a WLAN, the legacy devices that do not recognize the FT AKM's beacons and probe responses will not be able to join the WLAN. We need a way to identify the Client device capability and allow 11r capable device to join on the WLAN as an FT enabled device and at the same time to allow legacy device to join as an 11i/WPA2 device.

Cisco Mobility Express Release 8.4 will enable 802.11r on an 802.11i-enabled WLAN selectively for iOS devices. The capable iOS devices will identify this functionality and perform an FT Association on the WLAN. The Cisco Wireless infrastructure will allow FT association on the WLAN from devices that can negotiate FT association on a non-FT WLAN. In addition, with Mobility Express running AireOS 8.4, 802.11k and 11v features are enabled by default on an SSID. These features help clients roam better by telling them when to roam and providing them with information about neighboring APs so that no time is wasted scanning when

roaming is needed. Since iOS devices support dual band, the 802.11k neighbor list is updated on dual-band, adaptively for iOS devices.

To configure 11k, r, v on a WLAN, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Enable Expert View on Cisco Mobility Express. Expert View is available on the top banner of the Cisco Mobility Express WebUI as shown below and enabled various configurable parameters which are not available in Standard view. | |
| **Step 2** | Navigate to Wireless Settings > WLANs. On the Add new WLAN or Edit WLAN window, click on the Advanced tab. Configure 802.11k, r, v as needed on this page. | |
| **Step 3** | Click Apply. | |

## Configuring Fast Lane

Apple iOS device mark QoS as per IETF recommendations. With Mobility Express running AireOS 8.4, one can enable the Fastlane feature from CLI, which enables several beneficial functions:

Your WLC QoS configuration is optimized globally to better support real-time applications

iOS 10 devices can send upstream voice traffic without the requirement to perform WMM TSPEC/TCLAS negotiation. The infrastructure will honor the voice marking for these devices.

You can apply a QoS profile to your iOS 10 devices, and decide which applications should receive QoS marking upstream, and which applications should be sent as best effort or background.

To configure Fast Lane on a WLAN from CLI, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Login to the controller CLI. | |
| **Step 2** | Enable Fast Lane using the CLI below: | `(Cisco Controller) >config qos fastlane enable 1`<br><br>`Warning: This command will temporarily disable all WLANs and Networks. Active WLANs and networks will be re-enabled automatically after the configuration completes. This command will also override the file named AUTOQOS-AVC-PROFILE, if it exists, and will apply it to the WLAN, if Application Visibility is enabled. Are you sure that you want to continue? (y/N)y` |

# Cisco Mobility Express with CMX Cloud

## Cisco CMX Cloud

Cisco Connected Mobile Experiences Cloud (Cisco CMX Cloud) is an simple and scalable offering which enables delivery of wireless guest access and in-venue analytics, integrating seamlessly with Cisco wireless infrastructure.

This cloud-delivered Software-as-a-Service (SaaS) offering is quick to deploy and intuitive to use. It is based on CMX 10.x code and is compatible with Cisco Mobility Express Release 8.3. It offers the following services:

- Connect for Guest Access-Providing an easy-to-use guest-access solution for visitors through a custom portal using various authentication methods including social, self-registration, and Short Message Service (SMS).
- Presence Analytics-Detecting all Wi-Fi devices (the "devices") in the venue and providing analytics on their presence, including dwell times, new vs. repeat visitors, and peak time.

## Cisco CMX Cloud Solution Compatibility Matrix

- Cisco Mobility Express running AireOS Release 8.3 and later.
- All Cisco Mobility Express supported Access Points.

## Minimum Requirements for Cisco CMX Cloud Deployment

Below are the minimum requirements for CMX Cloud deployment:

1. Verify Cisco CMX Cloud Solution Compatibility Matrix above.
2. Recommended browser is Chrome 45 or later.
3. Signup at https://cmxcisco.com for 60 day trial or go to Cisco Commerce Workspace (CCW) and purchase license for your choice of CMX Cloud service.

## Enabling CMX Cloud Service on Mobility Express for Presence Analytics

After CMX Cloud Account has been created, next step is to configure and enable the CMX Cloud Service on primary Access Point so that it can send data to the CMX Cloud. To configure, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | On Cisco Mobility Express WebUI, navigate to Advanced > CMX. | |
| **Step 2** | Enter the CMX Server URL (Site URL). | |
| **Step 3** | Enter the CMX Server Token (Account Token). | |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | Click Apply. | **Note** Click the Test Link button to verify connectivity from primary AP to CMX Cloud Site using the configured information. |

## Configuring Site on CMX Cloud for Presence Analytics

To create a site and add Access Points to the site in CMX Cloud for Presence Analytics, follow the procedure below:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Login to CMX Cloud account at https://cmscisco.com/ | |
| **Step 2** | Navigate to Manage > Cloud Enabled WLC and verify that the IP address of the WLC shows up on the list. | |
| **Step 3** | Navigate to PRESENCE ANALYTICS > Manage. You should be in the Sites pane. Click on the Add Site button to create a site. | |
| **Step 4** | In the NEW SITE window, configure the following details: | • Enter the Name for the site<br>• Enter the Address for the site<br>• Select Timezone from the drop-down list<br>• Select the Signal Strength Threshold for Ignore, Passerby, and Visitors<br>• Enter the Minimum Dwell Time for Visitor (minutes) |
| **Step 5** | Click Save to create the Site. | |
| **Step 6** | After the Site is created, click on Access Points under PRESENCE ANALYTICS > Manage. | |
| **Step 7** | Select the Access Points and add them to the Site by clicking on Add to Site button and selecting the Site from the drop-down list. | |
| **Step 8** | Finally, navigate to Presence Analytics dashboard. Select the Site you created. Within a few minutes, you should begin to see Presence data get populated. | |

# Managing the Cisco Mobility Express Deployment

## Managing Access Points

Starting Release 8.4, Cisco Mobility Express supports up to 50 Access Points. To view the list or modify parameters on an Access Points, follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to **Wireless Settings > Access Points**. | **Note** The first Access Point with the P icon is the primary AP and the rest of them are Subordinate Access Points. |
| **Step 2** | To modify the parameters on an access point, click on the Edit button. The Access Point window will come up displaying the General parameters about the Access Point. | • Operating Mode(Read only field)-For a primary AP, this field displays AP & Controller. For other associated APs, this field displays AP only.<br>• AP Mac(Read only field)–Displays the MAC address of the Access Point.<br>• AP Model(Read only field)-Displays the model details of the Access Point.<br>• IP Configuration–Choose Obtain from DHCP to allow the IP address of the AP be assigned by a DHCP server on the network, or choose Static IP address. If you choose Static IP address, then you can edit the IP Address, Subnet Mask, and Gateway fields.<br>• AP Name–Edit the name of access point. This is a free text field.<br>• Location–Edit the location for the access point. This is a free text field. |
| **Step 3** | Under the Controller tab (Available only for primary AP), one can modify the following parameters: | • System Name–Enter the System Name for Mobility Express<br>• IP Address–IP address decides the login URL to the controller's web interface. The URL is in https://<ip address> format. If you change this IP address, the login URL also changes.<br>• Subnet Mask–Enter the Subnet Mask. |

| | Command or Action | Purpose |
|---|---|---|
| | | • Country Code–Enter the Country Code. |
| **Step 4** | Under Radio 1 (2.4 GHz) and Radio 2 (5 GHz), one can edit the following parameters: | • Admin Mode–Enabled/Disabled. This enables or disables the corresponding radio on the AP (2.4 GHz for 802.11 b/g/n or 5 Ghz for 802.11 a/n/ac).<br>• Channel–Default is Automatic. Automatic enables Dynamic Channel Assignment. This means that channels are dynamically assigned to each AP, under the control of the Mobility Express controller. This prevents neighboring APs from broadcasting over the same channel and hence prevents interference and other communication problems. For the 2.4GHz radio, 11 channels are offered in the US, up to 14 in other parts of the world, but only 1-6-11 can be considered non-overlapping if they are used by neighboring APs. For the 5GHz radio, up to 23 non-overlapping channels are offered. Assigning a specific value statically assigns a channel to that AP.<br>• 802.11 b/g/n–1 to 11.<br>• 802.11 a/n/ac –40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140, 149, 153, 157, 161, 165.<br>• Channel Width - 20 MHz for 2.4GHz and for 20, 40 and 80 for 5 GHz.<br>• Transmit Power - 1 to 8. The default value is Automatic.<br><br>This is a logarithmic scale of the transmit power, that is the transmission energy used by the AP, 1 being the highest,2 being half of it, 3 being 1/4th and so on. Selecting Automatic adjusts the radio transmitter output power based on the varying signal level at the receiver. This allows the transmitter to operate at less than maximum power for most of the time; when fading conditions occur, transmit power will be increased as needed until the maximum is reached. |
| **Step 5** | Click Apply. | |

# Primary AP Failover and Electing a New Primary

Cisco Mobility Express is supported on Cisco 1100 series Access Points. If you have a mix of these Access Points in a Cisco Mobility Express deployment, the primary AP election process determines which of the supported Access Point will be elected to run Mobility Express controller function in case of a Failover of the Active primary AP. VRRP is used to detect the failure of primary AP which initiates the election of a new primary.

**Note** Mobility Express uses MAC 00-00-5E-00-01-VRID where VRID is 1 so if there are other instances of VRRP running in the environment, use VRID other than 1 for those instances.

## Primary AP Failover

To have redundancy in the Mobility Express network, it must have two or more Mobility Express capable Access Points. These Access Points should have AP Image type as MOBILITY EXPRESS IMAGE and AP Configuration as MOBILITY EXPRESS CAPABLE. In an event of a failure of primary AP, another Mobility Express capable AP is elected as a primary automatically. The newly elected primary AP has the same IP and configuration as the original primary AP.

**Note** Given Access Point models support different scale limits in terms of the number of Access Points supported, it is highly recommended to have at least two or more Access Points which support the same scale limits.

**Note** Access Points, which have the Mobility Express Image but AP Configuration, is NOT MOBILITY EXPRESS CAPABLE, will not participate in the primary AP election process.

## Electing a new Primary Access Point

As mentioned above, primary Access Point election is based on a set of priorities. The priorities are as follows:

### Before you begin

Primary election process is based on a set of priorities. When an active primary Access Point fails, the election process gets initiated and it elects the Access Point with the highest priority as the primary AP.

**Note** During the primary Election process, even though the primary AP running the controller function is down, the remaining Access Points will fall into Standalone mode and will continue to service connected clients and switch data traffic locally. After the new primary is elected, the Standalone Access points will move to connected mode.

### Procedure

**Step 1** User Defined Primary–User can select an Access Point to be the primary Access Point. If such a selection is made, no new primary will be elected in case of a failure of the active primary. After five minutes, if the current primary is still not active, it will be assumed dead and primary Election will begin to elect a new primary. To manually define a primary, follow the procedure below:

a) Navigate to Wireless Settings > Access Points.
b) From the list of Access Points, click Edit icon of the Access Point which you would like to select as the primary AP.
c) Under the General tab, click on Make me Controller button.
d) Click Yes on the Confirmation window.

**Note** The previous primary will reboot and the selected Access Point will immediately launch the controller and become the active primary.

**Step 2** Next Preferred Primary - Admin can configure the Next Preferred Primary from CLI. When this is configured and the active primary AP fails, the one configured as the Next Preferred Primary will be elected as a primary. To configure the Next Preferred Primary, follow the procedure below:

a) Login to the CLI of the controller.
b) Execute the following CLI:

To configure the Next Preferred Primary, execute the following CLI:

```
(Cisco Controller) >config ap next-preferred-master <Cisco AP>
<Cisco AP> Enter the name of the Cisco AP
```

To see the Next Preferred Primary, execute the following CLI:

```
(Cisco Controller) >show ap next-preferred-master
```

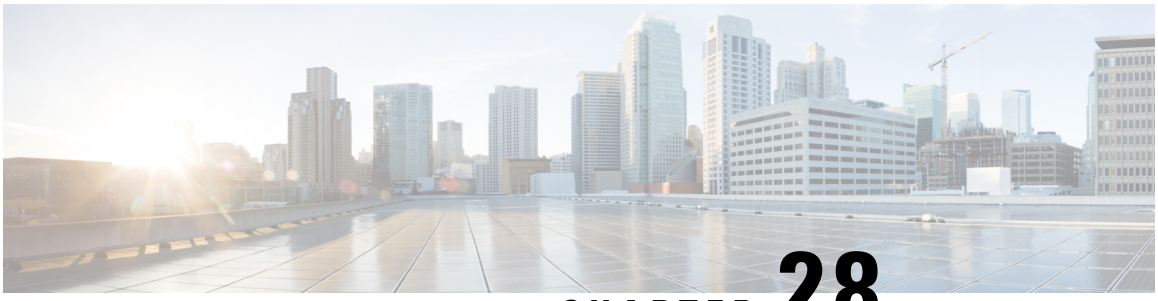
To clear the Next Preferred Primary, execute the following CLI:

```
Cisco Controller) >clear ap next-preferred-master
```

**Step 3** Most Capable Access Point– If the first two priorities are not configured, primary AP election algorithm will select the new primary based on the capability of the Access Point.

**Step 4** Least Client Load– If here are multiple Access Points with the same capability, the one with least client load is elected as the primary Access Point.

**Step 5** Lowest MAC Address–If all of the Access Points are the same and have the same client load, then Access Point with the lowest MAC will be elected as a primary.



CHAPTER 28

# Configuring Wi-Fi 6


- Wireless Device Overview, on page 429
- Wireless Connectivity for Cisco 1100 Series ISR, on page 429
- Module Managment, on page 430
- Deploying Cisco Embedded Wireless Controller (EWC), on page 433
- Using internal DHCP server on Cisco Mobility Express , on page 444
- Access Points, on page 446


## Wireless Device Overview

Cisco Embedded Wireless Controller on Catalyst Access Points are the next generation of wireless controllers built for the Intent-based networking. The Cisco controllers are IOS XE-based and integrates the RF Excellence from Cisco Catalyst 9105AX Series Access Points with Intent-based Networking capabilities of IOS XE to create the best-in-class wireless experience for your evolving and growing organization.

With a management system based on Cisco IOS XE software, wireless devices are Wi-Fi CERTIFIED™, 802.11a-compliant, 802.11b-compliant, 802.11g-compliant, and 802.11n-compliant wireless LAN transceivers.

By adhering to the 802.11ax Wave 2 standard, the Cisco 1100 Series WLAN offers a data rate of up to 1.488Gbps on the 5-GHz radio. This exceeds the data rates offered by access points that support the 802.11n standard.

The configuration data model is based on design principles of reusability, simplified provisioning, enhanced flexibility and modularization to help manage networks as they scale up and simplify the management of dynamically changing business and IT requirements.

## Wireless Connectivity for Cisco 1100 Series ISR

This module describes how to configure the WiFi card to the internal switch interface on the Cisco C1100 Integrated Services Routers (ISRs).

The WiFi card is connected to the internal switch interface, the *Wlan-GigabitEthernet* interface. The configuration of this interface is identical to the *GigabitEthernet 0/1/0* interface.

For Cisco 1131 and C1131X Series of ISRs, it is always *Wlan-GigabitEthernet 0/1/8*.

```
Router# show run int Wlan-GigabitEthernet 0/1/8
Building configuration...
```

```
Current configuration : 67 bytes
!
interface Wlan-GigabitEthernet0/1/8
switchport mode access

end
```

# Module Managment

The router configures, manages, and controls the supported interfaces and modules using the module management facility built in its architecture. This new centralized module management facility provides a common way to control and monitor all the modules in the system regardless of their type and application.

## Slot and Subslots for WLAN

This section contains information on slots and subslots for WLAN. Slots specify the chassis slot number in your router and subslots specify the slot where the service modules are installed.

The table below describes the slot number for the Cisco 1100 Series ISR models.

***Table 36: Slot Numbers for Cisco 1100 Series ISR Models***

| Cisco 1100 Series SKU | WiFi Slot |
|---|---|
| C1131X-8PLTEPWx | 0/3 |
| C1131-8PLTEPWx | 0/3 |
| C1131X-8PWx | 0/2 |
| C1131-8PWx | 0/2 |

## Supported WiFi Cards

The supported WiFi card Product IDs (PIDs) are as follows:

- ISR-AP1100AX-A
- ISR-AP1100AX-B
- ISR-AP1100AX-E
- ISR-AP1100AX-Q
- ISR-AP1100AX-Z

```
Router#show platform

Chassis type: C1131X-8PLTEPWB

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         C1131X-8PLTEPWB     ok                    3w2d
 0/0      C1131X-2x1GE        ok                    3w2d
```

```
 0/1      C1131X-ES-8         ok                   3w2d
 0/3      ISR-AP1101AX-B      out of service       19:03:2
R0        C1131X-8PLTEPWB     ok, active           3w2d
F0        C1131X-8PLTEPWB     ok, active           3w2d
P0        PWR-12V             ok                   3w2d

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         21052400            17.6.0
R0        21052400            17.6.0
F0        21052400            17.6.0
```

# Implementing Modules on Your Router

• Accessing Your Module Through a Console Connection, on page 378

## Accessing Your Module Through a Console Connection

Before you can access the modules, you must connect to the host router through the router console or through Telnet. After you are connected to the router, you must configure an IP address on the Gigabit Ethernet interface connected to your module. Open a session to your module using the **hw-module session** command in privileged EXEC mode on the router.

To establish a connection to the module, connect to the router console using Telnet or Secure Shell (SSH) and open a session to the switch using the **hw-module session** *slot/subslot* command in privileged EXEC mode on the router.

Use the following configuration examples to establish a connection:

- The following example shows how to open a session from the router using the **hw-module session** command:

```
Router# hw-module session slot/card
Router# hw-module session 0/2 endpoint 0

Establishing session connect to subslot 0/2
```

- The following example shows how to exit a session from the router, by pressing **Ctrl-A** followed by **Ctrl-Q** on your keyboard:

```
type ^a^q
picocom v1.7

port is        : /dev/ttyS3
flowcontrol    : none
baudrate is    : 9600
parity is      : none
databits are   : 8
escape is      : C-a
local echo is  : no
noinit is      : no
noreset is     : no
nolock is      : yes
send_cmd is    : sz -vv
receive_cmd is : rz -vv
imap is        :
omap is        :
emap is        : crcrlf,delbs,
```

```
Terminal ready
```

## Deactivating a Module

A module can be removed from the router without first being deactivated. However, we recommend that you perform a graceful deactivation (or graceful power down) of the module before removing it. To perform a graceful deactivation, use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode.

**Note** When you are preparing for an OIR of a module, it is not necessary to independently shut down each of the interfaces before deactivating the module. The **hw-module subslot** *slot/subslot* **stop** command in EXEC mode automatically stops traffic on the interfaces and deactivates them along with the module in preparation for OIR. Similarly, you do not have to independently restart any of the interfaces on a module after OIR.

The following example shows how to use the **show facility-alarm status** command to verify if any critical alarm is generated when a module is removed from the system:

```
Device# show facility-alarm status
System Totals  Critical: 8  Major: 0  Minor: 0

Source                          Time                Severity         Description [Index]
------                        --------              --------         -------------------
Power Bay 0                 Dec 01 2021 07:21:41       INFO           Power Ethernet Module
 Missing [0]
xcvr container 0/0/1        Dec 01 2021 07:22:28       INFO           Transceiver Missing
[0]
GigabitEthernet0/1/0        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/1        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/2        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/3        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/4        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/5        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/6        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
GigabitEthernet0/1/7        Dec 01 2021 07:21:57       CRITICAL       Physical Port Link
Down [1]
```

**Note** A critical alarm (Active Card Removed OIR Alarm) is generated even if a module is removed after performing graceful deactivation.

## Deactivating Modules and Interfaces in Different Command Modes

You can deactivate a module and its interfaces using the **hw-module subslot** command in one of the following modes:

- If you choose to use the **hw-module subslot** *slot/subslot* **stop** command in EXEC mode, you cause the module to gracefully shut down. The module is rebooted when the **hw-module subslot** *slot/subslot* **start** command is executed.

To deactivate a module and all of its interfaces before removing the module, use one of the following commands in global configuration mode.

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **hw-module subslot** *slot*/*subslot* [**reload** \| **stop** \| **start**]<br>**Example:**<br>`Router# hw-module subslot 0/2 stop` | Deactivates the module in the specified slot and subslot, where:<br>• *slot*—Specifies the chassis slot number where the module is installed.<br>• *subslot*—Specifies the subslot number of the chassis where the module is installed.<br>• **reload**—Stops and restarts the specified module.<br>• **stop**—Removes all interfaces from the module and the module is powered off.<br>• **start**—Powers on the module similar to a physically inserted module in the specified slot. The module firmware reboots and the entire module initialization sequence is executed in the IOSd and Input/Output Module daemon (IOMd) processes. |

## Reactivating a Module

If, after deactivating a module using the **hw-module subslot** *slot/subslot* **stop** command, you want to reactivate it without performing an OIR, use one of the following commands (in privileged EXEC mode):

- **hw-module subslot** *slot/subslot* **start**
- **hw-module subslot** *slot/subslot* **reload**

# Deploying Cisco Embedded Wireless Controller (EWC)

## Prerequisites for Deploying Embedded Wireless Controller (EWC) Solution

1. It is recommended not to have any other Cisco Wireless LAN Controllers; neither appliance nor virtual in the same network during set up or during daily operation of a Cisco Embedded Wireless Controller (EWC) network.

2. Decide on the first Access Point to be configured as a primary Access Point. This Access Point should be capable of supporting the Wireless LAN Controller function.
3. A DHCP server must be available on the network so that Access Points and clients can obtain an IP Address. Starting from Cisco IOS XE Release 17.7.x or later, one can configure a DHCP server on the primaryAccess Point as well but this is typically used for Site Survey.
4. To configure the EWC and AP integrated into C1100 series router, you must configure a DHCP server, SVI interface, and NAT on the router. For more information on configuring the AP, see **Prerequisites for Configuring the AP on the Router** section.

# Prerequisites for Configuring the AP on the Router

To configure the global parameters for your router, follow these steps:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **ip dhcp pool** *name*<br>**Example:**<br>`Device(config)#ip dhcp pool wireless` | Use this command to create a name for the DHCP server address pool and to enter the DHCP pool configuration mode. |
| **Step 2** | **networkip address subnet mask**<br>**Example:**<br>`Router(dhcp-config)#network 10.10.10.0 255.255.255.0` | Use this command to create a DHCP pool of IP addresses to be used by the Switched Virtual Interface (SVI) (Refer Step 11 and further for SVI). |
| **Step 3** | **default-router ip address**<br>**Example:**<br>`Router(dhcp-config)#default-router 10.10.10.1` | Use this command to assign the default gateway to clients of this DHCP pool. |
| **Step 4** | **dns-serverip address**<br>**Example:**<br>`Router(dhcp-config)#dns-server 192.0.2.1` | Use this command to assign the DNS server IP address to clients in this DHCP pool. |
| **Step 5** | **interface GigabitEthernet** *slot/subslot/port*<br>**Example:**<br>`Router(config)#interface GigabitEthernet 0/0/0` | Use the **interface gigabitEthernet** command to add the interface and set the IP address. **0/0/0** is the slot/subslot/port. |
| **Step 6** | **ip address dhcp**<br>**Example:** | Use this command to configure the ip address using DHCP and static ip. |

| | Command or Action | Purpose |
|---|---|---|
| | `Router(config-if)#ip address dhcp` | |
| **Step 7** | **ip nat outside**<br>**Example:**<br>`Router(config-if)#ip nat outside` | Use this command to connect the interface to the outside network. |
| **Step 8** | **interface Wlan-GigabitEthernet** *slot/subslot/port*<br>**Example:**<br>`Router(config)#interface Wlan-GigabitEthernet 0/1/8` | Use the Wlan-GigabitEthernet command to connect the Wi-Fi card of the internal switch interface. |
| **Step 9** | **switchport accessvlan** *number*<br>**Example:**<br>`Router(config-if)#switchport access vlan 199` | Use the **switchport access vlan** command to assign the port or range of ports into access ports. |
| **Step 10** | **switchport modeaccess**<br>**Example:**<br>`Router(config-if)#switchport mode access` | Use the **switchport modeaccess** command to to configure the VLAN membership mode. |
| **Step 11** | **interface vlan** *number*<br>**Example:**<br>`Router(config)#interface vlan 199` | Use the **interface vlan** *number* command in the configuration mode tocreate a Switched Virtual Interface (SVI) and enter the interface configuration (VLAN) mode for a specific VLAN or a range of VLANs. |
| **Step 12** | **description name**<br>**Example:**<br>`Router(config-if)#description Wireless` | Use this command to add a description for the Switched Virtual Interface (SVI). |
| **Step 13** | **ip address** *ip-address***subnet_mask**<br>**Example:**<br>`Router(config-if)#ip address 10.10.10.1 255.255.255.0` | Use this command to assign an IP address from the DHCP Pool (**Refer Step 2**). |
| **Step 14** | **ip nat inside**<br>**Example:**<br>`Router(config)#ip nat inside` | Connects the interface to the inside network, which is subject to NAT. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 15** | **ip nat inside source list** *number* **interface GigabitEthernet** *slot/subslot/port* overload<br>**Example:**<br>`Router(config)#ip nat inside source list 10 interface GigabitEthernet 0/0/0 overload` | Use this command to establish dynamic source translation, specifying the access list. |
| **Step 16** | **ip route 10.10.10.10 10.10.10.10** *default gateway ip-address*<br>**Example:**<br>`Router(config)#ip route 10.10.10.10 10.10.10.10 192.0.2.1` | Use this command to direct all the traffic to the default gateway of the router. |
| **Step 17** | **ip access-list standard** *number*<br>**Example:**<br>`Router(config)#ip access-list standard 10` | Use the ip access-list standard command to filter the traffic based on a set of rules. |
| **Step 18** | **number permitip address wildcard mask**<br>**Example:**<br>`Router(config)#10 permit 10.10.10.0 0.0.0.255` | Use this command to create ACL entries to permit or deny traffic. |

# Configuring the AP Using Day 0 Provisioning

There are 3 ways to configure the AP using day 0 provisioning:

### Procedure

**Step 1** To connect the SSID to CiscoAirProvision-XXXX, follow the steps added here: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/mobility-express/guide-c07-741338.html

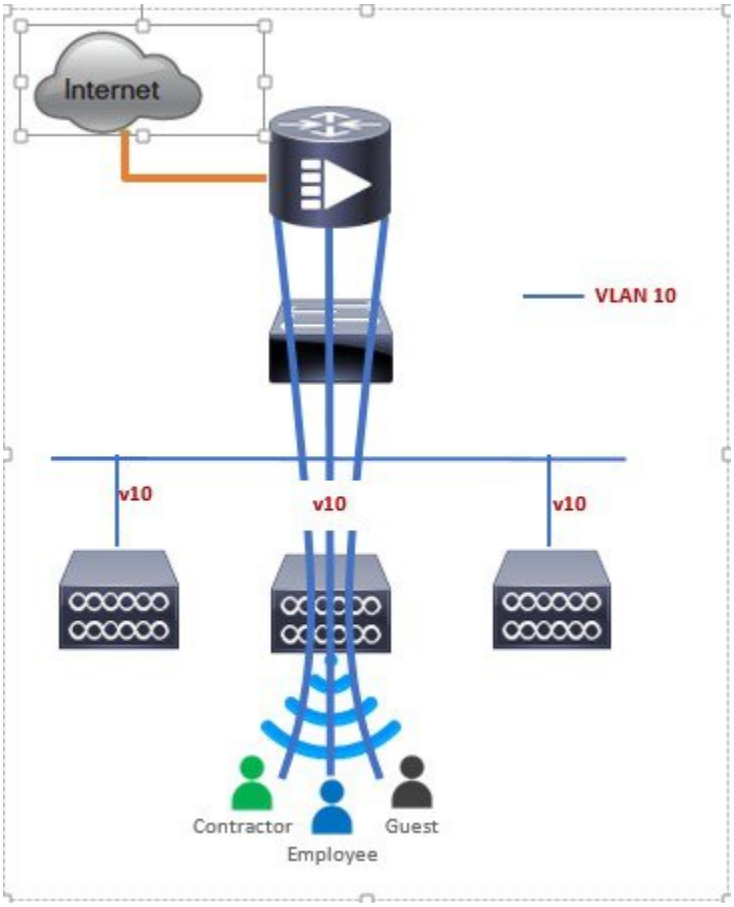
**Step 2** You can also scan the QR Code by using the Catalyst Wireless Application by following the steps added here: https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/mob-app/user-guide/cisco_catalyst_wireless_app_user_guide/getting_started.html

**Step 3** You can manually configure the AP using CLI by following the steps added here: https://www.cisco.com/c/en/us/td/docs/wireless/controller/ewc/17-6/config-guide/ewc_cg_17_6/overview_of_the_controller.html#task_gs1_qzh_kpb

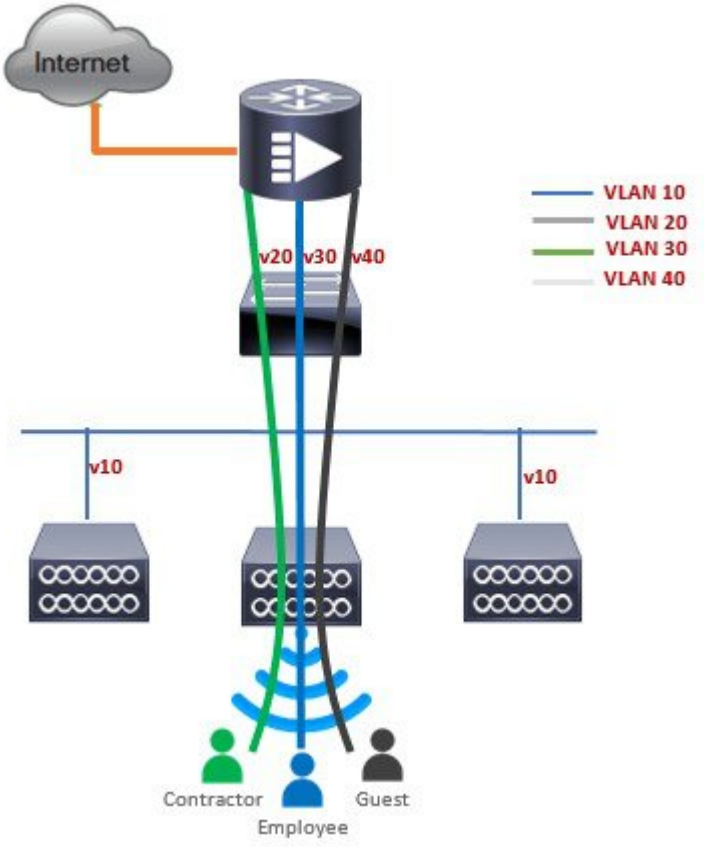
# Connecting Cisco Embedded Wireless Controller (EWC) Capable Access Point to the Network

Depending on the deployment, Embedded Wireless Controller (EWC) Capable Access Point to the Network capable Access Points can be connected to an access port or a trunk port on the switch.

If Access Points and WLANs are all on the same network, Embedded Wireless Controller (EWC) capable Access Points can connect to an access port on the switch as shown below.




On an Embedded Wireless Controller (EWC), management traffic is untagged. If Access Points and WLANs are all on different VLANs, the Embedded Wireless Controller (EWC) capable Access Points will connect to a trunk port on the switch and traffic for individual WLANs will be switched locally on individual VLANs. Shown below is a deployment with Access Points and WLANs on different VLANs.




```
interface Wlan-GigabitEthernet 0/1/8
description » Connected to Master AP «
switchport trunk native vlan 40
switchport trunk allowed vlan 10,20,30,40
switchport mode trunk
```

# Converting Access Point from CAPWAP to Cisco Embedded Wireless Controller (EWC)

One can convert an Access Point running CAPWAP to Embedded Wireless Controller (EWC) and vice versa.

Cisco Embedded Wireless Controller (EWC) support on 802.11ax Access Points is introduced in different IOS XE releases and it is important to note that before an Access Point can be converted to Cisco Embedded Wireless Controller (EWC), it must have the minimum IOS XE CAPWAP image which supports Cisco Embedded Wireless Controller (EWC) capability for that Access Point. Given below is the minimum IOS XE release for an Access Point which will support conversion from CAPWAP to Cisco Embedded Wireless Controller (EWC).

| Access Point | Minimum AireOS Release with CAPWAP image |
|---|---|
| Cisco 1100 Series | Cisco IOS XE Release 17.7.x |

Toperform a conversion on an Access Point running CAPWAP to Embedded Wireless Controller (EWC), follow the procedure below:

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Download the conversion imagefor the Access Point from cisco.com to the TFTP server. It is a tar file. Do not untar the file. The following table lists the Cisco Embedded Wireless Controller (EWC) softwarefor Cisco Wireless Release IOS XE 17.7. | |
| **Step 2** | Login to the Access Point | |
| **Step 3** | Execute AP#show version on the Access Point CLI. From the show version output, you can determine the AP Image type and AP Configuration and can then proceed with the conversion | Case 1: If the APis running a CAPWAP image for the conversion, execute the command below:<br>`Router#ap-type ewc-ap tftp://<TFTP Server IP>/<ap image path> tftp://<TFTP Server IP>/<controller image path>`<br>Example:<br>`APC884.A110.0104#ap-type ewc-ap tftp://10.74.9.8/ap1g8-tar_CS00012204433_fix`<br><br>`tftp://10.74.9.8/test/C9800-AP-iosxe-wlc.bin`<br>`Starting download eWLC image tftp://10.74.9.8/userid/C9800-AP-iosxe-wlc.bin ...`<br>`It may take a few minutes. If longer, please abort command, check network and try again.`<br>`##########################################################`<br>`100.0%`<br>`Image download completed.`<br>`Checking ...OK`<br>`Checking image size...OK`<br>`Checking image family...OK`<br>`Verifying ...[*08/25/2021 08:18:20.6120] [*08/25/2021 08:18:20.6120] CAPWAP State: Discovery`<br>`[*08/25/2021 08:18:20.6650] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)`<br>`OK`<br>`Versioning ...ws_management_version: 17.08.01.0.144557`<br>`Successfully downloaded and setup eWLC image.`<br>`Starting download AP image tftp://10.74.9.8/ap1g8-tar_CS00012204433_fix ...`<br>`It may take a few minutes. If longer, please abort command, check network and try again.`<br>`##########################################################`<br>`100.0%`<br>`Image download completed.` |

| | Command or Action | Purpose |
|---|---|---|
| | | Upgrading ...<br>status 'upgrade.sh: Script called with args:[NO_UPGRADE]'<br>do NO_UPGRADE, part1 is active part<br>status 'upgrade.sh: Script called with args:[-c PREDOWNLOAD]'<br>do PREDOWNLOAD, part1 is active part<br>status 'upgrade.sh: Start doing upgrade arg1=PREDOWNLOAD arg2=,from_cli arg3= ...'<br>status 'upgrade.sh: Using image /tmp/cli_part.tar on ax-bcm32 ...'<br>status 'Image signing verify success.'<br>[8/25/2021 8:20:40] : WARNING! Program shadow retry exhausted on flash version 45<br>[8/25/2021 8:20:40] : Shadow is now in-synced with master<br>[8/25/2021 8:20:40] : Verifying against bundle image btldr.img...<br>shared_printenv updated<br>status 'upgrade.sh: ***** part to upgrade is part2 *******'<br>status 'upgrade.sh: AP version1: part2 , img 8.8.1.10'<br>status 'upgrade.sh: BOARD generic case execute'<br>status 'upgrade.sh: Untar /tmp/cli_part.tar to /bootpart/part2...'<br>status 'upgrade.sh: Sync image to disk...'<br>[*08/25/2021 08:19:49.2690]<br>[*08/25/2021 08:19:49.2690] CAPWAP State: Discovery<br>[*08/25/2021 08:19:49.2810] Discovery Request sent to 255.255.255.255, discovery type UNKNOWN(0)<br>status 'upgrade.sh: AP version2: part2 8.8.1.10, img 8.8.1.10'<br>status 'upgrade.sh: AP backup version: 8.8.1.10'<br>status 'upgrade.sh: Finished upgrade task.'<br>status 'upgrade.sh: Cleanup for do_upgrade...'<br>status 'upgrade.sh: /tmp/upgrade_in_progress cleaned'<br>status 'upgrade.sh: Cleanup tmp files ...'<br>status 'upgrade.sh: Script called with args:[ACTIVATE]'<br>do ACTIVATE, part1 is active part<br>status 'upgrade.sh: activate part2, set BOOT to part2'<br>status 'upgrade.sh: AP primary version after reload: 8.8.1.10'<br>status 'upgrade.sh: AP backup version after reload: 17.8.0.4'<br>Successfully setup AP image.<br>Archive done.<br>APC884.A110.0104#[*08/25/2021 |

| | Command or Action | Purpose |
|---|---|---|
| | | `08:20:04.3370] Config Factory Reset triggered: clear saved config files..` |
| **Step 4** | If this is the first Access Point in the network, it will start the controller function and will broadcast the CiscoAirProvison SSID. | |

# Converting Access Point from Cisco Embedded Wireless Controller (EWC) to CAPWAP

There are typically two reasons why one would want to convert an Access Point running Embedded Wireless Controller (EWC) image to CAPWAP. There are as follows:

1. You want to keep the Access Point in a Embedded Wireless Controller (EWC) deploymentbut do not want the Access point to participate in the primary election process upon a failover of the primary AP.
2. You want to migrate one or more Access Points with Embedded Wireless Controller (EWC) to an appliance or vWLC based deployment. (Refer step 1.a in the Prerequisites.

1. If your reason to convert to CAPWAP is 1 above, follow the procedure below:
   a. Login to the Access Point CLI either through console or SSH and go to exec mode. If you are trying to convert the primary AP to CAPWAP, then **hw-module session 0/x** will lead you to the controller CLI. To get to the AP CLI, type **wireless ewc-ap ap shell username [name]** where the default name is "**Cisco**" at the controller prompt and login to the Access Point shell.
   b. Execute **AP#ap-type capwap** CLI. This will change the AP Configuration to NOT Embedded Wireless Controller (EWC) and the Access Point will no longer participate in the primary election process.

# Determining image on the Access Point

TheCisco 1100 Series ISR access points can either have CAPWAP image or the Cisco Embedded Wireless Controller (EWC) image which is capable of running the virtual Wireless LAN controller function on the Access Point. By default, the C1131 AP is shipped with EWC pre-installed. The CCO image consists only of the EWC image. One can manually switch to CAPWAP mode.

To determine the image and capability of an Access Point, follow the procedure below:

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Login to the Access Point CLI using a console and type **AP#show version** and check the full output of show version. The default login credentials are Username:**Cisco** and Password:**Cisco**. | |
| **Step 2** | If **show version** output does not display AP Image Type and AP Configuration parameters | `EWC#show version`<br>`Cisco IOS XE Software, Version 17.07.01`<br>`Cisco IOS Software [Cupertino], C9800-AP` |

| | Command or Action | Purpose |
|---|---|---|
| | as highlighted below, it means that the AP is running the CAPWAP image and a conversion to Cisco Embedded Wireless Controller (EWC) is required if you want to run the controller function on the Access Point. To convert from a CAPWAP Access Point to Embedded Wireless Controller (EWC), go to Conversion section. | Software<br>(C9800-AP-K9_IOSXE-UNIVERSALK9-M),<br>Version 17.7.1, RELEASE SOFTWARE (fc5)<br>Technical Support:<br>http://www.cisco.com/techsupport<br>Copyright (c) 1986-2021 by Cisco Systems,<br>Inc.<br>Compiled Sat 04-Dec-21 13:58 by mcpre<br><br>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.<br><br>ROM: IOS-XE ROMMON<br>WLCC884.A110.045C uptime is 1 week, 3 days, 1 hour, 2 minutes<br>Uptime for this control processor is 1 week, 3 days, 1 hour, 8 minutes<br>System returned to ROM by reload<br>System image file is "/tmp/sw/rp/0/0/rp_wlc/mount/usr/binos/bin/linux_iosd-image"<br>Last reload reason: reload<br><br>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.<br><br>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.<br><br>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.<br><br>AIR License Level: AIR Network Essentials<br>Next reload AIR license Level: AIR |

| | Command or Action | Purpose |
|---|---|---|
| | | Network Essentials<br>cisco ISR-AP1101AX-K (VXE) processor (revision VXE) with 342303K bytes of memory.<br>Processor board ID 00<br>2048K bytes of non-volatile configuration memory.<br>1989868K bytes of physical memory.<br>100000K bytes of AP Images at ap_images:.<br>513300K bytes of Backup Controller Image at backup_image:.<br>7774207K bytes of virtual hard disk at bootflash:.<br>25000K bytes of Temp trace export at tmp_trace_export:.<br>Installation mode is BUNDLE<br><br>Configuration register is 0x2102 |

# Configuring Cisco Embedded Wireless Controller (EWC)

# Configuring the controller using day 0 wizard

To configure the Web user interface:

### Before you begin

- When the AP has rebooted in the Embedded Wireless Controller (EWC) mode, it broadcasts a provisioning SSID ending with the last digits of the MAC address. You can connect to provisioning SSID using the PSK **password**.
- You can then open a browser and be redirected to mywifi.cisco.com, which takes you to the AP web UI. Enter the username as **webui** and password as **cisco**.

**Note** The web redirection to the Embedded Wireless Controller (EWC) configuration portal only works if you are connected to the provisioning SSID. It does not work if your laptop is connected to another Wi-Fi network or on the wired network. You cannot configure the AP from the wired network even if you enter the EWC IP address when it is in day0 wizard provisioning mode

### Procedure

**Step 1** Log on to the controller and in the **Configuration Setup Wizard**, go to the **General Settings** page.

**Step 2** In the **Configuration Mode** option, select **Non Mesh** and enter the following fields:

a) **Host Name**: Enter the hostname.

b) **Note** As required by the End User License Agreement, please ensure appropriate country code selection so that the unleashed network does not violate local and national regulatory restrictions. Improper country code assignment can disrupt wireless transmissions and may result in government imposed penalties and sanctions on operators of wireless networks utilizing devices set to improper country codes.

**Country**: From the drop-down list, choose the appropriate country code.

c) In the **Management User Settings** section, enter the username and password.

d) In the **Wireless Management Settings** section, check the **DHCP** check box, to display the DHCP server IP address.

e) In the **Wireless Network** section, click **Add** to create at least one WLAN.

**Step 3** Click **Finish**.

# Using internal DHCP server on Cisco Mobility Express

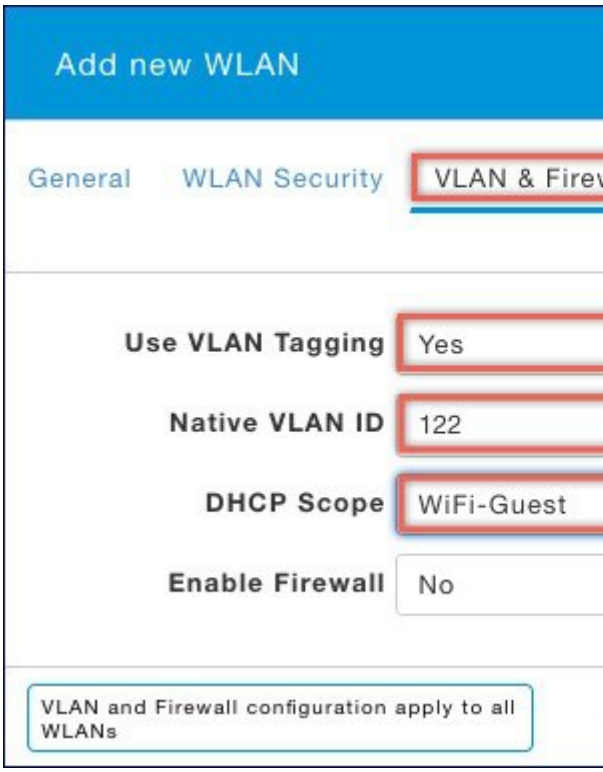
## Creating a DHCP Scope

Internal DHCP server can be enabled and DHCP scope created during Day 0 from Setup Wizard as well as in Day 1 using the controller WebUI. Typically, one would create DHCP scopes in Day 1 if they want to associate the scopes with WLANs.

To create a scope and associate it to a WLAN using the controller WebUI, follow the procedure below:

**Procedure**

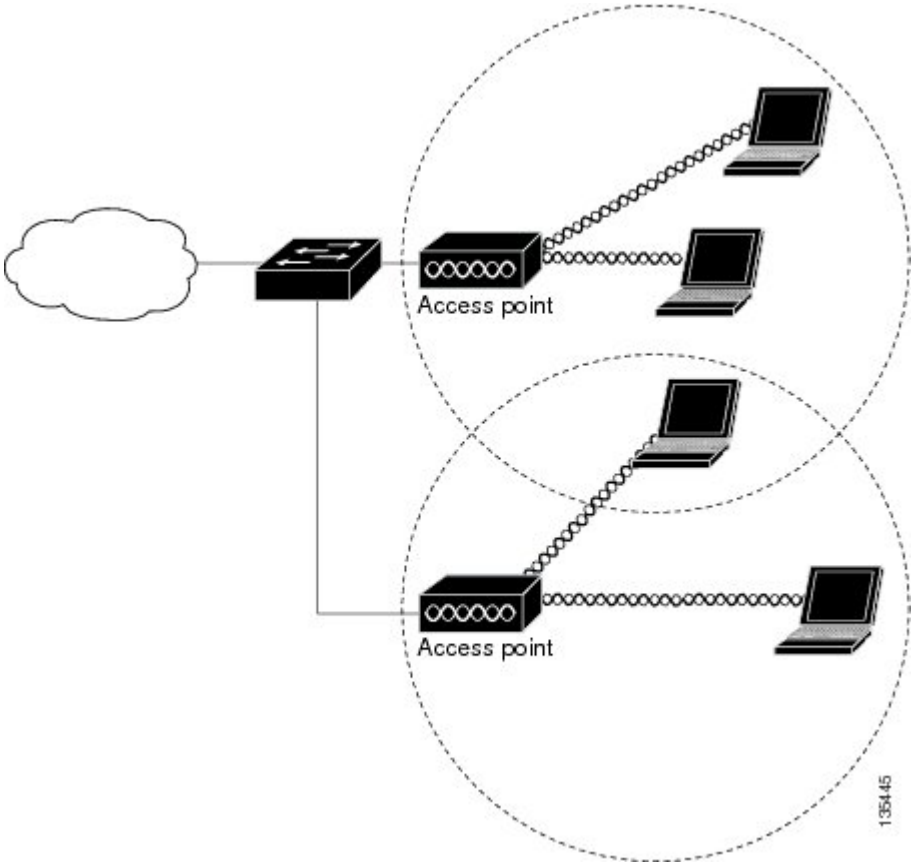
| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Navigate to Wireless Settings > DHCP Server > Add new Pool . The Add DHCP Pool window will pop up. | |
| **Step 2** | On the Add DHCP Pool window. Enter the following fields: | • Enter the Pool Name for the WLAN<br>• Enable the Pool Status<br>• Enter the VLAN ID for the WLAN<br>• Enter the Lease Period for the DHCP clients. Default is 1 Day<br>• Enter the Network/Mask<br>• Enter the Start IP for the DHCP pool<br>• Enter the End IP for the DHCP pool<br>• Enter the Gateway IP for the DHCP pool<br>• Enter the Domain Name (Optional) for the DHCP pool |

| | Command or Action | Purpose |
|---|---|---|
| | | • For Name Servers, select User Defined if one needs to enter IP addresses of Name Servers or select OpenDNS in which case OpenDNS Name Server IP addresses are automatically populated |
| **Step 3** | Click Apply. | |
| **Step 4** | After creating the scope, it is time to assign the VLAN mapped to the DHCP scope to the WLAN. To assign a VLAN to WLAN, navigate to Wireless Settings > WLANs . | |
| **Step 5** | If the WLAN does not exist, create a WLAN or if one does exist, edit the existing WLAN and click on the VLAN and Firewall tab. | |
| **Step 6** | On the VLAN and Firewall tab, configure the following: | • Select Yes for Use VLAN Tagging<br>• Enter the Native VLAN ID<br>• Select the DHCP Scope which was created previously for the WLAN. VLAN ID should be automatically populated after the DHCP scope is selected<br>  |
| **Step 7** | Click Apply. | |

# Access Points

An access point connected directly to a wired LAN provides a connection point for wireless users. If more than one access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. The figure below shows access points acting as root units on a wired LAN.

***Figure 8: Access Points as Root Units on a Wired LAN***




In an all-wireless network, an access point acts as a stand-alone root unit. The access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure below shows an access point in an all-wireless network.

## Configuring and Deploying the Access Point

This section describes how to connect the access point to a wireless LAN controller. The configuration process takes place on the controller. See the Cisco Wireless LAN Controller Configuration Guide for additional information.

## The Controller Discovery Process

The access point uses standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, inter-operable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP, and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

**Note** For additional information about the discovery process and CAPWAP, see the Cisco Wireless LAN Controller Software Configuration Guide. This document is available on Cisco.com.

**Note** CAPWAP support is provided in controller software release 8.5 or later. However, your controller must be running the release that supports Cisco 1100 Series access points.

**Note** You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

**Note** Make sure that the controller is set to the current time. If the controller is set to a time that has already passed, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- Layer 3 CAPWAP discovery—Can occur on different subnets than the access point and uses IP addresses and UDP packets.
- Locally stored controller IP address discovery—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the "Performing a Pre-Installation Configuration" section.

- DHCP server discovery—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43" section.
- DNS discovery—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name. Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

## Deploying the Access Point on the Wireless Network

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | Connect and power up the router. | |
| **Step 2** | Observe the wireless LAN LED (for LED descriptions, see "Checking the Wireless LAN LED" section ). | |
| **Step 3** | Reconfigure the Cisco wireless LAN controller so that it is not the primary controller. | **Note** A primary Cisco wireless LAN controller should be used only for configuring access points and not in a working network. |

# Checking the Wireless LAN LED

**Note** It is expected that there will be small variations in the LED color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect.

The wireless LAN status LED indicates various conditions which are described in Table.

LED port: WLAN (1 LED): 3-color LED: Green, Blue, Red

***Table 37: Wireless LAN LED***

| Message Type | LED State | Message Meanings |
|---|---|---|
| Association status | Green | Normal operating condition, but no wireless client associated. |
| | Blue | Normal operating condition, at least one wireless client association. |
| Boot loader status | Green | Executing boot loader |

| Message Type | LED State | Message Meanings |
|---|---|---|
| Boot loader error | Blinking Green | Boot loader signing verification failure |
| Operating status | Blinking Blue | Software upgrade in progress |
| | Alternating between Green and Red | Discovery/join process in progress |
| Access point operating system errors | Cycling through Red-Off-Green-Off-Blue-Off | General warning; insufficient inline power |

# Miscellaneous Usage and Configuration Guidelines

Using the reset command you can reset the AP to the default factory-shipped configuration.

```
hw-module subslot x/y error-recovery password_reset
```

**Note** Since this is an IOS command, you must run this command on the Cisco 1100 router console, instead of the AP console.

The AP configuration files are cleared. This resets all configuration settings to factory defaults, including passwords, encryption keys, the IP address, and the SSID. However, the regulatory domain provisioning is not reset.

**Note** When you run the **hw-module subslot x/y error-recovery password_reset** command, the AP module automatically reloads to restore the configuration settings and enters the maintenance mode. In the maintenance mode, the AP module is on power on mode. When the module configuration reset is confirmed through the console or web UI, the **hw-module subslot x/y reload force** command reloads the AP and then quits the maintenance mode.

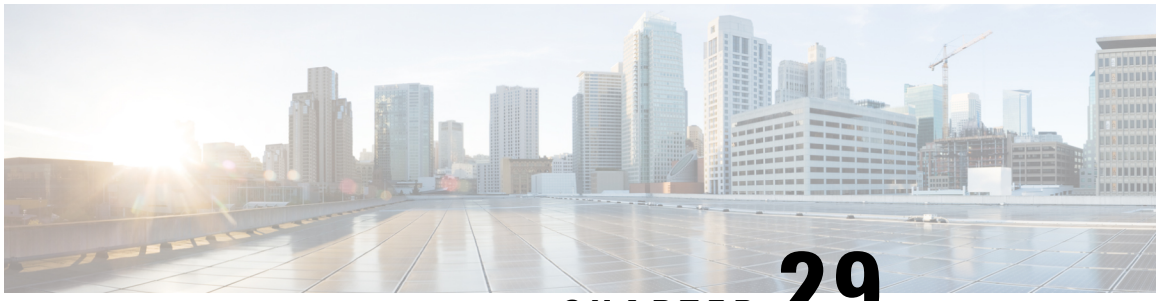
# Important Information for Controller-Based Deployments

Keep these guidelines in mind when you use the Cisco 1100 series access points:

- The access point can only communicate with Cisco wireless LAN controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

**Note** To configure the controller using day 0 wizard (GUI), follow the Non Mesh configuration steps only.

**Note** For more information on configuring the Embedded Wireless Networks, see the Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide.



CHAPTER 29

# Small Form-Factor Pluggables for Cisco ISR1000

Small Form-Factor Pluggables (SFPs) that are not Cisco certified are called third-party SFPs. Cisco approved means the SFPs have undergone rigorous testing with Cisco products and the SFPs are guaranteed to have 100% compatibility.

**Note** Cisco does not provide any kind of support for the third-party SFPs because they are not validated by Cisco.


- Configuring Third-Party SFPs, on page 451


# Configuring Third-Party SFPs

Third-party SFPs are manufactured by companies that are not on the Cisco-approved Vendor List (AVL). Currently, Cisco ISR1000 routers support only Cisco-approved SFPs. From Cisco IOS XE Fuji 16.9.1, Cisco ISR1000 routers recognize third-party SFPs.

### Procedure

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **configure terminal**<br>**Example:**<br>`Router# configure terminal` | Enters global configuration mode. |
| **Step 2** | **service unsupported-transceiver**<br>**Example:**<br>`Router(config)# service unsupported-transceiver` | Enables third-party SFP support. |
| **Step 3** | **interface type** *slot subslot port number*<br>**Example:**<br>`Router(config-if)# interface ethernet 0/3/0` | Selects an interface to configure. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 4** | **media-type sfp**<br>**Example:**<br>`Router(config-if)#media-type sfp` | Changes media type to SFP. |
| **Step 5** | **speed** *value*<br>**Example:**<br>`Router# speed 100` | Configures the speed of the interface.<br>**Note** For 100BASE SFPs, configure the speed to 100 Mbps only. Similarly, for 1000BASE SFPs, configure the speed to 1000 Mbps only. |
| **Step 6** | **shutdown**<br>**Example:**<br>`Router(config)# shutdown` | Disables the interface, changing its state from administratively UP to administratively DOWN. |
| **Step 7** | **no shutdown**<br>**Example:**<br>`Router(config-if)# no shutdown` | Enables the interface, changing its state from administratively DOWN to administratively UP. |
| **Step 8** | **exit**<br>**Example:**<br>`Router(config-if)#exit` | Exits the configuration mode and returns the global configuration mode. |

### Examples

This example shows how to configure a third-party SFP on a Cisco ISR1000 Series Router:

```
Router# configure terminal
Router(config)# interface ethernet 0/3/0
Router(config-if)# service unsupported-transceiver
Router(config)# interface ethernet 0/3/0
Router(config-if)# media-type sfp
Router(config-if)# speed 100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# exit
Router(config)# exit
```

CHAPTER 30

# Security Group Tagging

Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag (SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag.

Cisco TrustSec-capable devices have built-in hardware capabilities than can send and receive packets with SGT embedded in the MAC (L3) layer. This feature is called Layer 3 (L3)-SGT Imposition. It allows ethernet interfaces on the device to be enabled for L3-SGT imposition so that the device can insert an SGT in the packet to be carried to its next hop ethernet neighbor. SGT-over-Ethernet is a method of hop-by-hop propagation of SGT embedded in clear-text (unencrypted) ethernet packets. The inline identity propagation is scalable, provides near line-rate performance and avoids control plane overhead.

The Cisco TrustSec with SGT Exchange Protocol V4 (SXPv4) feature supports Cisco TrustSec metadata-based L3-SGT. When a packet enters a Cisco TrustSec-enabled interface, the IP-SGT mapping database (with dynamic entries built by SXP and/or static entries built by configuration commands) is analyzed to learn the SGT corresponding to the source IP address of the packet, which is then inserted into the packet and carried throughout the network within the Cisco TrustSec header.

As the tag represents the group of the source, the tag is also referred to as the Source Group Tag (SGT). At the egress edge of the network, the group assigned to the packet's destination becomes known. At this point, access control can be applied. With Cisco TrustSec, access control policies are defined between the security groups and are referred to as Security Group Access Control Lists (SGACL). From the view of any given packet, SGACL is simply being sourced from a security group and destined for another security group.

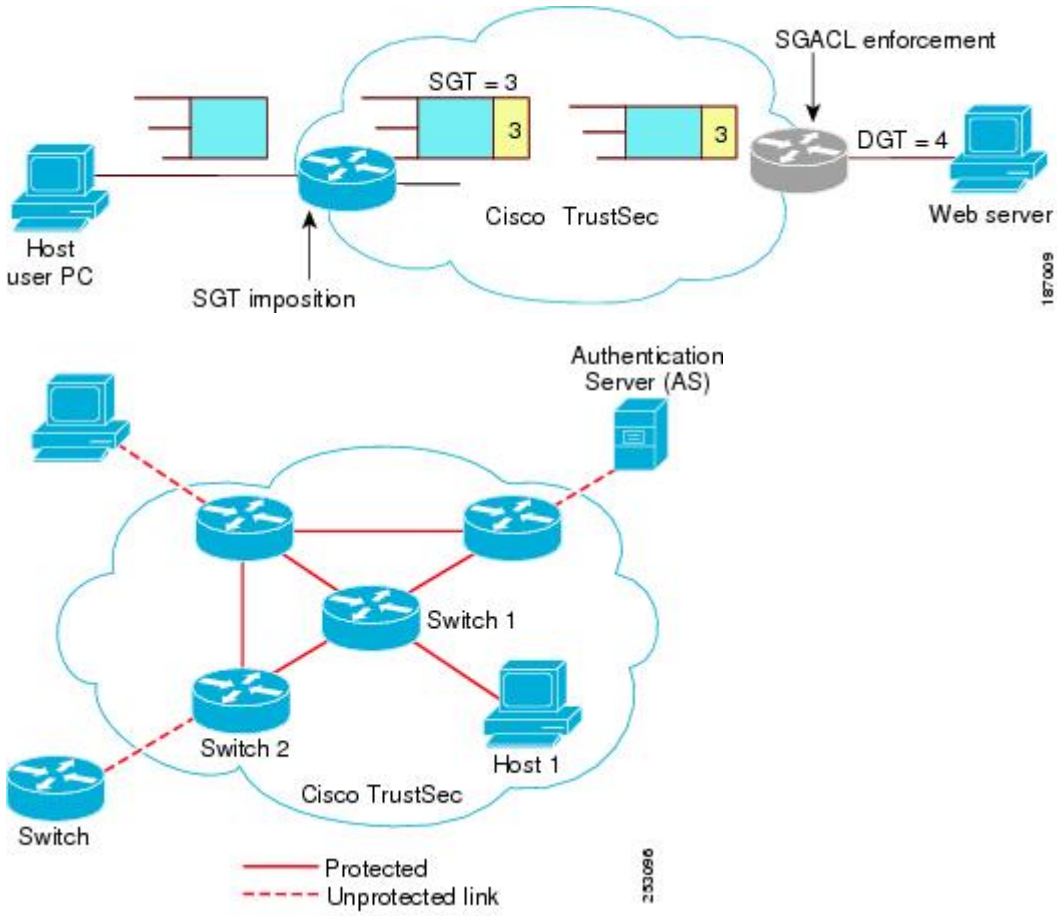
The SGT tag received in a packet from a trusted interface is propagated to the network, and is also be used for Identity firewall classification. When IPsec support is added, the received SGT tag is shared with IPSec for SGT tagging.

A network device at the ingress of Cisco TrustSec cloud needs to determine the SGT of the packet entering the Cisco TrustSec cloud so that it can tag the packet with that SGT when it forwards it into the Cisco TrustSec cloud. The SGT of a packet can be determined with these methods:

- SGT field on Cisco TrustSec header: If a packet is coming from a trusted peer device, it is assumed that the Cisco TrustSec header carries the correct SGT field. This situation applies to a network that is not the first network device in the Cisco TrustSec cloud for the packet.
- SGT lookup based on source IP address: In some cases, the administrator may manually configure a policy to decide the SGT of a packet based upon the source IP address. An IP address to SGT table can also be populated by the SXP protocol.

The following figures explains the topologies:

*Figure 9: Cisco TrustSec Network*





- Limitations for Security Group Tag, on page 454
- Configuring Security Group Tagging for Dynamic SGT and SGACL, on page 455
- Configuring SGT Tagging, on page 459
- Example 1: Static Security Group Tagging and Security Group ACL , on page 461
- Example 2: Dynamic Security Group Tagging and Security Group ACL, on page 461
- Troubleshoot the Security Group Tagging Configuration, on page 462
- Feature History for Cisco TrustSec, on page 462


# Limitations for Security Group Tag

The following are the limitations of the Cisco TrustSec feature:

- SGT and SGACL enforcement on switchport are not supported.
- Dynamic SGT and SGACL for ipv6 is not supported.
- The **cts manual** command is not support on SVI interface, while they are supported on on-board L3 interface.

# Configuring Security Group Tagging for Dynamic SGT and SGACL

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode. |
| **Step 3** | **aaa new-model**<br>**Example:**<br>`Device(config)# aa new-model` | Enables AAA.. |
| **Step 4** | **aaa authentication dot1x***{default \| listname}* **group***group-name*<br>**Example:**<br>`Device(config)# aaa authentication dot1x default group ise` | 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. |
| **Step 5** | **aaa authorization network***{default \| listname}***group** *group-name*<br>**Example:**<br>`Device(config)# aaa authentication network default group coa-ise` | 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. |
| **Step 6** | **dot1x system-auth-control**<br>**Example:**<br>`Device(config)# dot1x system-auth-control` | Globally enables 802.1X port-based authentication. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 7** | **dot1x system-auth-control**<br>**Example:**<br>`Device(config)# dot1x system-auth-control` | Globally enables 802.1X port-based authentication. |
| **Step 8** | **aaa group server radius {radius \| tacacs+}***group-name*<br>**Example:**<br>`Device(config)# aaa group server radius coa-ise` | Defines the AAA server group with a group name. Example: Device(config)# aaa group server radius group1 • All members of a group must be the same type, that is, RADIUS or TACACS+. This command puts the device in server group RADIUS configuration mode. |
| **Step 9** | **radius server** *server-name*<br>**Example:**<br>`Device(config)# radius server cts` | Specifies the name for the RADIUS server. |
| **Step 10** | **server** *ip-address***[ auth-port***port-number***[ acct-port***port-number*<br>**Example:**<br>`Device(config-sg-radius)# address ipv4 %{ise.ip} auth-port 1812 acct-port 1813` | Specifies the name for the RADIUS server. |
| **Step 11** | **pac key** *encyrption-key*<br>**Example:**<br>`Device(config-sg-radius)# pac key 0 cisco123` | Specifies the PAC encryption key (overrides the default).<br>• The encryption-key can be **0** (specifies that an unencrypted keys follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key. |
| **Step 12** | **policy-map type control subscriber***control-policy-name*<br>**Example:**<br>`Device(config)# policy-map type control subscriber simple_dot1x` | Defines a control policy for subscriber sessions. |
| **Step 13** | **event** *event-name***[match-all \| match-first]**<br>**Example:** | Specifies the type of event that triggers actions in a control policy if conditions are met. |

| | Command or Action | Purpose |
|---|---|---|
| | `Device(config-event-control-policymap)# event session-started match-all` | • match-all is the default behavior. |
| **Step 14** | **priority-number class {control-class-name \| always}[do-all \| do-until-failure \| do-until-success]**<br>**Example:**<br>`Device(config-event-control-policymap)# 10 class always do-until-failur` | Associates a control class with one or more actions in a control policy.<br>• A named control class must first be configured before specifying it with the control-class-name argument..<br>• do-until-failure is the default behavior. |
| **Step 15** | **action-number authenticate using {dot1x \| mab \| webauth}aaa {authc-list authc-list-name \| authz-list authz-list-name]} [merge] [parameter-map map-name] [priority priority-number] [replace \| replace-all] [retries number {retry-time seconds}**<br>**Example:**<br>`Device(config-event-control-policymap)# 10 authenticate using dot1x` | Optional) Initiates the authentication of a subscriber session using the specified method. |
| **Step 16** | **interface** *interface-id*<br>**Example:**<br>`Device(config)# interface gigabitethernet0/1` | Enter the interface to be added to the VLAN. |
| **Step 17** | **switchport access vlan** *vlan-id*<br>**Example:**<br>`Device(config-if)# switchport access vlan 22` | Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094 |
| **Step 18** | **switchport access mode**<br>**Example:**<br>`Device(config-if)# switchport mode access` | Assign the port to a VLAN. Valid VLAN IDs are 1 to 4094 |

| | Command or Action | Purpose |
|---|---|---|
| **Step 19** | **access-session closed**<br>**Example:**<br>`Device(config-if)# access-session closed` | The **access-session closed** command closes access to a port, preventing clients or devices from gaining network access before authentication is performed. |
| **Step 20** | **access-session port-control {auto \| force-authorized \| force-unauthorized }**<br>**Example:**<br>`Device(config-if)# access-session port-control auto` | Sets the authorization state of a port. |
| **Step 21** | **policy-map type control subscriber***control-policy-name*<br>**Example:**<br>`Device(config-if)# policy-map type control subscriber simple_coa` | Defines a control policy for subscriber sessions. |
| **Step 22** | **dot1x pae [supplicant \| authenticator \| both ]**<br>**Example:**<br>`Device(config-if)# dot1x pae authenticator` | [authenticator \|<br>Sets the Port Access Entity (PAE) type.<br>• supplicant—The interface acts only as a supplicant and does not respond to messages that are meant for an authenticator.<br>• authenticator-—The interface acts only as an authenticator and does not respond to any messages meant for a supplicant.<br>• both—The interface behaves both as a supplicant and as an authenticator and thus does respond to all dot1x messages. |
| **Step 23** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode. |

# Configuring SGT Tagging

**Procedure**

| | Command or Action | Purpose |
|---|---|---|
| **Step 1** | **enable**<br>**Example:**<br>`Device> enable` | Enables privileged EXEC mode.<br>Enter your password if prompted. |
| **Step 2** | **configure terminal**<br>**Example:**<br>`Device# configure terminal` | Enters global configuration mode.<br>aaa authorization network cts-list group |
| **Step 3** | **aaa authorization network***{default \| lcts-list}* **group***group-name*<br>**Example:**<br>`Device(config)# aaa authorization network cts-list group coa-ise` | Configures the device to use RADIUS authorization for all network-related service requests. |
| **Step 4** | **cts authorization list***mlist*<br>**Example:**<br>`Device(config)# cts authorization list cts-list` | Specifies a Cisco TrustSec AAA server group. Non-seed devices will obtain the server list from the authenticator. |
| **Step 5** | **cts sgt** *{sgt_number}*<br>**Example:**<br>`Device(config)# cts sgt 4` | Enables Cisco TrustSec. |
| **Step 6** | **interface** *interface-id***VLAN***VLAN-id*<br>**Example:**<br>`Device(config)# interface Vlan32` | Enter the interface to be added to the VLAN. |
| **Step 7** | **cts role-based {sgt-map \|sgt }**<br>**Example:**<br>`Device(config-if)# cts role-based sgt-map sgt` | Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.. |

| | Command or Action | Purpose |
|---|---|---|
| **Step 8** | **cts role-based enforcement**<br>**Example:**<br>`Device(configif)# cts role-based enforcement` | Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list. |
| **Step 9** | **ip access-list role-based** *rbacl-name*<br>**Example:**<br>`Device(configif)# ip access-list role-based sgacl1` | Creates a Role-based ACL and enters Role-based ACL configuration mode. |
| **Step 10** | **access-list permit icmp**<br>**Example:**<br>`Device(config-rb-acl)# 10 permit icmp` | |
| **Step 11** | **ipv6 access-list role-based** *rbacl-name*<br>**Example:**<br>`Device(configif-rb-acl)# ipv6 access-list role-based v6_acl` | Creates a Role-based ACL and enters Role-based ACL configuration mode. |
| **Step 12** | **sequence 10 permit icmp echo-reply** *ip-address*<br>**Example:**<br>`Device(configif-rb-acl)# sequence 10 permit icmp echo-reply` | |
| **Step 13** | **exit**<br>**Example:**<br>`Device(configif-rb-acl)# exit` | |
| **Step 14** | **cts role-based monitor enable** *from {sgt_num} to {dgt_num}***[ipv4 \| ipv6]**<br>**Example:**<br>`Device(configif)# cts role-based monitor enable from 4 to 32 sgacl1` | Enables monitor mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4 \| ipv6] Step 4 Group Tag (SGT)- Destination Group Tag (DGT) pair). |

| | Command or Action | Purpose |
|---|---|---|
| **Step 15** | **cts role-based permissions** *from {sgt_num} to {dgt_num}***[ipv4 \| ipv6]**<br>**Example:**<br>`Device(configif)# cts role-based permissions from 4 to 32 ipv6 v6_acl` | Enables role-base permissions mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4 \| ipv6] Step 4 Group Tag (SGT)-Destination Group Tag (DGT) pair). |
| **Step 16** | **end**<br>**Example:**<br>`Device(config-if)# end` | Exits Cisco TrustSec manual interface configuration mode and enters privileged EXEC mode. |

# Example 1: Static Security Group Tagging and Security Group ACL

This example shows how to enable an interface on the device for L3-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec.

```
Device# configure terminal
Device(config)# cts authorization list cts-list
Device(config)#cts sgt 4
Device(config)#interface Vlan32
Device(config-if)#ip address 192.168.32.2 255.255.255.0
Device(config-if)#ipv6 address 2001:DB8::1
Device(config-if)#cts role-based sgt-map sgt 32
Device(config-if)#cts role-based enforcement
Device(config-if)#ip access-list role-based sgacl1
Device(config-rb-acl#10 permit icmp
Device(config-rb-acl)#exit
Device(config)#ipv6 access-list role-based v6_acl
Device(config-rb-acl)#sequence 10 permit icmp echo-reply
Device(config-rb-acl)#cts role-based permissions from 4 to 32 sgacl1
Device(config-rb-acl)#cts role-based permissions from 4 to 32 ipv6 v6_acl
```

# Example 2: Dynamic Security Group Tagging and Security Group ACL

This example shows how to enable an interface on the device for L3-SGT tagging or imposition and defines whether the interface is trusted for Cisco TrustSec.

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)#aaa authentication dot1x default group coa-ise
Device(config)#aaa authorization network default group coa-ise
Device(config)#dot1x system-auth-control
```

```
Device(config)#aaa group server radius coa-ise
Device(config)#server name coa
Device(config)#radius server coa
Device(config-sg-radius)#address ipv4 %{ise.ip} auth-port 1812 acct-port 1813
Device(config-sg-radius)#pac key 0 cisco123
Device(config-sg-radius)#exit
Device(config)#policy-map type control subscriber simple_coa
Device(config)#event session-started match-all
Device(config)#10 class always do-until-failure
Device(config)#10 authenticate using dot1x
Device(config)#interface gigabitethernet0/1
Device(config-if)#switchport access vlan 22
Device(config-if)#switchport mode access
Device(config-if)#access-session closed
Device(config-if)#access-session port-control auto
Device(config-if)#dot1x pae authenticator
Device(config-if)#service-policy type control subscriber simple_coa
```

**Note** The Dynamic Security Group Tagging and Security Group ACL are configured on ISE server, after the 802.1x client is authenticated by ISE server. Subsequently, the corresponding SGT and SGACL will be downloaded from ISE and applied to the client.

# Troubleshoot the Security Group Tagging Configuration

You can use the following commands to troubleshoot the Cisco TrustSec configuration:

- **debug cts all**
- **debug rbm bindings debug**
- **debug condition interface <intf-name>**
- deb cts authorization events verbose
- **debug radius**

# Feature History for Cisco TrustSec

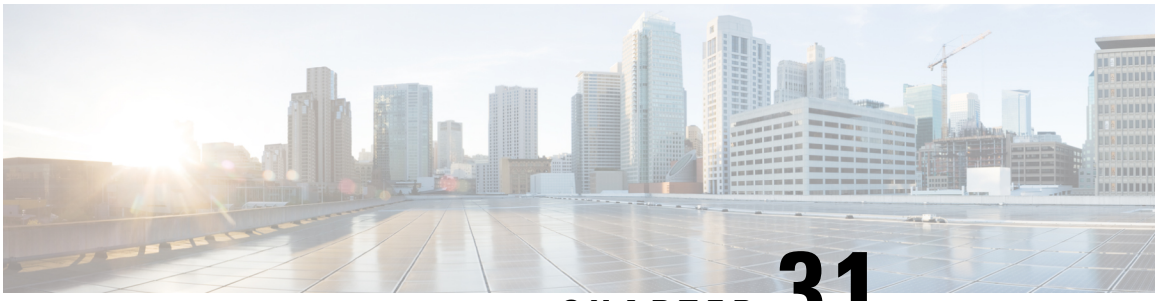
This table provides release and related information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

*Table 38: Feature Information for Cisco TrustSec*

| Feature Name | Releases | Feature Informatio |
|---|---|---|
| Cisco TrustSec Support on Cisco 1000 Series ISR SVI interface | IOS XE 17.5.1a | Each security group in a Cisco TrustSec domain is assigned a unique 16 bit tag called the Security Group Tag.<br>(SGT). The SGT is a single label indicating the privileges of the source within the entire network. It is in turn propagated between network hops allowing any intermediary devices (switches, routers) to enforce polices based on the identity tag. |

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.



CHAPTER 31

# System Messages

This chapter contains the following sections:


- Information About Process Management, on page 465
- How to Find Error Message Details, on page 465


## Information About Process Management

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

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

## How to Find Error Message Details

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

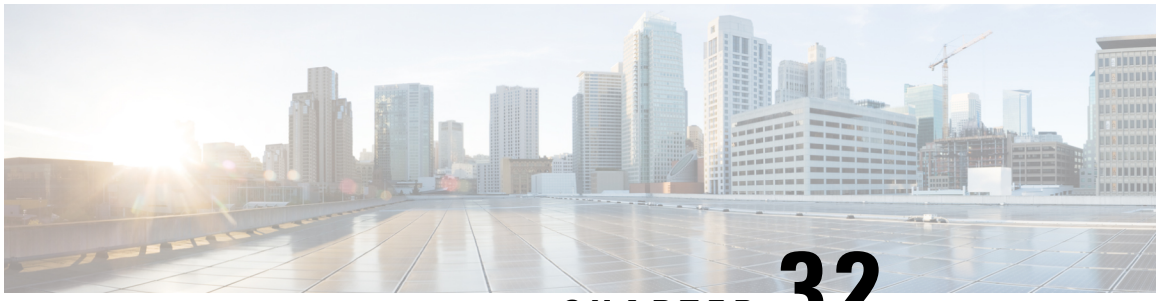
**Error Message**: `%PMAN-6-PROCSTART : The process [chars] has started`

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

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

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

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



CHAPTER 32

# Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a terminal or PC to the router by using the light-blue console port. With a connected terminal or PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface (Ethernet, ADSL, or telephone) by using Telnet. The Telnet option assumes that the interface is up and running.


- Before Contacting Cisco or Your Reseller, on page 471
- ADSL Troubleshooting, on page 472
- SHDSL Troubleshooting, on page 472
- VDSL2 Troubleshooting, on page 472
- show interfaces Troubleshooting Command, on page 473
- ATM Troubleshooting Commands, on page 475
- System Report, on page 479
- Software Upgrade Methods, on page 480
- Recovering a Lost Password, on page 481
- References, on page 486


# 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

# ADSL Troubleshooting

If you experience trouble with the ADSL connection, verify the following:

- The ADSL line is connected and is using pins 3 and 4. For more information on the ADSL connection, see the hardware guide for your router.
- The ADSL CD LED is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the ADSL LEDs, see the hardware installation guide specific for your router.
- The correct Asynchronous Transfer Mode (ATM) virtual path identifier/virtual circuit identifier (VPI/VCI) is being used.
- The DSLAM supports discrete multi-tone (DMT) Issue 2.
- The ADSL cable that you connect to the Cisco router must be 10BASE-T Category 5, unshielded twisted-pair (UTP) cable. Using regular telephone cable can introduce line errors.

# SHDSL Troubleshooting

Symmetrical high-data-rate digital subscriber line (SHDSL) is available on the Cisco 1000 Integrated Services Routes. If you experience trouble with the SHDSL connection, verify the following:

- The SHDSL line is connected and using pins 3 and 4. For more information on the G.SHDSL connection, see the hardware guide for your router.
- The G.SHDSL LED is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the G.SHDSL LED, see the hardware installation guide specific for your router.
- The correct asynchronous transfer mode (ATM) virtual path identifier/virtual circuit identifier (VPI/VCI) is being used.
- The DSLAM supports the G.SHDSL signaling protocol.

Use the **show controllers dsl 0** command in EXEC mode to view an SHDSL configuration.

# VDSL2 Troubleshooting

Very-high-data-rate digital subscriber line 2 (VDSL2) is available on the Cisco 1000 Series Integrated Services Routers. If you experience trouble with the VDSL2 connection, verify the following:

- The VDSL2 line is connected and using pins 3 and 4. For more information on the VDSL2 connection, see the hardware guide for your router.
- The VDSL2 LED CD light is on. If it is not on, the router may not be connected to the DSL access multiplexer (DSLAM). For more information on the VDSL2 LED, see the hardware installation guide specific for your router.
- The DSLAM supports the VDSL2 signaling protocol.

Use the **show controllers vdsl 0** command in EXEC mode to view a VDSL2 configuration. The debug vdsl 0 daemon state command can be used to enable the debug messages that print the state transition of VDSL2 training.

If there is trouble with the VDSL firmware file, you can reload or upgrade it without upgrading your Cisco IOS image. Use the command:

**controller vdsl 0 firmware** *flash:<firmware file name>*

to load the firmware file into the VDSL modem chipset. Then enter shutdown/no shutdown commands on the controller vdsl 0 interface. After this, the new firmware will be downloaded and the VDSL2 line starts training up.

**Note** Cisco 1000 series ISRs require that the router be reloaded (IOS reload) before the new VDSL firmware will be loaded.

If the command is not present or the named firmware file is corrupt or not available, the default firmware file *flash:vdsl.bin* is checked to be present and not corrupt. The firmware in this file is then downloaded to the modem chipset.

**Note** Cisco 1000 series ISRs will state the reason of failure during bootup if the new VDSL firmware fails to load after IOS reload.

# show interfaces Troubleshooting Command

Use the **show interface**s command to display the status of all physical ports (Ethernet, Fast Ethernet, and ATM) and logical interfaces on the router. Table 39: show interfaces Command Output Description , on page 474describes messages in the command output.

The following example shows how to view the status of Ethernet or Fast Ethernet Interfaces:

```
Router# show interfaces ethernet 0 **similar output for show interfaces fastethernet 0
command **
Ethernet0 is up, line protocol is up
Hardware is PQUICC Ethernet, address is 0000.0c13.a4db
(bia0010.9181.1281)
Internet address is 192.0.2.1/24
MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
 reliability 255/255., txload 1/255, rxload 1/255
 Encapsulation ARPA, loopback not set
 Keepalive set (10 sec)
```

The following example shows how to view the status of ATM Interfaces:

```
Router# show interfaces atm 0
ATM0 is up, line protocol is up
  Hardware is PQUICC_SAR (with Alcatel ADSL Module)
  Internet address is 192.0.2.1/8
  MTU 1500 bytes, sub MTU 1500, BW 640 Kbit, DLY 80 usec,
     reliability 40/255, txload 1/255, rxload 1/255
  Encapsulation ATM, loopback not set
  Keepalive not supported
  Encapsulation(s):AAL5, PVC mode
  10 maximum active VCs, 1 current VCCs
  VC idle disconnect time:300 seconds
  Last input 01:16:31, output 01:16:31, output hang never
  Last clearing of "show interface" counters never
  Input queue:0/75/0 (size/max/drops); Total output drops:0
  Queueing strategy:Per VC Queueing
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     512 packets input, 59780 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 1024 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     426 packets output, 46282 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to view the status of Dialer Interfaces:

```
Router# show interfaces dialer 1
Dialer 1 is up, line protocol is up
 Hardware is Dialer interface
 Internet address is 10.0.0.1/24
 MTU 1500 bytes, BW 100000 Kbit, DLY 100000 usec, reliability
  255/255. txload 1/255, rxload 1/255
 Encapsulation PPP, loopback not set
 Keepalive set (10 sec)
DTR is pulsed for 5 seconds on reset
LCP Closed
```

The table below describes possible command output for the **show interfaces** command.

***Table 39: show interfaces Command Output Description***

| Output | Cause |
|---|---|
| For ATM Interfaces | |
| ATM 0 is up, line protocol is up | The ATM line is up and operating correctly. |
| ATM 0 is down, line protocol is down | • The ATM interface has been disabled with the shutdown command.<br>or<br>• The ATM line is down, possibly because the ADSL cable is disconnected or because the wrong type of cable is connected to the ATM port. |
| ATM 0.*n* is up, line protocol is up | The specified ATM subinterface is up and operating correctly. |
| ATM 0.*n* is administratively down, line protocol is down | The specified ATM subinterface has been disabled with the shutdown command. |
| ATM 0.*n* is down, line protocol is down | The specified ATM subinterface is down, possibly because the ATM line has been disconnected (by the service provider). |
| For Ethernet/Fast Ethernet Interfaces | |
| Ethernet/Fast Ethernet *n* is up, line protocol is up | The specified Ethernet/Fast Ethernet interface is connected to the network and operating correctly. |
| Ethernet/Fast Ethernet *n* is up, line protocol is down | The specified Ethernet/Fast Ethernet interface has been correctly configured and enabled, but the Ethernet cable might be disconnected from the LAN. |

| Output | Cause |
|---|---|
| Ethernet/Fast Ethernet *n* is administratively down, line protocol is down | The specified Ethernet/Fast Ethernet interface has been disabled with the **shutdown** command, and the interface is disconnected. |
| For Dialer Interfaces | |
| Dialer *n* is up, line protocol is up | The specified dialer interface is up and operating correctly. |
| Dialer *n* is down, line protocol is down | • This is a standard message and may not indicate anything is actually wrong with the configuration.<br>or<br>• If you are having problems with the specified dialer interface, this can mean it is not operating, possibly because the interface has been brought down with the **shutdown** command, or the ADSL cable is disconnected. |

# ATM Troubleshooting Commands

Use the following commands to troubleshoot your ATM interface:

## ping atm interface Command

Use the **ping atm interface** command to determine whether a particular PVC is in use. The PVC does not need to be configured on the router to use this command. The below example shows the use of this command to determine whether PVC 8/35 is in use.

The following example shows how to determine if a PVC is in use:

```
Router# ping atm interface atm 0 8 35 seg-loopback

Type escape sequence to abort.
Sending 5, 53-byte segment OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 148/148/148 ms
```

This command sends five OAM F5 loopback packets to the DSLAM (segment OAM packets). If the PVC is configured at the DSLAM, the ping is successful.

To test whether the PVC is being used at the aggregator, enter the following command:

```
Router# ping atm interface atm 0 8 35 end-loopback

Type escape sequence to abort.
Sending 5, 53-byte end-to-end OAM echoes, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 400/401/404 ms
```

This command sends end-to-end OAM F5 packets, which are echoed back by the aggregator.

# show atm interface Command

To display ATM-specific information about an ATM interface, use the **show atm interface atm 0 command from** privileged EXEC mode.

The following example shows how to view information about an ATM interface:

```
Router# show atm interface atm 0
Interface ATM0:
AAL enabled: AAL5 , Maximum VCs:11, Current VCCs:0
Maximum Transmit Channels:0
Max. Datagram Size:1528
PLIM Type:INVALID - 640Kbps, Framing is INVALID,
DS3 lbo:short, TX clocking:LINE
0 input, 0 output, 0 IN fast, 0 OUT fast
Avail bw = 640
Config. is ACTIVE
```

The table below describes some of the fields shown in the command output.

***Table 40: show atm interface Command Output Description***

| Field | Description |
|---|---|
| ATM interface | Interface number. Always 0 for the Cisco 860 and Cisco 880 series access routers. |
| AAL enabled | Type of AAL enabled. The Cisco 860 and Cisco 880 series access routers support AAL5. |
| Maximum VCs | Maximum number of virtual connections this interface supports. |
| Current VCCs | Number of active virtual channel connections (VCCs). |
| Maximum Transmit Channels | Maximum number of transmit channels. |
| Max Datagram Size | Configured maximum number of bytes in the largest datagram. |
| PLIM Type | Physical layer interface module (PLIM) type. |

# debug atm Commands

Use the **debug** commands to troubleshoot configuration problems that you might be having on your network. The **debug** commands provide extensive, informative displays to help you interpret any possible problems.

## Guidelines for Using Debug Commands

Read the following guidelines before using debug commands to ensure appropriate results.

- All debug commands are entered in privileged EXEC mode.
- To view debugging messages on a console, enter the **logging console debug** command.
- Most **debug** commands take no arguments.
- To disable debugging, enter the **undebug all** command.
- To use **debug** commands during a Telnet session on your router, enter the **terminal monitor** command.

**Caution** Debugging is assigned a high priority in your router CPU process, and it can render your router unusable. For this reason, use **debug** commands only to troubleshoot specific problems. The best time to use debug commands is during periods of low network traffic so that other activity on the network is not adversely affected.

You can find additional information and documentation about the **debug** commands in the Cisco IOS Debug Command Reference.

## debug atm errors Command

Use the **debug atm errors** command to display ATM errors. The **no** form of this command disables debugging output.

The following example shows how to view the ATM errors:

```
Router# debug atm errors
ATM errors debugging is on
Router#
01:32:02:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:04:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:06:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:08:ATM(ATM0.2):VC(3) Bad SAP received 4500
01:32:10:ATM(ATM0.2):VC(3) Bad SAP received 4500
```

## debug atm events Command

Use the **debug atm events** command to display events that occur on the ATM interface processor and to diagnose problems in an ATM network. This command provides an overall picture of the stability of the network. The **no** form of this command disables debugging output.

If the interface is successfully communicating with the Digital Subscriber Line Access Multiplexer (DSLAM) at the telephone company, the modem state is 0x10. If the interface is not communicating with the DSLAM, the modem state is 0x8. Note that the modem state does not transition to 0x10.

The following example shows how to view the ATM interface processor events-success:

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:02: DSL: 2: Modem state = 0x10
00:03:05: DSL: 3: Modem state = 0x10
00:03:07: DSL: 4: Modem state = 0x10
00:03:09: DSL: Received response: 0x24
00:03:09: DSL: Showtime!
00:03:09: DSL: Sent command 0x11
00:03:09: DSL: Received response: 0x61
```

```
00:03:09: DSL: Read firmware revision 0x1A04
00:03:09: DSL: Sent command 0x31
00:03:09: DSL: Received response: 0x12
00:03:09: DSL: operation mode 0x0001
00:03:09: DSL: SM: [DMTDSL_DO_OPEN -> DMTDSL_SHOWTIME]
```

The following example shows how to view the ATM interface processor events—failure:

```
Router# debug atm events
Router#
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:02:57: DSL: Received response: 0x26
00:02:57: DSL: Unexpected response 0x26
00:02:57: DSL: Send ADSL_OPEN command.
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Using subfunction 0xA
00:02:57: DSL: Sent command 0x5
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
00:03:00: DSL: 1: Modem state = 0x8
```

## debug atm packet Command

Use the **debug atm packet** command to display all process-level ATM packets for both outbound and inbound packets. The output reports information online when a packet is received or a transmission is attempted. The **no** form of this command disables debugging output.

**Caution** Because the **debug atm packet** command generates a significant amount of output for every packet processed, use it only when network traffic is low, so that other system activities are not adversely affected.

The command syntax is:

debug atm **packet** [**interface atm** *number* [**vcd** *vcd-number* ][**vc** *vpi/vci number*]]

no debug atm **packet** [**interface atm** *number* [**vcd** *vcd-number* ][**vc** *vpi/vci number*]]

where the keywords are defined as follows:

**interface atm** *number* (Optional) ATM interface or subinterface number.

**vcd** *vcd-number* (Optional) Number of the virtual circuit designator (VCD).

**vc** *vpi/vci number* VPI/VCI value of the ATM PVC.

The below example shows sample output for the **debug atm packet** command.

```
Router# debug atm packet
Router#
01:23:48:ATM0(O):
VCD:0x1 VPI:0x1 VCI:0x64 DM:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FF01 9F80 0E00 0010 0E00 0001 0800 A103 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
```

```
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
01:23:48:ATM0(I):
VCD:0x1 VPI:0x1 VCI:0x64 Type:0x0 SAP:AAAA CTL:03 OUI:000000 TYPE:0800 Length:0x70
01:23:48:4500 0064 0008 0000 FE01 A080 0E00 0001 0E00 0010 0000 A903 0AF3 17F7 0000
01:23:48:0000 004C BA10 ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD ABCD
01:23:48:ABCD ABCD ABCD ABCD ABCD
01:23:48:
```

The table below describes some of the fields shown in the **debug atm packet** command output.

***Table 41: debug atm packet Command Output Description***

| Field | Description |
|---|---|
| ATM0 | Interface that is generating the packet. |
| (O) | Output packet. (I) would mean receive packet. |
| VCD: 0x*n* | Virtual circuit associated with this packet, where *n* is some value. |
| VPI: 0x*n* | Virtual path identifier for this packet, where *n* is some value. |
| DM: 0x*n* | Descriptor mode bits, where *n* is some value. |
| Length: *n* | Total length of the packet (in bytes) including the ATM headers. |

# System Report

System reports or crashinfo files save information that helps Cisco technical support representatives to debug problems that caused the Cisco IOS image to crash. It is necessary to collect critical crash information quickly and reliably and bundle it in a way that it can be identified with a specific crash occurrence. System reports are generated and saved into the '/core' directory, either on harddisk: or flash: filesystem. The system does not generate reports in case of a reload.

In case of a system crash, the following details are collected:

1. Full process core
    - IOSd core file and IOS crashinfo file if there was an IOSd process crash
2. Tracelogs
3. System process information
4. Bootup logs
5. Certain types of /proc information

This report is generated before the router goes down to rommon/bootloader. The information is stored in separate files which are then archived and compressed into the tar.gz bundle. This makes it convenient to get a crash snapshot in one place, and can be then moved off the box for analysis.

Device hostname, the ID of the module that generated the system report and its creation timestamp are embedded in the file name:

```
<hostname>_<moduleID>-system-report_<timestamp>.tar.gz
```

Example:

Router1_RP_0-system-report_20210204-163559-UTC

A device with hostname Router1 experienced an unexpected reload of RP0 module and the system-report was generated on 4th February 2021 at 4:39:59 PM UTC.

```
├── bootflash/
│   └── pd_info/
│       ├── dmesg_output-20210204-163538-UTC.log
│       ├── filesystems-20210204-163538-UTC.log
│       ├── memaudit-20210204-163538-UTC.log
│       ├── proc_cpuinfo-20210204-163538-UTC.log
│       ├── proc_diskstats-20210204-163538-UTC.log
│       ├── proc_interrupts-20210204-163538-UTC.log
│       ├── proc_oom_stats-20210204-163538-UTC.log
│       ├── proc_softirqs-20210204-163538-UTC.log
│       ├── system_report_trigger.log
│       └── top_output-20210204-163538-UTC.log
├── harddisk/
│   ├── core/
│   │   └── Router1_RP_0_hman_17716_20210212-123836-UTC.core.gz
│   └── tracelogs/
├── tmp/
│   ├── fp/
│   │   └── trace/
│   ├── maroon_stats/
│   ├── rp/
│   │   └── trace/
│   └── Router1_RP_0-bootuplog-20210204-163559-UTC.log
└── var/
    └── log/
        └── audit/
            └── audit.log
```

# Software Upgrade Methods

Several methods are available for upgrading software on the Cisco 860 and Cisco 880 series Integrated Services Routers, including:

- Copy the new software image to flash memory over LAN or WAN when the existing Cisco IOS software image is in use.
- Copy the new software image to flash memory over the LAN while the boot image (ROM monitor) is operating.
- Copy the new software image over the console port while in ROM monitor mode.
- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.

# Recovering a Lost Password

To recover a lost enable or lost enable-secret password, refer to the following sections:

1. Change the Configuration Register
2. Reset the Router
3. Reset the Password and Save your Changes (for lost enable secret passwords only)
4. Reset the Configuration Register Value.

**Note** Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

**Tip** See the "Hot Tips" section on Cisco.com for additional information on replacing enable secret passwords.

## Change the Configuration Register

To change a configuration register, follow these steps:

**Procedure**

**Step 1** Connect an ASCII terminal or a PC running a terminal emulation program to the CONSOLE port on the Fthe router.

**Step 2** Configure the terminal to operate at 9600 baud, 8 data bits, no parity, and 1 stop bit.

**Step 3** At the privileged EXEC prompt (r*outer_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
.
.
.


Suite License Information for Module:'esg'

--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot
--------------------------------------------------------------------------------
FoundationSuiteK9     None                  None           None
securityk9
appxk9
```

```
Technology Package License Information:

------------------------------------------------------------------
Technology    Technology-package           Technology-package
              Current       Type           Next reboot
------------------------------------------------------------------
appxk9           None             None             None
securityk9       None             None             None
ipbase           ipbasek9         None             ipbasek9

cisco C1111-8PLTELAWN (1RU) processor with 1464345K/6147K bytes of memory.
Processor board ID FGL212392WT
8 Virtual Ethernet interfaces
11 Gigabit Ethernet interfaces
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
6762495K bytes of flash memory at bootflash:.
7855044K bytes of USB flash at usb0:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2100

Router#
```

**Step 4** Record the setting of the configuration register.

**Step 5** To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the **config-register 0x01** command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

## Reset the Router

To reset the router, follow these steps:

**Procedure**

**Step 1** If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

**Note** Some terminal keyboards have a key labeled *Break* . If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

**Step 2** Press break. The terminal displays the following prompt:

**Example:**

```
rommon 2>
```

**Step 3** Enter **confreg 0x142** to reset the configuration register:

**Example:**

```
rommon 2> confreg 0x142
```

**Step 4** Initialize the router by entering the **reset** command:

**Example:**

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

**Example:**

```
--- System Configuration Dialog ---
```

**Step 5** Enter **no** in response to the prompts until the following message is displayed:

**Example:**

```
Press RETURN to get started!
```

**Step 6** Press **Return**. The following prompt appears:

**Example:**

```
Router>
```

**Step 7** Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:

**Example:**

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

**Example:**

```
Router#
```

**Step 8** Enter the **show startup-config** command to display an enable password in the configuration file:

**Example:**

```
Router# show startup-config
```

### What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

# Reset the Router

To reset the router, follow these steps:

**Procedure**

**Step 1** If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (|) again. Within 60 seconds, press the **Break** key. The terminal displays the ROM monitor prompt.

**Note** Some terminal keyboards have a key labeled *Break* . If your keyboard does not have a Break key, see the documentation that came with the terminal for instructions on how to send a break.

**Step 2** Press break. The terminal displays the following prompt:

**Example:**

```
rommon 2>
```

**Step 3** Enter **confreg 0x142** to reset the configuration register:

**Example:**

```
rommon 2> confreg 0x142
```

**Step 4** Initialize the router by entering the **reset** command:

**Example:**

```
rommon 2> reset
```

The router cycles its power, and the configuration register is set to 0x142. The router uses the boot ROM system image, indicated by the system configuration dialog:

**Example:**

```
--- System Configuration Dialog ---
```

**Step 5** Enter **no** in response to the prompts until the following message is displayed:

**Example:**

```
Press RETURN to get started!
```

**Step 6** Press **Return**. The following prompt appears:

**Example:**

```
Router>
```

**Step 7** Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:

**Example:**

```
Router> enable
```

The prompt changes to the privileged EXEC prompt:

**Example:**

```
Router#
```

**Step 8** Enter the **show startup-config** command to display an enable password in the configuration file:

**Example:**

```
Router# show startup-config
```

### What to do next

If you are recovering an enable password, do not perform the steps in the Reset the Password and Save Your Changes section. Instead, complete the password recovery process by performing the steps in the Reset the Configuration Register Value section.

If you are recovering an enable secret password, it is not displayed in the **show startup-config** command output. Complete the password recovery process by performing the steps in the Reset the Password and Save Your Changes section.

# Reset the Password and Save Your Changes

To reset your password and save the changes, follow these steps:

### Procedure

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

**Example:**

```
Router# configure terminal
```

**Step 2** Enter the **enable secret** command to reset the enable secret password in the router:

**Example:**

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

**Step 3** Enter **exit** to exit global configuration mode:

**Example:**

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

**Step 4** Save your configuration changes:

**Example:**

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

# Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

**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.

# References

Refer to the following troubleshooting scenarios from the Cisco ISR guides:

- Monitor CPU Usage - http://www.cisco.com/c/en/us/support/docs/routers/4000-series-integrated-services-routers/210760-Monitor-CPU-Usage-On-ISR4300-Series.html
- Memory Troubleshooting Guide for Cisco 4000 Series ISRs - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/troubleshooting/memorytroubleshooting/isr4000_mem.html
- Stuck in ROMMON Trouble Shooting - http://www.cisco.com/c/en/us/support/docs/routers/4000-series-integrated-services-routers/200678-Troubleshoot-Cisco-4000-Series-ISR-Stuck.html
- Monitoring Control Plane Resource & Hardware Alarms Trouble Shooting - https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg/bm_isr_4400_sw_config_guide_chapter_01000.html#concept_5A8508E657FA48E7B9563BE9073D4884
- SFP Modules Maintenance and Troubleshooting - http://www.cisco.com/c/en/us/support/docs/interfaces-modules/cwdm-gbic-sfp/72370-sfp-trcvr-mods.html

- How to Find Error Message Details - https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg/bm_isr_4400_sw_config_guide_chapter_01001.html#concept_AD47EC93DC3D4557B99BC155B8BB68FA
- IOS XE Syslog Messages - http://www.cisco.com/c/en/us/td/docs/ios/system/messages/guide/xemsg01.html
- Debugging AppNav/AppNav-XE and ISR-WAAS - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/appnav/isr/isr_appnav/isr_trblshoot.html
- Troubleshooting for Cisco Smart Licensing Client - https://www.cisco.com/c/en/us/td/docs/routers/access/4400/software/configuration/guide/isr4400swcfg/isr4400swcfg_chapter_010011.html#reference_C0E7BB9ED86D4FA18202EE72E87EB3A9
- Retrieving the License and Configuration Files - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/flashmemory/isr4000_flashmem.html#72593
- Power and Cooling System Trouble Shooting - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/troubleshooting/guide/isr4400trbl.html
- T1/E1 Data Clocking Trouble Shooting and Configuration - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/feature/guide/isr4400netclock.html#54707
- Troubleshooting Layer 2/3 Switch SW - http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/eesm/software/configuration/guide/4451_config.html#pgfId-1000127
- Best Practices for Implementing WAN MACsec and MKA - http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-16/macsec-xe-16-book/wan-macsec-mka-support-enhance.html#reference_66BBEB1DDF3147DB8B89B6BB6CEBB7DC
- QoS FAQ - http://www.cisco.com/c/en/us/products/collateral/routers/asr-1000-series-aggregation-services-routers/q-and-a-c67-731655.html
- SNMB Notification - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/technical_references/4400_mib_guide/isr4400_MIB/4400mib_04.html#42335
- Monitoring router interface through MIB - http://www.cisco.com/c/en/us/td/docs/routers/access/4400/technical_references/4400_mib_guide/isr4400_MIB/4400mib_05.html#96205