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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

© 2018–2019 Cisco Systems, Inc. All rights reserved.
CONTENTS

Full Cisco Trademarks with Software License 7

CHAPTER 1

Introduction 1
Accessing the CLI Using a Router Console 2
  Using the Console Interface 4
Accessing the CLI from a Remote Console 5
  Preparing to Connect to the Router Console Using Telnet 5
  Using Telnet to Access a Console Interface 5
CLISessionManagement 6
  Information About CLISessionManagement 6
  Changing the CLISessionTimeout 7
  Locking a CLISession 7

CHAPTER 2

Using Cisco IOS XE Software 9
  Understanding Command Modes 9
  Keyboard Shortcuts 11
  Using the no and default Forms of Commands 11
  Using the History Buffer to Recall Commands 12
  Managing Configuration Files 12
  Saving Configuration Changes 12
  Filtering Output from the show and more Commands 13
  Finding Support Information for Platforms and Cisco Software Images 13
    Using Cisco Feature Navigator 14
    Getting Help 14
      Finding Command Options: Example 14
    Using Software Advisor 18
CHAPTER 3

Basic Router Configuration 19

IR1101 Interface Naming 19
Basic Configuration 19
Configuring Global Parameters 22
Configuring the Gigabit Ethernet Interface 23
Configuring a Loopback Interface 24
Enabling Cisco Discovery Protocol 26
Configuring Command-Line Access 26
Configuring Static Routes 28
Configuring Dynamic Routes 30
    Configuring Routing Information Protocol 30
    Configuring Enhanced Interior Gateway Routing Protocol 31
Configuring the Serial Interface 31
    Specifying an Asynchronous Serial Interface 32
    Specifying Asynchronous Serial Encapsulation 32
    Configuring the Serial Port 32

CHAPTER 4

Configuring Secure Shell 33

Information About Secure Shell 33
    Prerequisites for Configuring Secure Shell 33
    Restrictions for Configuring Secure Shell 33
    SSH And Router Access 34
    SSH Servers, Integrated Clients, and Supported Versions 34
    SSH Configuration Guidelines 35
How to Configure Secure Shell 35
    Setting Up the IR1101 to Run SSH 35
    Configuring the SSH Server 36
    Monitoring the SSH Configuration and Status 38
    Configuring the Router for Local Authentication and Authorization 38
Information about Secure Copy 40
    Prerequisites for Secure Copy 40
    Restrictions for Configuring Secure Copy 40
### CHAPTER 5

**Installing the Software** 43
- Installing the Software 43
- Licensing 43
  - Cisco Software Licensing 43
  - Consolidated Packages 44
  - Network-Essentials 44
  - Network-Advantage 44
  - Related Documentation 44
  - How to Install the Software for Cisco IOS XE 45
- ROMMON Images 46
- File Systems 46
- Autogenerated File Directories and Files 47
- Flash Storage 48
- LED Indicators 48
- Related Documentation 49

### CHAPTER 6

**Prerequisites for Smart Licensing** 51
- Information About Smart Licensing 51
- Overview of Cisco Smart Software Manager 52
- Deployment Options for IR1101 Licensing 52
- Specific License Reservation 52
- To Register a Device in Cisco Smart Software Manager 53
- Renewing Smart Licensing Registration 53
- Enabling Specific License Reservation and Generating a Request Code 54
- Reserving a License in Cisco Smart Software Manager 55
- Registering Device with Specific License Reservation 59
- Monitoring Smart Licensing Configuration 60
- Example: Registering Smart Licensing Enabled Device 61
- IR1101 Licensing for Cisco IOS-XE release 16.10.1 61

### CHAPTER 7

**Web User Interface Management** 69
### Contents

- **Using Web User Interface for Day One Setup** 69
- **Configure LAN Settings** 70
- **Configure Primary WAN Settings** 70
- **Configure Secondary WAN Settings** 71
- **Configure Security Settings** 72
- **Summary Screen** 72

### Chapter 8

- **Configuring Ethernet Switch Ports** 75
  - Configuring VLANs 75
  - VLAN Trunking Protocol (VTP) 76
  - Configuring 802.1x Authentication 77
  - Configuring Spanning Tree Protocol 78
  - Configuring MAC Address Table Manipulation 79
  - Configuring Switch Port Analyzer 80
  - Configuring IGMP Snooping 81

### Chapter 9

- **Cisco 4G LTE-Advanced Configuration** 83
  - Cisco Fourth-Generation LTE Advanced on the Cisco IR1101 Series Integrated Services Router 83
    - Prerequisites for Configuring Cisco 4G LTE Advanced 84
    - Restrictions for Configuring Cisco 4G LTE Advanced 84
    - Features not Supported in 4G LTE Advanced 85
    - 4G LTE-Advanced LEDs 85
    - Cisco 4G LTE-Advanced Features 86
    - 4G GNSS and NMEA 87
      - Example: Connecting to a Server Hosting a GPS Application 87
    - Dual SIM Card 88
      - Auto SIM 88
    - Using a SIM Card 90
      - Changing the PIN 91
      - Locking and Unlocking a SIM Card Using a PIN 91
    - Configure CHV1 for Unencrypted Levels 91
    - Configure CHV1 for Unencrypted Level7 92
    - Short Message Service (SMS) Capabilities 93
    - Data Account Provisioning 94
## Contents

**CHAPTER 10**

**Configuring Cellular IPv6 Address** 145

- Cellular IPv6 Address 145
- IPv6 Unicast Routing 145
- Link-Local Address 145
- Global Address 146
- Configuring Cellular IPv6 Address 146
- Configuring a Deterministic IPv6 Host Address 149

**CHAPTER 11**

**Information About SCADA** 153

- Information About SCADA 153
- Role of the IR1101 153
- Key Terms 154
- Protocol Translation Application 154
- Prerequisites 155
- Guidelines and Limitations 156
- Default Settings 156
- Configuring Protocol Translation 156
  - Enabling the IR1101 Serial Port and SCADA Encapsulation 156
  - Configuring T101 and T104 Protocol Stacks 157
- Configuring the T101 Protocol Stack 157
  - EXAMPLE 160
- Configuring the T104 Protocol Stack 160
  - EXAMPLE 163
- Configuration Example 164
- Configuring the DNP3 Protocol Stacks 165
  - Configuring DNP3 Serial 165
    - EXAMPLE 167
  - Configuring DNP3 IP 167
    - EXAMPLE 169
- Starting and Stopping the Protocol Translation Engine 169
  - EXAMPLE 170
- Verifying Configuration 170
CHAPTER 12  Raw Socket Transport  175
   Raw Socket Transport  175
      Information About Raw Socket Transport  175
         TCP Transport  176
         UDP Transport  176
         Serial Data Processing  177
         VRF-Aware Raw Socket  177
      Prerequisites  177
      Guidelines and Limitations  177
   Default Settings  178
   Configuring Raw Socket Transport  178
      Enabling Raw Socket Transport on the Serial Interface  178
      Configuring Common Raw Socket Line Options  179
      Configuring Raw Socket TCP  180
      Configuring a Raw Socket UDP Peer-to-Peer Connection  183
   Verifying Configuration  184
   Configuration Example  184
      Raw Socket TCP  185
      Raw Socket UDP  185
      Raw Socket VRF  186

CHAPTER 13  System Messages  189
   Information About Process Management  189
   How to Find Error Message Details  189

CHAPTER 14  Environmental Monitoring  195
   Environmental Monitoring  195
   Environmental Monitoring and Reporting Functions  195
   Environmental Monitoring Functions  196
   Environmental Reporting Functions  197
   Additional References  203
      Technical Assistance  203
CHAPTER 15

**IOx Application Hosting** 205

Application Hosting 205

Information About Application Hosting 205

Need for Application Hosting 205

IOx Overview 205

Cisco Application Hosting Overview 205

IOXMAN 206

Application Hosting on the IR1101 Industrial Integrated Services Router 206

VirtualPortGroup 207

vNIC 208

How to Configure Application Hosting 208

Enabling IOx 208

Configuring a VirtualPortGroup to a Layer 3 Data Port 210

Installing and Uninstalling Apps 213

Overriding the App Resource Configuration 214

Verifying the Application Hosting Configuration 216

Configuration Examples for Application Hosting 217

Example: Enabling IOx 217

Example: Configuring a VirtualPortGroup to a Layer 3 Data Port 217

Example: Installing and Uninstalling Apps 218

Example: Overriding the App Resource Configuration 218

CHAPTER 16

**ROM Monitor Overview** 219

ROM Monitor Overview and Basic Procedures 219

ROM Monitor Overview 219

Access ROM Monitor Mode 220

Checking the Current ROMMON Version 220

Commonly Used ROM Monitor Commands 221

Examples 222

Changing the ROM Monitor Prompt 222

Displaying the Configuration Register Setting 222

Environment Variable Settings 222

Frequently Used Environmental Variables 223
<table>
<thead>
<tr>
<th>Chapter 17</th>
<th>Process Health Monitoring 227</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Monitoring Control Plane Resources 227</td>
</tr>
<tr>
<td></td>
<td>Avoiding Problems Through Regular Monitoring 227</td>
</tr>
<tr>
<td></td>
<td>Cisco IOS Process Resources 227</td>
</tr>
<tr>
<td></td>
<td>Overall Control Plane Resources 231</td>
</tr>
<tr>
<td></td>
<td>Monitoring Hardware Using Alarms 233</td>
</tr>
<tr>
<td></td>
<td>Router Design and Monitoring Hardware 233</td>
</tr>
<tr>
<td></td>
<td>BootFlash Disk Monitoring 233</td>
</tr>
<tr>
<td></td>
<td>Approaches for Monitoring Hardware Alarms 233</td>
</tr>
<tr>
<td></td>
<td>Viewing the Console or Syslog for Alarm Messages 233</td>
</tr>
<tr>
<td></td>
<td>Network Management System Alerts a Network Administrator when an Alarm is Reported Through SNMP 233</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 18</th>
<th>Troubleshooting 235</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Understanding Diagnostic Mode 235</td>
</tr>
<tr>
<td></td>
<td>Before Contacting Cisco or Your Reseller 236</td>
</tr>
<tr>
<td></td>
<td>show interfaces Troubleshooting Command 236</td>
</tr>
<tr>
<td></td>
<td>Software Upgrade Methods 236</td>
</tr>
<tr>
<td></td>
<td>Recovering a Lost Password 237</td>
</tr>
<tr>
<td></td>
<td>Change the Configuration Register 237</td>
</tr>
<tr>
<td></td>
<td>Configuring the Configuration Register for Autoboot 239</td>
</tr>
<tr>
<td></td>
<td>Reset the Router 239</td>
</tr>
<tr>
<td></td>
<td>Reset the Password and Save Your Changes 241</td>
</tr>
<tr>
<td></td>
<td>Reset the Configuration Register Value 242</td>
</tr>
<tr>
<td></td>
<td>Configuring a Console Port Transport Map 242</td>
</tr>
<tr>
<td></td>
<td>Viewing Console Port, SSH, and Telnet Handling Configurations 244</td>
</tr>
<tr>
<td></td>
<td>Using the factory reset Commands 246</td>
</tr>
</tbody>
</table>
Introduction

The Cisco IR1101 Industrial Integrated Services Router is a next generation modular industrial router which has a Base module with additional Pluggable Modules that can be added. The Pluggable Module provides the flexibility of adding different interfaces to the IR1101 platform.

The IR1101 is the first IoT platform to run the Cisco IOS-XE operating system. IOS-XE is a Linux based OS that comes with many enhancements and more features compared to the classic IOS version.

The following figure shows the front panel of the IR1101 and highlights some of its capabilities:

Figure 1: IR1101 Front Panel

Table 1: Front Panel Descriptions

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SFP GigE WAN Port (Combo port of #3 below)</td>
</tr>
<tr>
<td>2</td>
<td>Type A USB 2.0 Host Port</td>
</tr>
<tr>
<td>3</td>
<td>RJ45 GigE WAN Port (Combo port of #1 above)</td>
</tr>
<tr>
<td>4</td>
<td>Asynchronous Serial Port (DTE only)</td>
</tr>
<tr>
<td>5</td>
<td>RJ45 Fast Ethernet LAN Ports</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>6</td>
<td>Grounding Point (On side of device)</td>
</tr>
<tr>
<td>7</td>
<td>DC Power and Alarm Input</td>
</tr>
<tr>
<td>8</td>
<td>Type B Mini-USB Console Port</td>
</tr>
<tr>
<td>9</td>
<td>Reset Button</td>
</tr>
<tr>
<td>10</td>
<td>Pluggable Module Slot (ex. 4G/LTE module)</td>
</tr>
</tbody>
</table>


- Accessing the CLI Using a Router Console, on page 2
- Accessing the CLI from a Remote Console, on page 5
- CLI Session Management, on page 6

## Accessing the CLI Using a Router Console

Cisco IR1101 routers have console port with only USB support. The console cable (Cisco P/N CAB-CONSOLE-USB, 6ft long) is not included and must be ordered.

The console port is a USB 2.0 mini USB Type B connector which is located on the front panel of the chassis. The default baud rate is 9600.

If your laptop or PC warns you that you do not have the proper drivers to communicate with the router, you can obtain them from your computers manufacturer, or go here: [https://www.silabs.com/products/mcu/Pages/USBtoUARTBridgeVCPDrivers.aspx](https://www.silabs.com/products/mcu/Pages/USBtoUARTBridgeVCPDrivers.aspx)

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

--- System Configuration Dialog ---

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

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

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

Would you like to enter basic management setup? [yes/no]: **yes**

Configuring global parameters:

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

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

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

Enter enable password: <your-password>

The virtual terminal password is used to protect access to the router over a network interface.

Enter virtual terminal password: <your-password>

Setup account for accessing HTTP server? [yes]: <return>

Username [admin]: <your-username>
Password [cisco]: <your-password>
Password is UNENCRYPTED.

Configure SNMP Network Management? [no]: <return>

Current interface summary

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

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/0/0</td>
<td>unassigned</td>
<td>NO</td>
<td>unset</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/0/1</td>
<td>unassigned</td>
<td>YES</td>
<td>unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/0/2</td>
<td>unassigned</td>
<td>YES</td>
<td>unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/0/3</td>
<td>unassigned</td>
<td>YES</td>
<td>unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>FastEthernet0/0/4</td>
<td>unassigned</td>
<td>YES</td>
<td>unset</td>
<td>up</td>
<td></td>
</tr>
<tr>
<td>Async0/2/0</td>
<td>unassigned</td>
<td>YES</td>
<td>unset</td>
<td>down</td>
<td></td>
</tr>
<tr>
<td>Vlan1</td>
<td>unassigned</td>
<td>YES</td>
<td>unset</td>
<td>up</td>
<td></td>
</tr>
</tbody>
</table>

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

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

Configuring interface Vlan1:

Configure IP on this interface? [no]: yes

IP address for this interface: 192.168.1.1
Subnet mask for this interface [255.255.255.0] : <return>
Class C network is 192.168.1.0, 24 subnet bits; mask is /24

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

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

The following configuration command script was created:

hostname <your-hostname>
enable secret 9 $9$26f174fvoEdMgUSXZYs814phbgpXsb48l9bzCng3u4Bc2kh1STsoLoHNes
enable password <your-enable-password>
line vty 0 4
password <your-password>
username <your-username> privilege 15 password <your-password>
no snmp-server
!
interface GigabitEthernet0/0/0
shutdown
no ip address
!
interface FastEthernet0/0/1
!
interface FastEthernet0/0/2
!
interface FastEthernet0/0/3
!
interface FastEthernet0/0/4
!
interface Vlan1
no shutdown
ip address 192.168.1.1 255.255.255.0
no mop enabled
ip dhcp pool wDHCPool
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
!
end

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

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

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

Press RETURN to get started! <return>

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

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

**Using the Console Interface**

**Step 1** Enter the following command:

```
Router > enable
```

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

```
Password: enablepass
```

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

```
Router#
```

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

**Step 3** To exit the console session, enter the `quit` command:
Accessing the CLI from a Remote Console

The remote console of the IR1101 can be accessed through Telnet or the more secure SSH. Details on telnet access follow in this chapter. For details on SSH access see the SSH chapter located here: Configuring Secure Shell, on page 33

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

Preparing to Connect to the Router Console Using Telnet


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

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

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

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

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

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

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

Using Telnet to Access a Console Interface

**Step 1**

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

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

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

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

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

**Step 2** Enter your login password:

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

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

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

```
Router> enable
```

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

```
Password: enablepass
```

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

```
Router#
```

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

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

```
Router# logout
```

---

**CLI Session Management**

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

**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

Step 1 configure terminal
Enters global configuration mode.

Step 2 line console 0

Step 3 session-timeout minutes
The value of minutes sets the amount of time that the CLI waits before timing out. Setting the CLI session timeout increases the security of a CLI session. Specify a value of 0 for minutes to disable session timeout.

Step 4 show line console 0
Verifies the value to which the session timeout has been set, which is shown as the value for " Idle Session ".

Locking a CLI Session

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

Step 1 Router# configure terminal
Enters global configuration mode.

Step 2 Enter the line upon which you want to be able to use the lock command.
Router(config)# line console 0

Step 3 Router(config)# lockable
Enables the line to be locked.

Step 4 Router(config)# exit

Step 5 Router# lock
The system prompts you for a password, which you must enter twice.
Password: <password>
Again: <password>
Locked
CHAPTER 2

Using Cisco IOS XE Software

This chapter contains the following sections:

- Understanding Command Modes, on page 9
- Keyboard Shortcuts, on page 11
- Using the no and default Forms of Commands, on page 11
- Using the History Buffer to Recall Commands, on page 12
- Managing Configuration Files, on page 12
- Saving Configuration Changes, on page 12
- Filtering Output from the show and more Commands, on page 13
- Finding Support Information for Platforms and Cisco Software Images, on page 13

Understanding Command Modes

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

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

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

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

The following table describes how to access and exit various common command modes of the Cisco IOS XE software. It also shows examples of the prompts displayed for each mode.
### Table 2: Accessing and Exiting Command Modes

<table>
<thead>
<tr>
<th>Command Mode</th>
<th>Access Method</th>
<th>Prompt</th>
<th>Exit Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>User EXEC</td>
<td>Log in.</td>
<td>Router&gt;</td>
<td>Use the <code>logout</code> command.</td>
</tr>
<tr>
<td>Privileged EXEC</td>
<td>From user EXEC mode, use the <code>enable</code> command.</td>
<td>Router#</td>
<td>To return to user EXEC mode, use the <code>disable</code> command.</td>
</tr>
<tr>
<td>Global configuration</td>
<td>From privileged EXEC mode, use the <code>configure terminal</code> command.</td>
<td>Router(config)#</td>
<td>To return to privileged EXEC mode from global configuration mode, use the <code>exit</code> or <code>end</code> command.</td>
</tr>
<tr>
<td>Interface configuration</td>
<td>From global configuration mode, specify an interface using an <code>interface</code> command.</td>
<td>Router(config-if)#</td>
<td>To return to global configuration mode, use the <code>exit</code> command. To return to privileged EXEC mode, use the <code>end</code> command.</td>
</tr>
</tbody>
</table>
| Diagnostic                    | The router boots up or accesses diagnostic mode in the following scenarios:  
                                  • In some cases, diagnostic mode will be reached when the Cisco IOS process or processes fail. In most scenarios, however, the router will reload.  
                                  • A user-configured access policy is configured using the `transport-map` command that directs a user into diagnostic mode.  
                                  • A break signal (`Ctrl-C`, `Ctrl-Shift-6`, or the `send break` command) is entered and the router is configured to go to diagnostic mode when the break signal is received. | Router(diag)# | If failure of the Cisco IOS process is the reason for entering diagnostic mode, the Cisco IOS problem must be resolved and the router rebooted to get out of diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or by using a method that is configured to connect to the Cisco IOS CLI. |
Exit Method

Prompt

Access Method

Command Mode

ROM monitor

To exit ROM monitor mode, manually boot a valid image or perform a reset with autoboot set so that a valid image is loaded.

From privileged EXEC mode, use the `reload` EXEC command. Press the `Break` key during the first 60 seconds while the system is booting.

Table 3: Keyboard Shortcuts

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Key Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move the cursor back one character.</td>
<td>Ctrl-B or the Left Arrow key¹</td>
</tr>
<tr>
<td>Move the cursor forward one character.</td>
<td>Ctrl-F or the Right Arrow key¹</td>
</tr>
<tr>
<td>Move the cursor to the beginning of the command line.</td>
<td>Ctrl-A</td>
</tr>
<tr>
<td>Move the cursor to the end of the command line.</td>
<td>Ctrl-E</td>
</tr>
<tr>
<td>Move the cursor back one word.</td>
<td>Esc B</td>
</tr>
<tr>
<td>Move the cursor forward one word.</td>
<td>Esc F</td>
</tr>
</tbody>
</table>

Using the no and default Forms of Commands

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

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

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

The following table lists the history substitution commands.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ctrl-P or the Up Arrow key(^1)</td>
<td>Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.</td>
</tr>
<tr>
<td>Ctrl-N or the Down Arrow key(^1)</td>
<td>Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key.</td>
</tr>
<tr>
<td>Router# show history</td>
<td>While in EXEC mode, lists the last few commands you entered.</td>
</tr>
</tbody>
</table>

\(^1\) The arrow keys function only on ANSI-compatible terminals such as VT100s.

Managing Configuration Files

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


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

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

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

Saving Configuration Changes

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

```
Router# copy running-config startup-config
Building configuration...
```
It may take a few minutes to save the configuration. After the configuration has been saved, the following output is displayed:

\[ \text{[OK]} \]
Router#

This task saves the configuration to the NVRAM.

**Filtering Output from the show and more Commands**

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

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

\[ \text{show command } | \{ \text{append | begin | exclude | include | redirect | section | tee} \} \text{ regular-expression} \]

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
```

**Finding Support Information for Platforms and Cisco Software Images**

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

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

The group of features 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.

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.

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

Finding Command Options: Example

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

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

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

**Table 5: Finding Command Options**

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Router&gt; enable</strong>&lt;br&gt;<strong>Password: &lt;password&gt;</strong>&lt;br&gt;<strong>Router#</strong></td>
<td>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 “&gt;”, for example, <strong>Router&gt; to Router#</strong></td>
</tr>
<tr>
<td><strong>Router# configure terminal</strong>&lt;br&gt;Enter configuration commands, one per line. End with CNTL/Z.&lt;br&gt;<strong>Router(config)#</strong></td>
<td>Enter the configure terminal privileged EXEC command to enter global configuration mode. You are in global configuration mode when the prompt changes to <strong>Router (config)#</strong></td>
</tr>
<tr>
<td><strong>Router(config)# interface GigabitEthernet ?</strong>&lt;br&gt;&lt;0-0&gt; GigabitEthernet interface number</td>
<td>Enter interface configuration mode by specifying the interface that you want to configure, using the interface GigabitEthernet global configuration command. Enter ? to display what you must enter next on the command line. When the &lt;cr&gt; symbol is displayed, you can press Enter to complete the command. You are in interface configuration mode when the prompt changes to <strong>Router(config-if)#</strong></td>
</tr>
<tr>
<td><strong>Router(config)# interface GigabitEthernet 0/?</strong>&lt;br&gt;&lt;0-5&gt; Port Adapter number</td>
<td></td>
</tr>
<tr>
<td><strong>Router (config)# interface GigabitEthernet 0/0/?</strong>&lt;br&gt;&lt;0-63&gt; GigabitEthernet interface number</td>
<td></td>
</tr>
<tr>
<td><strong>Router (config)# interface GigabitEthernet 0/0/0?</strong>&lt;br&gt;. &lt;0-71&gt;</td>
<td></td>
</tr>
<tr>
<td><strong>Router(config-if)#</strong></td>
<td></td>
</tr>
</tbody>
</table>
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.

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

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>Router(config-if)# ip address 172.16.0.1 255.255.255.0 ?</code> secondary</td>
<td>Enter the IP subnet mask. This example uses the 255.255.255.0 IP subnet mask.</td>
</tr>
<tr>
<td><code>secondary address</code></td>
<td>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.</td>
</tr>
<tr>
<td><code>&lt;cr&gt;</code></td>
<td><code>&lt;cr&gt;</code> is displayed. Press Enter to complete the command, or enter another keyword.</td>
</tr>
<tr>
<td><code>Router(config-if)# ip address 172.16.0.1 255.255.255.0</code></td>
<td>Press Enter to complete the command.</td>
</tr>
</tbody>
</table>

**Using Software Advisor**

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

**Using Software Release Notes**

See the release notes for information about the following:

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

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

This chapter contains the following sections:

• IR1101 Interface Naming, on page 19
• Basic Configuration, on page 19
• Configuring Global Parameters, on page 22
• Configuring the Gigabit Ethernet Interface, on page 23
• Configuring a Loopback Interface, on page 24
• Enabling Cisco Discovery Protocol, on page 26
• Configuring Command-Line Access, on page 26
• Configuring Static Routes, on page 28
• Configuring Dynamic Routes, on page 30
• Configuring the Serial Interface, on page 31

IR1101 Interface Naming

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

<table>
<thead>
<tr>
<th>Hardware Interface</th>
<th>Naming Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gigabit Ethernet combo port</td>
<td>gigabitethernet 0/0/0</td>
</tr>
<tr>
<td>Fast Ethernet ports</td>
<td>fastethernet0/1-0/0/4</td>
</tr>
<tr>
<td>Cellular Interface</td>
<td>cellular 0/1/0</td>
</tr>
<tr>
<td>Asynchronous Serial Interface</td>
<td>async 0/2/0</td>
</tr>
</tbody>
</table>

Basic Configuration

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

Current configuration : 5812 bytes

! Last configuration change at 23:29:27 UTC Tue Nov 6 2018

! version 16.10
service timestamps debug datetime msec
service timestamps log datetime msec
! Call-home is enabled by Smart-Licensing.
service call-home
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core

hostname Router

boot-start-marker
boot-end-marker

! no aaa new-model
call-home
! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
! the email address configured in Cisco Smart License Portal will be used as contact email
! address to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
avactive
destination transport-method http
no destination transport-method email

! login on-success log

! crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
! crypto pki trustpoint TP-self-signed-864728352
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-864728352
revocation-check none
rsakeypair TP-self-signed-864728352

! crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F7D0D0101 0B050030
32310E30 OC600355 040A1A306 43697363 6F312303 1E060355 04031317 43697363
6F204C69 63656E73 696E6720 312030 1E060355 04031317 43697363 6F204C69 63656e73
696e6720 312030 1E060355 04031317 43697363 6F204C69 63656e73 696e6720 312030 1E060355
32310E30 OC600355 040A1A306 43697363 6F312303 1E060355 04031317 43697363 6F204C69 63656e73
696e6720 312030 1E060355 04031317 43697363 6F204C69 63656n73 696n6720 312030 1E060355
3834375A 170D3338 30353330 31393438 34375A30 32310E30 OC600355 040A1A306
43697363 6F312303 1E060355 04031317 43697363 6F204C69 63656e73 696e6720 312030 1E060355
32310E30 OC600355 040A1A306 43697363 6F312303 1E060355 04031317 43697363 6F204C69 63656e73
696e6720 312030 1E060355 04031317 43697363 6F204C69 63656e73 696e6720 312030 1E060355
52666F74 20434130 82012230 0D06092A 864886F7 0D010101 05000032 010F0030
82010A02 82010100 A6C6BD6E 131E05F7 1F54A72C 2CD6866E 17222EA1 F1E9FD64D
CBB4C798 212AA147 C655D9D7 94713B8D 8711441E 1AAF071A 9CAE63B8 8A3E520
1C939D78 462F239 C659F715 B9C0A59 5BB85CBD 0CEBE3A7 700A8BF7 D9F256EE
4AA4E90D DB6FD3C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 285436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0B2D32C 55BD7180
Basic Router Configuration

68E69491 20F320E7 94E871D7 AE3BCC84 F1068E0F 539BA42B 42C68BB7
C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
48E93E4A 1B3E6A17 60AF8333 3D3B4C73 E8300D06 092A8648 86F70D01 01B0500
03820101 00507F24 3932A668 86025DFB EE83AE5C 64DF6860 49631C78 240DA905
604ECCDE FF4FE2DB 77FC460E C636FDBD DD44681E 3A5673AB 6C9E3D8B
D98987BF E40BD9E6 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
467A3DF4 03820101 00507F24 3932A668 86025DFB EE83AE5C 64DF6860 49631C78 240DA905
quit
Configuring Global Parameters

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

SUMMARY STEPS

1. configure terminal
2. hostname name
3. enable password password

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode when using the console port.</td>
</tr>
<tr>
<td>Example:</td>
<td>Use the following to connect to the router with a remote terminal:</td>
</tr>
</tbody>
</table>
| ```
Router> enable
``` | |
Basic Router Configuration

Configuring the Gigabit Ethernet Interface

The default configuration for the Gigabit Ethernet Interface (GI0/0/0) on the IR1101 is Layer 3 (L3). It is possible to configure the interface as a Layer 2 (L2) interface. The Gigabit Ethernet Interface on the IR1101 is a combo port, which means it is a RJ45+SFP connector. The correct connector must be selected, refer to the IR1101 Industrial Integrated Services Router Hardware Installation Guide here: https://www.cisco.com/c/en/us/td/docs/routers/access/1101/hardware/installation/guide/1101hwinst.html

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

SUMMARY STEPS

1. `interface GigabitEthernet slot/bay/port`
2. `ip address ip-address mask`
3. `ipv6 address ipv6-address/prefix`
4. `ipv6 unicast-routing`
5. `no shutdown`
6. `exit`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the configuration mode for an interface on the router.</td>
</tr>
<tr>
<td><code>interface GigabitEthernet slot/bay/port</code></td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# <code>interface GigabitEthernet 0/0/0</code></td>
<td></td>
</tr>
</tbody>
</table>
### Purpose

Sets the IP address and subnet mask for the specified interface. Use this Step if you are configuring an IPv4 address.

**Example:**

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

### Step 2

**Command or Action:**

```
ip address ip-address mask
```

**Example:**

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

### Step 3

**Command or Action:**

```
ipv6 address ipv6-address/prefix
```

**Example:**

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

Sets the IPv6 address and prefix for the specified interface. Use this step instead of Step 2, if you are configuring an IPv6 address. IPv6 unicast-routing needs to be set-up as well, see further information in the [IPV6 Addressing and Basic Connectivity Configuration Guide](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-16-10/ip6b-xe-16-10-book/read-me-first.html) located here:

### Step 4

**Command or Action:**

```
ipv6 unicast-routing
```

**Example:**

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

Enables forwarding of IPv6 unicast data packets.

### Step 5

**Command or Action:**

```
no shutdown
```

**Example:**

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

Enables the interface and changes its state from administratively down to administratively up.

### Step 6

**Command or Action:**

```
exit
```

**Example:**

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

Exits the configuration mode of interface and returns to the global configuration mode.

---

## Configuring a Loopback Interface

### Before you begin

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

To configure a loopback interface, follow these steps.

### SUMMARY STEPS

1. **interface type number**
2. (Option 1) **ip address ip-address mask**
3. (Option 2) **ipv6 address ipv6-address/prefix**
4. **exit**
### DETAILED STEPS

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

### Example

**Verifying Loopback Interface Configuration**

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

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

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

### Enabling Cisco Discovery Protocol

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

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

### Configuring Command-Line Access

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

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

#### SUMMARY STEPS

1. `line [aux | console | tty | vty] line-number`
2. `password password`
3. `login`
4. `exec-timeout minutes [seconds]`
5. `exit`
6. `line [aux | console | tty | vty] line-number`
7. `password password`
8. `login`
9. `end`

#### DETAILED STEPS

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

The following configuration shows the command-line access commands. Note that transport input none is the default, but if SSH is enabled this must be set to ssh.

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

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

Configuring Static Routes

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

To configure static routes, follow these steps.

SUMMARY STEPS

1. (Option 1) ip route prefix mask {ip-address | interface-type interface-number [ip-address]}
2. (Option 2) ipv6 route prefix/mask {ipv6-address | interface-type interface-number [ipv6-address]}
3. end

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Specifies a static route for the IP packets. (If you are configuring an IPv6 address, use the ipv6 route command described below.)</td>
</tr>
<tr>
<td>(Option 1) ip route prefix mask {ip-address</td>
<td>interface-type interface-number [ip-address]}</td>
</tr>
<tr>
<td>Router(config)# ip route 192.10.2.3 255.255.0.0 10.10.10.2</td>
<td></td>
</tr>
<tr>
<td>(Option 2) ipv6 route prefix/mask {ipv6-address</td>
<td>interface-type interface-number [ipv6-address]}</td>
</tr>
<tr>
<td>Router(config)# ipv6 route 2001:db8:2::/64 2001:db8:3::0</td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action | Purpose
--- | ---
Step 3 | end
Example: | Exits global configuration mode and enters privileged EXEC mode.
Router(config)# end

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

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

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

**Verifying Configuration**

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

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

```
Router# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, p - periodic downloaded static route
Gateway of last resort is not set

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

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

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

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

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

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

Configuring Routing Information Protocol

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

**SUMMARY STEPS**

1. `router rip`
2. `version {1 | 2}`
3. `network ip-address`
4. `no auto-summary`
5. `end`

**DETAILED STEPS**

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

Verifying Configuration

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

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

Gateway of last resort is not set

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

Configuring Enhanced Interior Gateway Routing Protocol

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

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


Configuring the Serial Interface

This section describes configuring serial interface management.

The IR1101 supports asynchronous serial interface protocols used for SCADA, Raw Socket, or reverse Telnet. It has a single serial interface, designated async 0/2/0. The serial interface is DTE only.

**Note**
Specifying an Asynchronous Serial Interface

To specify an asynchronous serial interface and enter interface configuration mode, use one of the following commands in global configuration mode.

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config)# interface async 0/2/0</td>
<td>Enters interface configuration mode.</td>
</tr>
</tbody>
</table>

Specifying Asynchronous Serial Encapsulation

The asynchronous serial interfaces support the following serial encapsulation methods:

- Raw-TCP
- Raw-UDP
- SCADA

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router(config-if)# encapsulation {raw-tcp</td>
<td>raw-udp</td>
</tr>
</tbody>
</table>

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

The remaining encapsulation methods are defined in their respective books and chapters describing the protocols or applications.

Configuring the Serial Port

To configure the serial port perform the steps in the following example:

IR1101#sh run int async 0/2/0
Building configuration...
Current configuration : 62 bytes
!
interface Async0/2/0
no ip address
encapsulation raw-tcp
end
IR1101#show line

<table>
<thead>
<tr>
<th>Tty Line Typ</th>
<th>Tx/Rx</th>
<th>A Modem</th>
<th>Rety AccO AccI</th>
<th>Uses</th>
<th>Noise</th>
<th>Overruns</th>
<th>Int</th>
</tr>
</thead>
<tbody>
<tr>
<td>* 0 0 CTY</td>
<td></td>
<td>- -</td>
<td>- -</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>0/2/0 50 TTY</td>
<td>9600/9600</td>
<td>- - -</td>
<td>- -</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>74 74 VTY</td>
<td></td>
<td>- -</td>
<td>- -</td>
<td>3</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>75 75 VTY</td>
<td></td>
<td>- -</td>
<td>- -</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>76 76 VTY</td>
<td></td>
<td>- -</td>
<td>- -</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>77 77 VTY</td>
<td></td>
<td>- -</td>
<td>- -</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
<tr>
<td>78 78 VTY</td>
<td></td>
<td>- -</td>
<td>- -</td>
<td>0</td>
<td>0</td>
<td>0/0</td>
<td>-</td>
</tr>
</tbody>
</table>

Line(s) not in async mode -or- with no hardware support:
1-49, 51-73, 79-726
Configuring Secure Shell

This section contains the following topics:

- Information About Secure Shell, on page 33
- How to Configure Secure Shell, on page 35
- Information about Secure Copy, on page 40
- Additional References, on page 42

Information About Secure Shell

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

Prerequisites for Configuring Secure Shell

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

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

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the IR1101 for secure shell.

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


- This software release supports IP Security (IPSec).
- The IR1101 supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2, which Cisco recommends due to its better security.
- The -l keyword and userid: {number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

**SSH And Router Access**

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

**SSH Servers, Integrated Clients, and Supported Versions**

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

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

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

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

- TACACS+
- RADIUS
- Local authentication and authorization
SSH Configuration Guidelines

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

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

- If you get CLI error messages after entering the `crypto key generate rsa` global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the `crypto key generate rsa` command.

- When generating the RSA key pair, the message `No hostname specified` might appear. If it does, you must configure an IP hostname by using the `hostname` global configuration command.

- When generating the RSA key pair, the message `No domain specified` might appear. If it does, you must configure an IP domain name by using the `ip domain-name` global configuration command.

- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Related Tasks

- Setting Up the IR1101 to Run SSH, on page 35
- Configuring the Router for Local Authentication and Authorization, on page 38

How to Configure Secure Shell

Setting Up the IR1101 to Run SSH

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

Before you begin

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

SUMMARY STEPS

1. `configure terminal`
2. `hostname hostname`
3. `ip domain-name domain_name`
4. `crypto key generate rsa`
5. `end`

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring the SSH Server

Follow these steps to configure the SSH server:

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1101# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

**Step 2**

**hostname hostname**

**Example:**

IR1101(config)# hostname your_hostname

**Purpose:** Configures a hostname and IP domain name for your device.

**Note**

Follow this procedure only if you are configuring the device as an SSH server.

**Step 3**

**ip domain-name domain_name**

**Example:**

IR1101(config)# ip domain-name your_domain_name

**Purpose:** Configures a host domain for your device.

**Step 4**

**crypto key generate rsa**

**Example:**

IR1101(config)# crypto key generate rsa

**Purpose:** Enables the SSH server for local and remote authentication on the device and generates an RSA key pair. Generating an RSA key pair for the device automatically enables SSH.

We recommend that a minimum modulus size of 1024 bits.

When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use.

**Note**

Follow this procedure only if you are configuring the device as an SSH server.

**Step 5**

**end**

**Example:**

IR1101(config)# end

**Purpose:** Returns to privileged EXEC mode.

---

### Configuring Secure Shell

**SUMMARY STEPS**

1. configure terminal
2. ip ssh version [2]
3. ip ssh {timeout seconds | authentication-retries number}
4. Use one or both of the following:
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1** configure terminal  
Example: IR1101# configure terminal | Enters global configuration mode. |
| **Step 2** ip ssh version [2]  
Example: IR1101(config)# ip ssh version 2 | (Optional) Configures the device to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2. |
| **Step 3** ip ssh {timeout seconds | authentication-retries number}  
Example:  
IR1101(config)# ip ssh timeout 90  ip ssh authentication-retries 2 | Configures the SSH control parameters:  
- Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the device uses the default time-out values of the CLI-based sessions.  
- By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes.  
- Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5.  
Repeat this step when configuring both parameters. |
| **Step 4** Use one or both of the following:  
- line vty line_number[ending_line_number]  
- transport input ssh  
Example: IR1101(config)# line vty 1 10  
or  
IR1101(config-line)# transport input ssh | (Optional) Configures the virtual terminal line settings.  
- Enters line configuration mode to configure the virtual terminal line settings. For the line_number and ending_line_number arguments, the range is from 0 to 15.  
- Specifies that the device prevents non-SSH Telnet connections, limiting the device to only SSH connections. |
### Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show ip ssh</td>
<td>Shows the version and configuration information for the SSH server.</td>
</tr>
<tr>
<td>show ssh</td>
<td>Shows the status of the SSH server.</td>
</tr>
</tbody>
</table>

### Configuring the Router for Local Authentication and Authorization

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

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

1. configure terminal
2. aaa new-model
3. aaa authentication login default local
4. aaa authorization exec local
5. aaa authorization network local
6. username name privilege level password encryption-type password
7. end

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>IR1101# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>

| **Step 2** aaa new-model                                | Enables AAA                                                              |
| **Example:**                                           |                                                                         |
| IR1101(config)# aaa new-model                           |                                                                         |

| **Step 3** aaa authentication login default local       | Sets the login authentication to use the local username database. The default keyword applies the local user database authentication to all ports. |
| **Example:**                                           |                                                                         |
| IR1101(config)# aaa authentication login default local  |                                                                         |

| **Step 4** aaa authorization exec local                 | Configures user AAA authorization, check the local database, and allow the user to run an EXEC shell. |
| **Example:**                                           |                                                                         |
| IR1101(config-line)# aaa authorization exec local       |                                                                         |

| **Step 5** aaa authorization network local              | Configures user AAA authorization for all network-related service requests. |
| **Example:**                                           |                                                                         |
| IR1101(config-line)# aaa authorization network local    |                                                                         |

| **Step 6** username name privilege level password encryption-type password | Enters the local database, and establishes a username-based authentication system. |
| **Example:**                                                   |                                                                         |
| IR1101(config-line)# username your_user_name privilege 1 password 7 secret567 | Repeat this command for each user.  
1. For name, specify the user ID as one word. Spaces and quotation marks are not allowed.  
2. (Optional) For level, specify the privilege level the user has after gaining access. The range is 0 to 15. Level 15 gives privileged EXEC mode access. Level 0 gives user EXEC mode access.  
3. For encryption-type, enter 0 to specify that an unencrypted password follows. Enter 7 to specify that a hidden password follows.  
4. For password, specify the password the user must enter to gain access to the switch. The password must be from |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 7</strong> end</td>
<td>Exits line configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> IR1101(config-line)# end</td>
<td></td>
</tr>
</tbody>
</table>

**Information about Secure Copy**

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

**Prerequisites for Secure Copy**

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

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

**Restrictions for Configuring Secure Copy**

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

**Configuring Secure Copy**

To configure the Cisco IR1101 for Secure Copy (SCP) server-side functionality, perform the following steps.
### SUMMARY STEPS

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

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device&gt; enable</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device# configure terminal</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>aaa new-model</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa new-model</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>aaa authentication login {default</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# aaa authentication login default group tacacs+</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>username name [privilege level] password encryption-type encrypted-password</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You may omit this step if a network-based authentication mechanism, such as TACACS+ or RADIUS, has been configured.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# username superuser privilege 2 password 0 superpassword</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>ip scp server enable</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Device(config)# ip scp server enable</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td><strong>exit</strong>&lt;br&gt; <strong>Example:</strong>&lt;br&gt; Device(config)# exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>show running-config</strong>&lt;br&gt; <strong>Example:</strong>&lt;br&gt; Device# show running-config</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>debug ip scp</strong>&lt;br&gt; <strong>Example:</strong>&lt;br&gt; Device# debug ip scp</td>
</tr>
</tbody>
</table>

**Example**

IR1101# `copy scp <somefile> your_username@remotehost:/<some/remote/directory>`

### Additional References

The following sections provide references related to the SSH feature.

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
</table>
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 simple method is similar to a typical Cisco router image installation and management that is supported across Cisco routers.

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

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.
The IR1101 uses Smart Licensing, which is discussed in detail in the next chapter. The IR1101 does not support the Right to Use licenses, and supports only the Specific License Reservation (SLR)

**Consolidated Packages**

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

---

**Note**

All of the IOS-XE feature set may not apply to the IR1101. Some features may not have been implemented yet, or are not appropriate for this platform.

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

One of the following image-based licenses can be pre-installed on the IR1101 router:

- Network-Essentials
- Network-Advantage

---

**Note**


**Network-Essentials**

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

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

**Network-Advantage**

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

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

**Related Documentation**

For further information on software licenses, see [Information About Smart Licensing, on page 51](#).
How to Install the Software for Cisco IOS XE

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

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

Installing the Cisco IOS XE Release

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

Note

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

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

Router# configure terminal
  Router(config)#boot sys bootflash:ir1101-universalk9.16.10.01.SPA.bin
  Router(config)#config-register 0x2102
  Router(config)#exit
  Router# *Nov 7 00:07:06.784: %SYS-5-CONFIG_I: Configured from console by console
  Router# show run | inc license
  license udi pid IR1101-K9 sn FCW2150TH0F
  license boot level network-advantage
  Router# reload ?
  /noverify Don't verify file signature before reload.
  /verify Verify file signature before reload.
  at Reload at a specific time/date
  cancel Cancel pending reload
  in Reload after a time interval
  pause Pause during reload
  reason Reload reason
  <cr> <cr>
  Router#reload /verify
  System configuration has been modified. Save? [yes/no]: yes
  Building configuration...

  [OK]
  *Nov 7 00:08:48.101: %SYS-2-PRIVCFG_ENCRYPT: Successfully encrypted private config file
  Verifying file integrity of bootflash:/ir1101-universalk9.16.10.01.SPA.bin...............
  ....................................
  Embedded Hash SHA1: B0315BDC4F545D624BB128CE0FFAA468E6EF7587
  Computed Hash SHA1: B0315BDC4F545D624BB128CE0FFAA468E6EF7587
  Starting image verification
  Hash Computation: 100%Done!
Digital signature successfully verified in file bootflash:/ir1101-universalk9.16.10.01.SPA.bin
Signature Verified

Proceed with reload? [confirm]


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

Press RETURN to get started!

**ROMMON Images**

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

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

---

**Note**

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

---

**File Systems**

The following table provides a list of file systems that can be seen on the Cisco IR1101 router.

**Table 7: Router File Systems**

<table>
<thead>
<tr>
<th>File System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootflash:</td>
<td>Boot flash memory file system.</td>
</tr>
<tr>
<td>flash:</td>
<td>Alias to the boot flash memory file system above.</td>
</tr>
<tr>
<td>cns:</td>
<td>Cisco Networking Services file directory.</td>
</tr>
</tbody>
</table>
### File System Description

<table>
<thead>
<tr>
<th>File System</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nvrn:</td>
<td>Router NVRAM. You can copy the startup configuration to NVRAM or from NVRAM.</td>
</tr>
<tr>
<td>obfl:</td>
<td>File system for Onboard Failure Logging (OBFL) files.</td>
</tr>
<tr>
<td>system:</td>
<td>System memory file system, which includes the running configuration.</td>
</tr>
<tr>
<td>tar:</td>
<td>Archive file system.</td>
</tr>
<tr>
<td>tmpsz:</td>
<td>Temporary system files file system.</td>
</tr>
<tr>
<td>usbflash0:</td>
<td>The Universal Serial Bus (USB) flash drive file systems. <strong>Note</strong> The USB flash drive file system is visible only if a USB drive is installed in the USB port.</td>
</tr>
</tbody>
</table>

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.

The USB port could be considered a potential security risk. If you wish to disable the USB port, use these steps:

```
Configure terminal
platform usb disable
exit

show platform usb
```

## 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 8: Autogenerated Files

<table>
<thead>
<tr>
<th>File or Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crashinfo files</td>
<td>Crashinfo files may appear in the bootflash: file system. These files provide descriptive information of a crash and may be useful for tuning or troubleshooting purposes. However, the files are not part of router operations, and can be erased without impacting the functioning of the router.</td>
</tr>
<tr>
<td>core directory</td>
<td>The storage area for .core files. If this directory is erased, it will automatically regenerate itself at bootup. The .core files in this directory can be erased without impacting any router functionality, but the directory itself should not be erased.</td>
</tr>
<tr>
<td>managed directory</td>
<td>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.</td>
</tr>
<tr>
<td>File or Directory</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>tracelogs directory</td>
<td>The storage area for trace files. Trace files are useful for troubleshooting. If the Cisco IOS process fails, for instance, users or troubleshooting personnel can access trace files using diagnostic mode to gather information related to the Cisco IOS failure. Trace files, however, are not a part of router operations, and can be erased without impacting the router's performance.</td>
</tr>
</tbody>
</table>

**Important Notes About Autogenerated Directories**

Important information about autogenerate directories include:

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

**Note**

Altering autogenerating files on the bootflash: may have unpredictable consequences for system performance.

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

---

**Flash Storage**

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

**Note**

Flash storage is required for successful operation of a router.

---

**LED Indicators**

For information on LEDs on the router, see "LED Indicators" in the "Product Overview" section of the Hardware Installation Guide for the Cisco IR1101 Industrial Integrated Services Router.

To monitor the LED status of the system, the alarm and interface ports, the show LED command line is supported in IOS mode.

```
Router# show LED
SYSTEM LED : Green
Custom LED : Off
VPN LED : Off
ALARM LED : Off
```
GigabitEthernet0/0/0 LED : On
FastEthernet0/0/1 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off

LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Green
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : Off

Related Documentation

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

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

- You must have a Cisco username and password to login into Cisco Smart Software Manager.
- You must accept the Smart Software Licensing Agreement on Cisco Smart Software Manager to register devices.

Information About Smart Licensing

Smart Licensing is a cloud-based, software license management solution that allows you to manage and track the status of your license, hardware and software usage trends. Smart Licensing also enables you to automate time-consuming, manual licensing tasks. Smart Licensing helps simplify three core functions:

- **Purchasing:** The software that you have installed in your network can automatically self-register themselves, without using traditional licenses like Product Activation Keys (PAKs), CSL, Honor Based License (HBL) or Right-to-Use (RTU).

- **Management:** You can automatically track activations against your license entitlements. Additionally, there is no need to install the license file on every node. You can create license pools (logical grouping of licenses) to reflect your organization structure. Smart Licensing offers you Cisco Smart Software Manager, a centralized portal that enables you to manage all your Cisco software licenses from one centralized website.
• Reporting: Through the portal, Smart Licensing offers an integrated view of the licenses you have purchased and what has been actually deployed in your network. You can use this data to make better purchase decisions, based on your consumption.

Overview of Cisco Smart Software Manager

Cisco Smart Software Manager enables you to manage all of your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you organize and view your licenses in groups called virtual accounts (collections of licenses and product instances). Use the Cisco Smart Software Manager to do the following tasks:

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

The Cisco Smart Software Manager Help describes the procedures for carrying out these tasks. You can access the Cisco Smart Software Manager on https://software.cisco.com/#, by clicking Smart Software Licensing link under License tab. Login using the username and password provided by Cisco.

Note
Use Chrome 32.0, Firefox 25.0 or Safari 6.0.5 web browsers to access the Cisco Smart Software Manager. Also, ensure that Javascript 1.5 or a later version is enabled in your browser.

Deployment Options for IR1101 Licensing

The only supported licensing deployment for IR1101 is Specific License Reservation.

Specific License Reservation

Specific License Reservation (SLR) allows devices, in highly secure networks, to be associated with smart licenses without connecting to Cisco Smart Software Manager. Excess Licenses can be reserved in Cisco Smart Software Manager and associated with devices with their unique device information (UDI).

Note
Pre-authorization is required from Cisco to enable Specific License Reservation
Specific License Reservations provides limited or no functionality to certain Smart Licensing features such as transfer of licenses between products, license usage, asset management et c.

To Register a Device in Cisco Smart Software Manager

To register a device with token in Cisco Smart Software Manager, perform this procedure:

**SUMMARY STEPS**

1. enable
2. license smart register *token_ID*

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong> license smart register <em>token_ID</em></td>
<td>Registers the device with the back-end server. Registration of the device changes the License Authorization Status from Eval Mode to Authorized shown in “show license summary”.</td>
</tr>
<tr>
<td>Example: device# license smart register idtoken NmE1Yzg0OWMtYmJ4</td>
<td></td>
</tr>
</tbody>
</table>

Renewing Smart Licensing Registration

In general, your registration is automatically renewed every 30 days. Use this option to make an on-demand manual update of your registration. Thus, instead of waiting 30 days for the next registration renewal cycle, you can issue this command to instantly find out the status of your license.

To renew smart licensing registration, perform this procedure:

**SUMMARY STEPS**

1. enable
2. license smart renew {auth | id}

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode.</td>
</tr>
<tr>
<td>Example: device&gt; enable</td>
<td>Enter your password if prompted.</td>
</tr>
</tbody>
</table>
Renew your ID or authorization with Cisco Smart Licensing. If ID certification renewal fails, then the product instance goes to an unidentified state and starts consuming the evaluation period.

| Step 2 | `license smart renew {auth | id }` |
|--------|----------------------------------|
| Example: | `device# license smart renew auth Tue Apr 22 09:12:37.086 PST` |

Authorization periods are renewed by the Smart Licensing system every 30 days. As long as the license is in an 'Authorized' or 'Out-of-compliance' (OOC), the authorization period is renewed. Grace period starts when an authorization period expires. During the grace period or when the grace period is in the 'Expired' state, the system continues to try renew the authorization period. If a retry is successful, a new authorization period starts.

Enabling Specific License Reservation and Generating a Request Code

To enable Specific License Reservation and to generate a request code, perform this procedure:

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. `license smart reservation`
4. `exit`
5. `license smart reservation request local`
6. `license smart reservation install [auth-code | file <filename>]`
7. `license smart reservation cancel`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>enable</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>device&gt; enable</code></td>
</tr>
<tr>
<td></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td>Example:</td>
<td><code>device# configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>license smart reservation</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Enables Specific License Reservation. Use the no form of this command to disable Specific License Reservation.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>device(config)# license smart reservation</td>
<td>Exits configuration mode, and returns the device to global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>device(config)# exit</td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td></td>
</tr>
<tr>
<td>license smart reservation request local</td>
<td>Generates a request code to be entered in the Cisco Smart Software Manager. The request code can be generated for the following:</td>
</tr>
<tr>
<td>Example:</td>
<td>• all - Generates a request code for all connected devices.</td>
</tr>
<tr>
<td>device# license smart reservation request local</td>
<td>• local - Generates a request code for the active device.</td>
</tr>
<tr>
<td></td>
<td>• universal - Generates a universal request code. This mode of request is deprecated and will not be supported for further releases.</td>
</tr>
<tr>
<td>Step 6</td>
<td></td>
</tr>
<tr>
<td>license smart reservation install [auth-code</td>
<td>file &lt;filename&gt;]</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>device# license smart reservation install</td>
<td></td>
</tr>
<tr>
<td>Step 7</td>
<td></td>
</tr>
<tr>
<td>license smart reservation cancel</td>
<td>This command is used to cancel the reservation request made via the command &quot;license smart reservation request local&quot;, and transition back to an unregistered state.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>device# license smart reservation cancel</td>
<td></td>
</tr>
</tbody>
</table>

### Reserving a License in Cisco Smart Software Manager

**Step 1**  
Login to Cisco Smart Software Manager at [https://software.cisco.com/#](https://software.cisco.com/#).

**Step 2**  
Select **Smart Software Licensing** then the **Inventory** tab.
You must log in to the portal using a Cisco provided username and password.

**Step 3**  
From the Virtual Account sub-page, select the Licenses tab and click on the License Reservation button as shown in the following image.

**Figure 3: Smart Software Licensing**

On the Smart License Reservation page, enter the request code generated by the device from the `license smart reservation request local` command. Hit the Enter key then click on the Next button.

**Step 4**
Step 5  Enable the **Reserve a Specific License** checkbox. For the required license, enter the number in the Quantity to Reserve field (normally 1 for a device). In the following example we enter “1” for Cisco IR1101 Network Advantage and “1” for Cisco IR1101 Network Essentials”. Then click the **Next** button.

**Figure 5: Select Licenses**

<table>
<thead>
<tr>
<th>License</th>
<th>Description</th>
<th>Expires</th>
<th>Available</th>
<th>Quantity To Reserve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IR1101 IPBase License</td>
<td>Cisco P Base Smart License for Cisco IR1101 Ind…</td>
<td>2018-Dec-10</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Cisco IR1101 Security License</td>
<td>Cisco Security Smart License for Cisco IR1101 Ind…</td>
<td>2018-Dec-11</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Cisco IR1101 Network Advantage</td>
<td>Cisco P Base Smart License for Cisco IR1101 Ind…</td>
<td>2018-Dec-10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Cisco IR1101 Security with No Payload Encryption</td>
<td>Cisco Security No Payload Encryption Smart Live…</td>
<td>2018-Dec-10</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Cisco IR1101 AppKit License</td>
<td>Cisco AppKit Smart License for Cisco IR1101 Indus…</td>
<td>2018-Dec-10</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Cisco IR1101 Network Essentials</td>
<td>Cisco P Base Smart License for Cisco IR1101 Ind…</td>
<td>2018-Dec-10</td>
<td>10</td>
<td></td>
</tr>
</tbody>
</table>

Step 6  The **Review and Confirm** tab is displayed. Make sure that you have the correct licenses reserved. When done, click the **Generate Authorization Code** button.
Step 7

Once the authorization code is generated, click either the **Download as File** or the **Copy to Clipboard** button for use in the `license smart reservation install [auth-code | file <filename>]` command.
Registering Device with Specific License Reservation

To register device with specific license reservation, perform this procedure:

**SUMMARY STEPS**

1. `enable`
2. `license smart reservation install auth-code | auth-code-file`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><code>enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong> <code>device&gt; enable</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Registers the device.</td>
</tr>
<tr>
<td>`license smart reservation install auth-code</td>
<td>auth-code-file`</td>
</tr>
<tr>
<td><strong>Example:</strong> <code>device&gt; license smart reservation install file bootflash:network-advantage_auth_code.txt</code></td>
<td></td>
</tr>
</tbody>
</table>
# Monitoring Smart Licensing Configuration

Use the privileged EXEC commands in the following table to monitor your PIM snooping configurations.

**Table 9: Commands to Monitor Smart Licensing Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show license status</code></td>
<td>Displays the compliance status of Smart Licensing. Following are the possible status:</td>
</tr>
<tr>
<td></td>
<td>• Enabled: Indicates that Smart Licensing is enabled.</td>
</tr>
<tr>
<td></td>
<td>• Waiting: Indicates the initial state after your device has made a license entitlement request. The device establishes communication with Cisco and successfully registers itself with the Cisco license manager.</td>
</tr>
<tr>
<td></td>
<td>• Authorized: Indicates that your device is able to communicate with the Cisco license manager, and is authorised to initiate requests for license entitlements.</td>
</tr>
<tr>
<td></td>
<td>• Out-Of-Compliance: Indicates that one or more of your licenses are out-of-compliance. You must buy additional licenses.</td>
</tr>
<tr>
<td></td>
<td>• Eval Period: Indicates that Smart Licensing is consuming the evaluation period. You must register the device with the Cisco Licensing manager, else your license expires.</td>
</tr>
<tr>
<td></td>
<td>• Grace Period: Indicates that connectivity to the Cisco license manager is lost. You must try restore connectivity to renew the authorization period.</td>
</tr>
<tr>
<td></td>
<td>• Disabled: Indicates that Smart Licensing is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Invalid: Indicates that Cisco does not recognize the entitlement tag as it is not in the database.</td>
</tr>
<tr>
<td><code>show license all</code></td>
<td>Displays all entitlements in use. It can also be used to check if Smart Licensing is enabled. Additionally, it shows associated licensing certificates, compliance status, UDI, and other details.</td>
</tr>
<tr>
<td><code>show license tech support</code></td>
<td>Displays the output of the license commands.</td>
</tr>
<tr>
<td><code>show license usage</code></td>
<td>Displays the license usage information.</td>
</tr>
</tbody>
</table>
### Command Purpose

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show license reservation</td>
<td>Displays overall license reservation status and its information.</td>
</tr>
<tr>
<td>show license summary</td>
<td>Displays the summary of all active licenses.</td>
</tr>
</tbody>
</table>

### Example: Registering Smart Licensing Enabled Device

```
Device> enable
Device# license smart register idtoken NmE1Yzg0OWMtYmJ4
license smart register: Registration process is in progress. Please check the syslog for the registration status and result.
```

### IR1101 Licensing for Cisco IOS-XE release 16.10.1

With IOS-XE release 16.10.1, the IR1101 supports boot level licenses Network-Essentials and Network-Advantage. Both of these licenses are available in the universalk9 and universalk9_npe images. With release 16.10.1, Network-Advantage is a superset of Network-Essentials, so the license are mutually exclusive and Network-Essentials will be the default license level. Displaying the license consumption and boot level configuration will have either Network-Essentials or Network-Advantage but not both at the same time.

There are two important things to consider with licensing the IR1101:

If you have performed a write erase, or used the reset button, you will need to add the license.

```
IR1101# config term
IR1101# license smart reservation
```

If you perform a factory reset all, this will erase the license with no way to recover it unless you get the authorization file from the smart account.

The following shows an example of the different licensing:

```
IR1101# show license summary
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: Allowed

License Authorization:
Status: AUTHORIZED - RESERVED

License Usage:
License Entitlement tag Count Status
-------------------------------------------------------------------------------------------------------------------------------
Cisco IR1101 Network... (IR1101_Network_Advantage) 1 AUTHORIZED

IR1101# show license status
Smart Licensing is ENABLED
```

Utility:
Status: DISABLED
License Reservation is ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 07 02:04:55 2018 UTC

License Authorization:
Status: AUTHORIZED - RESERVED on Nov 07 02:04:55 2018 UTC

Export Authorization Key:
Last return status: SUCCEEDED on Nov 07 02:04:55 2018 UTC
Features Authorized:
one

# IR1101# show license all
Smart Licensing Status
------------------------

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 07 02:04:55 2018 UTC

License Authorization:
Status: AUTHORIZED - RESERVED on Nov 07 02:04:55 2018 UTC

Export Authorization Key:
Last return status: SUCCEEDED on Nov 07 02:04:55 2018 UTC
Features Authorized:
one

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

License Usage
------------

Cisco IR1101 Network Advantage (IR1101_Network_Advantage):
Description: Cisco Network Advantage Smart License for Cisco IR1101
Count: 1
Version: 1.0
Status: AUTHORIZED
Export status: NOT RESTRICTED
Reservation:
Reservation status: SPECIFIC INSTALLED
Total reserved count: 1

Product Information
---------------------
UDI: PID:IR1101-K9,SN:FCW2150THOF

Agent Version
-------------
Smart Agent for Licensing: 4.5.5_rel/56
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
----------------
License reservation: ENABLED

Overall status:
Active: PID:IR1101-K9,SN:FCW2150THOF
Reservation status: SPECIFIC INSTALLED on Nov 07 02:04:55 2018 UTC
Export-Controlled Functionality: Allowed
Last Confirmation code: 9765d8c5

Specified license reservations:
Cisco IR1101 Network Advantage (IR1101_Network_Advantage):
Description: Cisco Network Advantage Smart License for Cisco IR1101 Industrial Integrated Services Router
Total reserved count: 1
Term information:
Active: PID:IR1101-K9,SN:FCW2150THOF
License type: TERM
Start Date: 2018-JUN-13 UTC
End Date: 2018-DEC-10 UTC
Term Count: 1

IR1101# show license tech support
Smart Licensing Tech Support info
Smart Licensing Status
-----------------------------
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
Status: REGISTERED - SPECIFIC LICENSE RESERVATION
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Nov 07 02:04:55 2018 UTC

License Authorization:
Status: AUTHORIZED - RESERVED on Nov 07 02:04:55 2018 UTC

Export Authorization Key:
Last return status: SUCCEEDED on Nov 07 02:04:55 2018 UTC
Features Authorized:
<none>

Utility:
Status: DISABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Evaluation Period:
Evaluation Mode: EXPIRED
Evaluation Period Remaining: Expired on Nov 05 08:27:16 2018 UTC

License Usage
---------------
Handle: 1
License: Cisco IR1101 Network Advantage
Entitlement tag: regid.2018-04.com.cisco.IR1101_Network_Advantage,1.0_d2087fd8-364a-4ef3-bbaf-66111de3684b
Description: Cisco Network Advantage Smart License for Cisco IR1101 Industrial Integrated Services Router
Count: 1
Version: 1.0
Status: AUTHORIZED(3)
Status time: Nov 07 02:04:55 2018 UTC
Request Time: Nov 06 23:22:13 2018 UTC
Export status: NOT RESTRICTED

Product Information
-------------------
UDI: PID:IR1101-K9, SN:FCW2150TH0F

Agent Version
-------------
Smart Agent for Licensing: 4.5.5_rel/56
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Upcoming Scheduled Jobs
------------------------
Current time: Nov 07 02:10:15 2018 UTC
Daily: Nov 07 23:22:16 2018 UTC (21 hours, 12 minutes, 1 seconds remaining)
Init Flag Check: Not Available
Reservation request in progress warning: Not Available
Reservation configuration mismatch between nodes in HA mode: Nov 14 02:05:24 2018 UTC (6 days, 23 hours, 55 minutes, 9 seconds remaining)

License Certificates
---------------------
Production Cert: True
Not registered. No certificates installed

HA Info
-------
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: True

Reservation Info
----------------
License reservation: ENABLED

Overall status:
Active: PID:IR1101-K9, SN: FCW2150TH0F
Reservation status: SPECIFIC INSTALLED on Nov 07 02:04:55 2018 UTC
Export-Controlled Functionality: Allowed
Request code: <none>
Last return code: <none>
Last Confirmation code: 9765d8c5
Reservation authorization code:
<specificPLR><authorizationCode><flag>A</flag><version>C</version><piid>928ad52c-2904-4446-8b10-7b468137c1c9</piid><timest ... 04.com.cisco.IR1101_Network_Advantage,1.0_d2087fd8-364a-4ef3-bbaf-66111de3684b</tag><count>1</count><startDate>2018-JUN-13 UTC</startDate><endDate>2018-DEC-10 UTC</endDate><licenseType>TERM</licenseType><displayName>Cisco IR1101 Network Advantage</displayName><tagDescription>Cisco Network Advantage Smart License for Cisco IR1101 Industrial Integrated Services Router</tagDescription><subscriptionID></subscriptionID></entitlement></entitlements></authorizationCode><signature>MEUCIE ... iB4bvfDiJNMaAiEArh+lyR+SAgM9Y2qKNXVWoXRbcaGsxEQZw6f4yQ6qYzI=</signature><udi>P:IR1101-K9,S:FCW2150TH0F</udi></specificPLR>

Specified license reservations:
Cisco IR1101 Network Advantage (IR1101_Network_Advantage):
  Description: Cisco Network Advantage Smart License for Cisco IR1101 Industrial Integrated Services Router
  Total reserved count: 1
  Term information:
    Active: PID:IR1101-K9, SN: FCW2150TH0F
    License type: TERM
    Start Date: 2018-JUN-13 UTC
    End Date: 2018-DEC-10 UTC
    Term Count: 1
    Subscription ID: <none>

Other Info
----------
Software ID: regid.2018-04.com.cisco.IR1101,1.0_e40b8e7c-fd51-418c-a981-a49697dd08f5
Agent State: authorized
TS enable: True
Transport: Callhome
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type: Production
sizeof(char) : 1
sizeof(int) : 4
sizeof(long) : 4
sizeof(char *) : 8
sizeof(time_t) : 4
sizeof(size_t) : 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: True
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2
SmartAgentCmReTrySend: True
SmartAgentCmClient: True
SmartAgentCmClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
enableByDefault: False
conversionAutomatic: True
show license usage
License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 29 days, 13 hours, 48 minutes, 12 seconds

(IR1101_Network_Advantage):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Reservation:
    Reservation status: NOT INSTALLED

(IR1101_Network_Essentials):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Reservation:
    Reservation status: NOT INSTALLED

show license reservation
License reservation: ENABLED

Overall status:
Active: PID:IR1101-K9,SN:FCW2150TH0F
Reservation status: SPECIFIC INSTALLED on Nov 07 02:04:55 2018 UTC
Export-Controlled Functionality: Allowed
Last Confirmation code: 9765d8c5

Specified license reservations:
Cisco IR1101 Network Advantage (IR1101_Network_Advantage):
  Description: Cisco Network Advantage Smart License for Cisco IR1101 Industrial Integrated
          Services Router
  Total reserved count: 1
  Term information:
  Active: PID:IR1101-K9,SN:FCW2150TH0F
  License type: TERM
  Start Date: 2018-JUN-13 UTC
  End Date: 2018-DEC-10 UTC
  Term Count: 1

show version
Prerequisites for Smart Licensing

IR1101 Licensing for Cisco IOS-XE release 16.10.1

Cisco IOS-XE software, Version 16.10.01
Cisco IOS Software (Gibraltar), ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1prd7, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 31-Oct-18 23:27 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 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, 51 minutes
Uptime for this control processor is 2 hours, 52 minutes
System returned to ROM by reload
System image file is "usb0:ir1101-universalk9.16.10.01prd7.SPA.bin"
Last reload reason: Reload Command

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

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

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

Technology Package License Information:

-----------------------------------------------------------------------------------------------
Technology-package Technology-package
Current Type Next reboot
-----------------------------------------------------------------------------------------------
network-advantage Smart License network-advantage

Smart Licensing Status: REGISTERED - SPECIFIC LICENSE RESERVATION/AUTHORIZED - RESERVED

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711867K/6147K bytes of memory.
Processor board ID FCW2150TH0F
1 Virtual Ethernet interface
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:.
0K bytes of WebUI ODM Files at webui:.
30670832K bytes of USB Flash at usbflash0:.

Configuration register is 0x0

IR1101#
CHAPTER 7

Web User Interface Management

• Using Web User Interface for Day One Setup, on page 69
• Configure LAN Settings, on page 70
• Configure Primary WAN Settings, on page 70
• Configure Secondary WAN Settings, on page 71
• Configure Security Settings, on page 72
• Summary Screen, on page 72

Using Web User Interface for Day One Setup

To configure the Web user interface:

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

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

Step 2  Set up the authentication options to log into Web UI. You can use one of these methods to authenticate:

a) You can authenticate using local database. To use a local database for Web UI authentication, ensure to have the `ip http authentication local` command in the running configuration. This command is preconfigured on the device. If the command is not present, configure the device as shown in this example:

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

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

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

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

b) Authenticate using AAA options. To use AAA authentication for Web UI, ensure to configure ‘ip http authentication aaa’ on the device. Also, ensure that the required AAA server configuration is present on the device.
Device #configure terminal
Device (config)#ip http authentication local

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

Configure LAN Settings

Refer to the following image for LAN Settings:

Step 1 Select the interface from the drop-down list.
Step 2 Enter the IP address and subnet mask.
Step 3 Note Ensure that you do not use addresses that would conflict with what was previously created in the initial configuration dialog.
Check the Use this as DHCP Server check box, and enter the DHCP pool name and network address. Select the appropriate time zone from the drop-down list.
Step 4 Check the Configure Management Interface check box, and enter the IP address of the management interface.
Step 5 Click Primary WAN Settings.

Configure Primary WAN Settings

Refer to the following image for WAN Settings:
Step 1 Select the primary WAN type for configuring the primary WAN connection. You can configure 3G/4G or Ethernet, as primary WAN depending on the WAN types supported by the router.

Step 2 Select the interface from the drop-down list.

Step 3 Check the Get DNS Server info directly from ISP check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.

Step 4 Check the Get IP automatically from ISP check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

Step 5 Check the Enable NAT check box to enable NAT. It is recommended to enable NAT.

Step 6 Enter the username and password provided by the service provider.

Step 7 Click Security / APP Visibility WAN Settings.

Configure Secondary WAN Settings
For advanced configuration, you should configure the secondary WAN connection. Refer to the following image for Backup WAN:
Step 1  Select the secondary WAN type for configuring the secondary WAN connection. You can configure 3G/4G or Ethernet, as a secondary WAN depending on the WAN types supported by the router.

Step 2  Select the interface from the drop-down list.

Step 3  Check the Get DNS Server info directly from ISP check box to get the DNS server information directly from the service provider. You can also manually enter the Primary DNS and Secondary DNS.

Step 4  Check the Get IP automatically from ISP check box to get the IP address information directly from the service provider. You can also manually enter the IP address and subnet mask.

Step 5  Check the Enable NAT check box to enable NAT. It is recommended to enable NAT.

Step 6  Enter the user name and password provided by the service provider.

## Configure Security Settings

### Before you begin
This screen only appears when Advanced Mode is selected at first launch.

**Step 1**  Check the Enable Cisco Recommended Security Settings check box to ensure that all passwords are not shown in plain text. The passwords are encrypted.

**Step 2**  Click Day 0 Config Summary.

**Step 3**  To preview the configuration, click CLI Preview. After you preview the configuration, click Finish to complete the Day Zero setup.

## Summary Screen

Refer to the following image for the Router Summary:
Step 1  Review the settings that you have configured so far to verify they are accurate.

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

Step 3  Close the CLI Preview window.

Step 4  Click **Finish** to save all of your settings.
Configuring Ethernet Switch Ports

This chapter contains the following sections:

- Configuring VLANs, on page 75
- VLAN Trunking Protocol (VTP), on page 76
- Configuring 802.1x Authentication, on page 77
- Configuring Spanning Tree Protocol, on page 78
- Configuring MAC Address Table Manipulation, on page 79
- Configuring Switch Port Analyzer, on page 80
- Configuring IGMP Snooping, on page 81

Configuring VLANs

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

On the IR1101, all the Fast Ethernet ports are set up in vlan1, which does not need to be created. The default for the Gigabit Ethernet port (gi0/0/0) is Layer 3. If needed, the Gigabit Ethernet port (gi0/0/0) could be set up as Layer 2 and added into vlan1. For example:

```
#config terminal
interface gi0/0/0
switchport
exit
```

The following is an example of a vlan configuration:

```
IR1101#show vlan
VLAN Name VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
---- ----- -------------- ------ ------- -------- ----- -------- ------ ------ ------
1 default           active Fa0/0/1, Fa0/0/2, Fa0/0/3, Fa0/0/4
1002 fddi-default   act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default  act/unsup
```

Cisco IR1101 Integrated Services Router Software Configuration Guide
You can assign a given port to a vlan by following these steps:

```
interface fastethernet0/0/4
switchport access vlan 4

interface vlan 4
ip v4 address ...
ipv6 address autoconf

show vlan
```

IOS-XE version 16.10.1 and above supports Embedded Packet Capture (EPC), which provides an embedded systems management facility that helps in tracing and troubleshooting packets. This feature allows network administrators to capture data packets flowing through, to, and from a Cisco device. The network administrator may define the capture buffer size and type (circular, or linear), the maximum number of bytes of each packet to capture, and the direction of the traffic flow - ingress or egress, or both. The packet capture rate can be throttled using further administrative controls. For example, you can use the available options for filtering the packets to be captured using an Access Control List; and, optionally, further defined by specifying a maximum packet capture rate or by specifying a sampling interval. For additional details see the guide located here: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/epc/configuration/xe-16-10/epc-xe-16-10-book/nm-packet-capture-xe.html

**VLAN Trunking Protocol (VTP)**

VTP is a Layer 2 messaging protocol that maintains VLAN configuration consistency by managing the addition, deletion, and renaming of VLANs on a network-wide basis. VTP minimizes 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.

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

---

**Cisco IR1101 Integrated Services Router Software Configuration Guide**
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, 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:


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

This example shows how to configure an IR1101 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 FastEthernet 0/0/1
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:


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 FastEthernet 0/0/1
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 FastEthernet 0/0/1
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 state 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:

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 FastEthernet 0/0/1 vlan 3
Router(config)# end

The following example shows setting the aging timer.

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

Configuring Switch Port Analyzer

The Cisco IR1101 supports local SPAN only, and up to one SPAN session. You can analyze network traffic passing through ports by using SPAN to send a copy of the traffic to another port on the switch or on another switch that has been connected to a network analyzer or other monitoring or security device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports to a destination port for analysis. SPAN does not affect the switching of network traffic on the source ports. You must dedicate the destination port for SPAN use. Except for traffic that is required for the SPAN or RSPAN session, destination ports do not receive or forward traffic.

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

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


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 FastEthernet 0/0/1
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 FastEthernet 0/0/1
Router(config)# end

The following example shows how to remove gigabit ethernet as a SPAN source for SPAN session 1:
Configuring IGMP Snooping

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

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

Use the `ip igmp snooping enable` command to configure IGMP Snooping on the IR1101.

By default, IGMP snooping is globally enabled in the IR1101.

MLD snooping is also supported on the IR1101, and further information can be found in this documentation set: https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-1/configuration_guide/b_161_consolidated_3850_eg/b_161_consolidated_3850_eg_chapter_01100.html
Configuring IGMP Snooping
Cisco 4G LTE-Advanced Configuration

This section contains the following topics:

- Cisco Fourth-Generation LTE Advanced on the Cisco IR1101 Series Integrated Services Router, on page 83

Cisco Fourth-Generation LTE Advanced on the Cisco IR1101 Series Integrated Services Router


The IR1101 offers LTE support through the use of Pluggable Modules. You can find a list of the supported Pluggable Modules in the IR1101 Industrial Integrated Services Router Hardware Installation Guide.

Cisco LTE Pluggable Modules support the following 4G/3G 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 100 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.

- **3G Evolution-Data Optimized (EVDO or DOrA) Mode**—EVDO is a 3G telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. DOrA refers to EVDO Rev-A. EVDO uses multiplexing techniques including Code Division Multiple Access (CDMA), as well as Time Division Multiple Access (TDMA), to maximize both individual users' throughput and the overall system throughput.

It is important to understand the architecture of the IR1101 series and the relationship between Modems, SIMs, Interface and Controller. The following table helps to illustrate these relationships.

<table>
<thead>
<tr>
<th>Router</th>
<th>Controller</th>
<th>SIM</th>
<th>Modem SubSlot</th>
<th>PDN Interface</th>
<th>Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1101</td>
<td>0/1/0</td>
<td>0/1</td>
<td>0/1</td>
<td>Cellular 0/1/0</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cellular 0/1/1</td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Router</th>
<th>Controller</th>
<th>SIM</th>
<th>Modem SubSlot</th>
<th>PDN Interface</th>
<th>Line</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR1101 (dual modem)</td>
<td>0/3/0</td>
<td>0/1</td>
<td>0/3</td>
<td>Cellular 0/3/0</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Note: Only available in a future expansion module.


For more information on Cisco 4G LTE Advanced SKUs, faceplates, and LED descriptions, see the Cisco IR1101 Series Integrated Services Router (ISR) Hardware Installation Guide here: https://www.cisco.com/c/en/us/td/docs/routers/access/1101/hardware/installation/guide/1101hwinst.html

---

**Prerequisites for Configuring Cisco 4G LTE Advanced**

- 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. Please refer to the RSSI/SNT values as displayed through `show cellular 0/1/0 all` or the LED of the pluggable modem.

- You must have 4G LTE 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 4G LTE or router.

- The standalone antenna that supports GPS capabilities must be installed for the GPS feature to work.

---

**Restrictions for Configuring Cisco 4G LTE Advanced**

- 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 bandwidth is asymmetric with the downlink data rate being greater than the uplink data rate.

- 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 4G LTE Advanced**

The following features are not supported on Cisco 4G LTE Advanced on the IR1101, when compared to Classic IOS:

• TTY support or Line
• Chat script/dialer string
• DM log output to USB flash is not supported.

**4G LTE-Advanced LEDs**

LED status can be obtained through the show led CLI, or visually on the pluggable modem card. The following is an example of the show led CLI:

IR1101#show led
SYSTEM LED : Green
Custom LED : Off
VPN LED : Off
ALARM LED : Off
GigabitEthernet0/0/0 LED : On
FastEthernet0/0/1 LED : Off
FastEthernet0/0/2 LED : Off
FastEthernet0/0/3 LED : Off
FastEthernet0/0/4 LED : Off
LTE module Enable LED : Green
LTE module SIM 0 LED : Green
LTE module SIM 1 LED : Off
LTE module GPS LED : Green
LTE module RSSI 0 LED : On
LTE module RSSI 1 LED : On
LTE module RSSI 2 LED : On
LTE module RSSI 3 LED : Off

The following table describes the LED behavior in 4G LTE-Advanced.
### Table 10: 4G LTE-Advanced LED Indicators

<table>
<thead>
<tr>
<th>LED</th>
<th>Color/Bar and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LTE SIM(0) &amp; SIM(1)</td>
<td>Green (Solid)</td>
</tr>
<tr>
<td></td>
<td>Green Blink</td>
</tr>
<tr>
<td></td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td>Amber (Solid)</td>
</tr>
<tr>
<td>EN</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td>Amber (Solid)</td>
</tr>
<tr>
<td></td>
<td>Green (Solid)</td>
</tr>
<tr>
<td>RSSI - Uses Bars for LED Indication</td>
<td>Four Bar</td>
</tr>
<tr>
<td></td>
<td>Three Bar</td>
</tr>
<tr>
<td></td>
<td>Two Bar</td>
</tr>
<tr>
<td></td>
<td>One Bar</td>
</tr>
<tr>
<td></td>
<td>0 or No Bar</td>
</tr>
<tr>
<td>GPS</td>
<td>Green (Solid)</td>
</tr>
<tr>
<td></td>
<td>Off</td>
</tr>
</tbody>
</table>

### Cisco 4G LTE-Advanced Features

Cisco 4G LTE-Advanced supports the following major features:

- Global Navigation Satellite System (GNSS) (requires a GNSS compliant antenna) 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 (single SIM on the P-LTE-VZ pluggable)
- Auto SIM
- NeMo
• Mobile Network IPv6
• Public Land Mobile Network (PLMN) selection
• IPv6
• Multiple PDN
• LTE Link Recovery

4G GNSS and NMEA

Active GNSS is supported on the SubMiniature version A (SMA) port. Active GNSS antenna is supported only in the standalone mode. An Active GNSS 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 GNSS receiver. Active GNSS antennae require power from the GNSS receiver SMA port to operate.

National Marine Electronics Association (NMEA) streams GNSS data either from a 4G LTE 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 GNSS-based application.

The following GNSS and NMEA features are supported on the Cisco 4GLTE-Advanced:

• GNSS standalone mode (satellite-based GNSS)
• Cisco IOS-XE CLI display coordinates.
• External application displays router map location
• Objects in the CISCO-WAN-3G-MIB supports GNSS and NMEA features
• The Cisco 4G LTE-Advanced only support NMEA over IP and uses show commands in the platform

Note

Assisted GNSS mode is not supported.

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 4G LTE-Advanced 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 0/1/0 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**

**Note**
The P-LTE-VZ pluggable which supports Verizon is a single SIM.

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.

```shell
controller cellular 0/1/0
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.

```shell
controller cellular 0/1/0
lte failovertimer <3-7>
```

You can also manually switch the SIM slot via the command line interface.

```shell
lte sim activate slot <0-1>
```

**Auto SIM**

The Auto SIM feature detects the SIM and loads the corresponding firmware. For example, if an AT&T SIM is detected, the modem loads the AT&T 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.

The P-LTE-US and P-LTE-GB pluggable modules on the IR1101 support Auto SIM.

**Note**
Auto SIM is always enabled by default.
Enable Auto SIM

SUMMARY STEPS

1. configure terminal
2. Cellular slots/sub-slots/interface lte firmware-activate firmware-index

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Cellular slots/sub-slots/interface lte firmware-activate firmware-index</td>
<td>Activates the firmware index.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# cellular 0/1/0 lte firmware-activate 1</td>
<td></td>
</tr>
</tbody>
</table>

Example: List the firmware when Auto-SIM is Enabled

```
Device# show cellular 0/1/0
firmware      Idx Carrier  FwVersion  PriVersion  Status
1  ATT        02.28.00.00  002.035_000  Inactive
2  GENERIC    02.28.00.00  002.035_000  Active
3  ROGERS     02.28.00.00  001.012_000  Inactive
4  SPRINT     02.14.03.02  002.012_000  Inactive
5  VERIZON    02.28.00.00  002.042_000  Inactive
```

Firmware Activation mode = AUTO

Disable Auto SIM

SUMMARY STEPS

1. configure terminal
2. controller cellular slots/sub-slots/interface
3. no lte firmware auto-sim

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
</tbody>
</table>
Example: List the firmware when Auto-SIM is Disabled

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>controller cellular</td>
<td>Specifies the controller interface.</td>
</tr>
<tr>
<td>slots/sub-slots/interface</td>
<td></td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>no lte firmware auto-sim</td>
<td>Disable auto SIM.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# no lte firmware auto-sim</td>
<td></td>
</tr>
</tbody>
</table>

Example: List the firmware when Auto-SIM is Disabled

```
Device# show cellular 0/1/0 firmware
Idx  Carrier   FWVersion  PriVersion  Status
 1    ATT       02.28.00.00  002.035_000  Active
 2    GENERIC   02.28.00.00  002.035_000  Inactive
 3    ROGERS    02.28.00.00  001.012_000  Inactive
 4    SPRINT    02.14.03.02  002.012_000  Inactive
 5    VERIZON   02.28.00.00  002.042_000  Inactive
```

Firmware Activation mode = Manual

Using a SIM Card

Cisco 4G LTE-Advanced 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 4G LTE-Advanced and used without an authorization code.

The SIM can be initially locked with a PIN code (4 to 8 digits 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 4G LTE-Advanced in which the locked SIM resides is moved to a different 4G LTE-Advanced 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 4G LTE-Advanced slot number. This will ensure that the SIM card will not be used in any unauthorized device, or, if there are multiple 4G LTE-Advanced in a single ISR, that the appropriate PIN is applied to each 4G LTE-Advanced 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.

#### SUMMARY STEPS

1. `cellular slots subslots interface lte sim change-pin current-pin new-pin`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Locks or unlocks the SIM card using a PIN code.</td>
</tr>
<tr>
<td><code>cellular slots subslots interface lte sim change-pin current-pin new-pin</code></td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# cellular 0/1/0 lte sim lock 1111 1234</td>
<td></td>
</tr>
</tbody>
</table>

#### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Locks or unlocks the SIM card using a PIN code.</td>
</tr>
<tr>
<td>`cellular unit lte sim {lock</td>
<td>unlock} pin`</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# cellular 0/1/0 lte sim lock 1111</td>
<td></td>
</tr>
</tbody>
</table>

#### Configure CHV1 for Unencrypted Levels

Use either of these commands:

- `lte sim authenticate 0 pin`
- `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.

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> cellular slots subslots interface</td>
<td>Enters the cellular controller configuration mode or</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td>lte sim authenticate 7 1111 slot 0</td>
<td></td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> service password-encryption</td>
<td>Enables password encryption.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router (config)# service password-encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> username privilege var password pin</td>
<td>Creates username and password.</td>
</tr>
<tr>
<td>Example:</td>
<td>name - specifies the username, pin — A 4 to 8 digits PIN code.</td>
</tr>
<tr>
<td>Router (config)# username SIM privilege 0 password 1111</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> do show run</td>
<td>i name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# do show run</td>
<td>i SIM</td>
</tr>
<tr>
<td><strong>Step 4</strong> username privilege 0 password pin</td>
<td>Enters the cellular controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> lte sim authenticate 7pin OR lte sim authenticate 7 pin slot {0</td>
<td>1}</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Device(config-controller)# lte sim authenticate 055A575E70 | 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.  
**Note** The slot keyword and its options are available only on platforms that supports Dual-SIM feature. |

**Step 6**

**exit**  
**Example:**  
Router(config-controller)# exit  
(Optional) Exits the cellular controller configuration mode.

**Step 7**

**no username name**  
**Example:**  
Router(config-controller)# no username SIM  
(Optional) Removes the username and password created in Step 3.

**Step 8**

**no service password-encryption name**  
**Example:**  
Router(config-controller)# no service password-encryption  
(Optional) Removes the username and password created in Step 3.

### Short Message Service (SMS) Capabilities

Cisco 4G LTE-Advanced 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 4G LTE-Advanced also have the capability to revert from LTE SMS to 3G technology if necessary.

A sending device behind a Cisco 4G LTE-Advanced 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.
Data Account Provisioning

One or more modem data profiles can be created to provision a modem on a 4G LTE 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.

**Configuring Cisco 4G LTE Advanced**

For 4G-LTE-Advanced, the numbering for slot 0, module 0, and port 0 is 0/1/0 for all commands.
Verifying Modem Signal Strength and Service Availability

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show cellular unit network</code></td>
<td>Displays information about the carrier network, cell site, and available service.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show cellular 0/1/0 network</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show cellular unit radio</code></td>
<td>Shows the radio signal strength.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show cellular 0/1/0 radio</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show cellular unit profile</code></td>
<td>Shows information about the modem data profiles created.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show cellular 0/1/0 profile</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show cellular unit security</code></td>
<td>Shows the security information for the modem, such as SIM and modem lock status.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show cellular 0/1/0 security</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td><strong>Purpose</strong></td>
</tr>
<tr>
<td><code>show cellular unit all</code></td>
<td>Shows consolidated information about the modem, profiles created, radio signal strength, network security, and so on.</td>
</tr>
<tr>
<td>Example:</td>
<td>Router# show cellular 0/1/0 all</td>
</tr>
</tbody>
</table>

**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 4G LTE Advanced 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 4G LTE Advanced. The following are the default internet profile numbers for the modems:

<table>
<thead>
<tr>
<th>Modem</th>
<th>Profile Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP7607 (Global)</td>
<td>Profile 1</td>
</tr>
</tbody>
</table>
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 0/1/0`.

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 4G LTE Advanced 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.

For the 4G LTE Advanced, the `unit` argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Creates, modifies, or deletes a modem data profile in the privileged EXEC mode.</td>
</tr>
<tr>
<td>`cellular unit lte profile create</td>
<td>delete</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>Router# cellular 0/1/0 lte profile create 2 apn.com pap username pwd ipv4</code></td>
<td></td>
</tr>
</tbody>
</table>

- The `profile-number` argument specifies the profile number created for the modem.
- (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.
- (Optional) The `authentication` parameter specifies the authentication type used. Acceptable parameters are `chap`, `none` (no authentication), `pap`, and `pap_chap` (PAP or CHAP authentication).
• (Optional) The *username* and *password* arguments are given by a service provider. These are mandatory when an authentication type other than *none* is used.

• (Optional) The *PDP* 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).

The *show cellular slot* profile displays configured profile list.

**Note**

Single asterisk (*) displayed against data profile.

Double asterisk (**) displayed against attached profile.

---

**Example**

```bash
router# show cellular 0/1/0 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 = 100.119.136.44
PDP IPV6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64 Scope: Global
Access Point Name (APN) = VZWINTERNET
Authentication = None
  Primary DNS address = 198.224.173.135
  Secondary DNS address = 198.224.174.135
  Primary DNS IPV6 address = 2001:4888:68:FF00:608:D:0:0
  Secondary DNS IPV6 address = 2001:4888:61:FF00:604:D:0:0

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

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 0/1/0 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.
```

Configuration Examples

The following example shows how to change a default profile on 4G LTE Advanced:

```
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 0/1/0 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 = 100.119.136.44
PDP IPV6 address = 2600:1010:B00E:1E11:192D:3E20:199B:3A70/64 Scope: Global
Access Point Name (APN) = VZWINTERNET
Authentication = None
  Primary DNS address = 198.224.173.135
  Secondary DNS address = 198.224.174.135
  Primary DNS IPV6 address = 2001:4888:68:FF00:608:D:0:0
  Secondary DNS IPV6 address = 2001:4888:61:FF00:604:D:0:0

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

**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 4G LTE Advanced, the unit argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> cellular unit lte sim {lock</td>
<td>unlock} pin</td>
</tr>
<tr>
<td>Example: Router# cellular 0/1/0 lte sim lock 1111</td>
<td><em>pin</em>A code (4 to 8 digits long) provided by your carrier to lock or unlock the SIM card.</td>
</tr>
</tbody>
</table>

**Changing the PIN Code**

Perform this task to change the PIN code of a SIM.
For the 4G LTE Advanced, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>cellular unit lte sim change-pin pin new-pin</code></td>
<td>Changes the assigned PIN code. SIM should be in locked state when the PIN is being changed.</td>
</tr>
</tbody>
</table>

Example:
```
Router# cellular 0/1/0 lte sim change-pin 1111 1234
```

### Verifying the Security Information of a Modem

Perform this task to verify the security information of a modem.

### Note

For the 4G LTE Advanced, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

### Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show cellular unit security</code></td>
<td>Shows the security information of the modem, including the SIM lock status.</td>
</tr>
</tbody>
</table>

Example:
```
Router# show cellular 0/1/0 security
```

### 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 101.

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 4G LTE Advanced, the *unit* argument identifies the router slot, module slot, and port separated by slashes (0/1/0).
### Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> controller cellular unit</td>
<td>Enters the cellular controller configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> lte sim authenticate 0 pin</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note</strong> 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 101.</td>
<td></td>
</tr>
</tbody>
</table>

### 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 (0/1/0).
SUMMARY STEPS

1. configure terminal
2. service password-encryption
3. username name privilege 0 password pin
4. do show run | i name
5. controller cellular unit
6. lte sim authenticate {0 | 7} pin
7. exit
8. no username name
9. no service password-encryption

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> service password-encryption</td>
<td>Enables password encryption.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# service password-encryption</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> username name privilege 0 password pin</td>
<td>Creates username and password.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# username SIM privilege 0 password 1111</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• name—Specifies the username.</td>
</tr>
<tr>
<td></td>
<td>• pin— Specifies the four- to eight-digit PIN code.</td>
</tr>
<tr>
<td><strong>Step 4</strong> do show run</td>
<td>i name</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# do show run</td>
<td>i SIM</td>
</tr>
<tr>
<td><strong>Step 5</strong> controller cellular unit</td>
<td>Enters the cellular controller configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> lte sim authenticate {0</td>
<td>7} pin</td>
</tr>
</tbody>
</table>
### Applying a Modem Profile in a SIM Configuration

**SUMMARY STEPS**

1. `configure terminal`
2. `controller cellular unit`
3. `lte sim data-profile number attach-profile number`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters the global configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>controller cellular unit</code></td>
<td>Enters the cellular controller configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# controller cellular 0/1/0</code></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><code>lte sim data-profile number attach-profile number</code></td>
<td>Applies the configured profile number to the SIM and its slot number. The default (primary) slot is 0. The <strong>attach profile</strong> is the profile used by the modem to attach to the LTE network. The <strong>data profile</strong> is the profile used to send and receive data over the cellular network.</td>
</tr>
</tbody>
</table>

**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 4G LTE Advanced, the unit argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

If a tunnel interface is configured with `ip unnumbered cellular 0/1/0`, it is necessary to configure the actual static IP address under the cellular interface, in place of `ip address negotiated`.

**SUMMARY STEPS**

1. `configure terminal`
2. `interface cellular unit`
3. `ip address negotiated`
4. `dialer in-band`
5. `dialer watch-group group-number`
6. `exit`
7. `ip route network-number network-mask {ip-address | interface} [administrative distance] [name name]`
8. `dialer-list dialer-group protocol protocol-name {permit | deny | list access-list-number | access-group}`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router# configure terminal</code></td>
<td></td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface cellular unit</code></td>
<td>Specifies the cellular interface.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config)# interface cellular 0/1/0</code></td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip address negotiated</code></td>
<td>Specifies that the IP address for a particular interface is dynamically obtained.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# ip address negotiated</code></td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td><code>dialer in-band</code></td>
<td>Enables DDR and configures the specified serial interface to use in-band dialing.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# dialer in-band</code></td>
<td></td>
</tr>
<tr>
<td>Step 5</td>
<td><code>dialer watch-group group-number</code></td>
<td>Specifies the number of the dialer access group to which the specific interface belongs.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Router(config-if)# dialer watch-group 1</code></td>
<td></td>
</tr>
</tbody>
</table>
Purpose
Command or Action

Step 6
exit
Example:
Router(config-if)# exit

Purpose
Enters the global configuration mode.

Step 7
ip route network-number network-mask {ip-address | interface} [administrative distance] [name name]
Example:
Router(config)# ip route 209.165.200.225 255.255.255.224 cellular 0/1/0

Purpose
Establishes a floating static route with the configured administrative distance through the specified interface.

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}
Example:
Router(config)# dialer-list 1 protocol ip list 1

Purpose
Creates a dialer list for traffic of interest and permits access to an entire protocol.

Configure Cellular Interface with dialer watch-group

To configure the cellular interface with dialer watch-group, enter the following commands starting in EXEC mode.

Note
For the 4G LTE Advanced, the unit argument identifies the router slot, module slot, and port separated by slashes (0/1/0).

SUMMARY STEPS

1. configure terminal
2. interface cellular unit
3. ip address negotiated
4. dialer in-band
5. ip address negotiated
6. dialer idle-timeout seconds
7. dialer watch-group group-number
8. exit
9. dialer-list dialer-group protocol protocol-name {permit | deny | list access-list-number | access-group}
10. access-list access-list-number permit ip-source-address
11. dialer watch-list watch-group number ip ip mask
12. dialer watch-list watch-group numberdelay route-check initial time in seconds
13. dialer watch-list watch-group number delay connected seconds
# DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| Step 1 | `configure terminal`  
**Example:**  
`Router# configure terminal` | Enters global configuration mode. |
| Step 2 | `interface cellular unit`  
**Example:**  
`Router(config)# interface cellular 0/1/0` | Specifies the cellular interface. |
| Step 3 | `ip address negotiated`  
**Example:**  
`Router(config-if)# ip address negotiated` | Specifies that the IP address for a particular interface is dynamically obtained. |
| Step 4 | `dialer in-band`  
**Example:**  
`Router(config-if)# dialer in-band` | Enables DDR and configures the specified serial interface to use in-band dialing. |
| Step 5 | `ip address negotiated`  
**Example:**  
`Router(config-if)# ip address negotiated` | Specifies that the IP address for a particular interface is dynamically obtained. |
| Step 6 | `dialer idle-timeout seconds`  
**Example:**  
`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 watch-group group-number`  
**Example:**  
`Router(config-if)# dialer watch-group 1` | Enables Dialer Watch on the specific interface. |
| Step 8 | `exit`  
**Example:**  
`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}`  
**Example:**  
`Router(config)# dialer-list 1 protocol ip list 1` | Creates a dialer list for traffic of interest and permits access to an entire protocol. |
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 10 access-list access-list-number permit ip-source-address</td>
<td>Defines traffic of interest.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# access-list 1 permit any</td>
<td></td>
</tr>
<tr>
<td>Step 11 dialer watch-list watch-group number ip ip mask</td>
<td>Defines traffic of interest.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dialer watch-list 1 ip 5.6.7.8 255.255.255</td>
<td></td>
</tr>
<tr>
<td>Step 12 dialer watch-list watch-group number delay route-check initial time in seconds</td>
<td>Defines traffic of interest.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dialer watch-list 1 delay route-check initial 60</td>
<td></td>
</tr>
<tr>
<td>Step 13 dialer watch-list watch-group number delay connected seconds</td>
<td>Defines traffic of interest.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# dialer watch-list 1 delay connected 1</td>
<td></td>
</tr>
</tbody>
</table>

### 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 4G LTE Advanced.

**Note**

For a 4G LTE-Advanced, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/1/0).

### SUMMARY STEPS

1. configure terminal
2. controller cellular *unit*
3. lte gps enable
4. lte gps mode standalone
5. lte gps nmea {ip | udp [source address][destination address][destination port] }
6. end
7. test cellular *unit* modem-power-cycle
8. show cellular *unit* gps
9. show cellular *unit* gps detail
### Detailed Steps

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td>configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Enters the controller cellular configuration mode.</td>
</tr>
<tr>
<td>controller cellular unit unit</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>(Optional) GPS is enabled by default. Use this command to enable the GPS feature if GPS has been disabled for any reason.</td>
</tr>
<tr>
<td>lte gps enable</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# lte gps enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Enables the standalone GPS mode.</td>
</tr>
<tr>
<td>lte gps mode standalone</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# lte gps mode standalone</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Enables NMEA. Cisco 4G LTE Advanced support only IP NMEA. Therefore, the IP interface and serial interface options are unavailable.</td>
</tr>
<tr>
<td>lte gps nmea {ip</td>
<td>udp [source address][destination address][destination port]}</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# lte gps nmea ip</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# lte gps nmea</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Exits the controller configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td>end</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>GPS can take effect only after modem power cycle.</td>
</tr>
<tr>
<td>test cellular unit unit modem-power-cycle</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# test cellular 0/1/0 modem-power-cycle</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Displays a summary of the following GPS data:</td>
</tr>
<tr>
<td>show cellular unit gps</td>
<td></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# show cellular 0/1/0 gps</td>
<td></td>
</tr>
<tr>
<td>GPS Feature = enabled</td>
<td></td>
</tr>
<tr>
<td>GPS Mode Configured = standalone</td>
<td></td>
</tr>
<tr>
<td>GPS Port Selected = Dedicated GPS port</td>
<td></td>
</tr>
<tr>
<td>GPS Status = GPS coordinates acquired</td>
<td></td>
</tr>
<tr>
<td>Last Location Fix Error = Offline [0x0]</td>
<td></td>
</tr>
<tr>
<td>Latitude = 37 Deg 25 Min 4.8915 Sec North</td>
<td></td>
</tr>
<tr>
<td>Longitude = 121 Deg 55 Min 8.5627 Sec West</td>
<td></td>
</tr>
<tr>
<td>Timestamp (GMT) = Wed Nov 7 21:54:18 2018</td>
<td></td>
</tr>
<tr>
<td>Fix type index = 0, Height = 8 m</td>
<td></td>
</tr>
<tr>
<td>Satellite Info</td>
<td></td>
</tr>
</tbody>
</table>
**Command or Action**

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
</table>
| Satellite #1, elevation 45, azimuth 303, SNR 20 *
Satellite #3, elevation 15, azimuth 296, SNR 21
Satellite #8, elevation 9, azimuth 227, SNR 27 *
Satellite #11, elevation 41, azimuth 270, SNR 27 *
Satellite #18, elevation 64, azimuth 258, SNR 29 *
Satellite #22, elevation 35, azimuth 303, SNR 22 *
Satellite #31, elevation 51, azimuth 140, SNR 24 *
Satellite #32, elevation 46, azimuth 43, SNR 22 *
Satellite #10, elevation 25, azimuth 97, SNR 0
Satellite #14, elevation 68, azimuth 26, SNR 0

*Satellite #1, elevation 45, azimuth 303, SNR 0
Satellite #3, elevation 15, azimuth 296, SNR 0

!!!... truncated !!!!

---

**Step 9**

**show cellular unit gps detail**

**Example:**

Router# `show cellular 0/1/0 gps detail`

GPS Feature = enabled
GPS Mode Configured = standalone
GPS Port Selected = Dedicated GPS port
GPS Status = GPS coordinates acquired
Last Location Fix Error = Offline (0x0)
Latitude = 37 Deg 25 Min 4.5209 Sec North
Longitude = 121 Deg 55 Min 8.5209 Sec West
Timestamp (GMT) = Wed Nov 7 21:53:52 2018
Fix type index = 0, Height = 7 m
HDOP = 1.5, GPS Mode Used = standalone

Satellite Info

<table>
<thead>
<tr>
<th>Purpose</th>
</tr>
</thead>
</table>
| Satellite #8, elevation 9, azimuth 227, SNR 31 *
Satellite #11, elevation 41, azimuth 270, SNR 32 *
Satellite #18, elevation 64, azimuth 258, SNR 33 *
Satellite #22, elevation 35, azimuth 303, SNR 26 *
Satellite #31, elevation 51, azimuth 140, SNR 27 *
Satellite #32, elevation 46, azimuth 43, SNR 22
Satellite #1, elevation 45, azimuth 303, SNR 0
Satellite #3, elevation 14, azimuth 296, SNR 0

!!!... truncated !!!!

**Configuring 4G SMS Messaging**

**Note**

For an 4G LTE Advanced, the *unit* argument identifies the router slot, module slot, and the port, and is separated by slashes (0/1/0).
SUMMARY STEPS

1. configure terminal
2. controller cellular unit
3. lte sms archive path FTP-URL
4. cellular unit lte sms view { all | ID | summary }
5. end
6. show cellular unit sms
7. cellular unit lte sms send number
8. cellular unit lte sms delete [ all | id ]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters the configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> controller cellular unit</td>
<td>Enters the controller cellular configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> lte sms archive path FTP-URL</td>
<td>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:</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router(config-controller)# lte sms archive path</td>
<td></td>
</tr>
<tr>
<td>ftp://username:password@172.25.211.175/SMS-LTE</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> cellular unit lte sms view { all</td>
<td>ID</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# cellular 0/1/0 lte sms view summary</td>
<td></td>
</tr>
<tr>
<td>ID FROM YY/MM/DD HR:MN:SC SIZE CONTENT</td>
<td></td>
</tr>
<tr>
<td>0 4442235525 12/05/29 10:50:13 137 Your entry last month has...</td>
<td></td>
</tr>
<tr>
<td>2 555333777 13/08/01 10:24:56 5 First</td>
<td></td>
</tr>
<tr>
<td>3 555333777 13/08/01 10:25:02 6 Second</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> end</td>
<td>Exits the configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td>Router# end</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> show cellular unit sms</td>
<td>Displays all the information in the text messages sent and received. Message information includes text messages sent successfully, received, archived, and messages pending to</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| `Router# show cellular 0/1/0 sms` | Incoming Message Information  
SMS stored in modem = 20  
SMS archived since booting up = 0  
Total SMS deleted since booting up = 0  
Storage records allocated = 25  
Storage records used = 20  
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 = ftp://lab:lab@1.3.150.1/outbox | 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**  
**Example:**  
`Router# cellular 0/1/0 lte sms send 15554443333 <sms text>`  
Enables a user to send a 4G LTE 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.  
**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 ]**  
**Example:**  
`Router# cellular 0/1/0 lte sms delete [ all | id ]`  
(Optional) Deletes one message ID or all of the stored messages from memory.

### 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.
## Configuring Modem DM Log Collection

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> controller cellular slot</td>
<td>Enters cellular controller configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> lte modem dm-log [autostop</td>
<td>Configures DM logging for LTE modem.</td>
</tr>
<tr>
<td></td>
<td>• autostop—Automatically stops DM log capturing based on:</td>
</tr>
<tr>
<td></td>
<td>• link-down—cellular interface link down event</td>
</tr>
<tr>
<td></td>
<td>• timer time—amount of time in minutes</td>
</tr>
<tr>
<td></td>
<td>• enable—Starts DM log capturing.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• filter location:filename—Specifies the DM log filter to use from the following locations:</td>
</tr>
<tr>
<td></td>
<td>—bootflash:file</td>
</tr>
<tr>
<td></td>
<td>—flash:file</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Bootflash and flash are the only valid locationsto store the DM log filter file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the DM log filter file is not specified, the generic filter file, which comes with the router will be used.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The DM log filter file needs to be in .sqf format.</td>
</tr>
<tr>
<td></td>
<td>• rotation—Enables continuous DM log capturing by replacing the oldest DM log files with the latest.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-controller)# lte modem dm-log enable</td>
<td></td>
</tr>
<tr>
<td>Step 4</td>
<td>Command or Action</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>end</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td>Router(config-controller)# end</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 5</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show cellular unit logs dm-log</td>
<td>(Optional) Displays DM log configuration and statistics.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Router# show cellular 0/1/0 logs dm-log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Integrated DM logging is on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>output path = Utility Flash</td>
<td></td>
</tr>
<tr>
<td></td>
<td>filter = MC74xx generic -</td>
<td></td>
</tr>
<tr>
<td></td>
<td>v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>maximum log size = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>maximum file size = 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>log rotation = disabled</td>
<td></td>
</tr>
<tr>
<td></td>
<td>33 packets sent to the modem, 4663 bytes, 0 errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>28521 packets received from the modem, 13500758 bytes, 0 input drops</td>
<td></td>
</tr>
<tr>
<td></td>
<td>28521 packets stored in utility flash, 13500758 bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>current file size = 13500758</td>
<td></td>
</tr>
<tr>
<td></td>
<td>current log size = 13500758</td>
<td></td>
</tr>
<tr>
<td></td>
<td>total log size = 13500758</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Utility Flash DM log files = (1) files</td>
<td></td>
</tr>
</tbody>
</table>

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 0/1/0
Router(config-controller)# lte modem dm-log filesize 512
```

The following example shows how to specify the filter file for LTE:

```
Router(config-controller)# controller cell 0/1/0
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 0/1/0
Router(config-controller)# lte modem dm-log rotation
```

The following example shows how to specify the maximum log size for LTE:
The following example shows how to enable DM log rotation for LTE:

```
Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log enable
```

The following example shows how to specify the maximum log size for LTE:

```
Router(config-controller)# controller cell 0/1/0
Router(config-controller)# lte modem dm-log size 1024
```

The following example shows what was configured on the router for DM log feature:

```
Router# show running-config | section controller
controller Cellular 0/1/0
    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 0/1/0 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
```

The following shows the DM log files created:

```
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-slot2-20180607-181125.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 how to disable/stop DM log capturing:

```
Router(config)#controller cellular 0/1/0
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.

To enable modem crashdump collection, perform the following steps.

Note

The integrated modem crashdump collection feature is supported only on 3G HSPA and 4G LTE Advanced based SKUs.

Before you begin

The device will need to be in boot-and-hold mode.

Router# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# controller cel 0/1/0
Router(config-controller)# lte modem crash-action?
boot-and-hold Remain in crash state

Router(config-controller)# lte modem crash-action boot-and-hold

This ensures that whenever the router crashes, it will stay in that state and will not try to recover. By default the crash-action is reset which means the modem will reset and try to recover itself whenever it crashes. The above boot-and-hold command is used to keep the modem in a crashed state so that you can capture crashdump using the following command:

Router# test cell-cwan 0/1/0 modem-crashdump?
off Disable Modem firmware crash dump
on Enable Modem firmware crash dump

Router# test cell-cwan 0/1/0 modem-crashdump on

This will capture the crashdump and store it in flash.

Procedure

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 1**

| test {cell-cwan} unit modem-crashdump {on location| off} |
|--------------------------------------------------------|

**Example:**

Router# test cell-host 0/1/0 modem-crashdump on local_uf

<table>
<thead>
<tr>
<th>Enables or disables modem crashdump collection.</th>
</tr>
</thead>
</table>

- **cell-host**
  - Keyword for fixed platform.

- **cell-cwan**
  - Keyword for LTE on a modular inside platform.

- **unit**
  - For LTE module, this is the router slot, module slot, and port separated by slashes (for example, 0/1/0). For fixed platform, this is the number 0.

- **on**
### 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.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>show cellular unit log error</code></td>
<td>Shows modem log error and dump information.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# show cellular 0/1/0 log error</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>test cellular unit modem-error-clear</code></td>
<td>(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!errcr=–1” for CDMA and “at!err=0” for GSM modems.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td><code>Router# test cellular 0/1/0 modem-error-clear</code></td>
<td></td>
</tr>
</tbody>
</table>

### Verifying the 4G LTE Advanced Router Information

You can verify the configuration by using the following show commands:

`show version`

```
Router#show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
```
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 09-Nov-18 18:08 by mcpre

Cisco IOS-XE software, Copyright (c) 2005-2018 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 14 hours, 36 minutes
Uptime for this control processor is 14 hours, 37 minutes
System returned to ROM by reload
System restarted at 08:47:04 GMT Mon Nov 12 2018
System image file is "bootflash:ir1101-universalk9.16.10.01.SPA.bin"
Last reload reason: Reload Command

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

A summary of U.S. laws governing Cisco cryptographic products may be found at:

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

Technology Package License Information:

<table>
<thead>
<tr>
<th>Technology-package</th>
<th>Type</th>
<th>Technology-package</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current</td>
<td>Smart License</td>
<td>Smart License</td>
</tr>
<tr>
<td>Next reboot</td>
<td>network-essentials</td>
<td>network-essentials</td>
</tr>
</tbody>
</table>

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711861K/6147K bytes of memory.
Processor board ID FCN222700MY
3 Virtual Ethernet interfaces
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
4098072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:
show platform

router# sh platform
Chassis type: IR1101-K9

Slot Type State Insert time (ago)
--------- ------------------- --------------------- -----------------
0 IR1101-K9 ok 1w1d
0/0 IR1101-ES-5 ok 1w1d
0/1 P-LTE-GB ok 1w1d
R0 IR1101-K9 ok, active 1w1d
F0 IR1101-K9 init, active 1w1d

show interfaces

router# sh interface cellular 0/1/0
Cellular 0/1/0 is up, line protocol is up
  Hardware is LTE Adv CAT6 - Europe/North America Multimode LTE/DC-HSPA+/HSPA+/HSPA/UMTS/IMT-2000
  Internet address is 10.14.162.11/32
  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
  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

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:

**SUMMARY STEPS**

1. configure terminal
2. controller cellular unit
3. {lte} modem link-recovery disable | no lte | modem link-recovery disable
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><code>configure terminal</code></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><code>controller cellular unit</code></td>
<td>Enters cellular controller configuration mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>`{lte} modem link-recovery disable</td>
<td>no lte</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router(config-controller)# lte modem link-recovery disable</td>
<td>Enables or disables the cellular modem link recovery feature.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Once we enable link-recovery, the default Cisco recommended values for link-recovery parameters are populated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We can change the values of link-recovery parameters from the default Cisco recommended values, by using cli for each parameter like in example.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Changing the default recommended cisco values is not advised as it will impact ideal performance of link-recovery feature.</td>
</tr>
<tr>
<td>4</td>
<td><code>end</code></td>
<td>Exits the configuration mode and returns to the privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong>&lt;br&gt;Router(config)# end</td>
<td></td>
</tr>
</tbody>
</table>

### 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 11: Link Recovery Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rssi onset-threshold</td>
<td>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.</td>
</tr>
<tr>
<td>monitor-timer</td>
<td>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.</td>
</tr>
<tr>
<td>wait-timer and debounce-count</td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 0/1/0 Interface Cellular0/1/0
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 0/1/0
Interface Cellular0/1/0
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 0/1/0 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 0/1/0 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]  

Configuration Examples for 4G LTE Advanced

Example: Basic Cellular Interface Configuration: Cisco 4G LTE Advanced

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 Cellular0/1/0  
description Basic-Config  
ip address negotiated  
load-interval 30  
dialer in-band  
dialer idle-timeout 0  
dialer watch-group 1  
pulse-time 1  
ip virtual-reassembly  
dialer watch-list 1 ip 5.6.7.8 255.255.255.255  
dialer watch-list 1 delay route-check initial 60  
dialer watch-list 1 delay connect 1  
dialer-list 1 protocol ip permit  
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0

Configuration Examples for Cisco 4G LTE Advanced

The following example shows how to configure Cisco 4G LTE Advanced:

!  
! Last configuration change at 19:14:26 UTC Fri Oct 19 2018  
!  
version 16.10  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service internal  
service call-home  
platform qfp utilization monitor load 80  
no platform punt-keepalive disable-kernel-core  
no platform punt-keepalive settings
hostname IR1101

boot-start-marker
boot system flash ir1101-universalk9.16.10.SSA.bin
boot-end-marker

no aaa new-model
call-home
  If contact email address in call-home is configured as sch-smart-licensing@cisco.com
  the email address configured in Cisco Smart License Portal will be used as contact email
  address to send SCH notifications.
call-home transport-method email
  If call-home transport-method configured is email
  the email address configured in Cisco Smart License Portal will be used as contact email
  address to send SCH notifications.

ip admission watch-list expiry-time 0

login on-success log

crypto pki trustpoint TP-self-signed-2240381033
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2240381033
  revocation-check none
  rsakeypair TP-self-signed-2240381033

crypto pki certificate chain TP-self-signed-2240381033
  certificate self-signed 01
  30820330 30820218 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  31312F30 2D6560355 04033126 494F533D 53656C662D5369676E65642D4365727469636174652D32323430333831303330820122300D0609 2A864886 F70D0101 0505000382010100 9F1269A8 349CFE9D E2801B79 4F82F1ED 44F8E434 E6A26A32 2F089779 6F8B85D0 942E0F8 FFC2F433 A0F7A08
  4E6F521B BF97A7EA 51563827 7D85417E CBBDE865 9C7B3E76 542DAB69 046DF4E
  3406A83F 6CCA8BD AC5BF38C 49CA95CF 5E5AE099 6A92122D 8B64412D 9972FBF
  2B1B8ED7 E1EAAD66 A52B216A DA2AEE76 9868C116 932EEFE4 A968FAF2 F394C361
  A7DA49AB 9402BB80 52CD0D39 763DDCCA E6F689C2 2881015B F380E17D A8854BE9
  FA2F1E76 0EC88583 E0C0BB86 B134A2CF 20046280 F908883D 51EF6E6A 719D19E9

Cisco IR1101 Integrated Services Router Software Configuration Guide

Cisco 4G LTE-Advanced Configuration Examples for Cisco 4G LTE Advanced
quit

crypto pki certificate chain SLA-TrustPoint
certificate ca 01

30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
3D103050 300D0635 040A1305 43697363 6F312030 0E063035 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 30820122 300D0609 2A864886 F70D0101 0B050030
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
3D103050 300D0635 040A1305 43697363 6F312030 0E063035 04031317 43697363
6F204C69 63656E73 696E6720 526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222E1A F1E6F6AD
CBB4C798 212AA147 C655D8D7 9F7138BD 871141E 1AAFF071 A99A6388 8A38E520
1C394D78 462EF239 C659F715 9B8CA5A5 5BB83C0D 0CFBEBEA 700A8BF7 D8F254EE
4AAE80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
7390A3EB 285436AD C847A2C5 DB553EB 69A9A535 8E59F3E3 0B050030
68E69491 20F320E7 94BE71D7 AE3BC884 F10684C7 4BC8E00F 539BA42B 42C868BB
C7470906 B4CB2D62 EA2FS05D CB062A4 6811D95B E8250FC4 5D5D58FB 8F27D191
C55F0D76 6F94CD3 3D92327 A88038BD 4E67D069 7CBADF88 F54F3686 9513SE48
DPC7C6C6 040D7D91 02030100 01A34230 40300E06 03551D01 0101FF04 04030201
06300F06 03551D13 0101FF04 05300001 01FF301D 06035510 0E041604 149DC85
4B3D31E5 1B364EA7 606A333 3D3B4C73 E8300D06 092A8648 86F70D01 013B500
03820101 00507F24 D9326A66 86025D9F E858A6EC 0D4F6BF6 4963C178 24DA00S
604EDC5E 04FED2BE 77FC6660 CD563FDB DD4668E 3A5673AB 9093D3B1 6C9E380B
D8987BF E04CD9DE 1AECA0C2 2198BBSC E895866D C986B64 5575146 6DFC6CA8
467A3DF4 4D565700 6ADF0FD0 CF830515 3C04FF7C 21E878AC 11ABCD2 55A9232C
7CA7B8E6 C1AF74F6 15Z9989B B1CFF9BB E973D7E7 5BDDEB69 2C8E3A9 17630808
5C8A04A9 92A2FE7F 494EA9E 07885737 3C7C8E9E 39F08E73 80002C6D 6D7ACECA E8BE7C9F 8028787B 35202C0 06E4616A 86823DBD 2303E8AE
418616A9 4093E049 4D10AB75 278826F9 392E355B 8862F3DE 0275156F 719BB2F0
D697DF7F 28

quit

license udi pid IR1101-K9 sn FCW2227XXXX
license boot level network-advantage
license smart transport callhome
diagnostic bootup level minimal

spanning-tree mode rapid-pvst
spanning-tree extend system-id
memory free low-watermark processor 50290

redundancy

controller Cellular 0/1/0
lte sim data-profile 3 attach-profile 1 slot 0
lte firmware auto-sim
lte modem link-recovery disable

controller Cellular 0/3/0
lte firmware auto-sim
lte modem link-recovery disable

vlans internal allocation policy ascending

interface GigabitEthernet0/0/0
ip address 175.1.1.1 255.255.255.0
interface FastEthernet0/0/1
shutdown
interface FastEthernet0/0/2
shutdown
!
interface FastEthernet0/0/3
shutdown
!
interface FastEthernet0/0/4
switchport access vlan 168
switchport mode access
!
interface GigabitEthernet0/0/5
!
interface Cellular0/1/0
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/1/1
no ip address
shutdown
!
interface Vlan1
no ip address
!
interface Vlan168
ip address 192.168.10.22 255.255.255.0
!
interface Async0/2/0
no ip address
encapsulation slip
!
!
ip default-gateway 172.27.138.129
ip forward-protocol nd
!
ip http server
ip http authentication local
ip http secure-server
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ip route 172.27.0.0 255.255.0.0 172.27.138.129
!
access-list 1 permit any
access-list 2 permit any
dialer watch-list 1 ip 5.6.7.8 255.255.255.255
dialer watch-list 1 delay route-check initial 60
dialer watch-list 1 delay connect 1
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
dialer-list 2 protocol ip permit
dialer-list 2 protocol ipv6 permit
ipv6 route ::/0 Cellular0/1/0
!
control-plane
!
line con 0
exec-timeout 0 0
transport input none
stopbits 1
speed 115200
line 0/2/0
line vty 0 4
  password cisco
  login
  transport input all
  transport output all
!
end

Cellular Back-off

Cellular Backoff is a feature introduced in IOS which addresses the concerns about Cisco LTE router not performing backoff in error handling. When PDP Context activation is failing, modems may receive from a cellular service provider. As a result, when some specific error codes (for example: 29, 33) are received by the modem from a cellular network, the router’s IOS incrementally adds interval in sending PDP Context Activation requests and any IP traffic such as not to load service provider network with requests that are known to IOS as failing. Once PDP Context is established and IP traffic is successful, the Cellular Backoff is removed for normal operation.

This back-off implementation will be a generic design and will NOT be specific to a particular service provider. There will be NO IOS CLI command to disable this new feature either.

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 Cellular0/1/0
tunnel destination a.b.c.d
interface Cellular0/1/0
ip address negotiated
no ip mroute-cache
dialer in-band
dialer-group 1

Example: 4G LTE Advanced as Backup with NAT and IPSec

The following example shows how to configure the 4G LTE Advanced 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...`).

```plaintext
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 Gi 0/0/0
   no ip address
   ip virtual-reassembly
   load-interval 30
   no atm ilmi-keepalive
   dsl operating-mode auto
!
backup interface Cellular0/1/0
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 Cellular0/1/0
ip address negotiated
ip nat outside
ip virtual-reassembly
no ip mroute-cache
dialer in-band
dialer idle-timeout 0
dialer watch-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 Cellular0/1/0 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
  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
  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 Cellular0/1/0
  !
exectimeout 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 0/1/0 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 0/1/0 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
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 0/1/0 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 0/1/0 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# sh cellular 0/1/0 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 0/1/0 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 0/1/0 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# sh cellular 0/1/0 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# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# controller cellular 0/1/0
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#

Cisco IR1101 Integrated Services Router Software Configuration Guide
131

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 0/1/0 security
Card Holder Verification (CHV1) = Enabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3
Router#!! SIM is in unlocked state.!!Router#
Router# cellular 0/1/0 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 0/1/0 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 0/1/0 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 verification
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# sh cellular 0/1/0 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.
lat 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# cellular 0/1/0
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# show cellular 0/1/0 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 0/1/0
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 IR1101 uses Sierra Wireless modems that are supported on Cisco 4G LTE Advanced. 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.

Prior to performing the cellular modem firmware upgrade, make sure of the following:

- The "microcode reload ..." command is issued only from router's base directory.
- The modem firmware directory must contain the following:
  - Only the *.cwe file
  - Only the *.nvu file
  - Only a matching pair of *.cwe and *.nvu files for the exact same version
- The modem firmware directory MUST NOT contain any other files

**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.

---

**Note**

Not all IR1101 cellular interfaces can support 2G (only P-LTE-GB), and may not support 3G (P-LTE-VZ).

Details about supported cellular pluggable module SKUs and modems can be found in the IR1101 Hardware Installation Guide here: https://www.cisco.com/c/en/us/td/docs/routers/access/1101/hardware/installation/guide/1101hwinst/pview.html#72641

You can determine which radio bands are supported by using the following command:

```
IR1101# show cellu 0/1/0 radio band
```

LTE bands supported by modem:
- Bands 1 3 7 8 20 28.
LTE band Preference settings for the active sim(slot 0):
- Bands 1 3 7 8 20 28.

Non-LTE bands supported by modem:
Index:
72 - GSM DCS band (1800)
73 - GSM Extended GSM (E-GSM) band (900)
87 - WCDMA (Europe, Japan, and China) 2100 band
114 - WCDMA Europe and Japan 900 band

Non-LTE band Preference settings for the active sim(slot 0):
Index:
72 - GSM DCS band (1800)
73 - GSM Extended GSM (E-GSM) band (900)
87 - WCDMA (Europe, Japan, and China) 2100 band
114 - WCDMA Europe and Japan 900 band

Band index reference list:

Indices 1-64 correspond to LTE bands 1-64.
Indices 65-128 correspond to Non-LTE bands.

---

Upgrading the Modem Firmware Manually With CLI

**SUMMARY STEPS**

1. Go to the Cisco Wireless WAN software download website at:
   http://software.cisco.com/download/navigator.html
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.

3. Select and download the appropriate firmware.

4. **terminal monitor**

5. **microcode reload cellular** pa-bay slot modem-provision [flash:<firmware_directory_name>]

6. **show cellular 0/1/0 hardware**

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Go to the Cisco Wireless WAN software download website at: <a href="http://software.cisco.com/download/navigator.html">http://software.cisco.com/download/navigator.html</a></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>On the Cisco Wireless WAN software page, go to <strong>Products -&gt; Cisco Interfaces and Modules -&gt; Cisco High-Speed WAN interface Cards</strong> and select your product from the list of available cards.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select and download the appropriate firmware.</td>
</tr>
</tbody>
</table>
| **Step 4** | **terminal monitor**  
  **Example:**  
  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>]  
  **Example:**  
  Router# microcode reload cellular 0 2 modem-provision bootflash:/<firmware_directory> | Initiates the firmware upgrade process. **Note** Modem firmware upgrade may take 10-15 mins from issuing the **microcode reload** command to the modem coming up. The router console will display ‘FW_UPGRADE: Firmware upgrade success.....’ message to indicate the firmware upgrade completed. The modem will reset itself and may take an additional 5 minutes to be up in-service.  
  • pa-bay—Use 0 for 4G LTE Advanced.  
  • slot—For 4G LTE Advanced, slot number, 0 to 3, where the 4G LTE Advanced is plugged in.  
  • For remote download, you can transfer this using the wireless link from Cisco.com onto flash. |
| **Step 6** | **show cellular 0/1/0 hardware** | Verifies the cellular modem type, model, carrier, firmware, PRI, SKU, IMEI and other modem details. |
Manual Modem Firmware Upgrade: Example

Router# sh cellu 0/1/0 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 Cellular0/1/0, 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: 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 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: Cellular0/1/0 Modem radio has been turned on
*Jul 6 10:21:57.276: %LINK-3-UPDOWN: Interface Cellular0/1/0, 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 0/1/0 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 0/1/0
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# show cellular 0/1/0 log dm-log
tegrated DM logging is off
Output path = bootflash:
Filter Type = Default
Filter Name = v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf
Maximum log size = 0 MB
Maximum file size = 0 MB
Log rotation = Disabled

IR1101# show cellular 0/1/0 log dm-log details
Integrated DM logging is off
Output path = bootflash:
Filter Type = Default
Filter Name = v11026_Generic_GSM_WCDMA_LTE_IP-no-data-packets.sqf
Maximum log size = 0 MB
Maximum file size = 0 MB
Log rotation = Disabled

0 Packets sent to the modem, 0 Bytes, 0 Errors
0 Packets received from the modem, 0 Bytes, 0 Input drops
0 Packets stored in file system, 0 Bytes, 0 Errors, 0 Aborts
0 Max rcv queue size

Current file size = 0 MB
Current log size = 0 MB
Total log size = 0 MB
IR1101#
SNMP MIBs

A MIB (Management Information Base) is a database of the objects that can be managed on a device. The managed objects, or variables, can be set or read to provide information on the network devices and interfaces. You can find complete information on MIBs and the MIB locator here: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

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 4G LTE Advanced:

- 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)
SNMP 4G LTE Advanced Configuration: Example

The following example describes how to configure 3G 4G MIB trap on the router:

```
controller Cellular 0/1/0
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 -95
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 4G LTE Advanced feature.

You can download the MIBs from the Cisco MIB Locator at [http://www.cisco.com/go/mibs](http://www.cisco.com/go/mibs).
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 cell0/1/0`
   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:

**SUMMARY STEPS**

1. Ensure at least one antenna is connected to the 'MAIN' RF port on the 4G module. Preferably both MAIN and DIV RF ports should be connected to antenna for better RF signal. Check to ensure the antenna are threaded and tightened.
2. If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved.
3. Contact your wireless service provider to verify if there is service availability in your area.

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Ensure at least one antenna is connected to the 'MAIN' RF port on the 4G module. Preferably both MAIN and DIV RF ports should be connected to antenna for better RF signal. Check to ensure the antenna are threaded and tightened.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> If you are using a remote antenna, move the antenna cradle and check if the RSSI has improved.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> Contact your wireless service provider to verify if there is service availability in your area.</td>
<td></td>
</tr>
</tbody>
</table>
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 0/1/0 all
Hardware Information
====================
Modem Firmware Version = SWI9X07Y_02.18.05.00
Device Model ID = WP7603
International Mobile Subscriber Identity (IMSI) = 001012345678901
International Mobile Equipment Identity (IMEI) = 359528080002501
Integrated Circuit Card ID (ICCID) = 89860000502000180722
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Factory Serial Number (FSN) = U3734285450506
Modem Status = Modem Online
Current Modem Temperature = 49 deg C
PRI SKU ID = 1103507, PRI version = 002.041_002, Carrier = GENERIC
OEM PRI version = 002.000

Profile Information
---------------------
Profile 1 = ACTIVE* **
-------
PDP Type = IPv4v6
PDP address = 192.1.1.21
PDP IPV6 address = FC01:ABAB:CDCD:EFE0:7DC4:256:B64F:22F8/64 Scope: Global
Access Point Name (APN) = broadband
Authentication = None
Primary DNS address = 192.1.1.2
Primary DNS IPV6 address = FC01:CAFE:0:0:0:0:0:1
Secondary DNS IPV6 address = 0:0:0:0:0:0:0:0

* = Default profile
** = LTE attach profile

Configured default profile for active SIM 0 is profile 1.

Data Connection Information
-----------------------------
Profile 1, Packet Session Status = ACTIVE
Cellular0/1/0:
Data Packets Transmitted = 31546 , Received = 57008
Data Transmitted = 5049096 bytes, Received = 7702570 bytes
IP address = 192.1.1.21
IPV6 address = FC01:ABAB:CDCD:EFE0:7DC4:256:B64F:22F8/64 Scope = Global
Primary DNS address = 192.1.1.2
Primary DNS IPV6 address = FC01:CAFE:0:0:0:0:0:1
Secondary DNS IPV6 address = 0:0:0:0:0:0:0:0

Profile 2, Packet Session Status = INACTIVE
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 = Thu Jan 10 8:31:28 1980
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = Test PLMN 1-1
Mobile Country Code (MCC) = 1
Mobile Network Code (MNC) = 1
Packet switch domain (PS) state = Attached
Registration state (EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1
Cell ID = 256
Negotiated network MTU = 1500

Radio Information

Radio power mode = online
LTE Rx Channel Number = 2175
LTE Tx Channel Number = 20175
LTE Band = 4
LTE Bandwidth = 20 MHz
Current RSSI = -68 dBm
Current RSRP = -102 dBm
Current RSRQ = -13 dB
Current SNR = 19.4 dB
Physical Cell Id = 0
Number of nearby cells = 1
Idx PCI (Physical Cell Id)
1 0
Radio Access Technology (RAT) Preference = AUTO
Radio Access Technology (RAT) Selected = LTE

LTE bands supported by modem:
- Bands 2 4 5 12.
LTE band Preference settings for the active sim(slot 0):
- Bands 2 4 5 12.

Non-LTE bands supported by modem:
Index:
88 - WCDMA US PCS 1900 band
90 - WCDMA US 1700 band
91 - WCDMA US 850 band

Non-LTE band Preference settings for the active sim(slot 0):
Index:
88 - WCDMA US PCS 1900 band
90 - WCDMA US 1700 band
91 - WCDMA US 850 band

Band index reference list:
Indices 1-64 correspond to LTE bands 1-64.
Indices 65-128 correspond to Non-LTE bands.

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
---------------------------------
<table>
<thead>
<tr>
<th>Idx</th>
<th>Carrier</th>
<th>FwVersion</th>
<th>PriVersion</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ATT</td>
<td>02.18.04.00</td>
<td>002.039_000</td>
<td>Inactive</td>
</tr>
<tr>
<td>2</td>
<td>GENERIC</td>
<td>02.18.05.00</td>
<td>002.041_002</td>
<td>Active</td>
</tr>
<tr>
<td>3</td>
<td>VERIZON</td>
<td>02.17.01.00</td>
<td>002.036_000</td>
<td>Inactive</td>
</tr>
</tbody>
</table>

Firmware Activation mode = MANUAL

FOTA Information
---------------------------------
FOTA server poll timer (mins) = Disable
FOTA server connection retry value = 0
FOTA status = Please re-configure FOTA poll timer

GPS Information
---------------------------------
GPS Feature = enabled
GPS Mode Configured = not configured
GPS Status = NMEA Disabled

SMS Information
-----------------
Incoming Message Information
-----------------------------
SMS stored in modem = 7
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 7
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 =
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 cellular 0/1/0 messages callcontrol

Modem Troubleshooting Using Integrated Modem DM Logging

As part of the 3G and 4G serviceability enhancement in Cisco IOS, 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 0/1/0 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 0/1/0 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]
Electronic Serial Number (ESN)
CHAPTER 10

Configuring Cellular IPv6 Address

This chapter contains the following sections:

• Cellular IPv6 Address, on page 145
• Configuring a Deterministic IPv6 Host Address, on page 149

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. Following are two examples of the same IPv6 address:

• 2001:CDBA:0000:0000:0000:0000:3257:9652
• 2001:CDBA::3257:9652 (zeros can be omitted)

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:cbda::3257:9652 /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.

The IR1101 supports the following address types:

Link-Local 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 cellular 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:

**SUMMARY STEPS**

1. configure terminal
2. ipv6 unicast-routing
3. interface cellular <slot/port/interface>
4. description <text>
5. ipv6 address <options>
6. load-interval <seconds>
7. dialer in-band
8. dialer idle-timeout <seconds>
9. dialer watch-group <group number>
10. ipv6 enable
11. pulse time <seconds>
12. ip virtual-reassembly
13. no shutdown
14. exit
15. access-list 1 permit any
16. dialer watch-list 1 <ipaddress> < mask>
17. dialer watch-list 1 delay route-check initial 60
18. dialer watch-list 1 delay connect 1
19. dialer-list 1 protocol ip permit
20. dialer-list 1 protocol ipv6 permit
21. ipv6 route <destination ipv6 prefix> / <destination mask> {forwarding router address | interface | other options}
22. end

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 unicast-routing</td>
<td>Enable IPv6 routing globally on the router.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>interface cellular &lt;slot/port/interface&gt;</td>
<td>Specifies the cellular interface. The IR1101 has the primary Cellular interface as 0/1/0.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config)# interface cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>description &lt;text&gt;</td>
<td>Provides a description for the cellular interface, if desired.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# description text</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 address &lt;options&gt;</td>
<td>Specifies that the IP address for a particular interface is dynamically obtained.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ipv6 address negotiated</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td>load-interval &lt;seconds&gt;</td>
<td>Specifies the length of time for which data is used to compute load statistics.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# load-interval 30</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td>dialer in-band</td>
<td>Enables DDR and configures the specified serial interface to use in-band dialing.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# dialer in-band</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td>dialer idle-timeout &lt;seconds&gt;</td>
<td>Specifies the dialer idle timeout period.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# dialer idle-timeout 0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td></td>
</tr>
<tr>
<td>dialer watch-group &lt;group number&gt;</td>
<td>Specifies the number of the dialer access group to which the specific interface belongs.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# dialer watch-group 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td></td>
</tr>
<tr>
<td>ipv6 enable</td>
<td>Enables IPv6.</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ipv6 enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td></td>
</tr>
<tr>
<td>pulse time &lt;seconds&gt;</td>
<td>Define pulse time</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# pulse-time 1</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td></td>
</tr>
<tr>
<td>ip virtual-reassembly</td>
<td>Enable Virtual Fragment Reassembly (default is ‘in’ only).</td>
</tr>
<tr>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td>Router(config-if)# ip virtual-reassembly</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>Step 13</td>
<td>no shutdown</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)#no shutdown</td>
</tr>
<tr>
<td>Step 14</td>
<td>exit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config-if)#exit</td>
</tr>
<tr>
<td>Step 15</td>
<td>access-list 1 permit any</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#access-list 1 permit any</td>
</tr>
<tr>
<td>Step 16</td>
<td>dialer watch-list 1 <code>&lt;ipaddress&gt;</code> <code>&lt;mask&gt;</code></td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#dialer watch-list 1 ip 5.6.7.8 255.255.255.255</td>
</tr>
<tr>
<td>Step 17</td>
<td>dialer watch-list 1 delay route-check initial 60</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#dialer watch-list 1 delay route-check initial 60</td>
</tr>
<tr>
<td>Step 18</td>
<td>dialer watch-list 1 delay connect 1</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#dialer watch-list 1 delay connect 1</td>
</tr>
<tr>
<td>Step 19</td>
<td>dialer-list 1 protocol ip permit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#dialer-list 1 protocol ip permit</td>
</tr>
<tr>
<td>Step 20</td>
<td>dialer-list 1 protocol ipv6 permit</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#dialer-list 1 protocol ipv6 permit</td>
</tr>
<tr>
<td>Step 21</td>
<td>ipv6 route <code>&lt;destination ipv6 prefix&gt;</code> <code>&lt;destination mask&gt;</code> {forwarding router address</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#ipv6 route ::/0 Cellular0/1/0</td>
</tr>
<tr>
<td>Step 22</td>
<td>end</td>
</tr>
<tr>
<td>Example:</td>
<td>Router(config)#end</td>
</tr>
</tbody>
</table>
Examples

The following example shows the Cellular IPv6 configuration:

```
lte sim data-profile 1 attach-profile 1 slot 0
lte sim data-profile 1 attach-profile 1 slot 1
lte interface 0 64 1111:2222:3333:0001
lte gqs mode standalone
lte modem dm-log size 2
lte modem dm-log filesize 1
lte modem dm-log rotation
lte modem link-recovery disable
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.255
!
interface Cellular0/1/0
  description Cell-to-CMW
  ip address negotiated
  load-interval 30
  dialer in-band
  dialer idle-timeout 0
  dialer watch-group 1
  ipv6 enable
  pulse-time 1
  ip virtual-reassembly
!
interface Cellular0/1/1
  no ip address
  shutdown
!
  ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
  ipv6 route ::/0 Cellular0/1/0
  ...
  access-list 1 permit any
  dialer watch-list 1 ip 5.6.7.8 255.255.255.255
  dialer watch-list 1 delay route-check initial 60
  dialer watch-list 1 delay connect 1
  dialer-list 1 protocol ip permit
  dialer-list 1 protocol ipv6 permit
```

Configuring a Deterministic IPv6 Host Address

Deterministic IPv6 addresses allow a user to configure a static, user-specified IPv6 address host portion for the interface. While IPv6 address network and subnet parts may be assigned by the ISP, the host part remains unchanged using this configuration. This allows devices to have known, pre-determined IPv6 addresses in their network.

To configure the a deterministic IPv6 host address, perform these steps:
SUMMARY STEPS

1. config terminal
2. ipv6 unicast-routing
3. interface Cellular <slot/port/interface>
4. enable ipv6
5. ipv6 address autoconfig
6. no shut
7. controller cellular <controller slot/port adapter/port>
8. lte interface <interface number> <address length 48-80> <deterministic address suffix>
9. end
10. clear int cellular 0/1/0

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> config terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> ipv6 unicast-routing</td>
<td>Enable IPv6 routing.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# ipv6 unicast-routing</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> interface Cellular &lt;slot/port/interface&gt;</td>
<td>Specifies the cellular interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# interface Cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> enable ipv6</td>
<td>Enables IPv6.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# enable ipv6</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ipv6 address autoconfig</td>
<td>Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6 processing on the interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# ipv6 address autoconfig</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> no shut</td>
<td>Shutdown Interface.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-if)# no shut</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> controller cellular &lt;controller slot/port adapter/port&gt;</td>
<td>Configure the controller.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# controller cellular 0/1/0</td>
<td></td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td><strong>lte interface &lt;interface number&gt; &lt;address length 48-80&gt; &lt;deterministic address suffix&gt;</strong> Specify in controller config the deterministic IPv6 address for cellular interface.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router(config)# lte interface 0 64 1111:2222:3333:1234</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td><strong>end</strong> Clears the cellular interface and forces the cellular interface to reacquire IP address.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# end</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td><strong>clear int cellular 0/1/0</strong></td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td>Router# clear int cellular 0/1/0</td>
</tr>
</tbody>
</table>

**Example**

The following example shows the configuration:

command Cellular 0/1/0
lte sim data-profile 1 attach-profile 1 slot 0
lte sim data-profile 1 attach-profile 1 slot 1
no lte firmware auto-sim
lte interface 0 64 1111:2222:3333:0001
lte gps mode standalone
lte modem dm-log size 2
lte modem dm-log filesize 1
lte modem dm-log rotation
lte modem link-recovery disable
!
!
!
interface Loopback0
  ip address 1.1.1.1 255.255.255.255
!
!
interface Cellular0/1/0
description Cell-to-CMW
ip address negotiated
load-interval 30
dialer in-band
dialer idle-timeout 0
dialer watch-group 1
dialer-group 1
ipv6 enable
pulse-time 1
ip virtual-reassembly
!
interface Cellular0/1/1
no ip address
shutdown
!
!
interface Cellular0/1/0
ip route 0.0.0.0 0.0.0.0 Cellular0/1/0
ipv6 route ::/0 Cellular0/1/0

...
...  
access-list 1 permit any  
dialer watch-list 1 ip 5.6.7.0 255.255.255.255  
dialer watch-list 1 delay route-check initial 60  
dialer watch-list 1 delay connect 1  
dialer-list 1 protocol ip permit  
dialer-list 1 protocol ipv6 permit  
!  
...
Information About SCADA

This section contains the following topics:

- Information About SCADA, on page 153
- Configuring the DNP3 Protocol Stacks, on page 165
- Starting and Stopping the Protocol Translation Engine, on page 169
- Verifying Configuration, on page 170
- Debug Commands, on page 171

Information About SCADA

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

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

On the IR1101, line is 0/2/0 same as the Async interface.

Role of the IR1101

In the network, the Control Center always serves as the master in the network when communicating with the IR1101. The IR1101 serves as a proxy master station for the Control Center when it communicates with the RTU.

The IR1101 provides protocol translation to serve as a SCADA gateway to do the following:

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

The IR1101 performs Protocol Translation for the following protocols:

- IEC 60870 T101 to/from IEC 60870 T104.
- DNP3 serial to DNP3 IP
Key Terms

The following terms are relevant when you configure the T101 and T104 protocol stacks on the IR1101:

- **Channel**—A channel is configured on each IR1101 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single T101 (RTU) or T104 (Control Center) protocol stack.
- **Link Address**—Refers to the device or station address.
- **Link Mode (Balanced and Unbalanced)**—Refers to the modes of data transfer.
  - An Unbalanced setting refers to a data transfer initiated from the master.
  - A Balanced setting can refer to either a master or slave initiated data transfer.
- **Sector**—Refers to a single RTU within a remote site.
- **Sessions**—Represents a single connection to a remote site.

The following terms are relevant when you configure the DNP3 protocol stacks on the IR1101:

- **Channel**—A channel is configured on the IR1101 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single DNP3 serial (RTU) or DNP3 IP (Control Center) protocol stack.
- **Link Address**—Refers to the device or station address.
- **Sessions**—Represents a single connection to a remote site.

Protocol Translation Application

In *Figure 9: Routers Within a SCADA System, on page 155* the IR1101 (installed within a secondary substation of the Utility Network) employs Protocol Translation to provide secure, end-to-end connectivity between Control Centers and RTUs within a SCADA System.

The IR1101 connects to the RTU (slave) through a RS232 connection. To protect the traffic when forwarded over public infrastructures (for example, cellular), the IR1101 forwards SCADA data from the RTU to the Control Center in the SCADA system through an IPSec tunnel (FlexVPN site-to-site or hub and spoke). The IPSec tunnel protects all traffic between the IR1101 and the Head-end aggregation router. SCADA traffic can be inspected through an IPS device positioned in the path of the SCADA traffic before it is forwarded to the proper Control Center.
Prerequisites

RTUs must be configured and operating in the network.

For each RTU that connects to the IR1101, you will need the following information for T101/T104:

- Channel information
  - Channel name
  - Connection type: serial
  - Link transmission procedure setting: unbalanced or balanced
  - Address field of the link (number expressed in octets)

- Session information
  - Session name
  - Size of common address of Application Service Data Unit (ASDU) (number expressed in octets)
  - Cause of transmission (COT) size (number expressed in octets)
  - Information object address (IOA) size (number expressed in octets)

- Sector information
  - Sector name
  - ASDU address, (number expressed in octets)

For each RTU that connects to the IR1101, you will need the following information for DNP3:

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

• Session information

• Session name

Guidelines and Limitations

Each channel supports only one session.

Each session supports only one sector.

Default Settings

<table>
<thead>
<tr>
<th>T101/T104 Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role for T101</td>
<td>Master</td>
</tr>
<tr>
<td>Role for T104</td>
<td>Slave</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DNP3 Parameters</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsolicited Response (DNP3-serial)</td>
<td>Not Enabled</td>
</tr>
<tr>
<td>Send Unsolicited Message (DNP3-IP)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Configuring Protocol Translation

This section includes the following topics:

Note

Before making any configuration changes to an IR1101 operating with Protocol Translation, please review the section on Starting and Stopping the Protocol Translation Engine, on page 169.

Enabling the IR1101 Serial Port and SCADA Encapsulation

Before you can enable and configure Protocol Translation on the IR1101, you must first enable the serial port on the IR1101 and enable SCADA encapsulation on that port.

Before you begin

Determine availability of serial port on the IR1101.

SUMMARY STEPS

1. configure terminal
2. interface async slot/port/interface
3. no shutdown
**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><strong>configure terminal</strong></td>
</tr>
</tbody>
</table>
| **Step 2** | **interface async slot/port/interface** | Enters the interface command mode for the async slot/port/interface.  
  *slot* – value of 0  
  *port* – value of 2  
  *interface* – value of 0 |
| **Step 3** | **no shutdown** | Brings up the port, administratively. |
| **Step 4** | **encapsulation scada** | Enables encapsulation on the serial port for protocol translation and other SCADA protocols. |

**EXAMPLE**

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

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

**Configuring T101 and T104 Protocol Stacks**

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

- Configuring the T101 Protocol Stack, on page 157
- Configuring the T104 Protocol Stack, on page 160
- Starting and Stopping the Protocol Translation Engine, on page 169

**Prerequisites**

Ensure that you have gathered all the required configuration information.

Enable the serial port and SCADA encapsulation.

**Configuring the T101 Protocol Stack**

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

**SUMMARY STEPS**

1. configure terminal
2. scada-gw protocol t101
### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>scada-gw protocol t101</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>channel <em>channel_name</em></td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>role master</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>link-mode {balanced</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>link-addr-size {none</td>
</tr>
</tbody>
</table>

*channel_name* – Identifies the channel on which the serial port of the IR1101 communicates to the RTU.

**Note**  
When the entered channel name does not already exist, the router creates a new channel.

Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| **Step 7** bind-to-interface async slot/port/interface | Defines the IR1101 serial interface on which the system sends its T101 protocol traffic.  
  *slot* – Value of 0  
  *port* – Value of 2  
  *interface* – Value of 0 |
| **Step 8** exit | Ends configuration of the channel and exits the channel configuration mode. Saves all settings. |
| **Step 9** session *session_name* | Enters the session configuration mode and assigns a name to the session. |
| **Step 10** attach-to-channel *channel_name* | Attaches the session to the channel.  
  Enter the same channel name that you entered in Step 3.  
  *channel_name* – Identifies the channel. |
| **Step 11** common-addr-size {one | two | three} | Defines the common address size in octets. |
| **Step 12** cot size {one | two | three} | Defines the cause of transmission such as spontaneous or cyclic data schemes in octets. |
| **Step 13** info-obj-addr-size {one | two | three} | Defines the information object element address size in octets. |
| **Step 14** link-addr-size {one | two | three} | Defines the link address size in octets. |
| **Step 15** link-addr *link_address* | Refers to the link address of the RTU.  
  **Note** The link address entered here must match the value set on the RTU to which the serial port connects.  
  *link_address* – Range of 0-65535. |
| **Step 16** exit | Exits the session configuration mode. |
| **Step 17** sector *sector_name* | Enters the sector configuration mode and assigns a name to the sector for the RTU.  
  *sector_name* – Identifies the sector. |
| **Step 18** attach-to-session *session_name* | Attaches the RTU sector to the session.  
  Enter the same session name that you entered in Step 9.  
  *session_name* – Identifies the session. |
| **Step 19** asdu-addr *asdu_address* | Refers to the ASDU structure address of the RTU. |
| **Step 20** exit | Exits the sector configuration mode. |
| **Step 21** exit | Exits the protocol configuration mode. |
EXAMPLE

This example shows how to configure the parameters for the T101 protocol stack for RTU_10.

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

Configuring the T104 Protocol Stack

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

**Before you begin**

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

Enable the serial port and SCADA encapsulation. (See Enabling the IR1101 Serial Port and SCADA Encapsulation, on page 156)

**SUMMARY STEPS**

1. configure terminal
2. scada-gw protocol t104
3. channel channel_name
4. k-value value
5. w-value value
6. t0-timeout value
7. t1-timeout value
8. t2-timeout value
9. t3-timeout value
10. tcp-connection {0|1} local-port {port_number | default} remote-ip {A.B.C.D | A.B.C.D/LEN | any} [vrf WORD]
11. exit
12. session session_name
13. attach-to-channel channel_name
14. cot size \{one | two | three\}
15. exit
16. sector sector_name
17. attach-to-session session_name
18. asdu-addr asdu_address
19. map-to-sector sector_name
20. Return to Step 1.

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2 scada-gw protocol t104</td>
<td>Enters the configuration mode for the T104 protocol.</td>
</tr>
<tr>
<td>Step 3 channel channel_name</td>
<td>Enters the channel configuration mode for the T104 protocol.</td>
</tr>
</tbody>
</table>

channel_name—Identifies the channel on which the router communicates with the Control Center.

Note When the entered channel name does not already exist, the router creates a new channel.

Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.

Step 4 k-value value | Sets the maximum number of outstanding Application Protocol Data Units (APDUs) for the channel. |

Note An APDU incorporates the ASDU and a control header.

value—Range of values from 1 to 32767. Default value is 12 APDUs.

Step 5 w-value value | Sets the maximum number of APDUs for the channel. |

value—Range of values from 1 to 32767. Default value is 8 APDUs.

Step 6 t0-timeout value | Defines the t0-timeout value for connection establishment of the T104 channel. |

Step 7 t1-timeout value | Defines the t1-timeout value for send or test APDUs on the T104 channel. |

Step 8 t2-timeout value | Defines the t2-timeout value for acknowledgements when the router receives no data message. |

Note The t2 value must always be set to a lower value than the t1 value on the T104 channel.
<table>
<thead>
<tr>
<th>Step 9</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>t3-timeout value</td>
<td>Defines the t3-timeout value for sending s-frames in case of a long idle state on the T104 channel.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** The t3 value must always be set to a higher value than the t1 value on the T104 channel.

<table>
<thead>
<tr>
<th>Step 10</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>tcp-connection {0</td>
<td>1} local-port {port_number</td>
<td>default} remote-ip {A.B.C.D</td>
</tr>
</tbody>
</table>

- **port-number** – value between 2000 and 65535.
- **default** – value of 2404.
- **A.B.C.D** – single host.
- **A.B.C.D/nn** – subnet A.B.C.D/LEN.
- **any** – any remote hosts 0.0.0.0/0.
- **WORD** – VRF name.

<table>
<thead>
<tr>
<th>Step 11</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits the channel configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>session session_name</td>
<td>Enters the session configuration mode and assigns a name to the session.</td>
<td></td>
</tr>
</tbody>
</table>

- **session_name** – Use the same name that you assigned to the channel in Step 3.

<table>
<thead>
<tr>
<th>Step 13</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach-to-channel channel_name</td>
<td>Defines the name of the channel that transports the session traffic.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 14</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>cot size {one</td>
<td>two</td>
<td>three}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 15</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>Exits the session configuration mode.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 16</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>sector sector_name</td>
<td>Enters the sector configuration mode and assigns a name to the sector for the Control Center.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 17</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>attach-to-session session_name</td>
<td>Attaches the Control Center sector to the channel.</td>
<td></td>
</tr>
</tbody>
</table>

- **session_name** – Use the same name that you assigned to the channel in Step 3.

<table>
<thead>
<tr>
<th>Step 18</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>asdu-addr asdu_address</td>
<td>Refers to the ASDU structure address. Value entered here must match the ASDU value on the RTU.</td>
<td></td>
</tr>
</tbody>
</table>

- **asdu_address** – **asdu_address** – Value of 1 or 2.

<table>
<thead>
<tr>
<th>Step 19</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>map-to-sector sector_name</td>
<td>Maps the Control Center (T104) sector to the RTU (T101) sector.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 20</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Return to Step 1.</td>
<td>Repeat all steps in this section for each Control Center active in the network.</td>
<td></td>
</tr>
</tbody>
</table>
EXAMPLE

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

To configure Control Center 1 (cc_master1), enter the following commands.

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

To configure Control Center 2 (cc_master2), enter the following commands.

```
router (config)# scada-gw protocol t104
router (config-t104)# channel cc_master2
router (config-t104-channel)# k-value 12
router (config-t104-channel)# w-value 8
router (config-t104-channel)# t0-timeout 30
router (config-t104-channel)# t1-timeout 15
router (config-t104-channel)# t2-timeout 10
router (config-t104-channel)# t3-timeout 30
router (config-t104-channel)# tcp-connection 0 local-port 2060 remote-ip 209.165.201.237
router (config-t104-channel)# tcp-connection 1 local-port 2061 remote-ip 209.165.200.27
router (config-t104-channel)# exit
router (config-t104)# session cc_master2
router (config-t104-session)# attach-to-channel cc_master2
router (config-t104-session)# cot-size two
router (config-t104-session)# exit
router (config-t104)# sector cc_master2-sector
router (config-t104-sector)# attach-to-session cc_master2
router (config-t104-sector)# asdu-adr 3
router (config-t104-sector)# map-to-sector rtu_sector
router (config-t104-sector)# exit
router (config-t104)# exit
router (config)#
```
The following example shows how to configure the serial port interface for T101 connection, configure T101 and T104 protocol stacks, and starts the Protocol Translation Engine on the IR1101.

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

router(config-t104)# session cc_master2
router(config-t104)# attach-to-channel cc_master2
router(config-t104)# cot-size two
router(config-t104)# exit
router(config-t104)# sector cc_master2-sector
router(config-t104-sector)# attach-to-session cc_master2
router(config-t104-sector)# asdu-adr 3
router(config-t104-sector)# map-to-sector rtu_sector
```
This example configures end-to-end communication between Control Centers and RTUs within a SCADA system using the DNP3 protocol stacks and starts the Protocol Translation Engine on the IR1101:

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

```

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

### Configuring the DNP3 Protocol Stacks

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

### Configuring DNP3 Serial

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

### SUMMARY STEPS

1. `configure terminal`
2. `scada-gw protocol dnp3-serial`
3. `channel channel_name`
4. `bind-to-interface async 0/2/0`
5. `link-addr source source_address`
6. `unsolicited-response enable`
7. `exit`
8. session session_name
9. attach-to-channel channel_name
10. link-addr dest destination_address
11. exit
12. exit

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>scada-gw protocol dnp3-serial</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>channel channel_name</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: When the entered channel name does not already exist, the router creates a new channel.</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>bind-to-interface async0/2/0</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>link-addr source source_address</td>
</tr>
<tr>
<td></td>
<td>source_address – Range of values from 1 to 65535.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>unsolicited-response enable</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command disables unsolicited responses.</td>
</tr>
<tr>
<td></td>
<td>The default is disabled.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>session session_name</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered session name does not already exist, the router creates a new session.</td>
</tr>
<tr>
<td></td>
<td>Entering the no form of this command deletes an existing session.</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>attach-to-channel channel_name</td>
</tr>
<tr>
<td></td>
<td>Note: Enter the same channel name that you entered in Step 3 above</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
</tr>
<tr>
<td>channel_name</td>
<td>Identifies the channel.</td>
</tr>
<tr>
<td>link-addr dest destination_address</td>
<td>Refers to the link address of the slave. Destination addresses range from 1 to 65535.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits session configuration mode.</td>
</tr>
<tr>
<td>exit</td>
<td>Exits protocol configuration mode.</td>
</tr>
</tbody>
</table>

**EXAMPLE**

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

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

### Configuring DNP3 IP

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

**SUMMARY STEPS**

1. configure terminal
2. scada-gw protocol dnp3-ip
3. channel channel_name
4. link-addr dest destination_address
5. send-unsolicited-msg enable
6. tcp-connection local-port [default | local_port] remote-ip [any | remote_ip | remote_subnet]
7. exit
8. session session_name
9. attach-to-channel channel_name
10. link-addr source source_address
11. map-to-session session_name
12. exit
13. exit
## DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> scada-gw protocol dnp3-ip</td>
<td>Enters configuration mode for the DNP-IP protocol.</td>
</tr>
<tr>
<td><strong>Step 3</strong> channel <em>channel_name</em></td>
<td>Enters channel configuration mode for the DNP-IP protocol.</td>
</tr>
<tr>
<td></td>
<td><em>channel_name</em> – Identifies the channel on which the router communicates with the Control Center.</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered channel name does not already exist, the router creates a new channel.</td>
</tr>
<tr>
<td></td>
<td>Entering the <code>no</code> form of this command deletes an existing channel. However, all sessions must be deleted before you can delete a channel.</td>
</tr>
<tr>
<td><strong>Step 4</strong> link-addr dest <em>destination_address</em></td>
<td>Refers to the link address of the master.</td>
</tr>
<tr>
<td></td>
<td><em>destination_address</em> – Range of values from 1 to 65535.</td>
</tr>
<tr>
<td><strong>Step 5</strong> send-unsolicited-msg enable</td>
<td>(Optional) Allow unsolicited messages.</td>
</tr>
<tr>
<td></td>
<td>The default is enabled.</td>
</tr>
<tr>
<td><strong>Step 6</strong> tcp-connection local-port [default</td>
<td>local_port ]</td>
</tr>
<tr>
<td></td>
<td>remote-ip [any</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> exit</td>
<td>Exits channel configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong> session <em>session_name</em></td>
<td>Enters session configuration mode and assigns a name to the session.</td>
</tr>
<tr>
<td></td>
<td>Note: When the entered session name does not already exist, the router creates a new session.</td>
</tr>
<tr>
<td></td>
<td>Entering the <code>no</code> form of this command deletes an existing session.</td>
</tr>
</tbody>
</table>
### Command or Action

<table>
<thead>
<tr>
<th>Step 9</th>
<th><code>attach-to-channel channel_name</code></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Attaches the session to the channel. Enter the same channel name that you entered in Step 3. <code>channel_name</code> – Identifies the channel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 10</th>
<th><code>link-addr source source_address</code></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Refers to the link address of the slave. <code>source_address</code> – Value of 1-65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 11</th>
<th><code>map-to-session session_name</code></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Maps the dnp3-ip session to an existing dnp3-serial session. Note: One dnp3-ip session can be mapped to only one dnp3-serial session.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 12</th>
<th><code>exit</code></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Exits session configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step 13</th>
<th><code>exit</code></th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Exits protocol configuration mode.</td>
</tr>
</tbody>
</table>

### EXAMPLE

This example shows how to configure the DNP3 IP parameters:

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

### Starting and Stopping the Protocol Translation Engine

You must start the Protocol Translation Engine to use Protocol Translation on the IR1101.

**Starting**– After enabling SCADA encapsulation on the IR1101 serial port and configuring the T101 and T104 protocols on the IR1101, you can start the Protocol Translation Engine.

**Stopping**– Before you can make any configuration changes to Protocol Translation on the IR1101 with an active Protocol Translation Engine, you must stop the engine.

### Before you begin

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

Enabling the IR1101 Serial Port and SCADA Encapsulation, on page 156
Configuring T101 and T104 Protocol Stacks, on page 157
SUMMARY STEPS

1. configure terminal
2. [no] scada-gw enable

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 [no] scada-gw enable</td>
<td>Starts (scada-gw enable) or stops (no scada-gw enable) the Protocol Translation Engine on the IR1101.</td>
</tr>
</tbody>
</table>

EXAMPLE

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

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

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

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

Verifying Configuration

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

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

```conf
router# show scada tcp
DNP3 network channel [test]: 4 max simultaneous connections
conn: local-ip: 3.3.3.21 local-port 20000 remote-ip 3.3.3.15 data-socket 1
Total:
  1 current client connections
  0 total closed connections
router# show scada statistics
DNP3 network Channel [test]:
  5 messages sent, 2 messages received
```
Debug Commands

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

Table 12: SCADA DNP3-IP Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada dnp3n application</td>
<td>DNP3-IP application trace</td>
</tr>
<tr>
<td>debug scada dnp3n datalink</td>
<td>DNP3-IP datalink trace</td>
</tr>
<tr>
<td>debug scada dnp3n event</td>
<td>DNP3-IP event trace</td>
</tr>
<tr>
<td>debug scada dnp3n physical</td>
<td>DNP3-IP physical trace</td>
</tr>
<tr>
<td>debug scada dnp3n transport</td>
<td>DNP3-IP transport trace</td>
</tr>
</tbody>
</table>

Table 13: SCADA DNP3-Serial Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada dnp3s application</td>
<td>DNP3-Serial application trace</td>
</tr>
<tr>
<td>debug scada dnp3s datalink</td>
<td>DNP3-Serial datalink trace</td>
</tr>
<tr>
<td>debug scada dnp3s event</td>
<td>DNP3-Serial event trace</td>
</tr>
<tr>
<td>debug scada dnp3s physical</td>
<td>DNP3-Serial physical trace</td>
</tr>
<tr>
<td>debug scada dnp3s transport</td>
<td>DNP3-Serial transport trace</td>
</tr>
</tbody>
</table>

Table 14: SCADA Driver Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada driver event</td>
<td>Driver event trace</td>
</tr>
<tr>
<td>debug scada driver packet</td>
<td>Driver packet trace</td>
</tr>
</tbody>
</table>

Table 15: SCADA Function Level Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada function config</td>
<td>Configuration trace</td>
</tr>
</tbody>
</table>
### Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada function control</td>
<td>Control trace</td>
</tr>
<tr>
<td>debug scada function file</td>
<td>File trace</td>
</tr>
<tr>
<td>debug scada function freeze</td>
<td>Freeze trace</td>
</tr>
<tr>
<td>debug scada function physical</td>
<td>Physical trace</td>
</tr>
<tr>
<td>debug scada function poll</td>
<td>Poll trace</td>
</tr>
<tr>
<td>debug scada function stack</td>
<td>Stack trace</td>
</tr>
<tr>
<td>debug scada function umode</td>
<td>Umode trace</td>
</tr>
</tbody>
</table>

#### Table 16: SCADA Protocol Layer Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada layer application</td>
<td>Application Layer</td>
</tr>
<tr>
<td>debug scada layer network-physical</td>
<td>Network Physical Layer</td>
</tr>
<tr>
<td>debug scada layer serial-physical</td>
<td>Serial Physical Layer</td>
</tr>
</tbody>
</table>

#### Table 17: SCADA T101 Trace Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada t101 application</td>
<td>T101 application trace</td>
</tr>
<tr>
<td>debug scada t101 datalink</td>
<td>T101 datalink trace</td>
</tr>
<tr>
<td>debug scada t101 event</td>
<td>T101 event trace</td>
</tr>
<tr>
<td>debug scada t101 physical</td>
<td>T101 physical trace</td>
</tr>
<tr>
<td>debug scada t101 transport</td>
<td>T101 transport trace</td>
</tr>
</tbody>
</table>

#### Table 18: SCADA T104 Trace Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada t104 application</td>
<td>T104 application trace</td>
</tr>
<tr>
<td>debug scada t104 datalink</td>
<td>T104 datalink trace</td>
</tr>
<tr>
<td>debug scada t104 event</td>
<td>T104 event trace</td>
</tr>
<tr>
<td>debug scada t104 physical</td>
<td>T104 physical trace</td>
</tr>
<tr>
<td>debug scada t104 transport</td>
<td>T104 transport trace</td>
</tr>
</tbody>
</table>
### Table 19: SCADA Protocol TCP Level Debug Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug scada tcp event</td>
<td>TCP event trace</td>
</tr>
<tr>
<td>debug scada tcp packet</td>
<td>TCP packet trace</td>
</tr>
</tbody>
</table>
CHAPTER 12

Raw Socket Transport

This section contains the following topics:

- Raw Socket Transport, on page 175

Raw Socket Transport

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

This document describes Raw Socket Transport for the IR1101 and provides a reference section describing the Raw Socket Transport commands.

This document includes the following sections:

Information About Raw Socket Transport

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

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

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

- TCP as the transport protocol, with built-in auto TCP connection retry mechanism.
- Up to 32 TCP sessions.
- Interface configuration as a server, client, or a combination of both.
- One server interface, but multiple clients.
- VRF-awareness, which enables the router to send Raw Socket Transport traffic to a server host connected through a Virtual Private Network (VPN) Virtual Routing and Forwarding (VRF) interface.

This section includes the following topics:
TCP Transport

TCP Raw Socket transport uses a client-server model. At most one server and multiple clients can be configured on a single asynchronous serial line. In client mode, the IR1101 can initiate up to 32 TCP sessions to Raw Socket servers, which can be other IR1101 routers or third-party devices.

Figure 1 shows a sample Raw Socket TCP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes several IR1101 routers. One IR1101 router (Router 1) acts as a Raw Socket server, listening for TCP connection requests from the other IR1101 routers (Router 2 and Router 3), which are configured as Raw Socket clients.

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

UDP Transport

UDP transport uses a peer-to-peer model. Multiple UDP connections can be configured on an asynchronous serial line.

Figure 2 shows a sample Raw Socket UDP configuration. In this example, serial data is transferred between RTUs and a utility management system across an IP network that includes two routers (Router 1 which is an IR1101 and Router 2 which is an IR807) that are configured as Raw Socket UDP peers.

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

---

**Note**

When you configure the serial link interface on the router as a server, the interface’s peer is the serial link interface on the client router and vice versa.
Serial Data Processing

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

- **Packet length**—You can specify a packet length that triggers the IR1101 to transmit the serial data to the peer. Once the IR1101 collects this much data in its buffer, it packetizes the accumulated data and forwards it to the Raw Socket peer.

- **Packet-timer value**—The packet timer specifies the amount of time the IR1101 waits to receive the next character in a stream. If a character is not received by the time the packet timer expires, the data the IR1101 has accumulated in its buffer is packetized and forwarded to the Raw Socket peer.

- **Special character**—You can specify a character that will trigger the IR1101 to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the special character (for example, a CR/LF) is received, the IR1101 packetizes the accumulated data and sends it to the Raw Socket peer.

See the “Configuring Common Raw Socket Line Options” procedure on page 6 for information about configuring the processing options.

VRF-Aware Raw Socket

The VRF-aware Raw Socket Transport feature enables you to isolate Raw Socket traffic using a VRF for efficient management and control of serial data. After configuring a VRF, you can associate the serial interface configured for Raw Socket Transport with the VRF. See the Raw Socket VRF, on page 186 for a configuration example.

Prerequisites

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

Guidelines and Limitations

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Raw Socket Transport</td>
<td>Disabled.</td>
</tr>
<tr>
<td>Packet length</td>
<td>No packet length is configured.</td>
</tr>
<tr>
<td>Serial Protocol</td>
<td>Asynchronous Communication Protocol</td>
</tr>
<tr>
<td>Packet timeout</td>
<td>15 ms.</td>
</tr>
<tr>
<td>Special character</td>
<td>No special character is configured.</td>
</tr>
<tr>
<td>Raw Socket mode</td>
<td>Best-effort mode is off, not supported on the IR1101.</td>
</tr>
<tr>
<td>TCP idle timeout</td>
<td>5 minutes.</td>
</tr>
</tbody>
</table>

Configuring Raw Socket Transport

This section includes the following topics:

Enabling Raw Socket Transport on the Serial Interface

To enable Raw Socket Transport on the IR1101 router, you must first enable an asynchronous serial port and enable Raw Socket TCP or UDP encapsulation for that port.

Before you begin

Determine availability of the serial port on the IR1101.

SUMMARY STEPS

1. configure terminal
2. interface async0/slot/port
3. no ip address
4. Do one of the following:
   • encapsulation raw-tcp
   •
   • encapsulation raw-udp

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface async0/slot/port</td>
<td>Enters the interface command mode for the async slot/port.</td>
</tr>
<tr>
<td>Step 3 no ip address</td>
<td>Disables IP processing on the interface.</td>
</tr>
</tbody>
</table>
### Configuring Common Raw Socket Line Options

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

#### Before you begin

Enable Raw Socket Transport as described in Enabling Raw Socket Transport on the Serial Interface, on page 178.

#### SUMMARY STEPS

1. `configure terminal`
2. `line 0/slot/port`
3. `raw-socket packet-length length`
4. `raw-socket packet-timer timeout`
5. `raw-socket spec-char ascii_char`

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td><code>line 0/slot/port</code></td>
</tr>
<tr>
<td></td>
<td>Enters line command mode for the serial slot/port.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>raw-socket packet-length length</code></td>
</tr>
<tr>
<td></td>
<td>Specifies the packet size that triggers the IR1101 to transmit the data to the peer. When the IR1101 accumulates this much data in its buffer, it packetizes the data and forwards it to the Raw Socket peer.</td>
</tr>
<tr>
<td></td>
<td><code>length</code>—2 to 1400 bytes.</td>
</tr>
<tr>
<td></td>
<td>By default, the packet-length trigger is disabled.</td>
</tr>
<tr>
<td>Step</td>
<td>Command or Action</td>
</tr>
<tr>
<td>------</td>
<td>------------------</td>
</tr>
<tr>
<td>4</td>
<td>raw-socket packet-timer timeout</td>
</tr>
<tr>
<td>5</td>
<td>raw-socket spec-char ascii_char</td>
</tr>
</tbody>
</table>

**What to do next**

Use the <code>no</code> form of these commands to return to the default values.

**EXAMPLE**

```
router# configure terminal
router(config)# line 0/2/0
router(config-line)# raw-socket packet-length 32
router(config-line)# raw-socket packet-timer 500
router(config-line)# raw-socket special-char 3
```

**Configuring Raw Socket TCP**

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

**Configuring the Raw Socket TCP Server**

**Before you begin**

Enable a serial port and Raw Socket TCP encapsulation for that port, as described in Enabling Raw Socket Transport on the Serial Interface, on page 178.

**SUMMARY STEPS**

1. configure terminal
2. line 0/slot/port
3. raw-socket tcp server <i>port [ip_address]</i>
4. raw-socket tcp idle-timeout <i>session_timeout</i>

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 2 line 0/slot/port</td>
<td>Enters line command mode for the serial slot/port.</td>
<td></td>
</tr>
</tbody>
</table>
| Step 3 raw-socket tcp server port [ip_address ] | Starts the Raw Socket Transport TCP server for an asynchronous line interface. In Raw Socket server mode, the IR1101 listens for incoming connection requests from Raw Socket clients.  
port –Port number the server listens on.  
ip_address –(Optional) Local IP address on which the server listens for connection requests. |
| Step 4 raw-socket tcp idle-timeout session_timeout | Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session closes. The client then automatically attempts to reestablish the TCP session with the server.  
This timeout setting applies to all Raw Socket Transport TCP sessions under this particular line.  
session_timeout –Currently configured session idle timeout in minutes. The default is 5 minutes. |

**What to do next**

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

**EXAMPLE**

This example shows how to configure a Raw Socket TCP server for an asynchronous serial line. The TCP server listens for TCP client connection requests on local port 4000 and local IP address 10.0.0.1. If no data is exchanged between the Raw Socket TCP server and one of the TCP clients for 10 minutes, then the TCP session closes, and the Raw Socket client attempts to reestablish the session with the Raw Socket server.

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

**Configuring the Raw Socket TCP Client**

**Before you begin**

Enable a serial port and Raw Socket TCP encapsulation for that port, as described in Enabling Raw Socket Transport on the Serial Interface, on page 178.

**SUMMARY STEPS**

1. configure terminal
2. **line 0/slot/port**
3. **raw-socket tcp client** *dest_ip_address* *dest_port* [*local_ip_address*] [*local_port*]
4. **raw-socket tcp idle-timeout** *session_timeout*
5. **raw-socket tcp keepalive** *interval*

### DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2 line 0/slot/port</td>
<td>Enters line command mode for the serial slot/port.</td>
</tr>
</tbody>
</table>
| **Step 3** raw-socket tcp client *dest_ip_address* *dest_port* [*local_ip_address*] [*local_port*] | Specifies settings for Raw Socket Transport TCP client sessions.  
*dest_ip_address* – Destination IP address of the remote Raw Socket server.  
*dest_port* – Destination port number to use for the TCP connection to the remote server.  
*local_ip_address* – (Optional) Local IP address that the client can also bind to.  
*local_port* – (Optional) Local port number that the client can also bind to. |
| **Step 4** raw-socket tcp idle-timeout *session_timeout* | Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session is closed. The client then automatically attempts to reestablish the TCP session with the server.  
*session_timeout* – Currently configured session idle timeout in minutes. The default is 5 minutes. |
| **Step 5** raw-socket tcp keepalive *interval* | Sets the Raw Socket Transport TCP session keepalive interval for the asynchronous line interface. The router sends keepalive messages based on the configured interval. You may need to configure this interval, for example, when sending raw TCP traffic over a cellular interface.  
*interval* – Currently configured keepalive interval in seconds. Range is 1-864000 seconds. The default is 1 second. |

### What to do next

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

This example shows how to configure a Raw Socket TCP client for an asynchronous serial line. The IR1101 (router), serving as a Raw Socket client, initiates TCP sessions with a Raw Socket server and forwards packetized serial data to it. The router collects streams of serial data in its buffer; when it accumulates 827 bytes in its buffer, the router packetizes the data and forwards it to the Raw Socket server. If the router and the Raw Socket server do not exchange any data for 10 minutes, then the TCP session with the Raw Socket server closes, and the router attempts to reestablish the session with the Raw Socket server.

```
router# configure terminal

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

Configuring a Raw Socket UDP Peer-to-Peer Connection

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

Before you begin

Enable a serial port and Raw Socket UDP encapsulation for that port, as described in Enabling Raw Socket Transport on the Serial Interface, on page 178.

SUMMARY STEPS

1. configure terminal
2. line 0/slot/port
3. raw-socket udp connection dest_ip_address dest_port local_port [local_ip_address ]

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enters configuration mode.</td>
</tr>
<tr>
<td>Step 2 line 0/slot/port</td>
<td>Enters line command mode for the serial slot/port.</td>
</tr>
</tbody>
</table>
| Step 3 raw-socket udp connection dest_ip_address dest_port local_port [local_ip_address ] | Specifies settings for Raw Socket Transport UDP connections.  
  dest_ip_address – Destination IP address to use for the UDP connection.  
  dest_port – Destination port number to use for the UDP connection.  
  local_port – Local port number for the UDP connection.  
  local_ip_address – (Optional) Local IP address for the UDP connection. |
What to do next

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

**EXAMPLE**

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

**Router A**

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

**Router B**

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

**Verifying Configuration**

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show running-config</code></td>
<td>Shows the configuration of the IR1101, including those features that are active and their settings.</td>
</tr>
<tr>
<td><code>show raw-socket tcp detail</code></td>
<td>Displays information about Raw Socket Transport TCP activity.</td>
</tr>
<tr>
<td><code>show raw-socket tcp sessions</code></td>
<td>Displays information about Raw Socket Transport TCP sessions.</td>
</tr>
<tr>
<td><code>show raw-socket tcp statistics</code></td>
<td>Displays Raw Socket Transport TCP statistics for each asynchronous serial line.</td>
</tr>
<tr>
<td><code>show raw-socket udp detail</code></td>
<td>Displays information about Raw Socket Transport UDP activity.</td>
</tr>
<tr>
<td><code>show raw-socket udp sessions</code></td>
<td>Displays information about Raw Socket Transport UDP sessions.</td>
</tr>
<tr>
<td><code>show raw-socket udp statistics</code></td>
<td>Displays Raw Socket Transport UDP statistics for each asynchronous serial line.</td>
</tr>
<tr>
<td><code>clear raw-socket statistics</code></td>
<td>Clears Raw Socket Transport statistics for a specific TTY interface or for all asynchronous serial lines.</td>
</tr>
</tbody>
</table>

**Configuration Example**

The following sections include Raw Socket Transport configuration examples:
Raw Socket TCP

The following example shows a Raw Socket Transport configuration in which an IR1101 router (Router 1) acts as the server, and another IR809 (Router 2) acts as the client.

The following table displays the configuration of the server and client IR1101s highlighted in Figure 3:

<table>
<thead>
<tr>
<th>IR1101 Server Configuration</th>
<th>IR807 Client Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface async0/2/0</td>
<td>interface async0</td>
</tr>
<tr>
<td>no ip address</td>
<td>no ip address</td>
</tr>
<tr>
<td>encapsulation raw-tcp</td>
<td>encapsulation raw-tcp</td>
</tr>
<tr>
<td>!</td>
<td>!</td>
</tr>
<tr>
<td>line 0/2/0</td>
<td>interface async1</td>
</tr>
<tr>
<td>raw-socket tcp server 5000 10.0.0.1</td>
<td>no ip address</td>
</tr>
<tr>
<td>raw-socket packet-timer 3</td>
<td>encapsulation raw-tcp</td>
</tr>
<tr>
<td>raw-socket tcp idle-timeout 5</td>
<td>!</td>
</tr>
<tr>
<td>...</td>
<td>line 1</td>
</tr>
<tr>
<td>raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9000</td>
<td>raw-socket tcp client 10.0.0.1 5000 10.0.0.2 9001</td>
</tr>
<tr>
<td>raw-socket packet-length 32</td>
<td>raw-socket packet-length 32</td>
</tr>
<tr>
<td>raw-socket tcp idle-timeout 5</td>
<td>raw-socket tcp idle-timeout 5</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

Raw Socket UDP

This example shows the configuration for a Raw Socket UDP connection between two IR1101 routers:

From Router1

interface GigabitEthernet0/1
ip address 192.168.0.8 255.255.255.0
duplex auto
speed auto
interface async0/2/0
no ip address
encapsulation raw-udp
line 0/2/0
raw-socket udp connection 192.168.0.2 2 2
Raw Socket VRF

The following example shows a Raw Socket VRF configuration in which two routers, configured for Raw Socket Transport, connect through a VRF. Router1 is an IR1101, serves as the Raw Socket TCP server, and Router2 is an IR807 serves as the Raw Socket TCP client.

Following are the configurations of Router1 and Router2 as shown in Figure 4:

Router1 Configuration

Defining VRF on the router:

```
vrf definition router1
    rd 100:1
    route-target export 100:3
    route-target import 100:3
```

Applying VRF configuration on the interface:

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

Applying raw-tcp on the serial interface:

```
raw-socket udp connection 192.168.0.8 2 2
```

Router2 Configuration

```
interface GigabitEthernet0/1
    ip address 192.168.0.2 255.255.255.0
    load-interval 60
    duplex auto
    speed auto
    no keepalive

interface async0/2/0
    no ip address
    encapsulation raw-udp
    line 0/2/0
    raw-socket udp connection 192.168.0.8 2 2
```

From Router2
interface async0/2/0
  vrf forwarding router1
  no ip address
  encapsulation raw-tcp

Applying raw-tcp on the line:

line 0/2/0
  raw-socket tcp server 5000 4.4.4.4

**Router2 Configuration**

Defining VRF on the router:

vrf definition router1
  rd 100:1
  route-target export 100:3
  route-target import 100:3

address-family ipv4

exit-address-family

Applying VRF configuration on the interface:

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

Applying raw-tcp on the serial interface:

interface async0
  vrf forwarding router1
  no ip address
  encapsulation raw-tcp

Applying raw-tcp on line:

line 1
  raw-socket tcp client 4.4.4.4 5000
System Messages

This chapter contains the following sections:

- Information About Process Management, on page 189
- How to Find Error Message Details, on page 189

Information About Process Management

You can access system messages by logging into 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.

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>%PMAN-0-PROCESS_NOTIFICATION : The process lifecycle notification component failed because [chars]</td>
<td></td>
</tr>
</tbody>
</table>
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.

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

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

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

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>An optional process has failed.</td>
<td>Note the time of the message and investigate the error message logs to learn more about the problem. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: <a href="http://www.cisco.com/tac">http://www.cisco.com/tac</a>. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: <a href="http://www.cisco.com/cisco/psn/bssprt/bss">http://www.cisco.com/cisco/psn/bssprt/bss</a>. If you still require assistance, open a case with the Technical Assistance Center at: <a href="http://tools.cisco.com/ServiceRequestTool/create/">http://tools.cisco.com/ServiceRequestTool/create/</a>, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the show logging and show tech-support commands and your pertinent troubleshooting logs.</td>
</tr>
</tbody>
</table>
A process that does not affect the forwarding of traffic has failed.

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

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

**Explanation**
The process has failed as the result of an error.

**Recommended Action**
This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: http://www.cisco.com/tac. With some messages, these tools and utilities will supply clarifying information. Search for resolved software issues using the Bug Search Tool at: http://www.cisco.com/cisco/psn/bssprt/bss. If you still require assistance, open a case with the Technical Assistance Center at: http://tools.cisco.com/ServiceRequestTool/create/, or contact your Cisco technical support representative and provide the representative with the information you have gathered. Attach the following information to your case in nonzipped, plain-text (.txt) format: the output of the `show logging` and `show tech-support` commands and your pertinent troubleshooting logs.
### Error Message: %PMAN-3-PROCFAIL_IGNORE

**Explanation:** A process failure is being ignored due to the user-configured debug settings.

**Recommended Action:** 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. Functionality 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

**Explanation:** The process [chars] has been held down (rc [dec]).

**Recommended Action:** This message will appear with other messages related to the process. Check the other messages to determine the reason for the failures and see if corrective action can be taken. If the problem persists, copy the message exactly as it appears on the console or in the system log. Research and attempt to resolve the issue using the tools and utilities provided at: [http://www.cisco.com/tac](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](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/](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

**Explanation:** The route processor is being reloaded because there is no ready standby instance.

**Recommended Action:** Ensure that the reload is not due to an error condition.

### Error Message: %PMAN-3-RELOAD_RP

**Explanation:** Reloading: [chars]

**Recommended Action:**
The RP is being reloaded.

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

**Explanation:** The system is being reloaded.

**Recommended Action:** 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:** The executable file used for the process is bad or has permission problem.

**Recommended Action:** 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:** The executable file used for the process is missing, or a dependent library is bad.

**Recommended Action:** 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:** The executable file used for the process is empty.

**Recommended Action:** Ensure that the named executable is non-zero in size.

---

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

**Explanation:** The process manager is exiting.

**Recommended Action:** 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:** The process has gracefully shut down.

**Recommended Action:** No user action is necessary. This message is provided for informational purposes only.

---

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

<table>
<thead>
<tr>
<th>Explanation</th>
<th>Recommended Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>The process has requested a stateless restart.</td>
<td>No user action is necessary. This message is provided for informational purposes only.</td>
</tr>
</tbody>
</table>
Environmental Monitoring

This chapter contains the following sections:

- Environmental Monitoring, on page 195
- Environmental Monitoring and Reporting Functions, on page 195
- Environmental Monitoring Functions, on page 196
- Environmental Reporting Functions, on page 197
- Additional References, on page 203

Environmental Monitoring

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

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

Environmental Monitoring and Reporting Functions

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

- Environmental Monitoring Functions, on page 196
- Environmental Reporting Functions, on page 197
Environmental Monitoring Functions

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

The router is expected to meet the following environmental operating conditions

- **Non-operating Temperature**: -40°F to 158°F (-40°C to 70°C)
- **Non-operating Humidity**: 5 to 95% relative humidity (non-condensing)
- **Operating Temperature**:
  - -40°F to 140°F (-40°C to 60°C) in a sealed NEMA cabinet with no airflow
  - -40°F to 158°F (-40°C to 70°C) in a vented cabinet with 40 lfm of air
  - -40°F to 167°F (-40°C to 75°C) in a forced air enclosure with 200 lfm of air
- **Operating Humidity**: 10% to 95% relative humidity (non-condensing)
- **Operating Altitude**: -500 to 5,000 feet. Derate max operating temperature 1.5°C per 1000 feet.

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

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

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

**Temperature and Voltage Exceed Max/Min Thresholds**

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

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

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

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

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

These commands show the current values of parameters such as temperature and voltage. The environmental monitoring system updates the values of these parameters every 60 seconds. Brief examples of these commands are shown below:

**show diag all eeprom: Example**

Router# `show diag all eeprom`

MIDPLANE EEPROM data:

- Product Identifier (PID) : IR1101-K9
- Version Identifier (VID) : V00
- PCB Serial Number : FOC21482ZQF
- PCB Serial Number : FOC21482CK
- PCB Serial Number : FOC21482SY7
- Top Assy. Part Number : 68-6479-01
- Top Assy. Revision : 13
- Hardware Revision : 0.2
- Asset ID :
- CLEI Code : UNASSIGNED
- Power/Fan Module P0 EEPROM data is not initialized

Power/Fan Module P1 EEPROM data is not initialized

Slot R0 EEPROM data:

- Product Identifier (PID) : IR1101-K9
- Version Identifier (VID) : V00
- PCB Serial Number : FOC21482ZQF
- PCB Serial Number : FOC21482CK
- PCB Serial Number : FOC21482SY7
- Top Assy. Part Number : 68-6479-01
- Top Assy. Revision : 13
- Hardware Revision : 0.2
- CLEI Code : UNASSIGNED
- Slot F0 EEPROM data:
Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED
Slot 0 EEPROM data:

Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
PCB Serial Number : FOC21482ZQF
PCB Serial Number : FOC214822CK
PCB Serial Number : FOC21482SY7
Top Assy. Part Number : 68-6479-01
Top Assy. Revision : 13
Hardware Revision : 0.2
CLEI Code : UNASSIGNED
SPA EEPROM data for subslot 0/0:

Product Identifier (PID) : IR1101-ES-5
Version Identifier (VID) : V01
PCB Serial Number : 68-2236-01
Top Assy. Revision : A0
Hardware Revision : 2.2
CLEI Code : CNUIAHSAAA
SPA EEPROM data for subslot 0/1 is not available
SPA EEPROM data for subslot 0/2 is not available
SPA EEPROM data for subslot 0/3 is not available
SPA EEPROM data for subslot 0/4 is not available
SPA EEPROM data for subslot 0/5 is not available

Router#

**show environment: Example**

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

Slot Sensor Current State Reading Threshold(Minor,Major,Critical,Shutdown)
-----------------------------------
R0 Temp: LM75BXXX Normal 43 Celsius (75 ,80 ,90 ,na )(Celsius)

Router#

**show environment all: Example**

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

**show inventory: Example**

Router# **show inventory**
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "IR1101 Base Chassis"
PID: IR1101-K9 , VID: V00 , SN: FCW2132TH0Z
NAME: "Module 0 - Mother Board", DESCR: "Cisco IR1101 motherboard"
PID: IR1101-K9 , VID: , SN:
NAME: "module subslot 0/0", DESCR: "IR1101-ES-5"
PID: IR1101-ES-5 , VID: V01 , SN:
NAME: "subslot 0/0 transceiver 0", DESCR: "GE SX"
PID: GLC-SX-MM-RGD , VID: V01 , SN: FNS16370HL4
NAME: "module subslot 0/1", DESCR: "P-LTE-US Module"
PID: P-LTE-US , VID: V01 , SN: FOC21333R92
NAME: "Modem 0 on Cellular0/1/0", DESCR: "Sierra Wireless WP7603"
PID: WP7603 , VID: 10000, SN: 35952808000794

**show platform: Example**

Router# **show platform**
Chassis type: IR1101-K9

Slot Type State Insert time (ago)
--------- ------------------ --------------------- -----------------
0 IR1101-K9 ok 01:52:41
0/0 IR1101-ES-5 ok 01:51:35
R0 IR1101-K9 ok, active 01:52:41
F0 IR1101-K9 init, active 01:52:41
Router#

**show platform diag: Example**

Router# **show platform diag**
Chassis type: IR1101-K9

Slot: 0, IR1101-K9
Running state : ok
Internal state : online
Internal operational state : ok
Physical insert detect time : 00:00:25 (5d02h ago)
Software declared up time : 00:01:07 (5d02h ago)
CPLD version :
Firmware version : 1.3

Sub-slot: 0/0, IR1101-ES-5
Operational status: ok
Internal state: inserted
Physical insert detect time: 00:02:21 (5d02h ago)
Logical insert detect time: 00:02:21 (5d02h ago)

Sub-slot: 0/1, P-LTE-US
Operational status: ok
Internal state: inserted
Physical insert detect time: 00:02:21 (5d02h ago)
Logical insert detect time: 00:02:21 (5d02h ago)

Slot: R0, IR1101-K9
Running state: ok, active
Internal state: online
Internal operational state: ok
Physical insert detect time: 00:00:25 (5d02h ago)
Software declared up time: 00:00:25 (5d02h ago)
CPLD version: 00000000
Firmware version: 1.2

Slot: F0, IR1101-K9
Running state: init, active
Internal state: online
Internal operational state: ok
Physical insert detect time: 00:00:25 (5d02h ago)
Software declared up time: 00:01:10 (5d02h ago)
Hardware ready signal time: 00:00:00 (never ago)
Packet ready signal time: 00:00:00 (never ago)
CPLD version: 00000000
Firmware version: 1.2

Router#

show platform software status control-processor: Example

Router# show platform software status control-processor
RP0: online, statistics updated 9 seconds ago
Load Average: healthy
1-Min: 0.32, status: healthy, under 5.00
5-Min: 0.33, status: healthy, under 5.00
15-Min: 0.35, status: healthy, under 5.00
Memory (kb): healthy
Total: 3959840
Used: 2894588 (73%), status: healthy
Free: 1065252 (27%)
Committed: 2435656 (62%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 0.50, System: 0.91, Nice: 0.00, Idle: 98.07
IRQ: 0.40, SIRQ: 0.10, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 0.81, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.20, SIRQ: 0.20, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.81, System: 2.65, Nice: 0.00, Idle: 95.41
IRQ: 1.12, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 7.66, System: 17.05, Nice: 0.00, Idle: 70.58
IRQ: 4.59, SIRQ: 0.10, IOwait: 0.00
show diag slot R0 eeprom detail: Example

Router# show diag slot R0 eeprom detail
Slot R0 EEPROM data:

EEPROM version : 4
Compatible Type : 0xFF
Controller Type : 3457
Hardware Revision : 0.2
PCB Part Number : 73-18820-03
Board Revision : 02
Deviation Number : 0
Fab Version : 02
PCB Serial Number : FOC22106KKH
Top Assy. Part Number : 68-6479-03
Top Assy. Revision : 04
Chassis Serial Number : FCW2213TH07
Deviation Number : 0
RMA Test History : 00
RMA Number : 0-0-0-0
RMA History : 00
Product Identifier (PID) : IR1101-K9
Version Identifier (VID) : V00
CLEI Code : UNASSIGNED
Manufacturing Test Data : 00 00 00 00 00 00 00 00
Field Diagnostics Data : 00 00 00 00 00 00 00 00
Chassis MAC Address : 682c.7b4d.7880
MAC Address block size : 128
Asset ID :
Asset Alias :
PCB Part Number : 73-18821-03
Board Revision : 03
Deviation Number : 0
Fab Version : 02
PCB Serial Number : FOC22106KHD
PCB Part Number : 73-19117-02
Board Revision : 02
Deviation Number : 0
Fab Version : 01
PCB Serial Number : FOC22106KJ9
Asset ID :
Router#

show version: Example

Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software [Gibraltar], ISR Software (ARMV8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1prd7, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Wed 31-Oct-18 23:27 by mcpre
Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc. All rights reserved. Certain components of Cisco IOS-XE software are licensed under the GNU General Public License ("GPL") Version 2.0. The software code licensed under GPL Version 2.0 is free software that comes with ABSOLUTELY NO WARRANTY. You can redistribute and/or modify such GPL code under the terms of GPL Version 2.0. For more details, see the documentation or "License Notice" file accompanying the IOS-XE software, or the applicable URL provided on the flyer accompanying the IOS-XE software.

ROM: IOS-XE ROMMON

Router uptime is 1 hour, 53 minutes
Uptime for this control processor is 1 hour, 54 minutes
System returned to ROM by reload
System image file is "usb0:ir1101-universalk9.16.10.01prd7.SPA.bin"
Last reload reason: Reload Command

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

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

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

Technology Package License Information:

-----------------------------------------------------------------------------------------------
Technology-package Technology-package
Current Type Next reboot
-----------------------------------------------------------------------------------------------
network-advantage Smart License network-advantage

Smart Licensing Status: UNREGISTERED/EVAL EXPIRED

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711867K/6147K bytes of memory.
Processor board ID FCW2150TH0F
1 Virtual Ethernet interface
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
32768K bytes of non-volatile configuration memory.
4038072K bytes of physical memory.
3110864K bytes of Bootflash at bootflash:.
0K bytes of WebUI ODM Files at webui:.
30670832K bytes of USB Flash at usbflash0:.

Configuration register is 0x0 (will be 0x2102 at next reload)

Router#
**show power: Example**

Router# show power
Main PSU :
Total Power Consumed: 8.16 Watts
Router#

**Additional References**

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

**MIBs**

<table>
<thead>
<tr>
<th>MIBs</th>
<th>MIBs Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>CISCO-ENTITY-FRU-CONTROL-MIB</td>
<td>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use the Cisco MIB Locator at: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>.</td>
</tr>
</tbody>
</table>

**Technical Assistance**

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

This section contains the following topics:

- Application Hosting, on page 205

Application Hosting

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

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

Information About Application Hosting

Need for Application Hosting

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

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

IOx Overview

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

IOx architecture for the IR1101 is different compared to other Cisco platforms that use the hypervisor approach. In other platforms, IOx runs as a virtual machine. IOx is running as a process on the IR1101.

The only type of container supported on the IR1101 is the LXC container.

Cisco Application Hosting Overview

The IR1101 enables the user to deploy the application using the app-hosting CLIs. These app-hosting CLIs are not available on the other older platforms. There are additional ways to deploy the applications using the Local Manager and Fog Director.
Application hosting provides the following services:

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

The container is referred to as the virtualization environment provided to run the guest application on the host operating system. The Cisco IOS-XE virtualization services provide manageability and networking models for running guest applications. The virtualization infrastructure allows the administrator to define a logical interface that specifies the connectivity between the host and the guest. IOx maps the logical interface into the Virtual Network Interface Card (vNIC) that the guest application uses.

Applications to be deployed in the containers are packaged as TAR files. The configuration that is specific to these applications is also packaged as part of the TAR file.

The management interface on the device connects the application hosting network to the IOS management interface. The Layer 3 interface of the application receives the Layer 2 bridged traffic from the IOS management interface. The management interface connects through the management bridge to the container/application interface. The IP address of the application must be on the same subnet as the management interface IP address.

IOXMAN

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

Application Hosting on the IR1101 Industrial Integrated Services Router

This section describes the application-hosting characteristics specific to the IR1101 Industrial Integrated Services Router.

Note

The IR1101 CPU is not based on x86 architecture like other Routers. Therefore, this requires the application to comply with the ARM 64-bits architecture.

Application hosting can be achieved using the app-hosting cli's as well using the Local Manager and Fog Director. Application hosting using Local Manager is done through the WebUI. In order to deploy the applications using Local Manager, WebUI should be enabled and then login to the Local Manager.
Figure 10: Local Manager

1. From the WebUI, click on **Configuration > Services > IOx**
2. Login using the username and password configured.
3. Follow the steps for the application lifecycle in the **Cisco IOx Local Manager Reference Guide** using this link: https://www.cisco.com/c/en/us/td/docs/routers/access/800/software/guides/iox/lm/reference-guide/1-7/b_iox_lm_ref_guide_1_7/b_iox_lm_ref_guide_1_7_chapter_011.html

The next section explains the deployment of an application using the app-hosting cli's.

**VirtualPortGroup**

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

VirtualPortGroup interfaces are configured by using the interface virtualportgroup command. Once these interfaces are created, IP address and other resources are allocated.

The VirtualPortGroup interface connects the application hosting network to the IOS routing domain. The Layer 3 interface of the application receives routed traffic from IOS. The VirtualPortGroup interface connects through the SVC Bridge to the container/application interface.

The following graphic helps to understand the relationship between the VirtualPortGroup and other interfaces, as it is different than the IR8x9 routers.
vNIC

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

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

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

How to Configure Application Hosting

Enabling IOx

Perform this task to enable access to the IOx Local Manager. The IOx Local Manager provides a web-based user interface that you can use to manage, administer, monitor, and troubleshoot apps on the host system, and to perform a variety of related activities.
In the steps that follow, IP HTTP commands do not enable IOX, but allow the user to access the WebUI to connect the IOX Local Manager.

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

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Steps</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. enable</td>
<td>Example: Device&gt;enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td>2. configure terminal</td>
<td>Example: Device(config)#configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>3. iox</td>
<td>Example: Device(config)#iox</td>
<td>Enables IOx</td>
</tr>
<tr>
<td>4. ip http server</td>
<td>Example: Device(config)#ip http server</td>
<td>Enables the HTTP server on your IP or IPv6 system.</td>
</tr>
<tr>
<td>5. ip http secure-server</td>
<td>Example: Device(config)#ip http secure-server</td>
<td>Enables a secure HTTP (HTTPS) server.</td>
</tr>
</tbody>
</table>
Configuring a Virtual Port Group to a Layer 3 Data Port

Multiple Layer 3 data ports can be routed to one or more Virtual Port Groups or containers. Virtual Port Groups and Layer 3 data ports must be on different subnets.

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

**SUMMARY STEPS**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 1.   | enable  | Enables privileged EXEC mode. Enter your password if prompted.  
      | Example: Device>enable |         |
| 2.   | configure terminal | Enters global configuration mode.  
      | Example: Device#configure terminal |         |
| 3.   | ip routing | Enables IP routing. The ip routing command must be enabled to allow external routing on Layer 3 data ports.  
      | Example: Device(config)#ip routing |         |
| 4.   | interface type number | Configures an interface and enters interface configuration mode  
      | Example: Device(config)#interface gigabitethernet 0/0/0 |         |
| 5.   | no switchport | Places the interface in Layer 3 mode, and makes it operate more like a router interface rather than a switch port.  
      | Example: Device(config-if)#no switchport |         |
| 6.   | ip address ip-address mask | Configures an IP address for the interface.  
      | Example: Device(config-if)#ip address 10.1.1.1 255.255.255.0 |         |
| 7.   | exit | Exits interface configuration mode and returns to global configuration mode.  
      | Example: Device(config-if)#exit |         |
| 8.   | interface type number | Configures an interface and enters interface configuration mode.  
<pre><code>  | Example: Device(config)#interface virtualportgroup 0 |         |
</code></pre>
<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
</table>
| 9.   | `ip address ip-address mask`  
   Example:  
   `Device(config-if)#ip address 192.168.0.1 255.255.255.0` | Configures an IP address for the interface. |
| 10.  | `end`  
   Example:  
   `Device(config-if)#end` | Exits interface configuration mode and returns to privileged EXEC mode. |
| 11.  | `configure terminal`  
   Enter configuration commands, one per line. End with CNTL/Z.  
   Example:  
   `Device#configure terminal` | Enters global configuration mode. |
| 12.  | `app-hosting appid app1`  
   Example:  
   `Device(config)#app-hosting appid app1` | Configures the application and enters the application configuration mode. |
| 13.  | `app-vnic gateway0 virtualportgroup 0 guest-interface 0`  
   Example:  
   `Device(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0` | Configures the application interface and the gateway of the application. |
| 14.  | `guest-ipaddress 192.168.0.2 netmask 255.255.255.0`  
   Example:  
   `Device(config-app-hosting-gateway0)#guest-ipaddress 192.168.0.2 netmask 255.255.255.0` | Configures the application Ethernet interface ip address. |
### Installing and Uninstalling Apps

#### SUMMARY STEPS

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

#### DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device&gt;enable</td>
</tr>
<tr>
<td>2.</td>
<td>app-hosting install appid application-name package package-path</td>
<td>Installs an app from the specified location. The app can be installed from any local storage location such as, flash, bootflash, and usbflash0.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device#app-hosting install appid lxc_app package flash:my_iox_app.tar</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>15.</td>
<td>app-default-gateway 192.168.0.1 guest-interface 0</td>
<td>Configures the default gateway for the application.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device(config-app-hosting-gateway0)# app-default-gateway 192.168.0.1 guest-interface 0</td>
</tr>
<tr>
<td>16.</td>
<td>end</td>
<td>Exits global configuration mode and returns to privileged EXEC configuration mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td>Device#end</td>
</tr>
<tr>
<td>Step</td>
<td>Command</td>
<td>Purpose</td>
</tr>
<tr>
<td>------</td>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>3.</td>
<td>app-hosting activate appid application-name</td>
<td>Activates the application. This command validates all application resource requests, and if all resources are available the application is activated; if not, the activation fails.</td>
</tr>
<tr>
<td>4.</td>
<td>app-hosting start appid application-name</td>
<td>Starts the application. Application start-up scripts are activated.</td>
</tr>
<tr>
<td>5.</td>
<td>app-hosting stop appid application-name</td>
<td>Stops the application.</td>
</tr>
<tr>
<td>6.</td>
<td>app-hosting deactivate appid application-name</td>
<td>Deactivates all resources allocated for the application.</td>
</tr>
<tr>
<td>7.</td>
<td>app-hosting uninstall appid application-name</td>
<td>Uninstalls the application. Uninstalls all packaging and images stored. All changes and updates to the application are also removed.</td>
</tr>
</tbody>
</table>

### Overriding the App Resource Configuration

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

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

## DETAILED STEPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>enable</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>Device&gt;enable</code></td>
</tr>
<tr>
<td>2.</td>
<td>configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>configure terminal</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>Device#configure terminal</code></td>
</tr>
<tr>
<td>3.</td>
<td>app-hosting appid name</td>
<td>Enables application hosting and enters application hosting configuration mode.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>app-hosting appid</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>Device(config)#app-hosting appid app1</code></td>
</tr>
<tr>
<td>4.</td>
<td>app-resource profile name</td>
<td>Configures the custom application resource profile, and enters custom application resource profile configuration mode. Only the custom profile name is supported.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>app-resource profile</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>Device(config-app-hosting)#app-resource profile custom</code></td>
</tr>
<tr>
<td>5.</td>
<td>cpu unit</td>
<td>Changes the default CPU allocation for the application. Resource values are application-specific, and any adjustment to these values must ensure that the application can run reliably with the changes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>cpu</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>Device(config-app-resource-profile-custom)#cpu 800</code></td>
</tr>
<tr>
<td>6.</td>
<td>memory memory</td>
<td>Changes the default memory allocation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Command: <code>memory</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Example: <code>Device(config-app-resource-profile-custom)#memory 512</code></td>
</tr>
</tbody>
</table>
Verifying the Application Hosting Configuration

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

**DETAILED STEPS**

1. **enable**
   Enables privileged EXEC mode. Enter your password if prompted.
   **Example:**
   
   ```
   Device>enable
   ```

2. **show iox-service**
   Displays the status of all IOx services
   **Example:**
   
   ```
   Device# show iox-service
   IOx Infrastructure Summary:
   -------------------------------
   IOx Service (CAF) : Running
   IOx Service (HA) : Running
   IOx Service (IOxman) : Running
   Libvirtd : Running
   ```

3. **show app-hosting detail**
   Displays detailed information about the application.
   **Example:**
   
   ```
   Device# show app-hosting detail
   ```

### Table: vCPU Allocation

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.</td>
<td><code>vcpu number</code></td>
<td>Changes the virtual CPU (vCPU) allocation for the application.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-app-resource-profile-custom)# vcpu 2</code></td>
<td></td>
</tr>
<tr>
<td>8.</td>
<td><code>end</code></td>
<td>Exits custom application resource profile configuration mode and returns to privileged EXEC mode.</td>
</tr>
<tr>
<td></td>
<td>Example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>Device(config-app-resource-profile-custom)# end</code></td>
<td></td>
</tr>
</tbody>
</table>
App id : app1
Owner : iox
State : RUNNING
Application
Type : lxc
Name : nt08-stress
Version : 0.1
Description : Stress Testing Application
Path : usbflash0: my_iox_app.tar
Activated profile name : custom
Resource reservation
Memory : 64 MB
Disk : 2 MB
CPU : 500 units
Attached devices
<table>
<thead>
<tr>
<th>Name</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>serial/shell</td>
<td>serial0</td>
</tr>
<tr>
<td>serial/aux</td>
<td>serial1</td>
</tr>
<tr>
<td>serial/syslog</td>
<td>serial2</td>
</tr>
<tr>
<td>serial/trace</td>
<td>serial3</td>
</tr>
</tbody>
</table>

Network interfaces
eth0:
   MAC address : 52:54:dd:fa:25:ee

4. show app-hosting list
Displays the list of applications and their status.
Example:

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

Configuration Examples for Application Hosting

See the following examples:

Example: Enabling IOx

```
Device> enable
Device# configure terminal
Device(config)# iox
Device(config)# ip http server
Device(config)# ip http secure-server
Device(config)# username cisco privilege 15 password 0 cisco
Device(config)# end
```

Example: Configuring a VirtualPortGroup to a Layer 3 Data Port

```
Device> enable
Device# configure terminal
Device(config)# ip routing
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# no switchport
```
Example: Installing and Uninstalling Apps

Device> enable
Device# app-hosting install appid app1 package flash:my_iox_app.tar
Device# app-hosting activate appid app1
Device# app-hosting start appid app1
Device# app-hosting stop appid app1
Device# app-hosting deactivate appid app1
Device# app-hosting uninstall appid app1

Example: Overriding the App Resource Configuration

Device# configure terminal
Device(config)# app-hosting appid app1
Device(config-app-hosting)# app-resource profile custom
Device(config-app-resource-profile-custom)# cpu 800
Device(config-app-resource-profile-custom)# memory 512
Device(config-app-resource-profile-custom)# vcpu 2
Device(config-app-resource-profile-custom)# end
CHAPTER 16

ROM Monitor Overview

- ROM Monitor Overview and Basic Procedures, on page 219

ROM Monitor Overview and Basic Procedures

This chapter provides an overview of ROM Monitor concepts and operations. This chapter includes the following main topics:

ROM Monitor Overview

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

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

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

Environmental Variables and the Configuration Register

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

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

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

**Accessing ROM Monitor Mode with a Terminal Connection**

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

**Network Management Access and ROM Monitor Mode**

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

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

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

---

**Note**

TFTP access variables are currently not supported on the IR1101 platform.

---

**Access ROM Monitor Mode**

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

**Checking the Current ROMMON Version**

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

```
Router#show rom-monitor r0
System Bootstrap, Version 1.2, RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.

Router# show romvar
ROMMON variables:
PS1 = rommon ! >
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
LICENSE_SUITE =
RET_2_RTS =
Diagnostic = 1
THRPUT =
USER_BOOT_PARAM = DEBUG_CONF=/bootflash/debug.conf
EULA_ACCEPTED = TRUE
BOOT_WDOG = DISABLE
LICENSE_BOOT_LEVEL =
BOOT = bootflash:sparrow_crashkernel.bin,1;
```
CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
RET_2_RCALTS =
BSI = 0
RANDOM_NUM = 1662155698

Router# reload

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

rommon 1 > set
PS1=rommon ! >
MCP_STARTUP_TRACEFLAGS = 00000000:00000000
LICENSE_SUITE =
RET_2_RTS =
Diagnostic = 1
THRPAT =
USER_BOOT_PARAM = DEBUG_CONF=/bootflash/debug.conf
EULA_ACCEPTED = TRUE
BOOT_WDOG = DISABLE
LICENSE_BOOT_LEVEL =
BOOT = bootflash:sparrow_crashkernel.bin,1;
CRASHINFO = bootflash:crashinfo_RP_00_00_20180619-204307-UTC
RET_2_RCALTS =
BSI = 0
RANDOM_NUM = 1662155698

**Commonly Used ROM Monitor Commands**

The following table summarizes the commands commonly used in ROM Monitor. For specific instructions on using these commands, refer to the relevant procedure in this document.

*Table 21: Commonly Used ROM Monitor Commands*

<table>
<thead>
<tr>
<th>ROMMON Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boot image</td>
<td>Manually boots a Cisco IOS XE software image.</td>
</tr>
<tr>
<td>boot image –o config-file-path</td>
<td>Manually boots the Cisco IOS XE software with a temporary alternative administration configuration file.</td>
</tr>
<tr>
<td>confreg</td>
<td>Changes the config-register setting.</td>
</tr>
<tr>
<td>dev</td>
<td>Displays the available local storage devices.</td>
</tr>
<tr>
<td>dir</td>
<td>Displays the files on a storage device.</td>
</tr>
<tr>
<td>reset</td>
<td>Resets the node.</td>
</tr>
<tr>
<td>set</td>
<td>Displays the currently set ROM Monitor environmental settings.</td>
</tr>
<tr>
<td>sync</td>
<td>Saves the new ROM Monitor environmental settings.</td>
</tr>
<tr>
<td>unset</td>
<td>Removes an environmental variable setting.</td>
</tr>
</tbody>
</table>
Examples

The following example shows what appears when you enter the ? command on a router:

rommon 1 > ?
alias set and display aliases command
boot boot up an external process
confreg configuration register utility
deve list the device table
dir list files in file system
help monitor built-in command help
history monitor command history
meminfo main memory information
repeat repeat a monitor command
reset system reset
set display the monitor variables
showmon display currently selected ROM monitor
sync write monitor environment to NVRAM
token display board's unique token identifier
unalias unset an alias
unset unset a monitor variable

Changing the ROM Monitor Prompt

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

rommon 8 > PS1="IR1101 rommon ! > "
IR1101 rommon 9 >

Changing the prompt is useful if you are working with multiple routers in ROM Monitor at the same time. This example specifies that the prompt should be “IR1101 rommon “, followed by the line number, and then followed by “ > “ by the line number.

Displaying the Configuration Register Setting

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

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

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

Environment Variable Settings

The ROM Monitor environment variables define the attributes of the ROM Monitor. Environmental variables are entered like commands and are always followed by the equal sign (=). Environment variable settings are entered in capital letters, followed by a definition. For example:
IP_ADDRESS=10.0.0.2

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

This section includes the following topics:

Frequently Used Environmental Variables

The following table shows the main ROM Monitor environmental variables. For instructions on how to use these variables, see the relevant instructions in this document. The IR1101 boot loader does not support netboot, so any setting like environment variables IP_ADDRESS, IP_SUBNET_MASK, DEFAULT_GATEWAY, TFTP_SERVER, TFTP_FILE are not used.

Table 22: Frequently Used ROM Monitor Environmental Variables

<table>
<thead>
<tr>
<th>Environmental variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT=path/file</td>
<td>Identifies the boot software for a node. This variable is usually set automatically when the router boots.</td>
</tr>
</tbody>
</table>

Displaying Environment Variable Settings

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

```
rommon 1 > showmon
System Bootstrap, Version 1.3(REL), RELEASE SOFTWARE
Copyright (c) 1994-2018 by cisco Systems, Inc.
IR1101-K9 platform with 4188160 Kbytes of main memory
MCU Version - Bootloader: 4, App: 4
MCU is in application mode.
```

Entering Environment Variable Settings

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

```
rommon 1 > confreg 0x0
rommon 1> BOOT_WDOG = DISABLE
rommon 1> BOOT = IR1101-K9_image_name
```

Saving Environment Variable Settings

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

```
rommon > sync
```

Note

Environmental values that are not saved with the sync command are discarded whenever the system is reset or booted.
Exiting ROM Monitor Mode

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

**SUMMARY STEPS**

1. `confreg`
2. Respond to each prompt as instructed.
3. `reset`

**DETAILED STEPS**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td></td>
</tr>
<tr>
<td><code>confreg</code></td>
<td>Initiates the configuration register configuration prompts.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>rommon 1&gt; confreg</code></td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td></td>
</tr>
<tr>
<td>Respond to each prompt as instructed.</td>
<td>See the example that follows this procedure for more information.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td><code>reset</code></td>
<td>Resets and initializes the router.</td>
</tr>
<tr>
<td><strong>Example:</strong></td>
<td></td>
</tr>
<tr>
<td><code>rommon 2&gt; reset</code></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Example**

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

ROMmon upgrade on the IR1101-K9 router is automatically done when the image is booted. The latest version of the ROMmon is bundled with the IOSXE image. An algorithm detects if the current running version is older than the bundled version, if so, it is automatically upgraded. If the current running version is equal to the bundled version no upgrade is executed. For every successful upgrade, the router is automatically rebooted in order for the new version to get loaded and executed.

SUMMARY STEPS

1. (Optional) Run the `show rom-monitor slot` command on the router to see the current release numbers of ROMmon on the hardware. See the Checking the Current ROMMON Version, on page 220 for information about interpreting the output of the command that you run.

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

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

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

DETAILED STEPS

<table>
<thead>
<tr>
<th>Step 1</th>
<th>(Optional) Run the <code>show rom-monitor slot</code> command on the router to see the current release numbers of ROMmon on the hardware. See the Checking the Current ROMMON Version, on page 220 for information about interpreting the output of the command that you run.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>If autoboott has not been enabled by using the <code>config-register 0x2102</code> command, run the <code>boot filesystem:/file-location</code> command at the ROMmon prompt to boot the Cisco IOSXE image, where <code>filesystem:/file-location</code> is the path to the consolidated package file. The ROMmon upgrade is not permanent for any piece of hardware until the Cisco IOSXE image is booted.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Run the <code>enable</code> command at the user prompt to enter the privileged EXEC mode after the boot is complete.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Run the <code>show rom-monitor slot</code> command to verify whether the ROMmon has been upgraded.</td>
</tr>
</tbody>
</table>
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 227
• Monitoring Hardware Using Alarms, on page 233

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 227
• Cisco IOS Process Resources, on page 227
• Overall Control Plane Resources, on page 231

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#33e0077971693714bd2b0bc347d77489
Address Bytes Prev Next Ref PrevF NextF what Alloc PC

Head Total(b) Used(b) Free(b) Lowest(b) Largest(b)
Processor 7F68ECD010 728952276 281540188 447412088 445683380 234766720
lsmpi_io 7F6852A1A8 6295128 6294304 824 824 412

Dynamic heap limit(MB) 200 Use(MB) 0

Processor memory
Address Bytes Prev Next Ref PrevF NextF what Alloc PC

Processor memory
Address Bytes Prev Next Ref PrevF NextF what Alloc PC

Cisco IR1101 Integrated Services Router Software Configuration Guide
The `show process cpu` command displays Cisco IOS CPU utilization average:

Router# `show process cpu`

CPU utilization for five seconds: 0% / 0%; one minute: 0%; five minutes: 0%

<table>
<thead>
<tr>
<th>PID</th>
<th>Runtime(ms)</th>
<th>Invoked uSecs</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>TTY</th>
<th>Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Chunk Manager</td>
</tr>
<tr>
<td>2</td>
<td>552</td>
<td>1205</td>
<td>458</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Load Meter</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>PKI Trustpool</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Retransmission o</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC ISSU Dispatch</td>
</tr>
<tr>
<td>6</td>
<td>36</td>
<td>13</td>
<td>2769</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>RF Slave Main Th</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>PKI Issu Mgmt</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>RO Notify Timers</td>
</tr>
<tr>
<td>9</td>
<td>4052</td>
<td>920</td>
<td>4404</td>
<td>0%</td>
<td>0.06%</td>
<td>0</td>
<td>Check heaps</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>101</td>
<td>118</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Pool Manager</td>
</tr>
<tr>
<td>11</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>DiscardQ Backgro</td>
</tr>
<tr>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Timers</td>
</tr>
<tr>
<td>13</td>
<td>163</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Platform appsess</td>
</tr>
<tr>
<td>14</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ATM AutoVC Perio</td>
</tr>
<tr>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ATM VC Auto Crea</td>
</tr>
<tr>
<td>16</td>
<td>76</td>
<td>3024</td>
<td>25</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0</td>
<td>IOSXE heartbeat</td>
</tr>
<tr>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>DB Lock Manager</td>
</tr>
<tr>
<td>18</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>DB Notification</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Apps Task</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ifIndex Receive</td>
</tr>
<tr>
<td>21</td>
<td>36</td>
<td>1210</td>
<td>29</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Event Notify</td>
</tr>
<tr>
<td>22</td>
<td>72</td>
<td>5904</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Mcast Pendin</td>
</tr>
<tr>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Platform appsess</td>
</tr>
<tr>
<td>24</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Platform appsess</td>
</tr>
<tr>
<td>25</td>
<td>15</td>
<td>1210</td>
<td>13</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Service NonC</td>
</tr>
<tr>
<td>26</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Zone Manager</td>
</tr>
<tr>
<td>27</td>
<td>64</td>
<td>5904</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Periodic Tim</td>
</tr>
<tr>
<td>28</td>
<td>76</td>
<td>5904</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Deferred For</td>
</tr>
<tr>
<td>29</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Process leve</td>
</tr>
<tr>
<td>30</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Seat Manager</td>
</tr>
<tr>
<td>31</td>
<td>8</td>
<td>346</td>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Check Queue</td>
</tr>
<tr>
<td>32</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Seat RX Cont</td>
</tr>
<tr>
<td>33</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Seat TX Cont</td>
</tr>
<tr>
<td>34</td>
<td>48</td>
<td>606</td>
<td>79</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Keep Alive M</td>
</tr>
<tr>
<td>35</td>
<td>28</td>
<td>1210</td>
<td>23</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Loadometer</td>
</tr>
<tr>
<td>36</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>IPC Session Deta</td>
</tr>
<tr>
<td>37</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>SENSOR-MGR event</td>
</tr>
<tr>
<td>38</td>
<td>4</td>
<td>606</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>Compute SRP rate</td>
</tr>
<tr>
<td>39</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>MEMLEAK PROCESS</td>
</tr>
<tr>
<td>40</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ARP Input</td>
</tr>
<tr>
<td>41</td>
<td>112</td>
<td>6331</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ARP Background</td>
</tr>
<tr>
<td>42</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ATM Idle Timer</td>
</tr>
<tr>
<td>43</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ATM Async PROC</td>
</tr>
<tr>
<td>44</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>CEF MIB API</td>
</tr>
</tbody>
</table>

--More--

...  

The `show process cpu platform sorted` command displays Cisco IOS CPU utilization average:

CPU utilization for five seconds: 11%, one minute: 12%, five minutes: 12%
Core 0: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 1: CPU utilization for five seconds: 1%, one minute: 3%, five minutes: 3%
Core 2: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 3: CPU utilization for five seconds: 42%, one minute: 42%, five minutes: 42%

<table>
<thead>
<tr>
<th>Pid</th>
<th>PPid</th>
<th>5Sec</th>
<th>1Min</th>
<th>5Min</th>
<th>Status</th>
<th>Size</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>18246</td>
<td>17700</td>
<td>34%</td>
<td>34%</td>
<td>34%</td>
<td>S</td>
<td>272500</td>
<td>qfp-ucode-sparr</td>
</tr>
<tr>
<td>18297</td>
<td>16477</td>
<td>1%</td>
<td>1%</td>
<td>1%</td>
<td>S</td>
<td>8460</td>
<td>nginx</td>
</tr>
<tr>
<td>25928</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2960</td>
<td>rotee</td>
</tr>
<tr>
<td>25664</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3532</td>
<td>pman.sh</td>
</tr>
<tr>
<td>24212</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/u8:0</td>
</tr>
<tr>
<td>19648</td>
<td>8282</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>220</td>
<td>sleep</td>
</tr>
<tr>
<td>19635</td>
<td>10903</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>212</td>
<td>sleep</td>
</tr>
<tr>
<td>18121</td>
<td>17675</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>10968</td>
<td>ngiolite</td>
</tr>
<tr>
<td>17979</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>1660</td>
<td>rotee</td>
</tr>
<tr>
<td>17863</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/1:0</td>
</tr>
<tr>
<td>17859</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2836</td>
<td>rotee</td>
</tr>
<tr>
<td>17737</td>
<td>17095</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>56828</td>
<td>iomd</td>
</tr>
<tr>
<td>17700</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3566</td>
<td>pman.sh</td>
</tr>
<tr>
<td>17675</td>
<td>12798</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3524</td>
<td>pman.sh</td>
</tr>
<tr>
<td>17518</td>
<td>16854</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>15024</td>
<td>hman</td>
</tr>
<tr>
<td>17312</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2828</td>
<td>rotee</td>
</tr>
<tr>
<td>17095</td>
<td>12798</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3568</td>
<td>pman.sh</td>
</tr>
<tr>
<td>17085</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2876</td>
<td>rotee</td>
</tr>
<tr>
<td>16942</td>
<td>2</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>0</td>
<td>kworker/0:1</td>
</tr>
<tr>
<td>16892</td>
<td>14768</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>108952</td>
<td>cpp_cp_svr</td>
</tr>
<tr>
<td>16854</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3568</td>
<td>pman.sh</td>
</tr>
<tr>
<td>16716</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2996</td>
<td>rotee</td>
</tr>
<tr>
<td>16664</td>
<td>15963</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>51096</td>
<td>cpp_sp_svr</td>
</tr>
<tr>
<td>16477</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3540</td>
<td>pman.sh</td>
</tr>
<tr>
<td>16326</td>
<td>15536</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>39652</td>
<td>cpp_ha_top_leve</td>
</tr>
<tr>
<td>15963</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3528</td>
<td>pman.sh</td>
</tr>
<tr>
<td>15779</td>
<td>15163</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>55208</td>
<td>cpp_driver</td>
</tr>
<tr>
<td>15730</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>1640</td>
<td>rotee</td>
</tr>
<tr>
<td>15536</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3528</td>
<td>pman.sh</td>
</tr>
<tr>
<td>15412</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>1716</td>
<td>rotee</td>
</tr>
<tr>
<td>15274</td>
<td>14681</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>15004</td>
<td>hman</td>
</tr>
<tr>
<td>15163</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3624</td>
<td>pman.sh</td>
</tr>
<tr>
<td>15083</td>
<td>14361</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>26792</td>
<td>cman_fp</td>
</tr>
<tr>
<td>14891</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2868</td>
<td>rotee</td>
</tr>
<tr>
<td>14768</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3568</td>
<td>pman.sh</td>
</tr>
<tr>
<td>14722</td>
<td>14127</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>27536</td>
<td>cmcc</td>
</tr>
<tr>
<td>14717</td>
<td>14108</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>15220</td>
<td>btman</td>
</tr>
<tr>
<td>14681</td>
<td>12798</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3572</td>
<td>pman.sh</td>
</tr>
<tr>
<td>14627</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2996</td>
<td>rotee</td>
</tr>
<tr>
<td>14361</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3596</td>
<td>pman.sh</td>
</tr>
<tr>
<td>14338</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2984</td>
<td>rotee</td>
</tr>
<tr>
<td>14314</td>
<td>1</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>2824</td>
<td>rotee</td>
</tr>
<tr>
<td>14155</td>
<td>13577</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>15128</td>
<td>btman</td>
</tr>
<tr>
<td>14127</td>
<td>12798</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3612</td>
<td>pman.sh</td>
</tr>
<tr>
<td>14108</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>3572</td>
<td>pman.sh</td>
</tr>
<tr>
<td>13813</td>
<td>13380</td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>S</td>
<td>252</td>
<td>inotifywait</td>
</tr>
</tbody>
</table>

--More--
Overall Control Plane Resources

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

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

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

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

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

Load Average

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

Memory Utilization

Memory utilization is represented by the following fields:

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

CPU Utilization

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

- CPU—Allocated processor
- User—Non-Linux kernel processes
- System—Linux kernel process
- Nice—Low-priority processes
- Idle—Percentage of time the CPU was inactive
- IRQ—Interrupts
• SIRQ—System Interrupts

• IOwait—Percentage of time CPU was waiting for I/O

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 4 seconds ago
Load Average: healthy
1-Min: 0.29, status: healthy, under 5.00
5-Min: 0.51, status: healthy, under 5.00
15-Min: 0.54, status: healthy, under 5.00
Memory (kb): healthy
Total: 4038072
Used: 2872136 (71%), status: healthy
Free: 1165936 (29%)
Committed: 2347228 (58%), under 90%
Per-core Statistics
CPU0: CPU Utilization (percentage of time spent)
User: 1.00, System: 0.70, Nice: 0.00, Idle: 97.88
IRQ: 0.30, SIRQ: 0.10, IOwait: 0.00
CPU1: CPU Utilization (percentage of time spent)
User: 0.70, System: 0.30, Nice: 0.00, Idle: 98.48
IRQ: 0.30, SIRQ: 0.20, IOwait: 0.00
CPU2: CPU Utilization (percentage of time spent)
User: 0.20, System: 1.11, Nice: 0.00, Idle: 97.87
IRQ: 0.40, SIRQ: 0.00, IOwait: 0.00
CPU3: CPU Utilization (percentage of time spent)
User: 8.23, System: 24.37, Nice: 0.00, Idle: 58.00
IRQ: 9.26, SIRQ: 0.11, IOwait: 0.00

Router# show platform software status control-processor brief
Load Average
Slot Status 1-Min 5-Min 15-Min
RP0 Healthy 0.28 0.46 0.52
Memory (kB)
Slot Status Total Used (Pct) Free (Pct) Committed (Pct)
RP0 Healthy 4038072 2872136 (71%) 1165936 (29%) 2347228 (58%)
CPU Utilization
Slot CPU User System Nice Idle IRQ SIRQ IOwait
RP0 0 0.70 0.20 0.00 98.58 0.30 0.20 0.00
1 1.10 0.90 0.00 97.59 0.30 0.10 0.00
2 0.40 1.31 0.00 97.87 0.40 0.00 0.00
3 8.00 26.55 0.00 56.33 8.99 0.11 0.00
Monitoring Hardware Using Alarms

Router Design and Monitoring Hardware

The router sends alarm notifications when problems are detected, allowing you to monitor the network remotely. You do not need to use show commands to poll devices on a routine basis; however, you can perform onsite monitoring if you choose.

BootFlash Disk Monitoring

The bootflash disk must have enough free space to store two core dumps. This condition is monitored, and if the bootflash disk is too small to store two core dumps, a syslog alarm is generated, as shown in the following example:

```
Oct 6 14:10:56.292: %FLASH_CHECK-3-DISK_QUOTA: R0/0: flash_check: Flash disk quota exceeded
[free space is 1429020 kB] - Please clean up files on bootflash.
```

Approaches for Monitoring Hardware Alarms

Viewing the Console or Syslog for Alarm Messages

The network administrator can monitor alarm messages by reviewing alarm messages sent to the system console or to a system message log (syslog).

Enabling the logging alarm Command

The `logging alarm` command must be enabled for the system to send alarm messages to a logging device, such as the console or a syslog. This command is not enabled by default.

You can specify the severity level of the alarms to be logged. All the alarms at and above the specified threshold generate alarm messages. For example, the following command sends only critical alarm messages to logging devices:

```
Router(config)# logging alarm critical
```

If alarm severity is not specified, alarm messages for all severity levels are sent to logging devices.

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

The SNMP is an application-layer protocol that provides a standardized framework and a common language used for monitoring and managing devices in a network.

SNMP provides notification of faults, alarms, and conditions that might affect services. It allows a network administrator to access router information through a network management system (NMS) instead of reviewing logs, polling devices, or reviewing log reports.

To use SNMP to get alarm notification, use the following MIBs:
• ENTITY-MIB, RFC4133 (required for the CISCO-ENTITY-ALARM-MIB, ENTITY-STATE-MIB and CISCO-ENTITY-SENSOR-MIB to work)

• CISCO-ENTITY-ALARM-MIB

• ENTITY-STATE-MIB

• CISCO-ENTITY-SENSOR-MIB (for transceiver environmental alarm information, which is not provided through the CISCO-ENTITY-ALARM-MIB)
Troubleshooting

This section describes the troubleshooting scenarios.

Before troubleshooting a software problem, you must connect a PC to the router via the console port. With a connected PC, you can view status messages from the router and enter commands to troubleshoot a problem.

You can also remotely access the interface by using Telnet. The Telnet option assumes that the interface is up and running.

- Understanding Diagnostic Mode, on page 235
- Before Contacting Cisco or Your Reseller, on page 236
- show interfaces Troubleshooting Command, on page 236
- Software Upgrade Methods, on page 236
- Recovering a Lost Password, on page 237

Understanding Diagnostic Mode

The router boots up or accesses diagnostic mode in the following scenarios:

- The IOS process or processes fail, in some scenarios. In other scenarios, the system resets when the IOS process or processes fail.
- A user-configured access policy was configured using the transport-map command that directs the user into the diagnostic mode.
- A send break signal (Ctrl-C or Ctrl-Shift-6) was entered while accessing the router, and the router was configured to enter diagnostic mode when a break signal was sent.

In the diagnostic mode, a subset of the commands that are available in user EXEC mode are made available to the users. Among other things, these commands can be used to:

- Inspect various states on the router, including the IOS state.
- Replace or roll back the configuration.
- Provide methods of restarting the IOS or other processes.
- Reboot hardware, such as the entire router, a module, or possibly other hardware components.
- Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.
The diagnostic mode provides a more comprehensive user interface for troubleshooting than previous routers, which relied on limited access methods during failures, such as ROMMON, to diagnose and troubleshoot Cisco IOS problems. The diagnostic mode commands can work when the Cisco IOS process is not working properly. These commands are also available in privileged EXEC mode on the router when the router is working normally.

Before Contacting Cisco or Your Reseller

If you cannot locate the source of a problem, contact your local reseller for advice. Before you call, you should have the following information ready:

- Chassis type and serial number
- Maintenance agreement or warranty information
- Type of software and version number
- Date you received the hardware
- Brief description of the problem
- Brief description of the steps you have taken to isolate the problem

show interfaces Troubleshooting Command

Use the show interfaces command to display the status of all physical ports and logical interfaces on the router. #unique_312unique_312_Connect_42_tab_1055127 describes messages in the command output.

The IR1101 supports the following interfaces:
- GigabitEthernet 0/0/0
- Cellular 0/1/0
- FastEthernet 0/0/1 to 0/0/4
- Async 0/2/0

Software Upgrade Methods

Several methods are available for upgrading software on the Cisco IR1101 Routers, including:

- Copy the new software image to flash memory over LAN or WAN when the existing Cisco IOS software image is in use.
- Copy the new software image to flash memory over the LAN while the boot image (ROM monitor) is operating.
- Copy the new software image over the console port while in ROM monitor mode.
- From ROM monitor mode, boot the router from a software image that is loaded on a TFTP server. To use this method, the TFTP server must be on the same LAN as the router.
Recovering a Lost Password

To recover a lost enable or lost enable-secret password, refer to the following sections:

1. Change the Configuration Register
2. Reset the Router
3. Reset the Password and Save your Changes (for lost enable secret passwords only)
4. Reset the Configuration Register Value.
5. If you have performed a write erase, or used the reset button, you will need to add the license.

   IR1101# config term
   IR1101# license smart reservation

Note

Recovering a lost password is only possible when you are connected to the router through the console port. These procedures cannot be performed through a Telnet session.

Tip

See the “Hot Tips” section on Cisco.com for additional information on replacing enable secret passwords.

Change the Configuration Register

To change a configuration register, follow these steps:

SUMMARY STEPS

1. Connect a PC to the CONSOLE port on the router.
2. At the privileged EXEC prompt (router_name #), enter the show version command to display the existing configuration register value (shown in bold at the bottom of this output example):
3. Record the setting of the configuration register.
4. To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the config-register 0x01 command from privileged EXEC mode.

DETAILED STEPS

Step 1  Connect a PC to the CONSOLE port on the router.
Step 2  At the privileged EXEC prompt (router_name #), enter the show version command to display the existing configuration register value (shown in bold at the bottom of this output example):

Example:

```
Router# show version
Cisco IOS XE Software, Version 16.10.01
Cisco IOS Software (ARMv8EL_LINUX_IOSD-UNIVERSALK9-M), Version 16.10.1, RELEASE
```
Cisco IOS-XE software, Copyright (c) 2005-2018 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 14 hours, 36 minutes
Uptime for this control processor is 14 hours, 37 minutes
System returned to ROM by reload
System restarted at 08:47:04 GMT Mon Nov 12 2018
System image file is "bootflash:ir1101-universalk9.16.10.01.SPA.bin"
Last reload reason: Reload Command

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

A summary of U.S. laws governing Cisco cryptographic products may be found at:

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

Technology Package License Information:

<table>
<thead>
<tr>
<th>Technology-package</th>
<th>Current Type</th>
<th>Technology-package</th>
<th>Next reboot</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-essentials</td>
<td>Smart License</td>
<td></td>
<td>network-essentials</td>
</tr>
</tbody>
</table>

Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco IR1101-K9 (ARM64) processor (revision 1.2 GHz) with 711861K/6147K bytes of memory.
Processor board ID FCW222700MY
3 Virtual Ethernet interfaces
4 FastEthernet interfaces
1 Gigabit Ethernet interface
1 Serial interface
1 terminal line
2 Cellular interfaces
32768K bytes of non-volatile configuration memory.
Step 3 Record the setting of the configuration register.

Step 4 To enable the break setting (indicated by the value of bit 8 in the configuration register), enter the `config-register 0x01` command from privileged EXEC mode.

- Break enabled—Bit 8 is set to 0.
- Break disabled (default setting)—Bit 8 is set to 1.

### Configuring the Configuration Register for Autoboot

**Note**

Alter the configuration register is only for advanced troubleshooting and should only be done with guidance from Cisco support.

The configuration register can be used to change router behavior. This includes controlling how the router boots. Set the configuration register to 0x0 to boot into ROM, by using one of the following commands:

- In Cisco IOS configuration mode, use the `config-reg 0x0` command.
- From the ROMMON prompt, use the `confreg 0x0` command.

**Note**

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

### Reset the Router

To reset the router, follow these steps:

**SUMMARY STEPS**

1. If break is disabled, turn the router off (O), wait 5 seconds, and turn it on (I) again. Within 60 seconds, press the Break key. The terminal displays the ROM monitor prompt.
2. Press break. The terminal displays the following prompt:
3. Enter `confreg 0x142` to reset the configuration register:
4. Initialize the router by entering the `reset` command:
5. Enter `no` in response to the prompts until the following message is displayed:
6. Press Return. The following prompt appears:
7. Enter the enable command to enter enable mode. Configuration changes can be made only in enable mode:
8. Enter the `show startup-config` command to display an enable password in the configuration file:
DETAILED STEPS

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:
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:

**SUMMARY STEPS**

1. Enter the `configure terminal` command to enter global configuration mode:
2. Enter the `enable secret` command to reset the enable secret password in the router:
3. Enter `exit` to exit global configuration mode:
4. Save your configuration changes:

**DETAILED STEPS**

**Step 1**

Enter the `configure terminal` command to enter global configuration mode:

Example:

```
Router# configure terminal
```

**Step 2**

Enter the `enable secret` command to reset the enable secret password in the router:

Example:

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

**Step 3**

Enter `exit` to exit global configuration mode:

Example:

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

**Step 4**

Save your configuration changes:

Example:

```
```
Reset the Configuration Register Value

To reset the configuration register value after you have recovered or reconfigured a password, follow these steps:

**SUMMARY STEPS**

1. Enter the `configure terminal` command to enter global configuration mode:

   **Example:**
   
   ```
   Router# configure terminal
   ```

2. Enter the `configure register` command and the original configuration register value that you recorded.

   **Example:**
   
   ```
   Router(config)# config-reg value
   ```

3. Enter `exit` to exit configuration mode:

   **Example:**
   
   ```
   Router(config)# exit
   ```

4. Reboot the router, and enter the recovered password.

**DETAILED STEPS**

**Step 1**

Enter the `configure terminal` command to enter global configuration mode:

**Example:**

```
Router# configure terminal
``` 

**Step 2**

Enter the `configure register` command and the original configuration register value that you recorded.

**Example:**

```
Router(config)# config-reg value
``` 

**Step 3**

Enter `exit` to exit configuration mode:

**Example:**

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

**Note**

To return to the configuration being used before you recovered the lost enable password, do not save the configuration changes before rebooting the router.

**Step 4**

Reboot the router, and enter the recovered password.

---

Configuring a Console Port Transport Map

This task describes how to configure a transport map for a console port interface on the router.

**SUMMARY STEPS**

1. `enable`
2. `configure terminal`
3. transport-map type console transport-map-name
4. connection wait [allow [interruptible] | none [disconnect]]
5. (Optional) banner [diagnostic | wait] banner-message
6. exit
7. transport type console console-line-number input transport-map-name

DETAILED STEPS

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> enable</td>
<td>Enables privileged EXEC mode. Enter your password if prompted.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router&gt; enable</td>
<td></td>
</tr>
<tr>
<td><strong>Step 2</strong> configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router# configure terminal</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> transport-map type console transport-map-name</td>
<td>Creates and names a transport map for handling console connections, and enters transport map configuration mode.</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config)# transport-map type console consolehandler</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> connection wait [allow [interruptible]</td>
<td>none [disconnect]]</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-tmap)# connection wait none</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) banner [diagnostic</td>
<td>wait] banner-message</td>
</tr>
<tr>
<td><strong>Example:</strong> Router(config-tmap)# banner diagnostic X Enter TEXT message. End with the character 'X'. --Welcome to Diagnostic Mode-- X</td>
<td></td>
</tr>
</tbody>
</table>

Note

- allow interruptible—The console connection waits for a Cisco IOS VTY line to become available, and also allows users to enter diagnostic mode by interrupting a console connection that is waiting for a Cisco IOS VTY line to become available. This is the default setting.

- none—The console connection immediately enters diagnostic mode.

Note

- Users can interrupt a waiting connection by entering Ctrl-C or Ctrl-Shift-6.

Note

- diagnostic—Creates a banner message seen by users directed to diagnostic mode because of the console transport map configuration.
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong></td>
<td>Users can interrupt a waiting connection by entering Ctrl-C or Ctrl-Shift-6.</td>
</tr>
<tr>
<td>• wait—Creates a banner message seen by users waiting for Cisco IOS VTY to become available.</td>
<td></td>
</tr>
<tr>
<td>• banner-message—Banner message, which begins and ends with the same delimiting character.</td>
<td></td>
</tr>
</tbody>
</table>

**Step 6**

**Example:**

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

**Purpose:**

Exits transport map configuration mode to re-enter global configuration mode.

**Step 7**

**Example:**

```
Router(config)# transport type console 0 input consolehandler
```

**Purpose:**

Applies the settings defined in the transport map to the console interface.

The transport-map-name for this command must match the transport-map-name defined in the transport-map type console command.

---

### Examples

The following example shows how to create a transport map to set console port access policies and attach to console port 0:

```
Router(config)# transport-map type console consolehandler
Router(config-tmap)# connection wait allow interruptible
Router(config-tmap)# banner diagnostic X
Enter TEXT message. End with the character 'X'.
--Welcome to diagnostic mode--
X
Router(config-tmap)# banner wait X
Enter TEXT message. End with the character 'X'.
Waiting for IOS vty line
X
Router(config-tmap)# exit
Router(config)# transport type console 0 input consolehandler
```

---

### Viewing Console Port, SSH, and Telnet Handling Configurations

Use the following commands to view console port, SSH, and Telnet handling configurations:

- `show transport-map`
- `show platform software configuration access policy`

Use the `show transport-map` command to view transport map configurations.

```
show transport-map [all | name transport-map-name | type [console]]
```

This command can be used either in user EXEC mode or privileged EXEC mode.
Example

The following example shows transport maps that are configured on the router: console port (consolehandler):

Router# show transport-map all
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map type console
Transport Map:
Name: consolehandler

REVIEW DRAFT - CISCO CONFIDENTIAL
Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode

Router# show transport-map type persistent ssh
Transport Map:
Name: consolehandler Type: Console Transport

Connection:
Wait option: Wait Allow Interruptable Wait banner:

Waiting for the IOS CLI Bshell banner:
Welcome to Diagnostic Mode

Use the show platform software configuration access policy command to view the current configurations for handling the incoming console port, SSH, and Telnet connections. The output of this command provides the current wait policy for each type of connection (Telnet, SSH, and console), as well as information on the currently configured banners.

Unlike the show transport-map command, the show platform software configuration access policy command is available in diagnostic mode so that it can be entered in scenarios where you need transport map configuration information, but cannot access the Cisco IOS CLI.

Example

The following example shows the show platform software configuration access policy command.

Router# show platform software configuration access policy
The current access-policies

Method : telnet
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*


***Return to ROMMON Prompt
```