



Cisco IR807 Industrial Integrated Services Router Software Configuration Guide

First Published: 2017-08-29

Last Modified: 2023-06-14

Americas Headquarters

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



CHAPTER 1

Preface

This preface describes the objectives, audience, organization, and conventions of this guide and describes related documents that have additional information.

- [Preface, on page 1](#)
- [Objective, on page 1](#)
- [Audience, on page 1](#)
- [Conventions, on page 2](#)
- [Searching Cisco Documents, on page 2](#)

Preface

This preface describes the objectives, audience, organization, and conventions of this guide and describes related documents that have additional information.



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

It contains the following sections:

Objective

This guide provides an overview of the software features and explains how to perform the configuration steps for the Cisco IR807 Integrated Services Routers.

Audience

This guide is intended for people who have a high level of technical ability, as well as knowledge of Cisco IOS and networking technologies.

Conventions

This section describes the conventions used in this guide.

NOTE: Means reader take note. Notes contain helpful suggestions or references to additional information and material.

CAUTION: This symbol means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

TIP: Means *the following information will help you solve a problem*. The tip information might not be troubleshooting or even an action, but could be useful information.

WARNING: IMPORTANT SAFETY INSTRUCTIONS Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

Searching Cisco Documents

To search an HTML document using a web browser, press **Ctrl-F** (Windows) or **Cmd-F** (Apple). In most browsers, the option to search whole words only, invoke case sensitivity, or search forward and backward is also available.

To search a PDF document in Adobe Reader, use the basic Find toolbar (**Ctrl-F**) or the Full Reader Search window (**Shift-Ctrl-F**). Use the Find toolbar to find words or phrases within a specific document. Use the Full Reader Search window to search multiple PDF files simultaneously and to change case sensitivity and other options. Adobe Reader's online help has more information about how to search PDF documents.



CHAPTER 2

Product Overview

This chapter provides an overview of the features available for the Cisco IR807 Integrated Services Router.

- [Product Overview, on page 3](#)
- [General Description, on page 3](#)
- [Hardware Overview, on page 4](#)
- [IR807 USB Ports, on page 8](#)
- [Software Overview, on page 8](#)
- [Antenna Recommendations, on page 8](#)
- [Related Documentation, on page 9](#)

Product Overview

This chapter provides an overview of the features available for the Cisco IR807 Integrated Services Routers and contains the following sections:

General Description

The IR807 routers are highly compact Cisco IOS routers with support for integrated 4G LTE wireless WAN capabilities.

Their benefits include:

- Easily and rapidly deployable
- Highly available and highly secure
- Reliable operation and seamless integration with SCADA systems
- Designed for power-constrained and harsh environments, tolerating a wide temperature range
- Compact, lightweight, and DIN rail mountable, with all input/output ports and connectors on the front panel for easy installation in space-constrained cabinets
- Well suited to industrial applications ranging from distribution automation for utilities to transportation and manufacturing, as well as remote asset management across the extended enterprise

These routers deliver enterprise-class features -- including highly secure data, voice, and video communications -- to stationary and mobile network nodes across wired and wireless links. The Cisco 807 industrial router supports enterprise-grade, wireline-like functionality such as:

- Dynamic Multipoint VPN (DMVPN)

- Quality of service (QoS) for cellular
- Multi-Virtual Route Forwarding (VRF) for cellular

For a complete listing of the routers capabilities, see:

<https://www.cisco.com/c/en/us/products/routers/807-industrial-integrated-services-routers/index.html>

Hardware Overview

This section covers the overview of the IR807.

SKU Information

[Table 1: Supported SKUs for Cisco IR807s, on page 4](#) lists the different SKUs available for the IR807. All SKUs support external antenna.

Table 1: Supported SKUs for Cisco IR807s



SKU ID	Description	Modem Type
IR807G-LTE-VZ-K9	North America (Verizon)	WP7601
IR807G-LTE-NA-K9	North America (AT&T)	WP7504
IR807G-LTE-GA-K9	EMEA	WP7502

Note: The IR807G-LTE-VZ-K9 SKU has a single SIM card socket. The IR807G-LTE-NA-K9 and IR807G-LTE-GA-K9 are equipped with dual SIM card sockets. Graphics in this guide show the dual SIM SKUs.

Front Panel Icons and LEDs

The IR807 uses icons to show the different features of the device. [Table 2: Icons with LEDs, on page 4](#) shows Icons and their associated LEDs with descriptions. LEDs are visible from the top cover and from the front panel. The LEDs allows easy visibility for wall and desk mounted installations regardless of chassis orientation. [Table 4: Icons only, on page 6](#) shows the Icons without associated LEDs and their descriptions.

Table 2: Icons with LEDs

Icon	Description/Activity	Icon	Description/Activity
	System - Power and System Status. Off — No power Green Steady on — Normal operation Green Flashing — Boot up phase or in ROM Monitor mode Amber Steady on — Power is OK but possible internal FPGA program failure		Alarm - Alarm Input Status Off — Normal operation Red - Alarm State on the Alarm Input




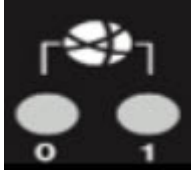

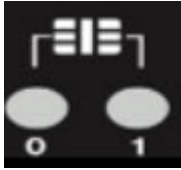













Icon	Description/Activity	Icon	Description/Activity
	<p>VPN</p> <p>Off — No VPN tunnel</p> <p>Steady Green — At least one VPN tunnel is up</p>		User Configurable LED
	<p>GPS - GPS Status</p> <p>Off — GPS not configured</p> <p>Steady Green — GPS configured</p> <p>Slow Flash — GPS Acquiring in Standalone GPS</p> <p>Fast Flash — GPS Acquiring in Assisted GPS</p> <p>Slow Flash is defined as the LED will be on for 0.25 seconds and off for 0.75 seconds. Fast Flash is defined as the LED will be on for 0.25 seconds and off for 0.25 seconds.</p>		<p>RJ45 Fast Ethernet Ports - Link Status 0:1</p> <p>Off — No link</p> <p>Steady Green — Link is up</p> <p>Flashing — Transmitting and Receiving data</p>
	<p>RSSI - Received Signal Strength Indication</p> <p>The RSSI LEDs are a 3 LED bar graph to indicate signal strength. Their functionality is described in the RSSI LED Table 3: RSSI LEDs, on page 5.</p>		<p>SIM Cards - SIM0/SIM1</p> <p>Off — No USIM</p> <p>Green — USIM installed and active</p>
			<p>WWAN - Wireless WAN Activity</p> <p>Off — Offline</p> <p>On — In Service</p> <p>Flash (on 200ms off 5 sec) — No Service</p> <p>Flash (on 1 sec off 1 sec) — Low Power Mode</p> <p>Flash (on 5 sec off 200ms) — Roaming</p> <p>Flash (on 400ms off 100ms) — Data Active</p>

Table 3: RSSI LEDs

RSSI	RSSI (2)	RSSI (1)	RSSI (0)
	Green	Green	Green/Amber
< -110dBm	Off	Off	Off

RSSI	RSSI (2)	RSSI (1)	RSSI (0)
-110 to -90dBm	Off	Off	On - Amber
-90 to -75dBm	Off	Off	On - Green
-75 to -60dBm	Off	On - Green	On - Green
> -60dBm	On - Green	On - Green	On - Green

Table 4: Icons only

Icon	Description	Icon	Description
	Console		USB 2.0 Type A Port for Storage and Networking
	Grounding point (located on side of device)		Reset Button
	DC Power Input (12V to 48V)		DC Power Return
	Alarm Common		Alarm IN
	Serial Ports		Fast Ethernet Ports
	Antenna 1 (TNC) Main		Antenna 2 (TNC) Div


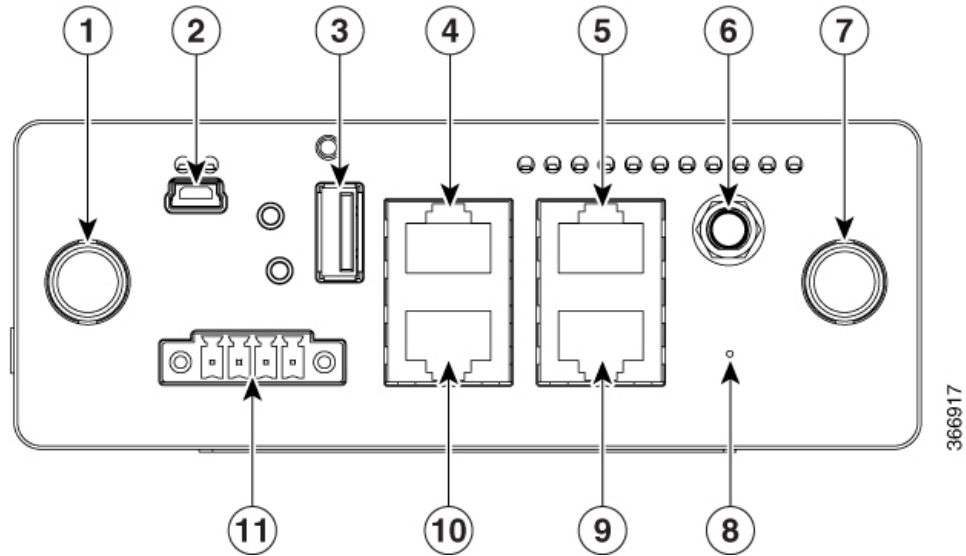
Icon	Description	Icon	Description
	Warning		

Figure 1: Cisco IR807 Front Panel, on page 7 shows the front panel details of the IR807.

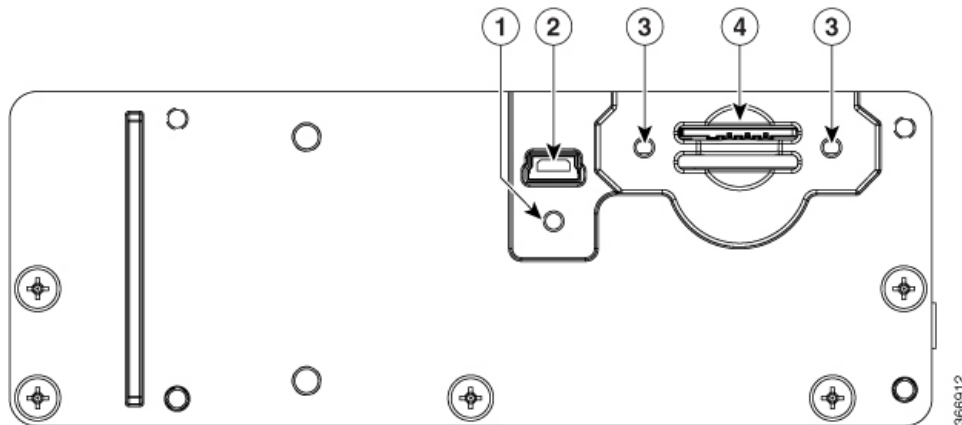
Figure 1: Cisco IR807 Front Panel



1	Antenna 1 (TNC) MAIN	7	Antenna 2 (TNC) MAIN
2	USB Console (Type B)	8	Reset Button
3	USB Type A	9	FE1 10/100
4	S0 (DTE)	10	S1 (DCE)
5	FE0 10/100 Base-T RJ-45	11	External DC
6	GPS (SMA)		

Figure 2: IR807 Back Panel, on page 8 shows the back panels details of the IR807.

Figure 2: IR807 Back Panel



1	Screw hole for protective cover over USB
2	USB Type B (under a protective cover) Reserved to be used with Modem for external provision
3	Screw holes for protective cover over SIMs (one on each side)
4	SIM0 (bottom) and SIM1 (top) Card Slots

IR807 USB Ports

The Console port is mini-USB type B port. 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 computer's manufacturer, or go here: <https://www.silabs.com/developers/usb-to-uart-bridge-vcp-drivers>

The USB Type A interface provides access to an external USB FLASH device (also known as a thumb drive or a USB key). The Cisco IOS software provides standard file system access to the flash device: read, write, erase, and copy, as well as formatting of the flash device with a FAT file system. The router can be booted from the USB drive.

Software Overview

The IR807 offers a rich IOS feature set. This marketing data sheet provides a complete list of all of the features. <https://www.cisco.com/c/en/us/products/routers/807-industrial-integrated-services-routers/index.html>

Antenna Recommendations

The IR807 is not shipped with antennas. They must be ordered separately.

NOTE: Poorly installed SIMO antennas, such that the two (or more in case of 3x3, 4x4 SIMO) antennas have a strong correlation coefficient. This may cause the two streams to interfere with each other (otherwise known as lack of diversity), since the system has trouble separating the two.

For detailed information about Cisco Antennas, please refer to the following guides:

Cisco Industrial Routers and Industrial Wireless Access Points Antenna Guide:

<https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/industrial-routers-and-industrial-wireless-antenna-guide.html>

Cisco Aironet Antennas and Accessories Reference Guide

http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-antennas-accessories/product_data_sheet09186a008008883b.html

Related Documentation

The following documentation is available:

- Cross-Platform Release Notes for Cisco IOS:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-7m/release/notes/15-7-3-m-rel-notes.html>

- All of the Cisco IR800 Industrial Integrated Services Router documentation can be found here:

<http://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/tsd-products-support-series-home.html>



CHAPTER 3

Basic Router Configuration

This chapter provides procedures for configuring the basic parameters of your Cisco router, including global parameter settings, routing protocols, interfaces, and command-line access.

- [Basic Router Configuration, on page 11](#)
- [Default Configuration, on page 11](#)
- [Bootstrap Sequence, on page 11](#)
- [Configuring Command-Line Access, on page 14](#)
- [No Service Password Recovery, on page 16](#)
- [Configuring WAN Interfaces, on page 17](#)
- [Configuring the Cellular Wireless WAN Interface, on page 18](#)
- [Configuring Router for Image and Configuration Recovery Using Push Button, on page 18](#)
- [Configuring a Loopback Interface, on page 19](#)
- [Additional Information, on page 20](#)

Basic Router Configuration

This chapter provides procedures for configuring the basic parameters of your Cisco router, including global parameter settings, routing protocols, interfaces, and command-line access.

Note: Individual router models may not support every feature described in this guide. Features that are not supported by a particular router are indicated whenever possible.

This chapter includes configuration examples and verification steps, as available.

Default Configuration

When you first boot up your Cisco router, some basic configuration has already been performed. All of the LAN and WAN interfaces have been created, and the console and vty ports are configured.

Bootstrap Sequence

The following graphic illustrates how the IR807 goes through its bootup process.

Figure 3: IR807 Boot



Displaying the platform information

Use the **show platform version** command to display information about the IR807:

```
IR807#sh platform version
Platform Revisions/Versions :
=====
CPLD : 0xDD
Rework Rev : 0
CPU Name : P1024SEC
CPU Ver : 1.1 [Val = SVR:0x80EC0211]
Core Rev : 5.1 [Val = PVR:0x80212051]
CCB CLOCK : 277 MHz
IOS :
Cisco IOS Software, IR800L Software (IR800L-UNIVERSALK9-M), Version 15.7M0a
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Wed 27-Sep-17 07:52 by rasurend
ROMMON (Upgrade) :
System Bootstrap, Version 15.5(20170504:175929) [
Copyright (c) 1994-2017 by cisco Systems, Inc.
```

If you are setting up 4G:

- You must have service availability on the IR807 from a carrier, and you must have network coverage where your router will be physically placed.
- You must subscribe to a service plan with a wireless service provider and obtain a SIM card.
- You must install the required antennas before you configure the 4G for the IR807. See the following URL for instructions on how to install the antennas:

<https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/industrial-routers-and-industrial-wireless-antenna-guide.html>

Where to find Software

The latest downloads for the IR807 can be found at:

<https://software.cisco.com/download/navigator.html?mdfid=286287045&flowid=75322>

Click on the link to take you to the specific software you are looking for.

IOS Image Files

The IOS release for the IR807 is Cisco IOS 15.8(3)M, and includes the following Cisco IOS images and additional information:

- IOS Image: ir800l-universalk9-mz.SPA.158-3.M
- Minimum Memory - DRAM 512 MB Flash 1024 MB
- Size - 61.55 MB

Upon download to your device, your flash directory will contain:

```
1 -rw-      3802056  Feb 24 1907 19:23:44 +00:00 2.7.1.SSA
2 drw-         0   Sep 3 2017 16:35:38 +00:00 eem
3 -rw-     64727636  Sep 3 2017 16:39:38 +00:00 ir800l-universalk9-mz.SSA.
4 -rw-     64765500  Oct 16 2017 21:35:56 +00:00 ir800l-universalk9-mz.SSA
```

You can verify your download using the following series of commands:

```
IR807#verify /md5 flash:ir800l-universalk9-mz.SSA
.....
.....MD5 of flash:ir800l-universalk9-mz.SSA Done!
verify /md5 (flash:ir800l-universalk9-mz.SSA) = 4623f2fbe458516b9f2166d11405569c
IR807#show software authenticity file flash:ir800l-universalk9-mz.SSA
File Name           : flash:ir800l-universalk9-mz.SSA
Image type          : Special
  Signer Information
    Common Name      : CiscoSystems
    Organization Unit : C8xx
    Organization Name : CiscoSystems
    Certificate Serial Number : 59CBBBA8
    Hash Algorithm    : SHA512
    Signature Algorithm : 2048-bit RSA
    Key Version       : A
IR807#show software authenticity keys
Public Key #1 Information
-----
Key Type           : Production (Primary)
Public Key Algorithm : RSA
Modulus (256 bytes) :
    C8:AE:59:5E:E2:52:8C:64:55:6C:C6:AB:89:FA:56:53:
    06:2B:72:6D:18:A5:24:8A:37:35:BC:88:24:97:47:5D:
    93:76:D0:09:AF:16:EB:86:68:3B:66:CC:80:53:A8:ED:
    17:00:D1:F9:2D:15:0A:F2:29:BC:7E:9C:FF:85:31:C6:
    B1:5D:C7:44:A3:01:0E:D8:85:C9:12:77:61:AE:07:B3:
    E4:CA:84:AD:FC:C0:4E:E9:87:A2:4F:61:D4:93:C8:0F:
    37:D0:11:7F:B7:FB:92:EE:EB:91:56:F3:13:FA:E7:27:
    0E:57:4C:EE:F2:78:5A:62:6D:A9:C3:49:AC:96:A0:B8:
    E8:06:02:14:E0:2F:17:E3:6A:96:34:17:5A:B5:46:1C:
    AA:D1:F4:F6:3B:4D:4B:6E:1E:1A:09:45:95:44:B4:7C:
    85:AD:CB:C7:CE:0A:7D:4A:5D:F3:6B:1B:31:01:A8:78:
    BE:2D:A0:3E:33:1A:80:D3:29:4F:53:D8:66:CE:7D:AB:
    DF:AE:1A:D3:1D:61:D1:73:1F:01:FB:7D:02:3E:71:6C:
    1A:1E:4B:2D:D0:C3:E9:05:EB:57:D4:D0:A3:89:36:91:
    80:85:09:5A:0D:1A:71:31:D0:95:A9:2F:E6:2F:D2:E9:
    BA:A0:47:96:B0:D9:32:66:F5:34:35:51:36:E3:17:4D
Exponent (4 bytes)  : 10001
Key Version         : A
Public Key #2 Information
```

```

-----
Key Type                : Special (Primary)
Public Key Algorithm    : RSA
Modulus (256 bytes)    :
    CE:BE:7A:25:8C:E4:45:79:5C:77:B8:1D:9E:94:78:61:
    B6:3D:64:4E:3C:36:25:11:9C:26:FF:D9:42:10:4C:86:
    F5:1C:AD:F1:49:A5:87:D3:4C:69:BF:08:E5:55:1C:59:
    CD:DA:62:9D:65:33:0D:B6:F1:F1:D1:AC:98:99:6B:CB:
    0B:3F:DA:E9:94:06:71:B3:78:B5:AA:85:C8:BE:64:CA:
    43:72:F2:B5:4B:C5:4D:FA:D9:CF:51:78:AD:45:9F:E8:
    CD:41:5A:A6:DE:B7:2E:75:85:EB:8C:7D:68:F2:D4:A1:
    5D:DD:B2:26:63:BB:7C:EB:79:80:33:80:05:B9:59:34:
    27:89:AA:92:04:61:0C:7D:E5:A5:DE:A0:40:60:73:64:
    5A:A7:06:C0:8A:04:CD:3A:1C:99:8D:B7:5C:C8:FE:97:
    70:9C:54:DF:AB:A7:8F:04:80:11:08:51:FF:7B:F5:73:
    C2:A1:C3:E3:A3:45:04:70:90:2D:EA:1E:AD:2C:75:5E:
    FF:55:EE:0D:75:D3:19:00:59:5C:F6:4C:E2:B7:5F:7A:
    8F:3E9B:21:AC:59:6F:7C:63:B0:62:B5:AA:B4:D8:04:
    65:07:8B:56:94:18:14:E3:12:AC:A5:3F:B0:BA:97:D4:
    83:22:2E:EC:38:2F:D5:01:39:BA:60:A5:A8:5F:85:87
Exponent (4 bytes)    : 10001
Key Version           : A
Public Key #3 Information
-----
Key Type                (Primary)
Public Key Algorithm    : RSA
Modulus (256 bytes)    :
    C8:AE:59:5E:E2:52:8C:64:55:6C:C6:AB:89:FA:56:53:
    06:2B:72:6D:18:A5:24:8A:37:35:BC:88:24:97:47:5D:
    93:76:D0:09:AF:16:EB:86:68:3B:66:CC:80:53:A8:ED:
    17:00:D1:F9:2D:15:0A:F2:29:BC:7E:9C:FF:85:31:C6:
    B1:5D:C7:44:A3:01:0E:D8:85:C9:12:77
E4:CA:84:AD:FC:C0:4E:E9:87:A2:4F:61:D4:93:C8:0F:
    37:D0:11:7F:B7:FB:92:E1:56:F3:13:FA:E7:27:
    0E:57:4C:EE:F2:78:5A:62:6D:A9:C3:49:AC:96:A0:B8:
    E8:06:02:14:E0:2F:17:E3:6A:96:34:17:5A:B5:46:1C:
    AA:D1:F4:F6:3B:4D:4B:6E:1E:1A:09:45:95:44:B4:7C:
    85:AD:CB:C7:CE:0A:7D:4A:5D:F3:6B:1B:31:01:A8:78:
    BE:2D:A0:3E:33:1A:80:D3:29:4F:53:D8:66:CE:7D:AB:
    DF:AE:1A:D3:1D:61:D1:73:1F:01:FB:7D:02:3E:71:6C:
    1A:1E:4B:2D:D0:C3:E9:05:EB:57:D4:D0:A3:89:36:91:
    80:85:09:5A:OD::31:D0:95:A9:2F:E6:2F:D2:E9:
    BA:A0:47:96:B0:D9:32:66:F5:34:35:51:36:E3:17:4D
Exponent (4 bytes)    : 10001
Key Version           : A

```

Configuring Command-Line Access

To configure parameters to control access to the router, perform the following steps, beginning in global configuration mode:

SUMMARY STEPS

1. line [aux | console | tty | vty] line-number
2. password password
3. login
4. exec-timeout minutes [seconds]
5. line [aux | console | tty | vty] line-number

6. password password
7. login
8. end

DETAILED STEPS

Step	Command or Action	Purpose
1	line [aux console tty vty] line-number Example: Router(config)# line console 0	Enters line configuration mode and specifies the type of line. This example specifies a console terminal for access.
2	password password Example: Router(config-line)# password 5dr4Hepw3	Specifies a unique password for the console terminal line.
3	login Example: Router(config-line)# login authentication default	Enables password checking at terminal session login.
4	exec-timeout minutes [seconds] Example: Router(config-line)# exec-timeout 5 30	Sets the time interval that the EXEC command interpreter waits until user input is detected. The default is 10 minutes. Optionally, add seconds to the interval value. This example shows a timeout of 5 minutes and 30 seconds. Entering a timeout of 0 0 specifies never to time out.
5	line [aux console tty vty] line-number Example: Router(config-line)# line vty 0 4	Specifies a virtual terminal for remote console access.
6	password password Example: Router(config-line)# password aldf2ad1	Specifies a unique password for the virtual terminal line.
7	login Example: Router(config-line)# login authentication default	Enables password checking at the virtual terminal session login.
8	end Example: Router(config-line)# end	Exits line configuration mode, and returns to privileged EXEC mode.

Configuring Global Parameters

To configure selected global parameters for your router, perform these steps:

SUMMARY STEPS

1. configure terminal
2. hostname name
3. enable secret password
4. no ip domain-lookup

DETAILED STEPS

Step	Command or Action	Purpose
1	configure terminal Example: Router# configure terminal	Enters global configuration mode when using the console port. If you are connecting to the router using a remote terminal, use the following: telnet router name or address Login: login id Password: ***** Router> enable
2	hostname name Example: Router(config)# hostname Router	Specifies the name for the router.
3	enable secret password Example: Router(config)# enable secret cr1ny5ho	Specifies an encrypted password to prevent unauthorized access to the router.
4	no ip domain-lookup Example: Router(config)# no ip domain-lookup	Disables the router from translating unfamiliar words (typos) into IP addresses.

No Service Password Recovery

The No Service Password-Recovery is a Cisco IOS Platform independent feature which is available in Cisco IOS classic devices.

The following events will cause the router to go into rommon mode as standard behavior:

- Manual boot setting was done in IOS mode
- If flash is corrupt



Note Ensure a valid Cisco IOS image is present in flash before enabling this feature.

For complete configuration information, refer to the following: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cfg/configuration/15-mt/sec-usr-cfg-15-mt-book/sec-no-svc-pw-recvry.html

Configuring WAN Interfaces

Configure the WAN interface for your router using one of the following as appropriate:

Configuring a Fast Ethernet Layer-3 Interface

To configure the Fast Ethernet interface, perform these steps, beginning in global configuration mode:

SUMMARY STEPS

1. interface type number hostname name
2. ip address ip-address mask
3. no shutdown
4. exit

DETAILED STEPS

Step	Command or Action	Purpose
1	interface type number Example: Router(config)# interface fastethernet 0 Router(config-if)#	Enters the configuration mode for a Fast Ethernet WAN interface on the router.
2	ip address ip-address mask Example: Router(config)# ip address 192.168.1.5 255.255.255.0 Router(config-if)#	Sets the IP address and subnet mask for the specified Fast Ethernet interface.
3	no shutdown Example: Router(config-if)# no shutdown	Enables the Ethernet interface, changing its state from administratively down to administratively up.
4	exit Example: Router(config-if)# exit	Exits configuration mode for the Fast Ethernet interface and returns to global configuration mode.

Configuring the Cellular Wireless WAN Interface

The IR807 series provides a wireless interface supporting 4G/LTE networks.

To configure the cellular wireless interface, follow these guidelines and procedures:

Prerequisites for Configuring the Wireless Interface

The following are prerequisites to configuring the wireless interface:

- You must have wireless service from a carrier, and you must have network coverage where your router will be physically placed.
- You must subscribe to a service plan with a wireless service provider.
- You must check your LEDs for signal strength.

Restrictions for Configuring the Cellular Wireless Interface

The following restrictions apply to configuring the Cisco wireless interface:

- A data connection can be originated only by the wireless interface. Remote dial-in is not supported.
- Because of the shared nature of wireless communications, the experienced throughput varies depending on the number of active users or the amount of congestion in a given network.
- Cellular networks have higher latency than wired networks. Latency rates depend on the technology and carrier. Latency may be higher when there is network congestion.
- VoIP is not currently supported.
- Any restrictions that are part of the terms of service from your carrier also apply to the Cisco wireless interface.

Configuring Router for Image and Configuration Recovery Using Push Button

A push button feature is available on the IR807. The reset button on the front panel of the router enables this feature.

Perform the following steps to use this feature:

1. Unplug power.
2. Press the reset button on the front panel of the router.
3. Power up the system while holding down the reset button. The system LED blinks four times indicating that the router has accepted the button push.

Using this button takes effect only during ROMMON initialization. During a warm reboot, pressing this button has no impact on performance. The following table shows the high level functionality when the button is pushed during ROMMON initialization.

ROMMON Behavior	IOS Behavior
<ul style="list-style-type: none"> • Boots using default baud rate. • Performs auto-boot. • Loads the *.default image if available on compact flash. Note: If no *.default image is available, the ROMMON will boot up with the first Cisco IOS image on flash. <p>Examples of names for default images: ir800l-universalk9-mz.SPA.157-3.M0a.default</p>	<p>If the configuration named customer-config.SN (SN is the serial number of the device) is available in nvram storage or flash storage, IOS will perform a backup of the original configuration and will boot up using this configuration.</p> <p>Note: You can only have one configuration file with customer-config.SN option. Having more than one file will result in uncertain operational behavior.</p>

Use the `show platform` command to display the current bootup mode for the router. The following sections show sample outputs when the button is not pushed and when the button is pushed.

Output When Button Is Not Pushed: Example

```
router# show platform boot-record
Platform Config Boot Record :
=====
Configuration Register at boot time : 0x0
Reset Button Status at Boot Time   : Not Pressed
```

Output When Button Is Pushed: Example

```
router# show platform boot-record
Platform Config Boot Record :
=====
Configuration Register at boot time : 0x0
Reset Button Status at Boot Time   : Pressed
Golden config file at location     : flash:/pnp-reset-config.cfg
Config Recovery Status             : Ok
```

Configuring a Loopback Interface

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

Perform these steps to configure a loopback interface, beginning in global configuration mode:

SUMMARY STEPS

1. interface type number
2. ip address ip-address mask
3. exit

DETAILED STEPS

Step	Command or Action	Purpose
1	interface type number Example: Router(config)# interface Loopback 0 Router(config-if)#	Enters configuration mode for the loopback interface.
2	ip address ip-address mask Example: Router(config-if)# ip address 192.168.1.1 255.255.255.0 Router(config-if)#	Sets the IP address and subnet mask for the loopback interface.
3	exit Example: Router(config-if)# exit Router(config)#	Exits configuration mode for the loopback interface and returns to global configuration mode.

Additional Information

Several additional resources for configuring IOS are available at:

<https://www.cisco.com/c/en/us/support/ios-nx-os-software/ios-software-release-15-6m-t/products-installation-and-configuration-guides-list.html>



CHAPTER 4

Cellular Interface Modules

This chapter provides configuration details for the cellular interface modules used in the IR807 routers.

- [Cellular Interface Modules, on page 21](#)
- [Cellular Interface, on page 21](#)
- [IR807 Cellular Technology Selection, on page 40](#)
- [GPS, on page 43](#)
- [Upgrading the Modems, on page 46](#)

Cellular Interface Modules

This chapter provides configuration details for the cellular interface modules used in the IR807 routers.

This chapter contains the following sections:

Cellular Interface

The IR807 routers use the Sierra Wireless WP7601 and WP750X series modems supporting Single Input Multiple Output (SIMO) on LTE.

SIMO is an antenna technology for wireless communications in which multiple antennas are used at the destination (receiver). The antennas are combined to minimize errors and optimize data speed. The source (transmitter) has only one antenna. SIMO is one of several forms of smart antenna technology, the others being MIMO (multiple input, multiple output) and MISO (multiple input, single output)

Installation of the SIM card(s) and antennas is covered in the IR807 Hardware Installation Guide under the Cisco 800 Series Industrial Integrated Services Routers page:

<http://www.cisco.com/c/en/us/support/routers/800-series-industrial-routers/tsd-products-support-series-home.html>

The software download page can be found here:

<https://software.cisco.com/download/navigator.html?mdfid=286288566&flowid=76082>

The Firmware Upgrade Guide for Cellular Modems can be found here:

http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/firmware/Firmware_Upgrade.html

Cisco 4G LTE Software Installation Guide

<http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/EHWIC-4G-LTESW.html>

After installing the SIM card(s) and antennas, check the cellular hardware, radio, network and SIM (Unlock SIM card if necessary).

4G LTE Dual SIMs

The Dual SIMs feature provides the following:

- A fail over mechanism in the event the primary SIM loses connectivity to one of the Mobile Service Provider networks. There is no automatic fall-back to the primary SIM, since a change only occurs when there is no signal from the carrier in use. A script is needed to reverse back to the primary. Both mobile provider networks must be supported by the given IR807 SKU, and it must be in an applicable region.
 - By default, SIM slot 0 is the primary, and SIM slot1 is the backup. Behavior may be changed using the `lte sim primary` command.
 - Profiles for each SIM are assigned by using the `lte sim profile` command. Each SIM has an associated Internet profile and an IMS profile in the CLI.
 - The fail-overs happen when there is no signal from the current carrier, and generally happen depending on the fail-over timer value that is set. The default value is 2 minutes. The range is from 0-7 minutes.

Radio Configuration

The following examples are of an IR807 cellular configuration:

```
IR807> enable
IR807# show ip int brief
Interface      IP-Address      OK?  Method  Status  Protocol
Async0         unassigned     YES  unset   up       down
Async1         unassigned     YES  unset   up       down
Cellular0      166.140.43.237 YES  IPCP    up       up
Single APN
Cellular1      10.61.25.231   YES  IPCP    up       up
Multi APN
FastEthernet0  10.65.217.109 YES  TFTP    administratively down  down
FastEthernet1  unassigned     YES  unset   administratively down  down
```

The output of this running configuration example has been edited for brevity:

```
! Last configuration change at 10:22:51 CET Thu Oct 12 2017 by admin
! NVRAM config last updated at 10:24:19 CET Thu Oct 12 2017 by admin
!
version 15.7
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone year
service password-encryption
service sequence-numbers
!
hostname ir807
!
boot-start-marker
boot system flash:ir8001-universalk9-mz.SSA
boot-end-marker
!
```



```
security authentication failure rate 10 log
security passwords min-length 6
logging buffered warnings
logging persistent size 850000000
no logging console
no logging monitor
enable secret 5 $1rAjYMLZ2e6K0lxR2bOo0
!
aaa new-model
!
aaa authentication login local_auth local
!
aaa session-id common
clock timezone CET 1 0
clock summer-time CET recurring last Sun Mar 3:00 last Sun Oct 2:00
clock calendar-valid
!
crypto pki trustpoint TP-self-signed-4288165946
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-4288165946
  revocation-check none
  rsakeypair TP-self-signed-4288165946
!
crypto pki certificate chain TP-self-signed-4288165946
no ip source-route
no ip gratuitous-arps
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.15.5
!
ip dhcp pool Test
  network 192.168.15.4 255.255.255.252
  default-router 192.168.15.5
!
no ip bootp server
no ip domain lookup
ip domain name local.cisco.com
ip cef
login block-for 20 attempts 3 within 15
login on-failure log
login on-success log
!
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
license udi pid IR807G-LTE-GA-K9 sn FCW211700GN
!
!
memory reserve console 4096
vtp mode transparent
username admin privilege 15 secret 5 $1$e2C.$DUDXjmv0
!
!
redundancy
!
controller Cellular 0
  lte modem link-recovery disable
no cdp advertise-v2
no cdp run
!
interface Cellular0
```

```
ip address negotiated
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat outside
ip virtual-reassembly in
encapsulation slip
dialer in-band
dialer idle-timeout 0
dialer string lte
dialer watch-group 1
ipv6 address autoconfig
async mode interactive
!
interface Cellular1
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
encapsulation slip
shutdown
!
interface FastEthernet0
ip address 192.168.101.1 255.255.255.0
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet1
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
ip nat inside
ip virtual-reassembly in
shutdown
duplex auto
speed auto
!
interface Async0
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
encapsulation scada
shutdown
!
interface Async1
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
encapsulation scada
shutdown
!
!
no ip forward-protocol nd
no ip http server
no ip http secure-server
!
```

```

!
ip nat inside source list 1 interface Cellular0 overload
ip nat inside source static tcp 192.168.101.10 80 interface Cellular0 80
ip ssh logging events
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
!
logging history size 500
no logging trap
logging facility local2
dialer watch-list 1 ip 8.8.8.8 0.0.0.0
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipv6 permit
ipv6 ioam timestamp
!
!
access-list 1 permit 0.0.0.0 252.255.255.255
!
!
!
control-plane
!
!
!
no vstack
banner login
=====
Test
=====
!
line con 0
  exec-timeout 5 0
  logging synchronous
  login authentication local_auth
  transport output telnet
line 2
  exec-timeout 5 0
  privilege level 0
  no activation-character
  no exec
  transport preferred none
  transport input all
  transport output none
  stopbits 1
line 3
  exec-timeout 5 0
  script dialer lte
  modem InOut
  no exec
  rxspeed 100000000
  txspeed 50000000
line 4
  exec-timeout 5 0
  privilege level 0
  no exec
  transport output none
line 5
  exec-timeout 5 0
  privilege level 0
  no exec
  transport output none
  stopbits 1

```

```

line 8
  exec-timeout 5 0
  privilege level 0
  no exec
  transport output none
  rxspeed 100000000
  txspeed 50000000
line vty 0 4
  exec-timeout 15 0
  login authentication local_auth
  transport input telnet ssh
  transport output none
!
exception memory ignore overflow processor
exception memory ignore overflow io
scheduler allocate 20000 1000
!
end

```

Test the modem configuration with a ping command:

```

IR807# ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/88/292 ms
IR807#

```

Cellular Provider Profiles

The following examples show modem profiles.

Verizon Profile

```

IR807# show cellular 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*

Profile 3 is used for Verizon
-----
PDP Type = IPv4v6
PDP address = 166.140.43.237
Access Point Name (APN) = we01.VZWSTATIC
Authentication = None
    Primary DNS address = 198.224.173.135
    Secondary DNS address = 198.224.174.135
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) = vzwenterprise
Authentication = None
  * - Default profile
  ** - LTE attach profile

```

ATT Profile

```

IR807# show cellular 0 profile
Profile 1 = ACTIVE* **
-----
PDP Type = IPv4
PDP address = 192.168.1.51
Access Point Name (APN) = keysight
Authentication = None
Primary DNS address = 0.0.0.0
Secondary DNS address = 0.0.0.0
* - Default profile
** - LTE attach profile
  * - Default profile
  ** - LTE attach profile

```

Sprint Profile

```

IR807#show cellular 0 profile
Profile 1 = INACTIVE* **
-----
PDP Type = IPv4v6
Access Point Name (APN) = otasn
Authentication = None
Profile 9 = INACTIVE
-----
PDP Type = IPv4v6
Access Point Name (APN) = cinet.spcs
Authentication = None
Profile 16 = INACTIVE
-----
PDP Type = IPv4v6
Access Point Name (APN) = otasn
Authentication = None
* - Default profile
** - LTE attach profile

```

Generic Profile

```

Profile 1 = INACTIVE* **
-----
PDP Type = IPv4
Access Point Name (APN) = keysight
Authentication = None
* - Default profile
** - LTE attach profile

```

Use the **show cellular hardware** command to view information about your device.

```
IR807# show cellular 0 hardware
Modem Firmware Version = SWI9X15Y_07.12.09.00
Modem Firmware built = 2017/04/26 23:34:19
Hardware Version = 1.0
Device Model ID: WP7504
Package Identifier ID: 1103235_9906722_WP7504_07.12.09.00_00_Cisco_001.001_000
International Mobile Subscriber Identity (IMSI) = 001012345678901
International Mobile Equipment Identity (IMEI) = 354937080100642
Integrated Circuit Card ID (ICCID) = 89600114082100035643
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Online
Current Modem Temperature = 37 deg C
PRI SKU ID = 1103235, PRI version = 001.028_000, Carrier = ATT
OEM PRI version = 01.01
IR807#
```

Creating a Cellular Profile for ATT

```
IR807#cellular 0 lte profile create 1 keysight none ipv4
Warning: You are attempting to modify a currently ACTIVE data profile.
This is not recommended and may affect the connection state
PDP Type = IPv4
Access Point Name (APN) = keysight
Authentication = NONE
Profile 1 already exists with above parameters. Do you want to overwrite? [confirm] <return>
Profile 1 will be overwritten with the following values:
PDP type = IPv4
APN = keysight
Authentication = NONE
Are you sure? [confirm] <return>
Profile 1 written to modem
IR807#
IR807#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line. End with CNTL/Z.
IR807(config)#controller cellular 0
IR807(config-controller)#
IR807(config-controller)#lte sim data-profile 1 attach-profile 1 slot 0
IR807#sh cellular 0 profile
Profile 1 = ACTIVE* **
-----
PDP Type = IPv4
PDP address = 192.168.1.51
Access Point Name (APN) = keysight
Authentication = None
Primary DNS address = 0.0.0.0
Secondary DNS address = 0.0.0.0
Profile 2 = INACTIVE
-----
PDP Type = IPv4
Access Point Name (APN) = keysight2
Authentication = None
Profile 3 = INACTIVE
-----
PDP Type = IPv4
Access Point Name (APN) = keysight
Authentication = None
* - Default profile
** - LTE attach profile
```

```
Configured default profile for active SIM 0 is profile 1.
IR807#
```

Creating a Cellular Profile for Verizon.

```
IR807# cellular 0/0 lte profile create 3 we01.VZWSTATIC
Warning: You are attempting to modify a currently ACTIVE data profile.

This is not recommended and may affect the connection state
PDP Type = IPv4v6
Access Point Name (APN) = we01.VZWSTATIC
Authentication = NONE
Profile 3 already exists with above parameters. Do you want to overwrite? [confirm] <return>
Profile 3 will be overwritten with the following values:
PDP type = IPv4
APN = we01.VZWSTATIC
Authentication = NONE
Are you sure? [confirm] <return>
Profile 3 written to modem
IR807# conf t
Enter configuration commands, one per line. End with CNTL/Z.
IR807(config)# controller cellular 0
IR807(config-controller)# lte sim data-profile 3 attach-profile 1
IR807(config-controller)# end
IR807#
IR807# show

*Oct 24 19:43:44.841: %SYS-5-CONFIG_I: Configured from console by consolecell
IR807# show cellular 1/0 profile
Profile 1 = ACTIVE* **
-----
PDP Type = IPv4
PDP address = 10.61.185.213
Access Point Name (APN) = m2m.com.attz
Authentication = None
    Primary DNS address = 8.8.8.8
    Secondary DNS address = 8.8.4.4
* - Default profile
** - LTE attach profile
```

Creating a Cellular Profile for ATT

```
IR807# cellular 1/0 lte profile create 1 m2m.com.attz
Warning: You are attempting to modify a currently ACTIVE data profile.

This is not recommended and may affect the connection state
PDP Type = IPv4
Access Point Name (APN) = m2m.com.attz
Authentication = NONE
Profile 1 already exists with above parameters. Do you want to overwrite? [confirm] <return>
Profile 1 will be overwritten with the following values:
PDP type = IPv4
APN = m2m.com.attz
Authentication = NONE
Are you sure? [confirm] <return>
Profile 1 written to modem
IR807#
IR807# conf t
Enter configuration commands, one per line. End with CNTL/Z.
IR807(config)# controller cellular 1
IR807(config-controller)#
```

```
IR807(config-controller)# lte sim data-profile 1 attach-profile 1
```

Note: Please issue a modem reset for the modified attach-profile to take effect.

```
IR807(config-controller)# end
IR807#
```

Controller Cellular 0 and NAT Configuration

Controller Cellular 0 is configured with default parameters. If a profile different from Profile 1 is set-up, it must be attached to controller cellular 0.

If the SIM in slot #1 must be used as primary, it is done under controller cellular 0

1. Show the controller cellular 0

```
IR807#show run | begin controller
controller Cellular 0
  lte sim data-profile 1 attach-profile 1 slot 0 !
Value set-up for configuration example
  lte sim max-retry 0
  lte failovertimer 0
  lte modem link-recovery rssi onset-threshold -110
  lte modem link-recovery monitor-timer 20
  lte modem link-recovery wait-timer 10
  lte modem link-recovery debounce-count 6
!
```

1. If the cellular interface obtains an IPv4 private address, NAT should be configured.

```
IR807#conf term
Enter configuration commands, one per line. End with CNTL/Z.
IR807(config)#inter cellular 0
IR807(config-if)#ip nat outside
IR807(config-if)interface fastethernet 0
IR807(config-if)ip nat inside
IR807(config-if) ip virtual-reassembly in
IR807(config)#access-list 10 permit 10.20.20.0 0.0.0.255
!
IPv4 subnet to be NATed
IR807(config)#ip nat inside source list 10 interface Cellular0 overload
!
NAT interface association
```

1. Once the Cellular configuration is done, ping a well-known IP address to test the connectivity.

```
IR807#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 340/472/740 ms
IR807#
```

1. Attached Cellular 0 profile must become “active” and “connection” shows IP address and traffic.

```
IR807#show cellular 0 profile
Profile 1 = ACTIVE* **
-----
PDP Type = IPv4
PDP address = 10.60.159.255
Access Point Name (APN) = LTE
```



```

Authentication = None
Primary DNS address = 212.27.40.240
Secondary DNS address = 212.27.40.241
* - Default profile
** - LTE attach profile
Configured default profile for active SIM 0 is profile 1.
IR807#show cellular 0 connection
Profile 1, Packet Session Status = ACTIVE
Cellular0:
Data Transmitted = 700 bytes, Received = 600 bytes
IP address = 10.60.159.255
Primary DNS address = 212.27.40.240
Secondary DNS address = 212.27.40.241
Profile 2, Packet Session Status = INACTIVE

```

What to do Next

Use the show interface cellular 0 command to display the negotiated IP address if operational.

```

IR807#show interfaces cellular 0
Cellular0 is up, line protocol is up
Hardware is 4G WWAN Modem - Global (Europe & Australia) Multimode LTE/DC-HSPA+/HSPA+/HSPA/U

Internet address is 10.123.161.59/32
MTU 1500 bytes, BW 384 Kbit/sec, DLY 100000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation SLIP, loopback not set
Keepalive not supported
Last input 00:22:41, output never, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/10 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  12 packets input, 1128 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
  51 packets output, 3364 bytes, 0 underruns
  0 output errors, 0 collisions, 0 interface resets
  0 unknown protocol drops
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
  DCD=up DSR=up DTR=up RTS=up CTS=up
IR807#

```

If the negotiated IP address is not operational:

```

IR807#show interfaces cellular 0
Cellular0 is up (spoofing), line protocol is up (spoofing)
Hardware is 4G WWAN Modem - Global (Europe & Australia) Multimode LTE/DC-HSPA+/HSPA+/HSPA/U

Internet address will be assigned dynamically by the network

```

Other Useful Commands

```

IR807# show cell 0 hardware

```

```

Modem Firmware Version = SWI9X15Y_07.12.09.00
Modem Firmware built = 2017/04/26 23:34:19
Hardware Version = 1.0
Device Model ID: WP7504
Package Identifier ID: 1103235_9906722_WP7504_07.12.09.00_00_Cisco_001.001_000
International Mobile Subscriber Identity (IMSI) = 001012345678901
International Mobile Equipment Identity (IMEI) = 354937080100642
Integrated Circuit Card ID (ICCID) = 89600114082100035643
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Online
Current Modem Temperature = 37 deg C
PRI SKU ID = 1103235, PRI version = 001.028_000, Carrier = ATT
OEM PRI version = 01.01
IR807#

```

```
IR807# show cell 0 security
```

```

Active SIM = 1
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

```

```
IR807#sh cellular 0 radio
```

```

Radio power mode = online
LTE Rx Channel Number = 2525
LTE Tx Channel Number = 20525
LTE Band = 5
LTE Bandwidth = 10 MHz
Current RSSI = -60 dBm
Current RSRP = -86 dBm
Current RSRQ = -10 dB
Current SNR = 30.0 dB
Physical Cell Id = 0x0
Number of nearby cells = 1
Idx PCI (Physical Cell Id)
-----

```

```

1 0
Radio Access Technology(RAT) Preference = LTE
Radio Access Technology(RAT) Selected = LTE
IR807# show cell 0 network

```

```

Current System Time = Sat Oct 10 9:12:59 2015
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = LTE
Mobile Country Code (MCC) = 208
Mobile Network Code (MNC) = 15
Packet switch domain(PS) state = Attached
Location Area Code (LAC) = 3910
Cell ID = 222094374

```

```
IR807#
IR807# show cell 0 radio
```

```

Radio power mode = ON
Channel Number = 3037
Current Band = Unknown
Current RSSI (RSCP) = -99 dBm
Current ECIO = -10 dBm
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = UMTS ( UMTS/WCDMA )
IR807# show cell 0 network

```

```

Current System Time = Sat Oct 10 9:12:59 2015
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = LTE
Mobile Country Code (MCC) = 208
Mobile Network Code (MNC) = 15
Packet switch domain(PS) state = Attached
Location Area Code (LAC) = 3910
Cell ID = 222094374

```

Output example showing the 7504 modem

```

IR807# show cell 0 all
Hardware Information
=====
Modem Firmware Version = SWI9X15Y_07.12.09.00
Modem Firmware built = 2017/04/26 23:34:19
Hardware Version = 1.0
Device Model ID: WP7504
Package Identifier ID: 1103235_9906722_WP7504_07.12.09.00_00_Cisco_001.001_000
International Mobile Subscriber Identity (IMSI) = 001012345678901
International Mobile Equipment Identity (IMEI) = 354937080100642
Integrated Circuit Card ID (ICCID) = 89600114082100035643
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Online
Current Modem Temperature = 37 deg C
PRI SKU ID = 1103235, PRI version = 001.028_000, Carrier = ATT
OEM PRI version = 01.01
Profile Information
=====
Profile 1 = ACTIVE* **
-----
PDP Type = IPv4
PDP address = 192.168.1.51
Access Point Name (APN) = keysight
Authentication = None
Primary DNS address = 0.0.0.0
Secondary DNS address = 0.0.0.0
Profile 2 = ACTIVE
-----
PDP Type = IPv4
PDP address = 192.168.1.54
Access Point Name (APN) = keysight2
Authentication = None
Primary DNS address = 0.0.0.0
Secondary DNS address = 0.0.0.0
Profile 3 = INACTIVE
-----
PDP Type = IPv4
Access Point Name (APN) = keysight
Authentication = None
* - Default profile
** - LTE attach profile
Configured default profile for active SIM 1 is profile 1.
Data Connection Information
=====
Profile 1, Packet Session Status = ACTIVE
Celluansmitted = 0 bytes, Received = 0 bytes
IP address = 192.168.1.51

```

Output example showing the 7504 modem

```

        Primary DNS address = 0.0.0.0
        Secondary DNS address = 0.0.0.0
Profile 2, Packet Session Status = ACTIVE
Cellular1:
    Data Transmitted = 0 bytes, Received = 0 bytes
    IP address = 192.168.1.54
    Primary DNS address = 0.0.0.0
    Secondary DNS address = 0.0.0.0
Profile 3, Packet Session Status = INACTIVE
Profile 4, Packet Session Status = INACTIVE
Profile 5, Packet Session Status = INACTIVE
Profile 6, Packet 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 = Mon Apr 3 23:39:5 2000
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 doma Attached
Registration state(EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 1
Cell ID = 1
Negotiated network MTU is 1430
Radio Information
=====
Radio power mode = online
LTE Rx Channel Number = 2525
LTE Tx Channel Number = 20525
LTE Band = 5
LTE Bandwidth = 10 MHz
Current RSSI = -60 dBm
Current RSRP = -86 dBm
Current RSRQ = -10 dB
Current SNR = 30.0 dB
Physical Cell Id = 0x0
Number of nearby cells = 1
Idx      PCI (Physical Cell Id)
-----
1
Radio Access Technology(RAT) Preference = LTE
Radio Access Technology(RAT) Selected = LTE
Modem Security Information
=====
Active SIM = 1
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

```

```

GPS Information
=====
GPS Info
-----
GPS Feature: enabled
GPS Port Sated GPS port
GPS Status: GPS mode or nmea not enabled
GPS auto tracking status: disabled (Mode is not set)
GPS auto tracking config: disabled
GPS Mode Configured: not configured/unknown
SMS Information
=====
Incoming Message Information
-----
SMS stored in modem = 0
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 0
Number of callbacks triggered by SMS = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Outgoing Message Information
-----
Total SMS sent successfully = 0
Total SMS send failure = 0
Number of outgoing SMS pending = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Last Outgoing SMS Status = SUCCESS
Copy-to-SIM Status = 0x0
Send-to-Network Status = 0x0
Report-Outgoing-Message-Number:
  Reference Number = 0
  Result Code = 0x0
  Diag Code = 0x0 0x0 0x0 0x0 0x0
SMS Archive URL =
Error Information
=====
This command is not supported on this platform.
Modem Crashdump Information
=====
Chassis Model Name is IR807G-LTE-NA-K9
Platform is MC73xx based
Modem crashdump logging: off
IR807#

```

Output example showing the 7502 modem

```

IR807#sh cell 0 all
Hardware Information
=====
Modem Firmware Version = SWI9X15Y_07.12.09.00
Modem Firmware built = 2017/04/26 23:34:19
Hardware Version = 1.0
Device Model ID: WP7502
Package Identifier ID: 1103234_9906721_WP7502_07.12.09.00_00_Cisco_001.001_000
International Mobile Subscriber Identity (IMSI) = 208103796469544
International Mobile Equipment Identity (IMEI) = 354938080100327
Integrated Circuit Card ID (ICCID) = 89331037162704055456
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Online

```

Output example showing the 7502 modem

```
Current Modem Temperature = 29 deg C
PRI SKU ID = 1103234, PRI version = 001.033_000, Carrier = Generic
OEM PRI version = 01.01
```

```
Profile Information
=====
```

```
Profile password Encryption level: 7
```

```
Profile 1 = INACTIVE* **
```

```
-----
```

```
PDP Type = IPv4
Access Point Name (APN) = sl2sfr
Authentication = None
```

```
* - Default profile
** - LTE attach profile
```

```
Configured default profile for active SIM 0 is profile 1.
```

```
Data Connection Information
=====
```

```
Profile 1, Packet Session Status = INACTIVE
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 = Wed Oct 11 8:24:34 2017
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = F SFR
Mobile Country Code (MCC) = 208
Mobile Network Code (MNC) = 10
Packet switch domain(PS) state = Attached
Registration state(EMM) = Registered
EMM Sub State = Normal Service
Tracking Area Code (TAC) = 46506
Cell ID = 604934
Network MTU is not Available
```

```
Radio Information
=====
```

```
Radio power mode = online
LTE Rx Channel Number = 1501
LTE Tx Channel Number = 19501
LTE Band = 3
```

```
LTE Bandwidth = 20 MHz
Current RSSI = -84 dBm
Current RSRP = -114 dBm
Current RSRQ = -13 dB
Current SNR = -1.0 dB
Physical Cell Id = 0x102
Number of nearby cells = 1
Idx      PCI (Physical Cell Id)
-----
1        258
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = LTE

Modem Security Information
=====
Active SIM = 0
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

GPS Information
=====

GPS Info
-----
GPS Feature: enabled
GPS Port Selected: Dedicated GPS port
GPS Status: GPS mode or nmea not enabled
GPS auto tracking status: disabled (Mode is not set)
GPS auto tracking config: disabled
GPS Mode Configured: not configured/unknown

SMS Information
=====
Incoming Message Information
-----
SMS stored in modem = 6
SMS archived since booting up = 0
Total SMS deleted since booting up = 0
Storage records allocated = 25
Storage records used = 6
Number of callbacks triggered by SMS = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0

Outgoing Message Information
-----
Total SMS sent successfully = 0
Total SMS send failure = 0
Number of outgoing SMS pending = 0
Number of successful archive since booting up = 0
Number of failed archive since booting up = 0
Last Outgoing SMS Status = SUCCESS
Copy-to-SIM Status = 0x0
Send-to-Network Status = 0x0
Report-Outgoing-Message-Number:
  Reference Number = 0
  Result Code = 0x0
  Diag Code = 0x0 0x0 0x0 0x0 0x0

SMS Archive URL =
```

```
Error Information
=====
```

This command is not supported on this platform.

```
Modem Crashdump Information
=====
Chassis Model Name is IR807G-LTE-GA-K9
Platform is MC73xx based
Modem crashdump logging: off
```

```
ir807-htab#sh run int async 0
Building configuration...
```

```
Current configuration : 124 bytes
!
interface Async0
no ip address
no ip redirects
no ip unreachable
no ip proxy-arp
encapsulation scada
shutdown
end
```

Accessing 4G Modem AT Commands

Note: A password must be added to the line configuration for security.

Get the line number associated to Cellular 0:

```
IR807#show line
Tty Typ Tx/Rx A Modem Roty AccO AccI Uses Noise Overruns Int
A 3 TTY - inout - - - 0 0 611/0 Ce0 - Single APN
I 8 TTY - inout - - - 0 0 0/0 Ce1 - Multi APN
```

Use one of the IR807 IP addresses along with 2000 + line number (2003)

```
IR807#telnet 1.1.1.1 2003
Trying 1.1.1.1, 2003 ... Open
```

Execute the 4G modem AT commands, for example AT!GSTATUS?:

```
at!gstatus?
Current Time: 1418Temperature: 37
Bootup Time: 5Mode: ONLINE
System mode: LTE PS state: Attached
LTE band: B5 LTE bw: 10 MHz
LTE Rx chan: 2525LTE Tx chan: 20525
EMM state: Registered Normal Service
EMM connection:RRC Connected RSSI (dBm): -60Tx Power: 1
RSRP (dBm): -86TAC: 0001 (1)
RSRQ (dB): -10Cell ID: 00000001 (1)
SINR (dB): 30.0
IMS Reg State: UNKNOWN IMS Mode: Not Support
IMS Srv State: UNKNOWN SMS,UNKNOWN VoIP
```

Disconnect using “SHIFT+CONTROL+6+x”, then confirm:


```
IR807#disc
Closing connection to 1.1.1.1 [confirm]enter
IR807#
```

Checking 4G Modem Firmware through AT Commands

To check the IR807 4G modem firmware, execute the 4G modem AT commands after connecting to the modem:

```
IR807#telnet 1.1.1.1 2002
Trying 1.1.1.1, 2002 ... Open
Connecting to virtual console, enter Ctrl-^ followed by x,
then "disconnect" to return to router prompt
/ #
/ #
/ # echo -e 'at!gstatus?\r\n' > /dev/ttyUSB2
/ # at!gstatus?
!GSTATUS:
Current Time: 1418Temperature: 37
Bootup Time: 5Mode: ONLINE
System mode: LTE PS state: Attached
LTE band: B5 LTE bw: 10 MHz
LTE Rx chan: 2525LTE Tx chan: 20525
EMM state: Registered Normal Service
EMM connection:RRC Connected
RSSI (dBm): -60Tx Power: 1
RSRP (dBm): -86TAC: 0001 (1)
RSRQ (dB): -10Cell ID: 00000001 (1)
SINR (dB): 30.0
IMS Reg State: UNKNOWN IMS Mode: Not Support
IMS Srv State: UNKNOWN SMS,UNKNOWN VoIP
OK
/ #
/ # echo -e 'at+cgcontrdp\r\n' > /dev/ttyUSB2
/ # at+cgcontrdp
+CGCONTRDP: 1,5,keysight,192.168.1.51,,,,
+CGCONTRDP: 2,8,keysight2,192.168.1.54,,,,
OK
/ # echo -e 'at+cgdcont?\r\n' > /dev/ttyUSB2
/ # at+cgdcont?
+CGDCONT: 1,"IP","keysight","0.0.0.0",0,0
+CGDCONT: 2,"IP","keysight2","0.0.0.0",0,0
+CGDCONT: 3,"IP","keysight","0.0.0.0",0,0
OK
/ # echo -e 'at!priid?\r\n' > /dev/ttyUSB2
/ # at!priid?
PRI Part Number: 9906722
Revision: 01.01
Carrier PRI: 9999999_9904367_SWI9X15Y_07.12.09.00_00_ATT_001.028_000OK
/ # echo -e 'at!impref?\r\n' > /dev/ttyUSB2
/ # at!impref?
!IMPREF:
preferred fw version: 07.12.09.00
preferred carrier name: ATT
preferred config name: ATT_001.028_000
current fw version: 07.12.09.00
current carrier name: ATT
current config name: ATT_001.028_000
OK
/ #
/ # echo -e 'at!gpsstatus?\r\n' > /dev/ttyUSB2
```

```

/ # at!gpsstatus?
Current time: 1980 01 06 6 00:45:40
1980 01 06 6 00:45:40 Last Fix Status = NONE
1980 01 06 6 00:45:40 Fix Session Status = NONE
No TTFE available
OK
/ # echo -e 'at!band=?\r\n' > /dev/ttyUSB2
/ # at!band=?
Index, Name
00, All Bands
02, North America 3G
07, merica
08, WCDMA ALL
09, LTE ALL
OK
/ #

```

IR807 Cellular Technology Selection

The cellular interface supports 4G/LTE networks. The IOS CLI can be used to select a particular technology that is most desirable in your local zone.

Use the cellular 0 lte technology command:

Verizon modem WP7601

```

IR807# cellular 0 lte technology ?
auto      Automatic LTE Technology Selection
lte       LTE

```

GA modem WP7502

```

IR807# cellular 0 lte technology ?
auto      Automatic Radio Access Technology(RAT) Selection
gsm       GSM
lte       LTE
umts      UMTS

```

NA modem WP7504 with ATT Firmware

```

IR807# cellular 0 lte technology ?

```

```

auto      Automatic Radio Access Technology(RAT) Selection
lte       LTE
umts      UMTS

```

NA modem WP7504 with Sprint Firmware

```

IR807# cellular 0 lte technology ?

```

```

auto      Automatic Radio Access Technology(RAT) Selection
lte       LTE
umts      UMTS
cdma-1xrtt CDMA 1xRTT
cdma-evdo CDMA EVDO Rev A

```

Note: The default technology type selection is **auto** and it is recommended to be used at all times. Although **gsm & umts** as part of the selection, the modem firmware does not support them on gsm/umts network. They will be used as **lte** selection on Verizon network.

Show the completed configuration: (output edited for brevity)

```
IR807#show run
Building configuration...
!
! Last configuration change at 16:59:31 UTC Thu Jun 29 2017
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname IR807
!
boot-start-marker
boot-end-marker
!
!
enable password lab
!
no aaa new-model
memory-size iomem 5
!
ip inspect WAAS flush-timeout 10
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
license udi pid IR807G-LTE-NA-K9 sn FCW211700HD
license boot module ir8001 level advipservices
!
!
!
redundancy
 notification-timer 120000
!
controller Cellular 0
 lte sim data-profile 1 attach-profile 1 slot 0
 lte modem link-recovery disable
!
interface Loopback1
 ip address 1.1.1.1 255.255.255.0
!
interface Cellular0
 ip address negotiated
 ip nat outside
 ip virtual-reassembly in
 encapsulation slip
 load-interval 30
 dialer in-band
 dialer idle-timeout 0
 dialer string lte
 dialer string multimode
 dialer-group 1
 no peer default ip address
```

```

    ipv6 address autoconfig
    async mode interactive
    routing dynamic
    !
interface Cellular1
    ip address negotiated
    ip nat outside
    ip virtual-reassembly in
    encapsulation slip
    load-interval 30
    dialer in-band
    dialer idle-timeout 0
    dialer string lte
    dialer string multimode
    dialer-group 1
    no peer default ip address
    async mode interactive
    routing dynamic
    !
interface FastEthernet0
    ip address 10.65.217.109 255.255.255.224
    duplex auto
    speed auto
    !
interface FastEthernet1
    no ip address
    duplex auto
    speed auto
    !
interface Async0
    no ip address
    encapsulation slip
    hold-queue 10 out
    !
interface Async1
    no ip address
    encapsulation scada
    !
ip forward-protocol nd
no ip http server
no ip http secure-server
!
!
ip route 10.0.0.0 255.0.0.0 FastEthernet0
ip route 192.168.1.51 255.255.255.255 Cellular0
ip route 192.168.1.52 255.255.255.255 Cellular1
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
dialer watch-list 1 ip 8.8.8.8 255.255.255.255
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
ipv6 ioam timestamp
!
access-list 1 permit any
access-list 101 permit ip any any
!
control-plane
line con 0
line 2
    no activation-character
    no exec

```

```

transport preferred none
transport input all
stopbits 1
line 3
  script dialer lte
  modem InOut
  no exec
  monitor
  transport input all
  transport output all
  rxspeed 100000000
  txspeed 50000000
line 4
line 5
  stopbits 1
line 8
  script dialer lte
  modem InOut
  no exec
  monitor
  transport input all
  transport output all
line vty 0 3
  password lab
  login
  transport input all
  transport output all
line vty 4
  password lab
  login local
  transport input all
  transport output all
!
scheduler allocate 20000 1000
!
end

```

GPS

The IR807 series can be configured to enable real-time location tracking of remote assets and geo-fence when used with IOT Field Network Director. Field Network Director receives GPS data directly from IOS, not NMEA.

Key Points:

- GPS must be configured under *controller cellular 0*.
- GPS data can be seen locally, or data stream can be forwarded to applications, i.e. RUBAN.

To configure GPS on the IR807 series, refer to the following examples.

```

IR807# conf term
IR807(config)#controller cellular 0
IR807(config-controller)#lte gps ?
  enable  enable GPS feature
  mode    select GPS mode
  nmea    enable NMEA data
IR807(config-controller)#lte gps mode standalone

IR807(config-controller)#lte gps nmea ip

```

```

IR807#show cellular 0 gps

GPS Info
-----
GPS Feature: enabled
GPS Port Selected: Dedicated GPS port
GPS State: GPS enabled
GPS Mode Configured: standalone
Latitude: 48 Deg 38 Min 31.2114 Sec North
Longitude: 2 Deg 13 Min 47.3992 Sec East
Timestamp (GMT): Wed Jul 22 08:05:28 2015
Fix type index: 0, Height: 94 m
Satellite Info
-----
Satellite #14, elevation 28, azimuth 310, SNR 31 *
Satellite #15, elevation 22, azimuth 171, SNR 39 *
Satellite #17, elevation 25, azimuth 45, SNR 34 *
Satellite #18, elevation 8, azimuth 248, SNR 25
Satellite #22, elevation 12, azimuth 281, SNR 24
Satellite #24, elevation 78, azimuth 90, SNR 35 *
Satellite #25, elevation 23, azimuth 241, SNR 27
Satellite #1, elevation 0, azimuth 0, SNR 0
Satellite #2, elevation 0, azimuth 0, SNR 0
Satellite #6, elevation 6, azimuth 85, SNR 0
Satellite #12, elevation 62, azimuth 241, SNR 0
Satellite #26, elevation 0, azimuth 0, SNR 0
Satellite #29, elevation 0, azimuth 0, SNR 0
IR807#

```

You can also configure IOS so that GPS can be streamed to another destination (port or address).

For example:

```

IR807#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IR807(config)#controller cellular 0
IR807(config-controller)#lte gps nmea ?
    ip      NMEA over IP interface
    serial  NMEA over serial interface
IR807(config-controller)#lte gps nmea ip ?
    udp     UDP Transport
    <cr>
IR807(config-controller)#lte gps nmea ip udp ?
    A.B.C.D Source address
IR807(config-controller)#lte gps nmea ip udp 10.3.4.5 ?
    A.B.C.D Destination address
IR807(config-controller)#lte gps nmea ip udp 10.1.1.1 10.3.4.5 ?
    <0-65535> Destination port
IR807(config-controller)#lte gps nmea ip udp 10.1.1.1 10.3.4.5 3456
Cellular Modem in HWIC slot 0/0 is still in reset, we recommend to re-execute this cmd after
60 seconds
IR807(config-controller)#

```

GPS NMEA Multiple Stream

Feature is new for release 15.8(3)M1.

Previous versions of IOS only allowed for a GPS NMEA Stream for one device. This release has support for up to 6 devices at one time. The existing CLI `lte gps nmea ip udp <src ip> <dest ip> <dest portno>` under controller configuration has been enhanced.

Setting up the Configuration

To Enable GPS NMEA Multiple Stream:

```
Router# Config t
Router(config)#Controller Cellular
<Cellular Interface Number>
Router(config-controller)#lte gps nmea ip udp
<source ip> <destination ip> <destination port> stream <1-6>
```

To Disable GPS NMEA Multiple Stream:

```
Router(config-controller)#no lte gps nmea ip udp
<source ip> <destination ip> <destination port> stream <1-6>
```

Examples for Enabling/Disabling GPS NMEA Multiple Stream

Enable Example:

```
Router#(config-controller)#lte gps nmea ip udp 10.0.0.1 10.0.0.11 2020 ? stream GPS NMEA
multiple stream suppor
t
Router#(config-controller)#lte gps nmea ip udp 10.0.0.1 10.0.0.11 2020 stream ? <1-6> Stream
Number
Router#(config-controller)#lte gps nmea ip udp 10.0.0.1 10.0.0.11 2020 stream 6
```

Disable Example:

```
Router#(config-controller)#no lte gps nmea ip udp 10.0.0.1 10.0.0.11 2020 stream 6
```

Warning Messages

If the destination ip address and port number already exists:

```
Router#sh run | sec cont
controller Cellular 0
  lte gps mode standalone
  lte gps nmea ip udp 10.10.0.1 10.10.0.10 2067 stream 1
Router(config-controller)#lte gps nmea ip udp 10.10.0.1 10.10.0.10 2067 stream 5
  Destination ip address 10.10.0.10 and destination port number 2067 is already exists for
  the stream no:1.
```

Please use different destination ip address and port number.

If the stream number already exists:

```
Router#sh run | sec cont
controller Cellular 0
  lte gps mode standalone
  lte gps nmea ip udp 10.10.0.1 10.10.0.10 2067 stream 1
```

```
Router(config-controller)#lte gps nmea ip udp 20.20.0.1 20.20.0.10 2057 stream 1
Stream number 1 is already active.
```

Please remove stream number configuration before creating it with different destination ip address and port number.

Upgrading the Modems

This section provides information about upgrading Cisco cellular modem firmware on the IR807. To make sure that the modem's firmware and other settings are upgraded correctly, certain packages need to be downloaded and upgraded on the modem. It is important to identify the modem and SKU type and follow the corresponding sequence.

There are three file types that will be upgraded on the WP75xx and WP76xx modems:

- Modem firmware with carrier PRI which is a .spk file
- Modem Legato and Yocto firmware file which is a .spk file
- Modem OEM PRI file which is a .nvu file

Refer to the following table for the SKU, Modem Type, and Firmware.

Table 5: Modem Firmware associated with each SKU

SKU ID	Modem Type	Firmware
IR807G-LTE-VZ-K9	WP7601	WP7601_02.18.05.00_00_VERIZON_002.041_001_fw.spk WP7601_02.18.05.00_Legato_Yocto_MCU.spk
IR807G-LTE-NA-K9	WP7504	WP7504_07.12.09.00_00_ATT_001.028_000.spk (For ATT) WP7504_07.12.09.00_00_SPRINT_001.020_000.spk (For Sprint) WP75xx_07.12.09.00_00_GENERIC_001.033_000.spk (For other carriers) WP7504_1103235_07.12.09.00_00_Cisco_001.001_000.nvu WP75xx_07.12.09.00_Legato_Yocto_MCU.spk
IR807G-LTE-GA-K9	WP7502	WP7502_1103234_07.12.09.00_00_Cisco_001.001_000.nvu WP75xx_07.12.09.00_00_GENERIC_001.033_000.spk WP75xx_07.12.09.00_Legato_Yocto_MCU.spk

The following rules apply when upgrading modems:

- Each of the files need to be upgraded separately. You cannot place them together in the same folder and perform a simultaneous upgrade.
- When switching from one carrier to another, only the Firmware file corresponding to the carrier needs to be upgraded. You do not need to re-upgrade with the OEM PRI and Legato-Yocto files. For example: If using an IR807G-LTE-NA-K9 with the ATT SIM in one slot and Sprint SIM in the other slot, simply upgrade with the firmware corresponding to the active SIM.

Firmware Upgrade Procedure

Note: The following example illustrates how to perform an upgrade using only a single file. You will need to perform the same steps with each modem file (*.spk and *.nvu) to complete the firmware upgrade. For more information refer to the Cisco Firmware Upgrade Guide for Cellular Modems guide, “Upgrading the modem firmware manually”:

https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/firmware/Firmware_Upgrade.html#pgfid-1023076

Perform the following steps to upgrade the modem firmware:

1. Go to the Cisco web page to download the latest certified firmware for your carrier by going to the following location: Products -> Cisco Interfaces and Modules -> LTE Wireless WAN Interfaces.
2. Create a directory in flash to host the firmware, which will be downloaded in step 3.

```
IR807# mkdir flash
Create directory filename [flash]? <enter>
>
Created dir flash:/flash
```

3. Download the firmware to the directory in the router flash over Ethernet/cellular /WAN interface. This can be done by hosting the firmware on an FTP or TFTP server, and connecting to that server via any WAN interface on the router. Below is a example showing the modem firmware downloaded onto the router flash over the FastEthernet interface:**Note:** Output edited for brevity.

```
IR807# copy tftp flash
Address or name of remote host []? 192.168.1.1
Source filename []? /<directory>
/WP75xx_07.12.09.00_Legato_Yacto_MCU.spk
Destination filename [WP75xx_07.12.09.00_Legato_Yacto_MCU.spk]?<enter>
>
/<directory>
/ WP75xx_07.12.09.00_Legato_Yacto_MCU.spk
Accessing tftp://192.168.1.1//<directory>
/WP75xx_07.12.09.00_Legato_Yacto_MCU.spk...
Loading /<directory>
/WP75xx_07.12.09.00_Legato_Yacto_MCU.spk from 192.168.1.1 (via FastEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 24444106 bytes]
24444106 bytes copied in 132.368 secs
```

4. Verify that the firmware is available on the newly created directory inside router flash by using the following command:

```
IR807# dir flash:WP75xx_07.12.09.00_Legato_Yacto_MCU
Directory of flash:/WP75xx_07.12.09.00_Legato_Yacto_MCU/
-rw- 24444106 Sep 4 2017 09:58:34 -08:00 WP75xx_07.12.09.00_Legato_Yacto_MCU.spk
```

5. Initiate a modem firmware upgrade using the microcode reload command. Ex : IR807# **microcode reload cellular 0 lte modem-provision flash:<directory>?**

```
IR807#microcode reload cellular 0 0 modem-provision flash:new-modem
Reload microcode? [confirm]<enter>
>
Log status of firmware download in router flash system?[confirm]<enter>
>
Firmware download status will be logged in flash:/fwlogfile
Microcode Reload Process launched for Cellular 33133484; hw type = 0x6F3
```

```

IR807#
*****
The interface will be Shut Down for Firmware Upgrade
This will terminate any active data connections.
*****
*Sep  4 05:55:01.570: %LINK-5-CHANGED: Interface Cellular0, changed state to reset
*Sep  4 05:55:02.570: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular0, changed
state to down
*Sep  4 05:55:06.570: %LINK-5-CHANGED: Interface Cellular0, changed state to administratively
down
*Sep  4 05:55:11.586: %LINK-5-CHANGED: Interface Cellular1, changed state to reset
*Sep  4 05:55:12.586: %LINEPROTO-5-UPDOWN: Line protocol on Interface Cellular1, changed
state to down
*Sep  4 05:55:16.586: %LINK-5-CHANGED: Interface Cellular1, changed state to administratively
down
*****
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.
*****
Sending F/W[WP75xx_07.12.09.00_Legato_Yacto_MCU.spk] to the card [24444106 bytes]:
Firmware file: WP75xx_07.12.09.00_Legato_Yacto_MCU.spk sent to the card
Modem Device ID: WP7502  MODEM F/W Boot Version: SWI9X15Y_07.12.09.00 r34123 CARMD-EV-FRMWR1
2017/04/26 23:34:19
Modem F/W App Version: SWI9X15Y_07.12.09.00 r34123 CARMD-EV-FRMWR1 2017/04/26 23:34:19
Modem SKU ID: 1103234
Modem Package Identifier: 1103234_9906721_WP7502_07.11.22.00_00_Cisco_001.000_000  Modem
Carrier String: 1
Modem PRI Ver: 01.00  Modem Carrier Name: GENERIC
Modem Carrier Revision: 001.033_000
Firmware Upgrade is in Progress...
F/W Upgrade: Firmware Upgrade has Completed Successfully
IR807#

```

Verifying the firmware

```

IR807#sh cellular 0 hardware

Modem Firmware Version = SWI9X15Y_07.12.09.00
Modem Firmware built = 2017/04/26 23:34:19
Hardware Version = 1.0
Device Model ID: WP7502
Package Identifier ID: 1103234_9906721_WP7502_07.11.22.00_00_Cisco_001.000_000
International Mobile Subscriber Identity (IMSI) = 001012345678901
International Mobile Equipment Identity (IMEI) = 354938080100459
Integrated Circuit Card ID (ICCID) = 89600114082100035643
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) =
Modem Status = Online
Current Modem Temperature = 33 deg C
PRI SKU ID = 1103234, PRI version = 001.033_000, Carrier = Generic
OEM PRI version = 01.00
IR807#

```

AutoSim and Firmware Based Switching running the WP7504 Modem

The AutoSim feature will identify the SIM card of the Carrier inserted and correspondingly load the correct modem firmware. The advantages of the AutoSim feature are:

- Ease of Ordering Carrier Specific SKUs
- Quicker failover times in dual-sim deployments

Auto-SIM is supported in Sierra wireless WP7504 modem on the IR807. The WP7502 and WP7601 modems do not support this feature. A CLI is available in the cellular controller to enable/disable Auto-SIM. The modem in Auto-SIM mode selects the right carrier firmware after a SIM slot switch and an automatic modem reset. During bootup, if the Auto-SIM configuration on the modem doesn't match to the IOS configuration, the corresponding Auto-SIM or manual mode is pushed to the modem.

After an Auto-SIM configuration change, the modem is automatically reset; the default is "auto-sim" enabled:
controller cellular 0

```
[no] lte firmware auto-sim
```

If Auto-SIM is disabled and the modem is in manual mode, select a carrier with a new exec CLI:

```
cellular lte firmware-activate <firmware-index>
```

Enable/Disable Auto-SIM:

```
(config)#controller cellular 0
(config)# [no] lte firmware auto-sim
default is auto-sim enabled
```

Manual mode:

```
controller cellular 0
no lte firmware auto-sim
```

The following CLI shows the firmware-index of the carrier in the modem:

```
show cellular 0 firmware
```

For additional information, see the following guide:

[Cisco 4G LTE and Cisco 4G LTE-Advanced Network Interface Module Software Configuration Guide](#)

MTU Selection for WP76xx modems

This new feature allows the user to configure the mtu setting under the controller, up to a value of 2000, for the WP76xx modems. This requires setting the mtu on the corresponding cellular interface to match the same value as the controller.

The following example shows the controller configuration commands:

```
router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
router#(config-controller)#lte modem mtu ?
<64-2000> Mtu value
```

Low Power Mode

This feature provides the reason for the modem going into a low power mode if the situation ever occurs. It uses the device power control information provided by the modem. A new CLI has been implemented **show cellular <interface> radio details**.

The following examples show the controller show commands:

```
router# show cellular <interface number> radio
Radio power mode = OFF, Reason = User Request
Channel Number = 0
Current Band = Unknown
Current RSSI = -128 dBm
Current ECIO = -2 dBm
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = AUTO
router# show cellular <interface number> radio details
Radio turned off under cellular controller configuration.
router#
```

Note: In the above **show cellular <interface number> radio** output, the Radio power mode shows **OFF** because the user has turned the radio off by choice. In all other cases, when the radio goes to Low Power mode, you will see the display Radio power mode = **low power**.

Enhancement to Modem Crash Action

If the modem corresponding to the cellular interface crashes, the modem will reset itself and come back up. However, in order to debug the cause of the crash, a full crash dump can be captured on the modem. The steps to capture the crashdump are outlined in:

[Generate 4G Modem Crash Dump](#)

-or

<https://www.cisco.com/c/en/us/td/docs/routers/access/800/819/user/guide/3G4G-enhancements-userguide.html#pgfid-1076594>

A new CLI has been added to simplify the configuration to put the modem in a diagnostic mode upon a crash. The CLI is **lte modem crash-action**. The device can be set to either reset, or to boot and hold.

The following examples show the new functionality of the configuration CLI:

```
Router(config-controller)#lte modem crash-action ?
boot-and-hold
Remain in crash state
reset
Reset the modem on crash
```

This CLI will set the flag to either 1 or 0 for reset and boot and hold respectively. This is the same as AT command **at!eroption= 0 / 1**

```
The following examples show the new functionality of the exec CLI:
Router(config-controller)#lte modem crash-action ?
boot-and-hold Remain in crash state
```

This CLI will set the flag on the modem, to either 1 - reset or 0 - boot and hold respectively. This is the same as AT command **at!eroption=?**.

The following examples show the new functionality of the exec CLI:

```
router#show cellular <your interface> logs modem-crash-action
Current modem crash action: Reset
```

Note: This feature is only used while debugging modem crash dump and should be used **ONLY** as advised by Cisco TAC. **Please do not enable this feature before consulting with Cisco TAC.**



CHAPTER 5

Configuring the Serial Interface

This chapter describes configuring serial interface management.

- [Configuring the Serial Interface, on page 53](#)
- [Configuring Raw Socket, on page 54](#)

Configuring the Serial Interface

This chapter describes configuring serial interface management.

The IR807 supports asynchronous serial interface protocols used for Raw Socket, SCADA Protocol Translation or reverse Telnet. It has two serial interfaces, designated async 0 and async 1.

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.

Command or Action	Purpose
Router(config)# interface async 0	Enters interface configuration mode.

Specifying Asynchronous Serial Encapsulation

By default, asynchronous serial lines use the SCADA serial encapsulation method, which provides the communication between the Control Center and the RTU. The asynchronous serial interfaces support the following serial encapsulation methods:

- PPP
- Raw-TCP
- Raw-UDP
- SCADA
- SLIP

Command or Action	Purpose
Router(config-if)# encapsulation {scada ppp raw-tcp raw-udp slip}	Configures asynchronous serial encapsulation.

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:

```
IR807#sh run int async 0
Building configuration...
Current configuration : 62 bytes
!
interface Async0
no ip address
encapsulation raw-tcp
end
IR807#sh run | sec line
line con 0
stopbits 1
line 1
exec-timeout 0 0
raw-socket tcp server 502
no exec
transport preferred none
transport input all
transport output none
stopbits 1
```

Configuring Raw Socket

On the IR807, async 0 is associated with Line 5, and async 1 is associated with Line 4. In the following example, raw-socket (tcp) is configured on async 0:

```
IR807# interface Async0
no ip address
encapsulation raw-tcp
```

If the IR807 is configured as a raw-socket TCP client:

```
line 5
raw-socket tcp client 10.0.0.254 5000
stopbits 1
```

If IR807 is configured as a raw-socket TCP server:

```
line 5
raw-socket tcp server 10000
stopbits 1
```


Note: In the example above, 10000 is for raw-socket tcp server configuration. Avoid using the ports from 1 to 1023 for the raw-socket TCP server's local port.

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.



Note The corresponding port used for configuration mapping should be changed on the Head end application server as well.

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enters global configuration mode.
Step 2	interface async <i>number</i>	Enters interface command mode for the serial slot/port.
Step 3	no ip address	Disables IP processing on the interface.
Step 4	Do one of the following: <ul style="list-style-type: none"> • encapsulation raw-tcp • encapsulation raw-udp 	Enables Raw Socket TCP encapsulation or UDP encapsulation for the serial port.
Step 5	raw-socket packet-timer <i>timeout</i>	Specifies the maximum time in milliseconds the router waits to receive the next character in a stream. If a character is not received by the time the packet-timer expires, the accumulated data is packetized and forwarded to the Raw Socket peer. Options are 25ms or 50ms.
Step 6	raw-socket packet-length <i>length</i>	Specifies the packet size that triggers the IR807 to transmit the data to the peer. When the IR807 accumulates this much data in its buffer, it packetizes the data and forwards it to the Raw Socket peer. <i>length</i> — 2 to 1400 bytes. By default, the packet-length trigger is disabled.
Step 7	raw-socket tcp server <i>port</i>	Starts the Raw Socket Transport TCP server for an asynchronous line interface. In Raw Socket server mode, the IR807 listens for incoming connection requests from Raw Socket clients. <i>port</i> —Port number the server listens on.

	Command or Action	Purpose
		<i>ip_address</i> —(Optional) Local IP address on which the server listens for connection requests.
Step 8	raw-socket tcp keepalive <i>interval</i>	Sets the Raw Socket Transport TCP session keepalive interval for the asynchronous line interface. The router sends keepalive messages based on the configured interval. You may need to configure this interval, for example, when sending raw TCP traffic over a cellular interface. Currently configured keepalive interval in seconds. Range is 1-864000 seconds.
Step 9	raw-socket tcp idle-timeout <i>session_timeout</i>	Sets the Raw Socket Transport TCP session timeout for the asynchronous line interface. If no data is transferred between the client and server over this interval, then the TCP session is closed. The client then automatically attempts to reestablish the TCP session with the server
Step 10	raw-socket mode best-effort	Enable best-effort mode for the serial line. When this mode is enabled, older packets are dropped from the head of the queue when the queue is full. By default, best-effort mode is off.
Step 11	exit	Exits global configuration mode.

Example Configuration

```

!
interface Async1
no ip address
encapsulation raw-tcp
!
line 4
raw-socket tcp keepalive 300
raw-socket tcp server 8004
raw-socket packet-timer 50
raw-socket tcp idle-timeout 60
transport input all
transport output all
!

```

Configuring Raw Socket TCP

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

Configuring the Raw Socket TCP Server

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enters configuration mode.
Step 2	<code>line slot/port</code>	Enters line command mode for the serial slot/port.
Step 3	<code>raw-socket tcp server port [ip_address]</code>	Starts the Raw Socket Transport TCP server for an asynchronous line interface. In Raw Socket server mode, the IR807 listens for incoming connection requests from Raw Socket clients. <i>port</i> —Port number the server listens on. <i>ip_address</i> —(Optional) Local IP address on which the server listens for connection requests.
Step 4	<code>raw-socket tcp idle-timeout session_timeout</code>	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. <i>session_timeout</i> —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 1/1
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

Procedure

	Command or Action	Purpose
Step 1	configure terminal	Enters configuration mode.
Step 2	line slot/port	Enters line command mode for the serial slot/port.
Step 3	raw-socket tcp client <i>dest_ip_address dest_port</i> <i>[local_ip_address] [local_port]</i>	Specifies settings for Raw Socket Transport TCP client sessions. <i>dest_ip_address</i> —Destination IP address of the remote Raw Socket server. <i>dest_port</i> —Destination port number to use for the TCP connection to the remote server. <i>local_ip_address</i> —(Optional) Local IP address that the client can also bind to. <i>local_port</i> —(Optional) Local port number that the client can also bind to.

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 IR807 (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 1/1
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.

Procedure

	Command or Action	Purpose
Step 1	<code>configure terminal</code>	Enters configuration mode.
Step 2	<code>line slot/port</code>	Enters line command mode for the serial slot/port.
Step 3	<code>raw-socket udp connection dest_ip_address dest_port local_port [local_ip_address]</code>	Specifies settings for Raw Socket Transport UDP connections. <i>dest_ip_address</i> —Destination IP address to use for the UDP connection. <i>dest_port</i> —Destination port number to use for the UDP connection. <i>local_port</i> —Local port number for the UDP connection. <i>local_ip_address</i> —(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 1/1
router(config-line)# raw-socket udp connection 192.168.0.2 5000 7000
router(config-line)# raw-socket mode best-effort
router(config-line)# exit
router(config)#
```

Router B

```
router# configure terminal
router(config)# line 1/1
router(config-line)# raw-socket udp connection 192.168.0.8 7000 5000
router(config-line)# raw-socket mode best-effort
router(config-line)# exit
router(config)#
```

Reverse Telnet

Reverse telnet allows you to telnet to a device, and then connect from that device to the console of another device. This is useful for devices that do not have remote access built into them. This section provides an overview of what is required for setup.



Note This setup requires a straight through cable that goes from the console port of the console-only device to the AUX port on your router.

Follow these steps to configure the IR807:

Configure the AUX Port

```
router#configure terminal
router(config)#line aux 0
router(config-line)#modem InOut
router(config-line)#transport input all
router(config-line)#speed 19200
router(config-line)#exit
```

Create a Loopback Address

```
router#configure terminal
router(config)#int loopback 0
router(config-if)#ip address 10.0.0.1 255.0.0.0
router(config-if)#no shut
router(config-if)#exit
```

Determine Which Line is the AUX Port

Outside of configuration mode (hit CTRL-Z to get out), enter the command **show line**

```
router#sh line
  Tty Typ      Tx/Rx      A Modem  Roty  AccO  AccI   Uses   Noise  Overruns  Int
    0 CTY          - -          - -    - -    0       0      0/0      -
  225 AUX  19200/19200 - inout   - -    - -    0       0      0/0      -
* 226 VTY          - -          - -    - -   10      0      0/0      -
  227 VTY          - -          - -    - -    0       0      0/0      -
  228 VTY          - -          - -    - -    0       0      0/0      -
  229 VTY          - -          - -    - -    0       0      0/0      -
  230 VTY          - -          - -    - -    0       0      0/0      -
```



CHAPTER 6

Protocol Translation

This chapter provides details about configuring Protocol Translation on the Cisco IR807 Integrated Services Router for operation within a Supervisory Control and Data Acquisition (SCADA) system.

- [Protocol Translation, on page 61](#)
- [Information About SCADA, on page 61](#)
- [Configuring Protocol Translation, on page 63](#)
- [Configuring the DNP3-Serial and DNP3-IP Protocol Stacks, on page 68](#)
- [Starting the Protocol Translation Engine, on page 71](#)
- [Verifying the Protocol Translation Configuration, on page 71](#)

Protocol Translation

This chapter provides details about configuring Protocol Translation on the Cisco IR807 Integrated Services Router for operation within a Supervisory Control and Data Acquisition (SCADA) system.

This chapter includes the following sections:

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.

Role of the IR807

In the network, the Control Center always serves as the master in the network when communicating with the IR807. The IR807 serves as a proxy master station for the Control Center when it communicates with the RTU.

The IR807 provides IEC 60870 T101 to IEC 60870 T104 protocol translation to serve as a SCADA gateway to do the following:

- Receive data from RTUs (T101) and relay configuration commands from the Control Center (T104) to RTUs.
- Receive configuration commands from the Control Center and relay RTU data to the Control Center
- Terminate incoming T104 requests from the Control Center, when an RTU is offline.

Key Terms

The following terms are relevant when you configure the T101 and T104 protocol stacks on the IR807:

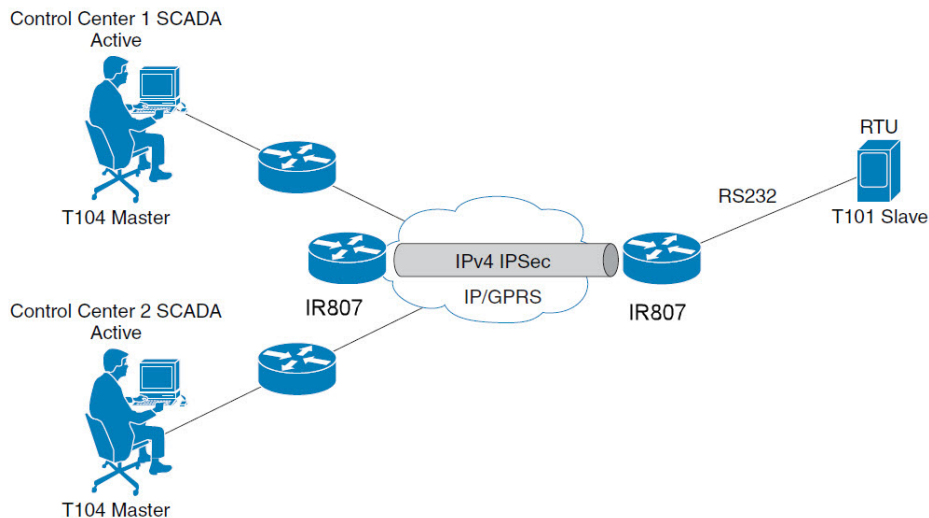
- Channel – A channel is configured on each IR807 serial port interface to provide a connection to a single RTU for each IP connection to a remote Control Center. Each connection transports a single T101 (RTU) or T104 (Control Center) protocol stack.
- Link Address – Refers to the device or station address.
- 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.

Protocol Translation Application

In [Figure 4: IR807 Routers Providing Connectivity and Security within a SCADA System](#), on page 63, the IR807 (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 IR807 connects to the RTU (slave) through a RS232 connection. The IR807 securely forwards SCADA data from the RTU to the Control Center in the SCADA system through an IPsec tunnel. You can terminate the IPsec tunnel on either a Cisco 2010 Connected Grid Router (IR807) or a head-end router (such as the Cisco ASR 1000). However, only the IR807 inspects the SCADA traffic before it forwards the traffic to the proper Control Center.

Figure 4: IR807 Routers Providing Connectivity and Security within a SCADA System



Configuring Protocol Translation

This section includes the following topics:

Enabling the IR807 Serial Port and T101 Encapsulation

Before you can enable and configure Protocol Translation on the IR807, you must first enable the serial port on the IR807 and enable SCADA encapsulation on that port (By default both the Async 0 and Async 1 in IR807 are encapsulated with SCADA only).

	Command	Purpose
1	configure terminal	Enters the global configuration mode.
2	interface serial slot/port	Enters the interface command mode for the serial port. Note: The slot/port configuration for the serial port is 1.
3	no shutdown	Brings up the port, administratively.
4	encapsulation t101	Enables encapsulation on the serial port.

EXAMPLE

This example shows how to enable Async port 0 and how to enable encapsulation on that port to support Scada communication.

```
IR807#
config terminal
```

```

IR807(config)#
interface Async 0
IR807(config-if)
#encapsulation scada
IR807(config-if)#
no shutdown
IR807(config-if)#
end

```

Configuring T101 and T104 Protocol Stacks

After enabling Protocol Translation feature on the IR807, you must configure the 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

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

	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	scada-gw protocol t101	Enters the configuration mode for the T101 protocol stack.
3	channel <i>channel_name</i>	Enters the channel configuration mode for the T101 protocol stack. <i>channel_name</i> – Identifies the channel on which the IR807 communicates to the RTU. When the entered channel name does not already exist, the system creates a new channel. Entering the no form of this command deletes the channel. However, all sessions must be deleted before deleting the channel.
4	link-mode { balanced unbalanced }	Configures the link-mode as either balanced or unbalanced. unbalanced – Refers to a data transfer initiated by the RTU. balanced – Refers to either a master or slave link mode.
5	link-addr-size { none one two }	Defines the link address size in octets.
6	bind-to-interface serial <i>slot/port</i>	Defines the IR807 serial interface on which the T101 protocol traffic is sent. <i>port</i> – Value of 0 or 1.
7	{ no } day-of-week enable	Include Day of week information in timestamps.
8	exit	Ends configuration of the channel and exits the channel configuration mode. Saves all settings.
9	session <i>session_name</i>	Enters the session configuration mode and configures the session.

	Command	Purpose
10	attach-to-channel <i>channel_name</i>	Attaches the session to the channel. Enter the same channel name that you entered in the <code>channel</code> command. <i>channel_name</i> – Identifies the channel.
11	common-addr-size { one two }	Defines the common address size in octets.
12	cot size { one two }	Defines the cause of transmission such as COT data schemes in octets.
13	info-obj-addr-size { one two three }	Defines the information object element size.
14	link-addr <i>link_address</i>	Refers to the link address of the RTU. Note: The link address entered here must be the link address of the RTU to which the serial port is connected. <i>link_address</i> – Value of 1 or 2.
15	exit	Exits the session configuration mode.
16	sector <i>sector_name</i>	Enters the sector configuration mode and identifies the sector for the RTU. <i>sector_name</i> – Identifies the sector.
17	attach-to-session <i>session_name</i>	Attaches the RTU sector to the session. Enter the same session name that you entered in the <code>session</code> command. <i>session_name</i> - Identifies the session.
19	asdu-addr <i>asdu_address</i>	Refers to the ASDU structure address of the RTU.
20	exit	Exits the sector configuration mode.
21	exit	Exits the protocol configuration mode.

EXAMPLE

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

```

IR807# configure terminal
IR807(config)#scada-gw protocol t101
IR807(config-t101)#channel t101_serial_channel_1
IR807(config-t101-channel)#link-mode unbalanced
IR807(config-t101-channel)#link-addr-size one
IR807(config-t101-channel)#bind-to-interface Async0
IR807(config-t101-channel)#no day-of-week enable
IR807(config-t101-channel)#exit
IR807(config-t101-channel)#session t101_serial_session_1
IR807(config-t101-session)#attach-to-channel t101_serial_channel_1
IR807(config-t101-session)#common-addr-size two
IR807(config-t101-session)#cot-size one
IR807(config-t101-session)#info-obj-addr-size two
IR807(config-t101-session)#link-addr 3

```

```

IR807(config-t101-session)#exit
IR807(config-t101-session)#sector t101_serial_sector_1
IR807(config-t101-sector)#attach-to-session t101_serial_session_1
IR807(config-t101-sector)#asdu-addr 3
IR807(config-t101-sector)# exit
IR807(config-t101)# exit
IR807(config)#

```

Configuring the T104 Protocol Stack

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

	Command	Purpose
1	configure terminal	Enters configuration mode.
2	scada-gw protocol t104	Enters the configuration mode for the T104 protocol.
3	channel <i>channel_name</i>	Enters the channel configuration mode for the T104 protocol. <i>channel_name</i> – Identifies the channel on which the router communicates with the Control Center. Note: When the entered channel name does not exist, IR807 creates a new channel. Entering the no form of this command deletes the channel. However, all sessions must be deleted before deleting the channel.
4	k-value <i>value</i>	Sets the maximum number of outstanding APDUs for the channel. Note: An APDU incorporates the ASDU and the channel name. <i>value</i> – Range of values from 1 to 32767. Default is 1.
5	w-value <i>value</i>	Sets the maximum number of APDUs for the channel. <i>value</i> – Range of values from 1 to 32767. Default is 1.
6	t0-timeout <i>value</i>	Defines the t0-timeout value for connection establishment on the T104 channel.
7	t1-timeout <i>value</i>	Defines the t1-timeout value for send or test on the T104 channel.
8	t2-timeout <i>value</i>	Defines the t2-timeout value for acknowledgment when the router receives no data message. Note: The t2 value must always be set to a value greater than the t1 value on the T104 channel.

	Command	Purpose
9	t3-timeout <i>value</i>	Defines the t3-timeout value for sending s idle state on the T104 channel. Note: The t3 value must always be set to a value on the T104 channel.
10	tcp-connection {0 1} local-port <i>port_number</i>	Sets the value for the Control Center as de Center.
11	{no } day-of-week enable	Include Day of week information in times
12	{no } send-ei enable	Send End of Initialization when T104 sess
13	exit	Exits the channel configuration mode.
14	session <i>session_name</i>	Enters the session configuration mode and session. <i>session_name</i> – Use the same name that yo previously.
15	attach-to-channel <i>channel_name</i>	Defines the name of the channel that trans
16	exit	Exits the session configuration mode.
17	sector <i>sector_name</i>	Enters the sector configuration mode and sector for the Control Center.
18	attach-to-session <i>session_name</i>	Attaches the Control Center sector to the <i>session_name</i> – Use the same name that yo previously.
19	asdu-addr <i>asdu_address</i>	Refers to the ASDU structure address. Val match the ASDU value on the RTU. <i>asdu_address</i> – <i>asdu_address</i>
20	map-to-sector <i>sector_name</i>	Maps the Control Center (T104) sector to
21	Return to Step 1 .	Repeat all steps in this section for each Co network.

EXAMPLE

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

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

```
IR807# configure terminal
IR807(config)#scada-gw protocol t104
```

```

IR807(config-t104)#channel t104_ip_channel_1
IR807(config-t104-channel)#k-value 12
IR807(config-t104-channel)#w-value 8
IR807(config-t104-channel)#t0-timeout 30
IR807(config-t104-channel)#t1-timeout 15
IR807(config-t104-channel)#t2-timeout 10
IR807(config-t104-channel)#t3-timeout 30
IR807(config-t104-channel)#tcp-connection 0 local-port default remote-ip any
IR807(config-t104-channel)#no day-of-week enable
IR807(config-t104-channel)#no send-ei enable
IR807(config-t104-channel)#exit
IR807(config-t104)#session t104_ip_session_1
IR807(config-t104-session)#attach-to-channel t104_ip_channel_1
IR807(config-t104-session)#exit
IR807(config-t104)#sector t104_ip_sector_1
IR807(config-t104-sector)#attach-to-session t104_ip_session_1
IR807(config-t104-sector)#asdu-addr 3
IR807(config-t104-sector)#map-to-sector t101_serial_sector_1

```

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

```

IR807(config)#scada-gw protocol t104
IR807(config-t104)#channel t104_ip_channel_2
IR807(config-t104-channel)#k-value 12
IR807(config-t104-channel)#w-value 8
IR807(config-t104-channel)#t0-timeout 30
IR807(config-t104-channel)#t1-timeout 15
IR807(config-t104-channel)#t2-timeout 10
IR807(config-t104-channel)#t3-timeout 30
IR807(config-t104-channel)#tcp-connection 0 local-port 2400 remote-ip any
IR807(config-t104-channel)#no day-of-week enable
IR807(config-t104-channel)#no send-ei enable
IR807(config-t104-channel)#exit
IR807(config-t104)#session t104_ip_session_2
IR807(config-t104-session)#attach-to-channel t104_ip_channel_2
IR807(config-t104-session)#exit
IR807(config-t104)#sector t104_ip_sector_2
IR807(config-t104-sector)#attach-to-session t104_ip_session_2
IR807(config-t104-sector)#asdu-addr 3
IR807(config-t104-sector)#map-to-sector t101_serial_sector_2

```

Configuring the DNP3-Serial and DNP3-IP Protocol Stacks

After encapsulating the interface with SCADA protocol on the IR807, you must configure the DNP3-Serial and DNP3-IP protocol stacks, which allow end-to-end communication between Control Centers (DNP3-IP) and RTUs (DNP3-Serial) within a SCADA system.

Configuring the DNP3-Serial Protocol Stack

Configure the channel and session parameters for the DNP3-Serial protocol stack.

	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	scada-gw protocol dnp3-serial	Enters configuration mode for the DNP3 serial protocol.

	Command	Purpose
3	channel <i>channel_name</i>	Enters channel configuration mode for the DN <i>channel_name</i> – Identifies the channel on wh communicates to the RTU. Note: When the entered channel name does no creates a new channel. Entering the no form of this command deletes However, all sessions must be deleted before y
4	link-addr source <i>address</i>	Configure scada-gw dnp3 serial source (Maste <i>address</i> – source address
5	request-timeout <i>timeout</i>	Timeout for request <i>timeout</i> - Timeout in second
6	link-timeout <i>timeout</i>	Timeout for link <i>timeout</i> – Timeout in second
7	{no } unsolicited-response enable	Unsolicited Response
8	bind-to-interface async <i>port</i>	Defines the IR807 async interface on which th protocol traffic. <i>port</i> – Value of 0 or 1.
9	session <i>session_name</i>	Enters session configuration mode and assigns
10	attach-to-channel <i>channel_name</i>	Attaches the session to the channel. Enter the same channel name that you entered <i>channel_name</i> – Identifies the channel.
11	link-addr dest <i>address</i>	Configure scada-gw dnp3 serial destination (S <i>address</i> - destination address
12	exit	Exits session configuration mode.
13	exit	Exits protocol configuration mode.

Example

This example shows how to configure the parameters for the DNP3-Serial protocol stack for RTU_10.

```
IR807# configure terminal
IR807(config)#scada-gw protocol dnp3-serial
IR807(config-dnp3s)#channel dnp3_serial_channel_1
IR807(config-dnp3s-channel)#link-addr source 3
IR807(config-dnp3s-channel)#request-timeout 8
IR807(config-dnp3s-channel)#link-timeout 6
IR807(config-dnp3s-channel)#unsolicited-response enable
```

```

IR807 (config-dnp3s-channel) #bind-to-interface Async1
IR807 (config-dnp3s-channel) #session dnp3_serial_session_1
IR807 (config-dnp3s-session) #attach-to-channel dnp3_serial_channel_1
IR807 (config-dnp3s-session) #link-addr dest 4
IR807 (config-dnp3s-session) #exit
IR807 (config-dnp3s) #exit

```

Configuring the DNP3-IP Protocol Stack

Configure the channel and session parameters for the DNP3-IP protocol stack.

	Command	Purpose
1	configure terminal	Enters configuration mode.
2	scada-gw protocol dnp3-ip	Enters configuration mode for the DNP3-IP protocol.
3	channel <i>channel_name</i>	Enters channel configuration mode for the DNP3-IP protocol. <i>channel_name</i> – Identifies the channel on which the IR807 communicates with the Control Center. Note: When the entered channel name does not already exist, the IR807 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.
4	link-addr dest <i>address</i>	Configure scada-gw dnp3-ip destination(Master) channel link-addr <i>address</i> - destination address Note: The address should be same as mentioned during the dnp3-serial configuration under the channel
5	no send-unsolicited-msg enable	send unsolicited messages.
6	tcp-connection local-port <i>port_number remote-ip ip</i>	Sets the value for the Control Center as defined on the Control Center
7	exit	Exits channel configuration mode.
8	session <i>session_name</i>	Enters session configuration mode and assigns a name to the session. <i>session_name</i> - Use the same name that you assigned to the channel in Step 3.
9	attach-to-channel <i>channel_name</i>	Defines the name of the channel that transports the session traffic.
D	link-addr source <i>source_address</i>	Configure scada-gw dnp3 ip source (Slave) channel link-addr <i>address</i> - source address Note: The address should be same as mentioned during the dnp3-serial configuration under the session
ll	map-to-session <i>session_name</i>	Configure lower session mapping to dnp3 serial session <i>session_name</i> – dnp3-serial session name

	Command	Purpose
2	exit	Exits session configuration mode.

Starting the Protocol Translation Engine

Prerequisites

After configuring the T101 and T104 protocols on the IR807, you can start the Protocol Translation Engine.

	Command	Purpose
1	configure terminal	Enters global configuration mode
2	scada-gw enable	Starts the Protocol Translation Engine

```
IR807# configure terminal
IR807(config)# scada-gw enable
```

Verifying the Protocol Translation Configuration

After configuring the T101 and T104 or DNP3-Serial and DNP3-IP protocols on the IR807, you can verify the configuration, using the **show running-config | sec scada-gw** command:

```
IR807#sh run | sec scada-gw
scada-gw protocol t101
  channel t101_serial_channel_1
    bind-to-interface Async0
  session t101_serial_session_1
    attach-to-channel t101_serial_channel_1
  sector t101_serial_sector_1
    attach-to-session t101_serial_session_1
scada-gw protocol t104
  channel t104_ip_channel_1
    tcp-connection 0 local-port default remote-ip any
  session t104_ip_session_1
    attach-to-channel t104_ip_channel_1
  sector t104_ip_sector_1
    attach-to-session t104_ip_session_1
  map-to-sector t101_serial_sector_1
scada-gw protocol dnp3-serial
  channel dnp3_serial_channel_1
    unsolicited-response enable
    bind-to-interface Async1
  session dnp3_serial_session_1
    attach-to-channel dnp3_serial_channel_1
scada-gw protocol dnp3-ip
  channel dnp3_ip_channel_1
    tcp-connection local-port default remote-ip any
  session dnp3_ip_session_1
    attach-to-channel dnp3_ip_channel_1
```

```
map-to-session dnp3_serial_session_1
scada-gw enable
```



CHAPTER 7

Alarms

This chapter provides instructions for configuring the alarms on the IR807.

- [Alarms, on page 73](#)
- [Information About Alarms , on page 73](#)
- [Alarm Port, on page 73](#)
- [Alarm Conditions, on page 73](#)
- [Configuration Examples, on page 75](#)

Alarms

This chapter provides instructions for configuring the alarms on the IR807.

Information About Alarms

If the conditions present on the IR807 do not match the set parameters, the IR807 software triggers an alarm or a system message. By default, the IR807 software sends the system messages to a system message logging facility, or a syslog facility. You can also configure the IR807 to send Simple Network Management Protocol (SNMP) traps to an SNMP server.

Alarm Port

The IR807 has an alarm port on the front of the device. Additional details and instructions about connecting the alarm ports are found in the [IR807 Hardware Configuration Guide](#) .

Alarm Conditions

There are two conditions that generate an alarm:

- If the alarm is connected to a door switch or an enclosure and detects a door opening.
 - This is an external alarm and requires wiring. See the IR807 Hardware Installation Guide.
- When the internal temperature is too high.

- This is an internal alarm, no wiring required.

When either condition is met, the alarm LED turns red, and a syslog message and SNMP trap is triggered if configured.

SNMP Traps

SNMP is an application-layer protocol that provides a message format for communication between managers and agents. The SNMP system consists of an SNMP manager, an SNMP agent, and a management information base (MIB).

The `snmp-server enable traps` command can be changed so that the user can send alarm traps to an SNMP server. You can use alarm profiles to set environmental or port status alarm conditions to send SNMP alarm traps.

Syslog Messages

You can use alarm profiles to send system messages to a syslog server.

Configuration Commands

You can set the alarm severity to critical, major, minor, or none. The severity is included in the alarm message when the alarm is triggered.

You must first have an SNMP server setup to send SNMP messages to. Refer to the following documentation for instructions:

<https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/15-mt/snmp-15-mt-book/nm-snmp-cfg-snmp-support.html>

To configure and show alarms on the IR807, use the Command Line Interface (CLI).

Command	Purpose
<code>configure terminal</code>	Enters global configuration mode.
<code>alarm contact</code> <i>contact-number</i> description <i>string</i>	(Optional) Configures a description for the alarm contact number. The <i>contact-number</i> value is from 1 to 4. The description string is up to 80 alphanumeric characters in length and is included in any generated system messages.
<code>alarm contact</code> { <i>contact-number</i> / all } { severity critical major / minor none } trigger closed / open }}	Configures the trigger and severity for an alarm contact number or for all contact numbers. Enter a contact number (1 to 4) or specify that you are configuring all alarms. For severity , enter critical , major , minor or none . If you do not configure a severity, the default is minor . For trigger , enter open or closed . If you do not configure a trigger, the alarm is triggered when the circuit is closed .
<code>end</code>	Returns to privileged EXEC mode.
<code>show env alarm-contact</code>	Shows the configured alarm contacts.

Command	Purpose
<code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

Configuration Examples

Configure an alarm.

```
IR807#conf term
Enter configuration commands, one per line. End with CNTL/Z.
IR807(config)#alarm-contact 1 description

Your Descriptive Text Here
IR807(config)#alarm-contact 1 severity critical

IR807(config)#alarm-contact 1 trigger closed

IR807#
```

To show the alarm status:

```
IR807#show environment alarm-contact
!
No Alarm Present
ALARM CONTACT
  Status:      Not Asserted
  Description: Test Input Alarm
  Severity:    Critical
  Trigger:     Closed
```

Example of an alarm being generated:

```
IR807# !
*Nov 27 14:54:52.573: %IR800_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External alarm
asserted, Severity: Critical
```

To show the alarm status during an event:

```
IR807#show environment alarm-contact
ALARM CONTACT
  Status:      Asserted
  Description: Test Input Alarm
  Severity:    Critical
  Trigger:     Closed
```

Example of an alarm being cleared:

```
IR807# !
*Nov 27 14:55:02.573: %IR800_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_CLEAR: External alarm
cleared
IR807#
```

Enabling SNMP Traps

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	snmp-server enable traps alarms	Enables the switch to send SNMP traps.
3	end	Returns to privileged EXEC mode.
4	show alarm settings	Verifies the configuration.
5	copy running-config startup-config	(Optional) Saves your entries in the configuration file.



CHAPTER 8

Plug and Play (PnP)

Plug N Play Cloud Service is a Cisco hosted service for customers to configure devices shipped from Cisco. Configurations include specifying a Controller (APIC-EM) and a Configuration file.

- [Plug and Play \(PnP\), on page 77](#)
- [PNP using Ethernet, on page 77](#)

Plug and Play (PnP)

Plug N Play Cloud Service is a Cisco hosted service for customers to configure devices shipped from Cisco. Configurations include specifying a Controller (APIC-EM) and a Configuration file. An option was added to the **bundle install** command:

bundle install <bundle_image_name> rom-autoboot

When this option is specified, the IOS system image to boot will NOT be written into the running-config. Instead, it will be set into the rommon BOOT variable (BOOT=<system_image>) ONLY.

After **bundle install <bundle_image_name> rom-autoboot** and **write erase** commands, when the device reloads it will automatically boot up the IOS image saved in rommon BOOT. This also ensures the device does not have any startup configuration when it boots up so it will allow PNP to start up.

PNP can be started either using Ethernet or cellular 4G. If connected to both, Ethernet will take precedence over Cellular 4G.

PNP using Ethernet

PNP using Ethernet can be done in three different ways:

1. Specifying OPTION 43 on DHCP ROUTER

Example: **option 43 ascii 5A1D;B2;K4;I<APIC-EM_IP_ADDRESS>;J80**

1. Specifying DNS on DHCP ROUTER

Example: **domain-name test.com**

```
#conf t
#ip host pnpserver.test.com <APIC-EM address>
```

1. Specifying CCO's address by configuring devicehelper.cisco.com on DHCP ROUTER

```
#conf t
#ip host devicehelper.cisco.com <CCO_address>
```

PNP using 4G cellular can be done by configuring the device information (Serial number, PID and controller profile-APIC-EM) on CCO.

Once PNP is completed, issue a **write mem** command to save the configuration. PNP pushes the configuration but does not save it. The configuration must be saved after PNP is successfully completed.

To verify if PNP is completed or not, verify with the **sh run** command. At the bottom of the command output, there should be a pnp profile and the APIC EM address. This means the device was redirected to APIC-EM and the initial PNP was successfully done. Now once the configuration file is pushed from APIC-EM, verify this using the **sh pnp task** command and verify the Config-Upgrade Task should have Result: Success.

Note: The device should not be interrupted until PNP is completed. If the device is interrupted, PNP will stop. If at any point something goes wrong, reload the router without saving the configuration and PNP will start once again. Once PNP is completed it is necessary to save the configuration by issuing the **write mem** command.

```
IR800#sh run | b pnp
pnp profile pnp-zero-touch
transport https ipv4 172.27.122.132 port 443
end
IR800#sh pnp task
----- show pnp tasks -----
Certificate-Install Task - Last Run ID:5, ST:7201, Result:Success,
LT:117562, ET:4 ms
Src:[-], Dst:[-]
Device-Auth Task - Never Run
Device-Info Task - Last Run ID:9, ST:5301, Result:Success, LT:200634, ET:1 ms Src:[udi],
Dst:[pnp-zero-touch]
Image-Install Task - Never Run
SMU Task - Never Run
Config-Upgrade Task - Last Run ID:10, ST:5202, Result:Success, LT:267420, ET:984 ms
Src:[https://192.168.1.1:443/api/v1/file/onetimedownload/1530b4e5-beb8-4db3-b4df-28dc016464fc],
Dst:[running]
CLI-Config Task - Never Run
Licensing Task - Never Run
File-Transfer Task - Never Run
Redirection Task - Never Run
CLI-Exec Task - Last Run ID:12, ST:5401, Result:Success, LT:279464, ET:1 ms
Src:[cli-exec request], Dst:[running-exec]
Script Task - Never Run
```




CHAPTER 9

Configuring Virtual-LPWA

This chapter describes the details of configuring virtual-LPWA (VLPWA) interface on the IR807 series for the configuration of the Cisco LoRaWAN Gateway.

- [Configuring Virtual-LPWA, on page 79](#)
- [Configuring Virtual-LPWA Interface on the IR807 Series, on page 79](#)
- [Configuring SNMP TRAP for Modem Notifications, on page 83](#)
- [Configuring VLPWA Interface and Associated Cisco LoRaWAN Gateway, on page 84](#)
- [Configuring Clock for the Cisco LoRaWAN Gateway, on page 86](#)
- [Configuring Cisco LoRaWAN Gateway Timezone, on page 86](#)
- [Configuring IPSec on the Cisco LoRaWAN Gateway, on page 87](#)
- [Configuring SCEP on the Cisco LoRaWAN Gateway, on page 88](#)
- [Configuring Security Protection, on page 90](#)
- [Managing the Cisco LoRaWAN Gateway, on page 90](#)
- [Monitoring the LoRaWAN Gateway, on page 94](#)
- [Debugging the LoRaWAN Modem, on page 98](#)

Configuring Virtual-LPWA

This chapter describes the details of configuring virtual-LPWA (VLPWA) interface on the IR807 series for the configuration of the Cisco LoRaWAN Gateway.

This chapter contains the following sections:

Configuring Virtual-LPWA Interface on the IR807 Series

The Cisco LoRaWAN Gateway is connected to IR807 series via an Ethernet cable with PoE+ to work as a LoRaWAN gateway. By creating a VLPWA interface on the IR807 series, you can:

- Manage hardware and software of the Cisco LoRaWAN Gateway.
- Send and receive VLPWA protocol modem message to monitor the status of the Cisco LoRaWAN Gateway.
- Send SNMP traps to the IoT Field Network Director (IoT FND).

Note: You need to install the Activity Thingpark LRR software as the LoRa forwarder firmware, which is loaded through the Cisco IOS software, for the Cisco LoRaWAN Gateway to work.

Note: Refer to the LoRa Alliance LoRaWAN 1.0 specifications for more information.

You can find other documentation for the Cisco LoRaWAN Gateway at:

<http://www.cisco.com/c/en/us/support/routers/interface-module-lorawan/tsd-products-support-series-home.html>

Configuring Ethernet Interface and Creating VLPWA Interface

When you configure IP address for the Ethernet interface or Vlan interface, the IP address allocated must be aligned with the prefix configured for the DHCP pool allocated to the LoRaWAN interface.

The Cisco LoRaWAN Gateway communicates through IOS, therefore a private IPv4 address is assigned with NAT being configured.

Configuring IR807 for One Cisco LoRaWAN Gateway

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface on IR807 and create the VLPWA interface for one Cisco LoRaWAN Gateway.

Step	Command	Purpose
1	configure terminal	Enters global configuration mode.
2	interface FastEthernet <i>ID</i>	Configures the Fast Ethernet (FE) port.
3	ip address <i>address mask</i>	Configures the GE interface IP address. Note: The IP address should be the default DHCP pool.
4	ip nat inside	Identifies the interface as the NAT inside.
5	ip virtual-reassembly in	Enables virtual fragment reassembly (VFR).
6	exit	Exits to global configuration mode.
7	interface Virtual-LPWA <i>vlpwa-id</i>	Creates VLPWA interface. Note: The value of vlpwa-id should be a unique number which is specified in DHCP pool.
8	end	Exits to privileged EXEC mode.
9	write memory	Saves the configurations.

Configuring IR807 for Multiple Cisco LoRaWAN Gateways

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface on IR807 and create the VLPWA interface for multiple Cisco LoRaWAN Gateways.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface FastEthernet <i>ID</i>	Configures the Fast Ethernet (FE) port.

Step	Command or Action	Purpose
3	no shutdown	Enables the interface.
4	exit	Exits to privileged EXEC mode.
5	interface FastEthernet <i>ID.subID</i>	Configures sub-interface on the FE port.
6	encapsulation dot1Q <i>vlpwa-id native</i>	Configures IEEE802.1Q encapsulation of traffic on a interface.
7	ip address <i>address mask</i>	Configures the FE interface IP address. Note: The IP address should be the default router address in its associated DHCP pool.
8	ip nat inside	Identifies the interface as the NAT inside interface.
9	ip virtual-reassembly in	Enables virtual fragment reassembly (VFR) on the interface.
10	exit	Exits to global configuration mode.
11	interface Virtual-LPWA <i>vlpwa-id</i>	Creates VLPWA interface. Note: The value of <i>vlpwa-id</i> should be the same as the option 43 hex number which is specified in DHCP pool.
12	end	Exits to privileged EXEC mode.
13	write memory	Saves the configurations.

Configuring DHCP Pool for the Cisco LoRaWAN Gateway

The Cisco LoRaWAN Gateway connects to the IR807 series through the Ethernet interface. The communication between Cisco LoRaWAN Gateway firmware and IOS are conducted over IP. Therefore, an IP address must be assigned to the Cisco LoRaWAN Gateway through an IOS local DHCP server pool.

If you connect multiple Cisco LoRaWAN Gateways to a single IR807 router, each interface must have its own DHCP pool.

On the IR807 series, beginning in privileged EXEC mode, follow these steps to configure DHCP pool.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	ip dhcp pool <i>pool-name</i>	Creates a DHCP server address pool and enters DHCP pool configuration mode. Note: If you have changed the parameters of the DHCP server, you must perform a refresh using the no service dhcp <i>interface-type number</i> command and service dhcp <i>interface-type number</i> command.
3	network <i>network-number mask</i>	Specifies the subnet network number and mask of the DHCP address pool. Make sure to allow only one dhcp address releasable to modem.

Step	Command or Action	Purpose
4	<code>default-router address</code>	Specifies the IP address of the default router for a DHCP client. The default router address will be assigned to the associated VLAN interface afterwards.
5	<code>option 43 hex client-ID</code>	Enables vendor specific option 43 and assign the associated Cisco LoRaWAN Gateway client ID number as the hex value.
6	<code>dns-server address</code>	Defines DNS services.
7	<code>exit</code>	Exits to global configuration mode.
8	<code>ip dhcp excluded-address address</code>	Masks all redundant addresses including the default router in DHCP pool.
9	<code>end</code>	Exits to privileged EXEC mode.
10	<code>write memory</code>	Saves the configurations.

Examples

The following is an example of configuring DHCP pool on IR807:

```
IR807#configure terminal
IR807 (config)#ip dhcp pool modempool
IR807 (dhcp-config)#network 192.168.1.0 255.255.255.248
IR807 (dhcp-config)#default-router 192.168.1.1
IR807 (dhcp-config)#option 43 hex 01
IR807 (dhcp-config)#dns-server 192.168.1.1
IR807 (dhcp-config)#exit
IR807 (config)#
IR807 (config)#ip dhcp excluded-address 192.168.1.1
IR807 (config)#ip dhcp excluded-address 192.168.1.3 192.168.1.6
IR807 (config)#exit
IR807#
```

The following is an example on IR807 using the sub-interface method:

```
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.3 192.168.1.6
!
ip dhcp pool modempool1
network 192.168.1.0 255.255.255.248
default-router 192.168.1.1
option 43 hex 01
!
interface Virtual-LPWA1
!
interface FastEthernet1.101
encapsulation dot1Q 101 native
ip address 192.168.1.1 255.255.255.248
ip nat inside
ip virtual-reassembly in
!
end
```

The following is an example on IR807 using the VLAN method:

```

ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.3 192.168.1.6
!
ip dhcp pool modempool1
 network 192.168.1.0 255.255.255.248
 default-router 192.168.1.1
 option 43 hex 01
!
interface Virtual-LPWA1
!
interface FastEthernet1
 switchport access vlan 101
!
interface Vlan101
 ip address 192.168.1.1 255.255.255.248
!
end

```

Configuring SNMP TRAP for Modem Notifications

On the IR807 series, beginning in privileged EXEC mode, follow these steps to enable SNMP TRAP notifications for virtual-lpwa interface and its associated Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	snmp-server enable traps vlpwa	Enables virtual LPWA traps to monitor modem status changing.
3	snmp-server enable traps snmp linkup linkdown	Enables linkUp and linkDown traps to monitor modem heartbeat event.
4	end	Exits to privileged EXEC mode.
5	write memory	Saves the configurations.

The Modem feature status notifications and OIDs are listed in the following table:

Notification	OID
modem door open/close	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 1 };
modem exceeds maximum temperature threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 2 };
modem temperature returns to normal from overheat	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 3 };
modem falls below minimum temperature threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 4 };
modem temperature returns to normal from undercooling	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 5 };
modem FPGA upgrade starts	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 6 };
modem exceeds maximum CPU threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 7 };

Notification	OID
modem CPU usage returns to normal	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 8 };
modem exceeds maximum memory threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 9 };
modem memory usage returns to normal	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 10 };
modem exceeds maximum storage threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 11 };
modem storage usage returns to normal	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 12 };

When the SNMP linkUp and linkDown traps are enabled, the modem device status could be monitored. The modem device status notifications are listed below:

modem power on/off	interface FastEthernet_ID linkUp/linkDown
modem agent heartbeat	interface virtual-lpwa_ID linkUp/linkDown

Configuring VLPWA Interface and Associated Cisco LoRaWAN Gateway

On the IR807 series, beginning in privileged EXEC mode, follow these steps to configure one or multiple VLPWA interfaces and associated Cisco LoRaWAN Gateways.

Note: The following set-up refers to the Thingpark LoRa Forwarder software. When configuring the virtual-lpwa interface with other 3rd party network server, refer to the 3rd party vendor documentation.

Configuring IR807 for One Cisco LoRaWAN Gateway

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface Virtual-LPWA <i>vpwa-id</i>	Enters the vpwa interface which is to be configured.
3	lpwa modem environment <i>var1</i> [<i>var2</i>]	Specify the environment variables as the configuration for the LoRaWAN modem. Note: There are one or two environment variables to be configured.

Step	Command or Action	Purpose
4	lpwa packet-forwarder firmware [flash: nvram:] <i>firmware-name</i> auto-install [<i>if-not-installed</i> / <i>unconditional</i>]	Configures the packet-forwarder firmware (only Activity LRR is supported) which will be installed on the LoRaWAN modem from the IR807 series. For the values of auto-install method: <ul style="list-style-type: none"> • <i>if-not-installed</i> —Automatically install if there is no firmware already installed on modem. • <i>unconditional</i> —Automatically install this firmware unconditionally.
5	lpwa packet-forwarder public-key [flash: nvram:] <i>public-key file</i>	Configures the packet-forwarder public-key which will be installed on the LoRaWAN modem from the IR807 series.
6	end	Exits to privileged EXEC mode.
7	write memory	Saves the configurations.

Examples

The following is an example of configuring VLPWA interface on IR807:

```
interface Virtual-LPWA1
no ip address
lpwa packet-forwarder public-key flash:lrr-opk.pubkey
lpwa modem environment PKTFWD_ROOT /tmp/mdm/pktfwd/firmware
lpwa modem environment LXC_STORE_PATH /tmp/mdm/pktfwd/firmware/usr/etc/lrr
lpwa modem password root $l$0822455D0A16
lpwa modem ntp server ip fr.pool.ntp.org
lpwa modem timezone Europe/Paris
```

Configuring Cisco LoRaWAN Gateway Password

On the IR807 series, beginning in privileged EXEC mode, follow these steps to configure password for the Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface Virtual-LPWA <i>vpwa-id</i>	Enters the vpwa interface which is to be configured.
3	lpwa modem password <i>var1</i> [<i>var2</i>]	Specifies the password variables as the configuration for the LoRaWAN modem. The default account is root . Note: There are one or two environment variables to be configured. But currently only the root account is supported.

Step	Command or Action	Purpose
4	<code>lpwa modem password root [var2]</code>	Configures the password of the root account for LoRaWAN modem. The default password is NULL. The unencrypted (clear text) secret has the minimum length of 4 characters, and the maximum length of 25 characters.
5	<code>end</code>	Exits to privileged EXEC mode.
6	<code>write memory</code>	Saves the configurations.

Configuring Clock for the Cisco LoRaWAN Gateway

The modem clock can use either NTP or the GPS as its source. The default source is NTP.

Configuring NTP Server for the Cisco LoRaWAN Gateway

On the IR807 series, beginning in privileged EXEC mode, follow these steps to configure the NTP server for the Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	<code>configure terminal</code>	Enters global configuration mode.
2	<code>interface Virtual-LPWA vlpwa-id</code>	Enters the vlpwa interface which is to be configured.
3	<code>lpwa modem ntp server ip [var1]</code>	Specifies the NTP server variables as the configuration for the LoRaWAN modem. For the hostname of peer, refer to www.pool.ntp.org . Example: <code>lpwa modem ntp server ip 0.asia.pool.ntp.org</code>
4	<code>lpwa modem ntp server address [var2]</code>	Configures the IP address of peer. Example: <code>lpwa modem ntp server address 192.168.1.1</code>
5	<code>end</code>	Exits to privileged EXEC mode.
6	<code>write memory</code>	Saves the configurations.

Configuring Cisco LoRaWAN Gateway Timezone

On the IR807 series, beginning in privileged EXEC mode, follow these steps to configure timezone for the Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface Virtual-LPWA <i>vlpwa-id</i>	Enters the vlpwa interface which is to be configured.
3	lpwa modem timezone [<i>timezone</i>]	Specifies the timezone variables as the configuration for the LoRaWAN modem. The value is based on the IANA Timezone database. Please check the /usr/share/zoneinfo/ folder in your PC host. <i>timezone</i> —Name of time zone, for example, Asia/Shanghai. Example: <code>lpwa modem timezone Asia/Shanghai</code>
4	end	Exits to privileged EXEC mode.
5	write memory	Saves the configurations.

Configuring IPsec on the Cisco LoRaWAN Gateway

In virtual-lpwa mode, IPsec is set to protect the communications between the LoRaWAN gateway and the IR800 router.

On the IR800 series, beginning in privileged EXEC mode, follow these steps to configure IPsec for the Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface Virtual-LPWA <i>vlpwa-id</i>	Enters the vlpwa interface which is to be configured.
3	lpwa modem ipsec enable	Enables IPsec. By default, IPsec is disabled.
4	lpwa modem isakmp <i><xauth-user></i> <i><xauth-pw></i> <i><peer-ip></i> group <i><name></i> <i><psk-key></i> <i><lifetime></i>	Specifies the XAUTH credential's username, password, and the IP address of the right participant's interface. Matches this information to the IKEID group with group name, pre-shared key for remote peer, and lifetime in seconds.
5	end	Exits to privileged EXEC mode.
6	write memory	Saves the configurations.

Note: Only PSK (IKEv1) and RSA (IKEv2) are supported.

Configuring SCEP on the Cisco LoRaWAN Gateway

On the IR807 series, beginning in privileged EXEC mode, use these commands to configure Simple Certificate Enrollment Protocol (SCEP) on the Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface Virtual-LPWA <i>vlpwa-id</i>	Enters the vlpwa interface which is to be configured.

Step	Command or Action	Purpose
3	<p>Configure SCEP by using a configuration file or profile method. Choose one of the following:</p> <ul style="list-style-type: none"> • ipwa modem scep [flash:nvram: <SCEP_Configuration_File>] • ipwa modem scep [profile] 	<p>To configure by file, enter the SCEP configuration file. This file must be provided with the following formatted:</p> <pre>url <SCEP server URL used for enrollment> country <2 letter country name> province <Province/State> locality <Location> organization <Organization> unit <Organization Unit> common-name <Common Name> type <SCEP server type: NDES> persistent <Store certificates in modem; default is false> key-length <Length of keys; 1024, 2048 (default) or 4096></pre> <p>Example:</p> <p>ipwa modem scep flash:scep_conf</p> <p>SCEP Configuration File Example:</p> <pre>url http://172.19.234.54:80/certsrv/mscep/mscep.dll country CN province Nanning locality Nanning organization Cisco unit iot common-name cisco-iot type ndes persistent false key-length 1024</pre> <p>To configure the parameters individually, use the profile method.</p> <pre>IR807(config-if)#ipwa modem scep profile IR807(config-if-vlpwa-scep)#? Enter parameters for scep. country, locality, name, org, province, unit & url must all be present. country Country server located in default Set a command to its defaults exit Exit from if-vlpwa-scep sub mode keylen Specify key length 1024, 2048 or 4096 locality Locality of server name Name of the certificate no Negate a command or set its defaults organization Organization of the server persistent Specify persistency of the key province State or Province type Specify type unit Business unit within server organization url Specify url</pre> <p>Note: In either file or profile method, “ndes” is the default and only supported SCEP type. However, you can enter SCEP type as xpki in either method. This option may or may not work. It has not been tested and will not be officially supported until a future release.</p>
4	end	Exits to privileged EXEC mode.

Step	Command or Action	Purpose
5	write memory	Saves the configurations.

Note: Only PSK (IKEv1) and RSA (IKEv2) are supported.

Note: Without SCEP, the IPSec is done with pre-shared key. With SCEP, IPSec is done with RSA or certificates.

Configuring Security Protection

On the IR807 series, beginning in privileged EXEC mode, use these commands to configure security protection for the Cisco LoRaWAN Gateway.

Step	Command or Action	Purpose
1	configure terminal	Enters global configuration mode.
2	interface Virtual-LPWA <i>vlpwa-id</i>	Enters the vlpwa interface which is to be configured.
3	lpwa modem authentication mandatory enable	Enables mandatory security level in modem, which is disabled by default. When enabled, IR807 will shut down corresponding vlan or subinterface for ACT2 authentication failure or version mismatch to prevent further attacking. When disabled, IR807 will only send notifications to IoT FND when the same situations happen, without shutting down vlan or subinterface.
4	lpwa modem authentication timeout <i><subinterface/vlan name></i> > <i><subinterface/vlan number></i> time <i><time></i>	Specifies a timeout protection for a suspended vlpwa interface (one with no traffic up from corresponding vlan or subinterface). You need to set the subinterface or vlan manually with a time (in minute) threshold. If the mandatory security level is also enabled, the corresponding vlan or subinterface will be shut down after the time threshold. If the mandatory security level is disabled, only a notification will be sent to IoT FND.
5	end	Exits to privileged EXEC mode.
6	write memory	Saves the configurations.

Managing the Cisco LoRaWAN Gateway

Note: virtual-lpwa vlpwa-id packet-forwarder install and uninstall are not supported.

On the IR807 series, beginning in privileged EXEC mode, use these commands to manage the Cisco LoRaWAN Gateway.

Command	Purpose
virtual-lpwa <i>vlpwa-id</i> [modem packet-forwarder]	Management for the LoRaWAN modem virtual-LPWA interface: <ul style="list-style-type: none"> • modem—Manage the modem clock. • packet-forwarder—Manage the packet forwarder.
virtual-lpwa <i>vlpwa-id</i> modem [cacert clock delete install reboot upload]	Management for the LoRaWAN modem: <ul style="list-style-type: none"> • cacert—Clean the certificates stored in the modem. • clock—Manage the modem clock. • delete—Delete uploaded file(s) on the modem. • install—Install the modem firmware. • reboot—Reboot the modem hardware. • upload—Upload a file to the modem.
virtual-lpwa <i>vlpwa-id</i> packet-forwarder [restart start stop]	Management for the LoRaWAN modem packet-forwarder: <ul style="list-style-type: none"> • restart—Restart packet-forwarder. • start—Start packet-forwarder. • stop—Stop packet-forwarder.
virtual-lpwa <i>vlpwa-id</i> modem clock set hh:mm:ss {dd Mon yyyy}	Management the clock for the LoRaWAN modem: <p>hh:mm:ss—Current time.</p> <p>dd Mon yyyy—Day, month, and year.</p> <p>Example:</p> <pre>modem clock set 20:30:30 31 Mar 2016</pre>

Examples

The following is an example of setting the clock for the Cisco LoRaWAN Gateway:

```
IR807#virtual-lpwa 10 modem clock set 12:02:40 15 Apr 2016
Name: Virtual-LPWA 10
```

The following is an example of rebooting the Cisco LoRaWAN Gateway:

```
IR807#virtual-lpwa 10 modem reboot
Name: Virtual-LPWA 10
Modem reboot initiated.
```

The following is an example of restarting packet-forwarder:

```
IR807#virtual-lpwa 10 packet-forwarder restart
Name: Virtual-LPWA 10
Restarted
```

LoRaWAN Modem Firmware Upgrade

There are three methods to upgrade the LoRaWAN modem firmware image:

- Normal—It takes over 5 minutes to install the image.
- TFTP server—It takes over 3 minutes to install the image.
- External TFTP server—It takes more time than the other two methods, considering the unexpected network accessibility of a user-customized TFTP server.

Use the **virtual-lpwa 1 modem install firmware** command to upgrade the Cisco LoRaWAN Gateway firmware. The following upgrade options are available:

- external-tftp-factory—Install the firmware from external tftp and wipe user data on the LoRaWAN modem.
- external-tftp-normal—Install the firmware from external tftp and keep user data on the LoRaWAN modem.
- factory—Install the firmware and wipe the user data on the LoRaWAN modem.
- normal—Install the firmware and keep the user data on the LoRaWAN modem.
- tftp-factory—Upload the firmware image via tftp, install the firmware, and wipe user data on the LoRaWAN modem.
- tftp-normal—Upload the firmware image via tftp, install the firmware, and keep user data on the LoRaWAN modem.

Example

- Normal install:

```
IR807#virtual-lpwa 1 modem install firmware normal flash:ixm_mdm_i_k9-1.0.tar.gz
Name: Virtual-LPWA 1
Modem image installed successfully
The modem will reboot in 10 s.
IR807#
```

- TFTP install:

```
IR807 (config)#tftp-server flash:ixm_mdm_i_k9-1.0.tar.gz
IR807#virtual-lpwa 1 modem install firmware tftp-normal flash:ixm_mdm_i_k9-1.0.tar.gz
Name: Virtual-LPWA 1
Modem image installed successfully
The modem will reboot in 10 s.
IR807#
```

- External TFTP install (for which you need to manually enter the file URL):

```
IR807 (config)#tftp-server flash:ixm_mdm_i_k9-1.0.tar.gz
IR807#virtual-lpwa 1 modem install firmware external-tftp-normal
10.10.10.10:ixm_mdm_i_k9-1.0.tar.gz
Name : Virtual-LPWA 1
Modem image installed successfully
The modem will reboot in 10 s.
IR807#
```

Installing U-boot

To install u-boot with the firmware image or by itself, use the following command:

```
IR807#install firmware factory flash:ixm_mdm_i_k9-1.0.06.tar.gz
{only-u-boot
|u-boot
}
```

```

only-uboot  install uboot only
uboot       install uboot together
<cr>

```

If you execute the command without any u-boot parameters, only the firmware image will be installed.

LoRaWAN Gateway FPGA Upgrade

Every released Cisco LoRaWAN Gateway firmware image includes the FPGA image for RF board. When the image is installed successfully, the Cisco LoRaWAN Gateway will auto-reboot and start to upgrade the FPGA when bring up.

Note: The FPGA upgrade needs about 20 minutes to be finished. During this time, LRR can't work until the upgrade is completed. The FPGA upgrade will only happen if version differs.

You can check the status of the FPGA upgrade using the **show virtual-lpwa 1 modem info** command or **show virtual-lpwa 1 modem status** command.

Example

```

IR807#show virtual-lpwa 1 modem info
Name : Virtual-LPWA 1
ModemImageVer : 1.0
BootloaderVer : 20160708_cisco
ModemAgentVer : 1.02
SerialNumber : FOC20133FK0
PID : IXM-LORA-800-H-V2
UTCtime : 00:02:56.492 UTC Sat Aug 06 2016
IPv4Address : 10.20.20.4
IPv6Address : none
FPGAVersion :          ! Blank when FPGA is upgrading
TimeZone : CEST
LocalTime : Sat Aug 6 02:02:56 CEST 2016
ACT2 Authentication : PASS
IR807#show virtual-lpwa 1 modem status
Name : Virtual-LPWA 1
Status : Running
Uptime : 0:04:11.050000
Door : DoorClose
Upgrade Status : Ready  fpga upgrading -14.2%
IR807#show virtual-lpwa 1 modem info | begin IPv6
IPv6Address : none
FPGAVersion : 48          ! Correct FPGA version is displayed when upgrade is complete
TimeZone : CEST
LocalTime : Sat Aug 6 02:32:23 CEST 2016
ACT2 Authentication : PASS
IR807#

```

Uploading a File to the LoRaWAN Gateway

Customized files from the LRR package, for example, lrr.ini or custom.ini (AES key for geo-location), can be loaded from IOS if necessary by using the **virtual-lpwa 1 modem upload flash:filename** command.

Example

```

IR807# virtual-lpwa 1 modem upload flash:lgwx8_us920.ini

```

```
Name : Virtual-LPWA 1
Uploaded successfully
```

The environment variables should be defined correctly using the following commands:

```
IR807# configure terminal
IR807(config)#interface virtual-LPWA 1
IR807(config-if)#lpwa modem environment PKTFWD_ROOT /tmp/mdm/pktfwd/firmware/
IR807(config-if)#lpwa modem environment LXC_STORE_PATH /tmp/mdm/pktfwd/firmware/usr/etc/lrr
IR807(config-if)#exit
```

After proper installation of the LRR package, the output of the command shows the directory that contains customized files:

```
IR807# show virtual-lpwa 1 modem uploads
Name : Virtual-LPWA 1
Current folder: '/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr'
_parameters.sh
_system.sh
autoreboot_last
channels.ini
custom.ini
lgw.ini
lrr.ini
sysconfig_done
IR807# show virtual-lpwa 1 modem uploads detail
Name : Virtual-LPWA 1
Current folder: '/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr'
total 32
-rw-r--r-- 1 root root 143 Aug 11 20:26 _parameters.sh
-rw-r--r-- 1 root root 20 Aug 11 20:26 _system.sh
-rw-r--r-- 1 root root 0 Aug 16 09:33 autoreboot_last
-rw-rw-r-- 1 sshd sshd 2000 Aug 5 16:15 channels.ini
-rw-rw-r-- 1 sshd sshd 275 Aug 5 15:35 custom.ini
-rw-rw-r-- 1 sshd sshd 1576 Aug 5 16:18 lgw.ini
-rwxrwxr-x 1 sshd sshd 8017 Aug 24 13:53 lrr.ini
-rw-r--r-- 1 root root 29 Aug 11 20:26 sysconfig_done
IR807#
```

Monitoring the LoRaWAN Gateway

On the IR807 series, beginning in privileged EXEC mode, use these commands to monitor the Cisco LoRaWAN Gateway.

Command	Purpose
show virtual-lpwa <i>vlpwa-id</i> modem [<i>gps</i> <i>info</i> <i>ipsec</i> <i>led</i> <i>log</i> <i>statistics</i> <i>status</i> <i>uploads</i>]	Displays the information of the LoRaWAN modem: <ul style="list-style-type: none"> • gps—Displays modem GPS information. • info—Displays modem information. • ipsec—Displays modem IPsec status and detailed information. • led—Displays modem LED information. • log—Displays modem logs. • statistics—Displays modem statistics. • status—Displays modem status. • uploads—Lists uploaded files.

Command	Purpose
show virtual-lpwa vlpwa-id packet-forwarder [info log status]	Displays the information of the LoRaWAN modem packet-forwarder software: <ul style="list-style-type: none"> • info—Displays packet-forwarder information. • log—Displays packet-forwarder logs. • status—Displays packet-forwarder status.

Examples

The following is a sample output of the **show virtual-lpwa 4 modem info** command, which displays the modem information:

```
IR807# show virtual-lpwa 4 modem info
Name : Virtual-LPWA 4
ModemImageVer : 1.0.20
BootloaderVer : 20160830_cisco
ModemAgentVer : 1.02
SerialNumber : FOC20522TRZ
PID : IXM-LPWA-900-16-K9
UTCtime : 22:51:15.493 UTC Mon Feb 27 2017
IPv4Address : 192.168.4.2
IPv6Address : none
FPGAVersion : 58
TimeZone : UTC
LocalTime : Mon Feb 27 22:51:15 UTC 2017
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x2876fd04 MSB = 0x00f1400e
LoRaSerialNumber : FOC20522TUV
LoRaCalc :
<NA,NA,NA,56,38,111,102,94,85,77,69,59,50,40,31,22-NA,NA,NA,55,37,110,101,93,84,76,68,58,49,39,30,21>
CalTempCelsius : 34
CalTempCodeAD9361 : 91
RSSIOffset : -204.00,-204.00
-202.00,-202.00
AESKey : 1E5E364646EC3C3927F234FA8E200B3C
```

The following is sample outputs of the **show virtual-lpwa 3 modem log** commands, which display the modem logs:

```
IR807# show virtual-lpwa 3 modem log ?
  list  Modem log list
  name  Modem log name
IR807# show virtual-lpwa 3 modem log list
Name : Virtual-LPWA 3
=====
dmesg           Modem kernel activity log
mdmagent        Modem agent log
messages        Modem system activity log
ipsec           Modem IPSec status log
gps             Modem GPS status log
certs           Modem Certificates log
IR807# show virtual-lpwa 3 modem log name certs
Name : Virtual-LPWA 3
=====
Certificate
```

```

Serial Number: 303e77140000000000078
Certificate Usage: Digital Signature, Key Encipherment
Issuer: DC=com, DC=example, DC=LASSI, CN=LASSI-ROOT-CA
Subject: C=CN, ST=Nanning, L=Nanning, O=Cisco, OU=iot, CN=cisco-iot
CRL Distribution Points:
http://CN=LASSI-ROOT-CA,OU=iot,DC=example,DC=LASSI,DC=com,CertificateRevocationList2,Subject=Cisco-iot
-----
Validity Date:
  Not Before: Mar 29 17:35:17 2017 GMT
  Not After : Mar 29 17:45:17 2019 GMT
CA Certificate
Serial Number: 4371ebdb781925be4b638ed1c5ca523c
Certificate Usage: Digital Signature, Certificate Sign, CRL Sign
Issuer: DC=com, DC=example, DC=LASSI, CN=LASSI-ROOT-CA
Subject: DC=com, DC=example, DC=LASSI, CN=LASSI-ROOT-CA
Validity Date:
  Not Before: Dec  2 21:34:38 2016 GMT
  Not After : Dec  2 21:44:38 2021 GMT

```

```

IR807#show virtual-lpwa 10 modem log name dmesg
Name: Virtual-LPWA 10
=====
2016-06-03T07:21:23+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T07:32:26+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T07:43:29+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T07:54:32+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:05:35+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:16:38+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:27:41+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:38:44+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:49:47+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T09:00:50+08:00 lorawan kernel: ttyS1: 1 input overrun(s)

```

The following is a sample output of the **show virtual-lpwa 10 modem statistics** command, which displays the modem statistics information:

```

IR807#show virtual-lpwa 10 modem statistics
Name: Virtual-LPWA 10
Load Average: 0.00 0.04 0.05
Memory Usage: 0.22
Flash Usage: sys:0.03 app:0.04
Temperature: 44.5 C

```

The following is a sample output of the **show virtual-lpwa 10 modem status** command, which displays the modem status information:

```

IR807#show virtual-lpwa 10 modem status
Name: Virtual-LPWA 10
Status: Running
Uptime: 13:40:37.500000
Door: DoorClose
Upgrade Status: Ready

```

The following is a sample output of the **show virtual-lpwa 1 packet-forwarder info** command, which displays the packet-forwarder information, and the LRRID which is required when registering a LoRaWAN interface on Activity Thingpark LoRaWAN network server:

```

IR807#show virtual-lpwa 1 packet-forwarder info
Name : Virtual-LPWA 1
PublicKeyStatus : Installed
FirmwareStatus : Installed
PacketFwdVersion : 1.8.15

```

```
LRRID : 68ba477e
PartnerID : 0001
```

The following is a sample output of the **show virtual-lpwa 10 packet-forwarder status** command, which displays the packet-forwarder status:

```
IR807#show virtual-lpwa 10 packet-forwarder status
Name: Virtual-LPWA 10
Status: Running
```

The following is a sample output of the **show virtual-lpwa 10 packet-forwarder log list** command, which displays the packet-forwarder log list:

```
IR807#show virtual-lpwa 10 packet-forwarder log list
Name: Virtual-LPWA 10
=====
lrr.ini      lrr.ini information
config      Get the detail config
radio       Radio status
trace       LRR Trace log
```

The following is a sample output of the **show virtual-lpwa 10 packet-forwarder log name trace** command, which displays the packet-forwarder log name trace:

```
IR807#show virtual-lpwa 10 packet-forwarder log name trace
Name: Virtual-LPWA 10
=====
05:51:35.464 (6196) [../xlap.c:726] TCP Disconnected on RTU(0x7e7b0,lrc7.thingpark.com,2404)
  fd=7 conn=1 'connection closed (eot)'
05:51:35.464 (6196) [../main.c:2299] LAP LRC DISC (2648)
05:51:35.465 (6196) [../xlap.c:553] Lap reset partial on RTU(0x7e7b0,lrc7.thingpark.com,2404)
  outq=0 ackq=3
05:51:37.405 (6196) [../xlap.c:1492] keep DNS resolution 'lrc7.thingpark.com' =>
  '51.255.52.229'
05:51:37.405 (6196) [../xlap.c:1614] connect in progress on
RTU(0x7e7b0,lrc7.thingpark.com,2404) fd=7
05:51:37.405 (6196) [../xlap.c:784] CB_LapRequest(0x7e7b0,lrc7.thingpark.com,2404) fd=7
  conn=0 events=0 connect progress
05:51:37.756 (6196) [../xlap.c:1139] connect accepted on RTU(0x7e7b0,lrc7.thingpark.com,2404)
  fd=7
05:51:37.756 (6196) [../xlap.c:1397] (0x7e7b0,lrc7.thingpark.com,2404) from st='SSP_INIT'to
  st='SSP_STOPPED'(1000->2000)
05:51:37.756 (6196) [../main.c:2294] LAP LRC CNX
05:51:37.756 (6196) [../main.c:2075] LAP LRC TCP KEEPALIVE HIGH lrc=-1 fd=7 alive=1 idle=5
  intvl=5 cnt=20
```

Monitoring LED Status

Use the **show virtual-lpwa 1 modem led** command to display LED status of the Cisco LoRaWAN Gateway. For the LED definitions, see the *Cisco LoRaWAN Gateway Hardware Installation Guide*.

The following is a sample output of the **show virtual-lpwa 1 modem led** command:

```
IR807#sh virtual-lpwa 3 modem led
Name : Virtual-LPWA 3
LED1 : GREEN ON, Solid
LED2 : GREEN ON, Solid
```

Checking Connectivity

To check the connectivity between the Cisco LoRaWAN Gateway and Thingpark Network Server after the LRR software is installed, you must check the IP NAT translations, to make sure the TCP connection over port 2404 is established.

```
IR807#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 192.168.0.2:3348 10.16.16.3:3348 217.69.25.85:3348 217.69.25.85:3348
tcp 192.168.0.2:49901 10.16.16.3:49901 217.69.25.85:2404 217.69.25.85:2404
IR807#
```

Connection with port 2404 indicates a successful communication between the LoRaWAN interface and the LoRaWAN network server.

Note: Make sure that port 2404 is open on the firewall if the gateway is installed on a secured network. It also requires DNS resolution for the name of the LoRaWAN network server, in case DNS is filtered on the firewall.

Debugging the LoRaWAN Modem

On the IR807 series, beginning in privileged EXEC mode, use these commands to debug the Cisco LoRaWAN Gateway.

Command	Purpose
<code>debug vlpwa all</code>	Enables all vlpwa debug messages.
<code>undebug vlpwa all</code>	Disables all vlpwa debug messages.
<code>debug vlpwa [decode detail errors memory raw registry session timers trace]</code>	Enables the following vlpwa debug messages: <ul style="list-style-type: none"> • decode—Decoded packet information. • detail—Detailed trace information. • errors—Errors. • memory—Memory information. • raw—Raw packet information. • registry—Registry information. • session—Session information. • timers—Timers information. • trace—Trace information.



CHAPTER 10

Licensing

This chapter provides details on the licensing for the IR807.

- [Licensing, on page 99](#)

Licensing

This chapter provides details on the licensing for the IR807.

The IOS feature set is aligned with the IOT 15.x M/T release strategy. They are:

- IR800IUK9-15703M - Cisco IR800L Series UNIVERSAL
- IR800INPEK9-15703M – Cisco IR800L Series UNIVERSAL – NO PAYLOAD ENCRYPTION

The Software License PIDs are shown in [Table 6: Software License PIDs, on page 99](#)

Table 6: Software License PIDs

Software PID	Name	Description
SL-810-AIS	Cisco 800 Series Industrial Routers IP Base License	Routing (BGP, OSPF, RIP, EIGRP, ISIS,), PBR, IGMP/MLD, Multicast, QoS, AAA, Raw Sockets, Manageability
SL-810-ADVSEC	Cisco 800 Series Industrial Routers Security License	SSL, VPN, IPSec, DMVPN, FlexVPN, IOS Firewall

Licensing

Licenses are installed at manufacturing. If the advsecurity technology-package is not installed, the crypto related functions will not work. See additional information under [Hardware Crypto Support, on page 100](#)

To enable the RightToUse license, perform the following:

1. Accept the EULA
2. Enable the technology-package
3. Reload the IR807

Licensing CLI

```
IR807# show version
License Info:
License UDI:
-----
Device#   PID                               SN
-----
*1        IR807G-LTE-GA-K9                 FCW2132001S
License Information
  License Level: advipservices   Type: RightToUse
  Next reboot license Level: advipservices
IR807# license install flash:FCW2132001S_201710030808172450.lic
IR807# conf term
license accept end user agreement
license boot module ir8001 level advsecurity
license boot module ir8001 level advipservices
IR807#show license feature

Feature name      Enforcement  Evaluation  Subscription  Enabled  RightToUse
advipservices     no          yes         no             yes      yes
advsecurity       no          no          no             no       no
ios-ips-update    yes         yes         yes            no       yes
```

Hardware Crypto Support

Hardware and Software based crypto support is available. A security license must be installed to enable hardware based crypto support.

To see information relating to crypto support, use variations on the show crypto command:

```
IR807#show crypto engine configuration
  crypto engine name: Virtual Private Network (VPN) Module
  crypto engine type: hardware
  State: Enabled
  Location: onboard 0
  Product Name: Onboard-VPN
  HW Version: 1.0
  Compression: No
  DES: Yes
  3 DES: Yes
  AES CBC: Yes (128,192,256)
  AES CNTR: No
  Maximum buffer length: 4096
  Maximum DH index: 0000
  Maximum SA index: 0000
  Maximum Flow index: 0256
  Maximum RSA key size: 0000
  crypto lib version: 22.0.0
  crypto engine in slot: 0
  platform: VPN hardware accelerator
  crypto lib version: 22.0.0
IR807#sh crypto engine ?
accelerator      Show crypto accelerator information
brief            Show all crypto engines in the system
configuration    Show crypto engine config
connections      Show connection information
qos              Show QoS information
token           Show crypto token engine info
IR807#sh crypto engine brief
```

```

crypto engine name: Virtual Private Network (VPN) Module
crypto engine type: hardware
    State: Enabled
    Location: onboard 0
    Product Name: Onboard-VPN
    FW Version: 1
    Time running: 1335 seconds
    Compression: Yes
        DES: Yes
        3 DES: Yes
        AES CBC: Yes (128,192,256)
        AES CNTR: No
Maximum buffer length: 4096
    Maximum DH index: 0500
    Maximum SA index: 0500
    Maximum Flow index: 1000
Maximum RSA key size: 0000
crypto engine name: Cisco VPN Software Implementation
crypto engine type: software
    serial number: FF98383A
crypto engine state: installed
crypto engine in slot: N/A
IR807#sh crypto engine config
crypto engine name: Virtual Private Network (VPN) Module
crypto engine type: hardware
    State: Enabled
    Location: onboard 0
    Product Name: Onboard-VPN
    FW Version: 1
    Time running: 1358 seconds
    Compression: Yes
        DES: Yes
        3 DES: Yes
        AES CBC: Yes (128,192,256)
        AES CNTR: No
Maximum buffer length: 4096
    Maximum DH index: 0500
    Maximum SA index: 0500
    Maximum Flow index: 1000
Maximum RSA key size: 0000

crypto lib version: 22_421.0.0

crypto engine in slot: 0
    platform: VPN hardware accelerator
crypto lib version: 22_421.0.0

IR807#sh crypto engine accelerator stat
Device: Onboard VPN
Location: Onboard: 0
:Statistics for encryption device since the last clear
of counters 1404 seconds ago
    0 packets in
    0 bytes in
    0 paks/sec in
    0 Kbits/sec in
    0 packets decrypted
    0 bytes before decrypt
    0 bytes decrypted
    0 packets decompressed
    0 bytes before decomp
    0 bytes after decomp
    0 packets bypass decomp
    0 bytes bypass decompres
    0 packets out
    0 bytes out
    0 paks/sec out
    0 Kbits/sec out
    0 packets encrypted
    0 bytes encrypted
    0 bytes after encrypt
    0 packets compressed
    0 bytes before comp
    0 bytes after comp
    0 packets bypass compress
    0 bytes bypass compressi

```

```

0 packets not decompress          0 packets not compressed
0 bytes not decompressed          0 bytes not compressed
1.0:1 compression ratio          1.0:1 overall
Last 5 minutes:
0 packets in                      0 packets out
0 paks/sec in                    0 paks/sec out
0 bits/sec in                    0 bits/sec out
0 bytes decrypted                0 bytes encrypted
0 Kbits/sec decrypted            0 Kbits/sec encrypted
1.0:1 compression ratio          1.0:1 overall

```

Errors:

```

Total Number of Packet Drops = 0
Pad Error                     = 0
Data Error                     = 0
Packet Error                   = 0
Null IP Error                  = 0
Hardware Error                 = 0
CP Unavailable                 = 0
HP Unavailable                 = 0
AH Seq Failure                 = 0
Link Down Error                = 0
ESP Seq Failure                = 0
AH Auth Failure                = 0
ESP Auth Failure               = 0
Queue Full Error               = 0
API Request Error              = 0
Invalid Flow Error             = 0
Buffer Unavailable             = 0
QOS Queue Full Error          = 0
Packet too Big Error           = 0
AH Replay Check Failure        = 0
Too Many Particles Error      = 0
ESP Replay Check Failure       = 0
Input Queue Full Error         = 0
Output Queue Full Error        = 0
raw_PAK_alloc                  = 0
raw_PAK_free                   = 0
mod_exp_PAK_alloc              = 3
mod_exp_PAK_free               = 3
entropy_PAK_alloc              = 0
entropy_PAK_free               = 0
Pre-batch Queue Full Error     = 0
Post-batch Queue Full Error    = 0
batch_PAK_free                 = 0

```

BATCHING Statistics:

```

Batching Allowed
Batching currently Inactive

No of times batching turned on = 0
No of times batching turned off = 0
No of Flush Done                = 0
Flush Timer in Milli Seconds    = 8
Disable Timer in Seconds        = 20
Threshold Crypto Paks/Sec
to enable batching              = 10000

POST-BATCHING Enabled
Post-batch count, max_count     = 0, 16
Packets queued to post-batch queue = 0
Packets flushed from post-batch queue = 0

```



```
The Post-batch Queue Information
The Queuesize is                = 512
The no entries currently being used = 0
The Read Index is               = 0
The Write Index is              = 0
The entries in use are between Read and Write Index
```

The entries in use are

SEC MFIFO Statistics:

```
Channel 0 allocated times      = 3
Channel 1 allocated times      = 0
Channel 2 allocated times      = 0
Channel 3 allocated times      = 0
Channel 0 freed times         = 3
Channel 1 freed times         = 0
Channel 2 freed times         = 0
Channel 3 freed times         = 0
Sec MFIFO flush count         = 3
Sec MFIFO interrupt count     = 3
Sec MFIFO put back count      = 0
Sec MFIFO Timer flush count   = 0
Sec MFIFO Timer put back count = 0
Sec alloc workq count         = 0
Sec free workq count          = 64
```




CHAPTER 11

Network Management Solutions

This chapter provides details and links to the various methods of managing the IR807.

- [Network Management Solutions, on page 105](#)

Network Management Solutions

This chapter provides details and links to the various methods of managing the IR807.

Network Management Solutions (NMS) that are available for the IR807 consist of the following:

- [Cisco Configuration Professional Express, on page 105](#)
- [Cisco IoT Field Network Director, on page 105](#)

Cisco Configuration Professional Express

The Cisco Configuration Professional Express is an embedded, device-management tool that provides the ability to bootstrap and provision an Integrated Services Router (ISR) running IOS software 15.7(3)M0a and above. This is feature rich release with support for GPS, Gyroscope configuration, CPU Utilization Graph in Dashboard, Access CCP Express using a friendly URL, Allow users to secure console when creating new user in Wizard, SNMP Configuration, ACL Management IPv6, Policy Warning for VPN, VPN Tunnel Info listing and flow change, FQDN for DMVPN Spoke, DDNS Configuration, MTU + MSS options, Save Configuration Option, Preferences option for enable/disable of write memory, VPN combination configuration (Remote Access along with IP Sec and DMVPN Hub) as applicable to ISR and IR devices.

Note: The IR807 is supported with CCP Express version 3.5 and above.

Release Notes for CCP Express 3.5 are found at:

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/cisco_configuration_professional_express/v3_5/guide/release-notes/ccp-express-m-3-5.html

Cisco IoT Field Network Director

Note: The IR807 will be supported with IOT Field Network Director 4.1 targeted for release in late 2017.

It offers a single platform to manage a complete FAN solution, Raw Socket sessions management and monitoring.

Some of the key features are:

- Geographic Information System (GIS) map -based, visualization, monitoring, troubleshooting, and alarm notifications
- Group-based configuration management for FAN and industrial routers
- Rule-engine infrastructure for customizable threshold-based alarm processing and event generation
- Secure network infrastructure (inventory, rollback configuration, work order) of IR807
- Zero Touch Provisioning - Automatically provision IR807 and head-end routers with configuration
- Collect metrics and events from FAN Routers, Industrial Routers, Head-end routers, and CG-mesh endpoints, and store them in a database. Cellular metrics and statistics for cost optimization.
- Network status monitoring and diagnosis for issues. Location tracking (historical and geo-fence)
- Update firmware on groups of IR807
- North-bound integration API for transparent integration with utility head-end and operational systems, for example Outage Reporting System.
- Raw Socket management and monitoring

Detailed information about the IoT Field Network Director is found at the home page:

<http://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html>

Cisco Prime Infrastructure

Cisco Prime Infrastructure provides a single platform to manage an infrastructure with a broad range of static Cisco devices. It is available on the IR807 with Cisco Prime Infrastructure Version 3.2 Device Pack 1 with the Inventory support & subsequent releases for the complete support. For detailed information on the Cisco Prime Infrastructure, refer to the following:

https://www.cisco.com/c/dam/en/us/td/docs/net_mgmt/prime/infrastructure/3-2/release/notes/pi32-device-pack-readme.pdf

Note: Only Inventory and Configuration Archive are Supported for the IR829.

OID and Inventory

Note: Each of the different IR807 SKUs will show a different OID and modem

To find out information about your model, use the show inventory oid command:

WP7502

```
IR807# show inventory oid
NAME: "IR807G-LTE-GA-K9", DESCR: "IR807G-LTE-GA-K9 chassis, Hw Serial#: FCW2132002E, Hw
Revision: 0.2"
PID: IR807G-LTE-GA-K9 , VID: V00, SN: FCW2132002E
OID: 1.3.6.1.4.1.9.12.3.1.3.1953
NAME: "IR807 Motherboard on Slot 0", DESCR: "IR807 Motherboard"
PID: IR807G-LTE-GA-K9 , VID: V00, SN: FOC21281GGQ
OID: 1.3.6.1.4.1.9.12.3.1.9.5.336
NAME: "Modem 0 on Cellular0", DESCR: "Sierra Wireless WP7502 4G-GA"
PID: WP7502 , VID: 1.0, SN: 354938080100772
OID: 1.3.6.1.4.1.9.12.3.1.9.15.88
```

WP7504

```
IR807#sh inventory oid
NAME: "IR807G-LTE-NA-K9", DESCR: "IR807G-LTE-NA-K9 chassis, Hw Serial#: FCW2132004P, Hw
```

```
Revision: 0.2"
PID: IR807G-LTE-NA-K9 , VID: V00, SN: FCW2132004P
OID: 1.3.6.1.4.1.9.12.3.1.3.1953
NAME: "IR807 Motherboard on Slot 0", DESCR: "IR807 Motherboard"
PID: IR807G-LTE-NA-K9 , VID: V00, SN: FOC21281GG9
OID: 1.3.6.1.4.1.9.12.3.1.9.5.336
NAME: "Modem 0 on Cellular0", DESCR: "Sierra Wireless WP7504 4G-NA"
PID: WP7504 , VID: 1.0, SN: 354937080100642
OID: 1.3.6.1.4.1.9.12.3.1.9.15.88
```

WP7601

```
IR807#sh inventory OID
NAME: "IR807G-LTE-VZ-K9", DESCR: "IR807G-LTE-VZ-K9 chassis, Hw Serial#: FCW2132006N, Hw
Revision: 0.2"
PID: IR807G-LTE-VZ-K9 , VID: V00, SN: FCW2132006N
OID: 1.3.6.1.4.1.9.12.3.1.3.1953
NAME: "IR807 Motherboard on Slot 0", DESCR: "IR807 Motherboard"
PID: IR807G-LTE-VZ-K9 , VID: V00, SN: FOC21281GE9
OID: 1.3.6.1.4.1.9.12.3.1.9.5.336
NAME: "Modem 0 on Cellular0", DESCR: "Sierra Wireless WP7601 4G-VZ"
PID: WP7601 , VID: 10000, SN: 355731080001168
OID: 1.3.6.1.4.1.9.12.3.1.9.15.88
```

