Cisco Wireless Gateway for LoRaWAN Software Configuration Guide

First Published: 2017-06-22

Last Modified: 2018-09-10

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

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

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

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

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

CONTENTS

Preface

This document describes how to configure the Cisco LoRaWAN Gateway in your network.

This guide does not describe how to install the Cisco LoRaWAN Gateway. For information about how to install the Cisco LoRaWAN Gateway, see the hardware installation guide pertaining to your device.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note* . Notes contain helpful suggestions or references to material not covered in the manual.

Caution **Means** *reader be careful*. **In this situation, you might perform an action that could result in equipment damage or loss of data.**

Danger **IMPORTANT SAFETY INSTRUCTIONSMeans 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.SAVE THESE INSTRUCTIONS**

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Related Publications

- *Cisco LoRaWAN Interface Module Hardware Installation Guide*
- *Release Notes for the Cisco LoRaWAN Gateway*
- *Getting Started and Product Document of Compliance for the Cisco LoRaWAN Interface Module*
- *Cisco IR800 Integrated Services Router Software Configuration Guide*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What’s New in Cisco Product Documentation .

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What’s New in Cisco Product Documentation RSS feed . The RSS feeds are a free service.

CHAPTER 1

Overview

The Cisco LoRaWAN Gateway is a module from Cisco Internet of Things (IoT) extension module series. It can be connected to the Cisco 809 and 829 Industrial Integrated Services Routers (IR800 series) or be deployed as standalone for low-power wide-area (LPWA) access and is positioned as a carrier-grade gateway for indoor and outdoor deployment, including harsh environments. It adds a ruggedized remote LoRaWAN radio modem interface to create a gateway between the Cisco Field Network Director and a partner's LoRa network server.

Overview

The following models are covered by this document:

- IXM-LPWA-800-16-K9
- IXM-LPWA-900-16-K9

There are two LoRaWAN gateway modes as below:

- Virtual interface mode – IR800 series including the LoRaWAN module as a virtual interface
- Standalone mode – The LoRaWAN module working alone as an Ethernet backhaul gateway or attached to a cellular router through Ethernet

You can configure the LoRaWAN IXM running on virtual interface mode or standalone mode through CLI or Cisco IoT Field Network Director (IoT FND).

This guide will provide the configuration steps for standalone mode and guide you to swap between these two modes.

For detailed information of configuring virtual interface mode, see the "Configuring Virtual-LPWA" chapter of the Cisco IR800 Integrated Services Router Software Configuration Guide at: http://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/IR800config/VLPWA.html

For the information of software installation procedure, see the release notes of Cisco LoRaWAN Gateway at: http://www.cisco.com/c/en/us/support/routers/interface-module-lorawan/products-release-notes-list.html

For more information of IoT-FND, see https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html.

Switching to Virtual Mode

You can use the **switchover** EXEC command to switch to the virtual mode.

Note Once the IXM is switched over to virtual mode, you need to have an IR829/IR809 to bring it back to standalone mode.

Use this command, if you are fully aware of your environment and confident of switching over and managing it via IR8x9.

```
Gateway#switchover
```

Displaying System Information

Use the show commands to display system information.

Displaying Version Information

Use the **show version** command to display system version information.

```
Gateway#show version
Corsica Software, Version 2.0.10.K5, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012-2014, 2017 by Cisco Systems, Inc.
Compiled 12-Jun-2017.19:06:44UTC-04:00 by Corsica Team

ROM: Bootstrap program is Corsica boot loader
Firmware Version : 2.0.10.K5, RELEASE SOFTWARE
Bootloader Version: 20160830_cisco

Hostname:ipsecrsa uptime is 15 hours, 44 minutes
Using secondary system image

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

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

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

cisco model: IXM-LPWA-800-16-K9
Processor : ARMv7 Processor rev 1 (v7l) with 1026764K bytes of memory.
Last reset from power-on
```

```
Base ethernet MAC Address : 00:50:43:14:32:45
Model revision number: : B0
System serial number: : FOC20394ANP
```

Displaying Platform Status

Use the **show platform status** command to display the platform status:

```
Gateway#show platform status
Load Average : 1min:0.23 5min:0.22 15min:0.23
Memory Usage : 0.38
Flash Usage : sys:0.06 app:0.06
CPU Temperature : 39.0 C
Board Temperature: 39.5 C
Door Status : DoorClose
```

Displaying AES Key

The LoRaWAN Chip ID is used to obtain the AES key. On the Thingpark Network Server, the AES key is stored in the **custom.ini** file. The AES key can be displayed from CLI.

Note On other 3rd party network servers, the AES key may be stored in a different location.

Obtaining the AES key requires LoRaWAN geolocation. The AES key is used to decrypt the fine - timestamps required for LoRa Geo-location calculation. The AES keys are licensed via a partner.

Note The false AES key will report incorrect geo-localization information.

Use the **show aes key** command to display AES key.

- The following example shows an existing AES key:

```
Gateway#show aes key
AES KEY: 595EB592055421C06895E4D4CE0FE63D
```

- The following example shows an unknown key:

```
Gateway#show aes key
AES KEY: Unknown
```

Displaying GPS Information

The GPS antenna must be properly installed on the LoRaWAN interface for both LoRaWAN Class B endpoints and geolocation support.

GPS information can be displayed from Cisco IOS or from the LoRaWAN interface Linux shell.

- When there is no GPS antenna attached, the **show gps log** command will have an output like the following example:

```
Gateway#show gps log
Unknown
```

- When there is a GPS antenna attached, the **show gps log** command and the **show gps status** command will have an output like the following example:

```
Gateway#show gps log
$GNRMC,231503.00,A,3725.12517,N,12155.20795,W,0.353,241.48,040517,,,A*65
$GNVTG,241.48,T,,M,0.353,N,0.653,K,A*2D
$GNGGA,231503.00,3725.12517,N,12155.20795,W,1,04,5.85,72.2,M,-29.8,M,,*4B
$GNGSA,A,3,24,15,12,13,,,,,,,,,9.40,5.85,7.35*1B
$GNGSA,A,3,,,,,,,,,,,,,9.40,5.85,7.35*18
$GPGSV,3,1,10,02,22,184,,06,49,142,,12,24,297,27,13,16,212,26*75
$GPGSV,3,2,10,15,17,248,31,17,51,041,,19,74,024,16,24,44,305,35*7C
$GPGSV,3,3,10,28,25,087,,30,05,146,*7F
$GLGSV,1,1,00*65
$GNGLL,3725.12517,N,12155.20795,W,231503.00,A,A*6B
$GNZDA,231503.00,04,05,2017,00,00*7B

Gateway#show gps status
INFO: SPI speed set to 2000000 Hz
reading GPS data...
total data length: 0
reading GPS data...
total data length: 246
$GNRMC,,V,,,,,,,,,,N*4D
$GNVTG,
##PASS: GPS I2C interface check OK
```

- To display the GPS history information, use the following command:

```
Gateway#show gps history
Info: 23:31:50 3725.13869N 12155.17038W
GPS Satellites in View: 12
GPS Satellites in Use: 10
```

Displaying FPGA Information

Use the **show fpga** command to display the FPGA information, and the **show fpga version** command to display the FPGA version.

Note FPGA version may require specific LoRaWAN forwarder version from the LoRaWAN Network Server partner.

```
#show fpga
INFO: SPI speed set to 2000000 Hz
checking FPGA version...
FPGA version: 48
HAL version: 3.5.0
SX1301 #0 version: 103
SX1301 #0 chip ID: 1
SX1301 #1 version: 103
SX1301 #1 chip ID: 1
```

```
##PASS: FPGA version check OK

#show fpga version
FGPA version: 58
```

Displaying Inventory Information

The show inventory command displays the general Cisco LoRaWAN Gateway information.

Note After a firmware upgrade, the FPGAStatus may show it is under upgrade. Wait for "Ready" status before performing any other operation.

```
Gateway#show inventory
Name          : Gateway
ImageVer      : 20170427144502_DEV
BootloaderVer : 20160830_cisco_DEV
SerialNumber  : FOC20133FNF
PID           : IXM-LORA-900-H-V2
UTCTime       : 02:40:53.464 UTC Sat Aug 12 2023
IPv4Address   : 192.168.3.5
IPv6Address   : None
FPGAVersion   : 58
FPGAStatus    : Ready
ChipID        : LSB = 0x2866ff0b MSB = 0x00f14184
TimeZone      : UTC
LocalTime     : Sat Aug 12 02:40:53 UTC 2023
ACT2 Authentication: PASS
```

Displaying Radio Information

The **show radio** command displays the radio information.

```
Gateway#show radio
LORA_SN: FOC20195V3C
LORA_PN: 95.1602T00
LORA_SKU: 868
LORA_CALC:
<115,106,100,95,89,86,83,80,72,63,55,46,38,33,29,25-126,114,106,97,89,85,81,77,69,60,52,43,35,30,26,22>
CAL_TEMP_CELSIUS: 29
CAL_TEMP_CODE_AD9361: 91
RSSI_OFFSET: -203.46,-203.75
LORA_REVISION_NUM:
RSSI_OFFSET_AUS:

radio status:
off
```

Note The radio status is off by default. Please turn on radio before working with the packet forwarder. Use the following commands to turn on radio:

```
Gateway#configure terminal
Gateway(config)#no radio off
```

Note The LORA_CALC value is the Calibration table from manufacturing, which cannot be changed, but can be used for hardware troubleshooting.

Displaying Certificate Information

The **show sudi certificate** command displays the certificate information.

```
Gateway#show sudi certificate
Calculating... please wait for seconds...
Certificate:
  X509v3 Key Usage: critical
  Issuer: O=Cisco, CN=ACT2 SUDI CA
  Subject: serialNumber=PID:IXM-LPWA-900-16-K9 SN:FOC21182U6D, O=Cisco, OU=ACT-2 Lite SUDI,
 CN=IXM-LPWA-900-16-K9
  Signature Algorithm: sha256WithRSAEncryption, Digital Signature, Non Repudiation, Key
Encipherment
  Validity
    Not Before: May 16 19:21:43 2017 GMT
    Not After : May 16 19:21:43 2027 GMT
```

CHAPTER 2

Assigning IP Address and Domain Name Server

This chapter describes how to create the initial configuration (for example, assigning the IP address and default gateway information) for the Cisco LoRaWAN Gateway by using a variety of automatic and manual methods.

Note Information in this chapter about configuring IP addresses and DHCP is specific to IP Version 4 (IPv4).

Assigning IP Address

You can assign IP address through a DHCP server or manually.

Use a DHCP server for centralized control and automatic assignment of IP information after the server is configured.

Configuring DHCP

Understanding DHCP

DHCP provides configuration information to Internet hosts and internetworking devices. This protocol consists of two components: one for delivering configuration parameters from a DHCP server to a device and a mechanism for allocating network addresses to devices. DHCP is built on a client-server model, in which designated DHCP servers allocate network addresses and deliver configuration parameters to dynamically configured devices.

DHCP client support is enabled on the Fast Ethernet 0/1 or VLAN interface on the LoRaWAN Gateway for automatic IPv4 address assignment.

The DHCP server, which supplies the IP addresses to the LoRaWAN Gateway interfaces, does not need to be on the same subnet as the LoRaWAN Gateway. However, when the DHCP server and the LoRaWAN Gateway are on different subnets, DHCP relay must be active in the network. Generally, DHCP relay is configured on a LoRaWAN Gateway in the path between the LoRaWAN Gateway and the DHCP server. The DNS address and default gateway can also be assigned via DHCP.

Enabling DHCP on Interfaces

To assign IP address by negotiation via DHCP, use the **ip address dhcp** privileged EXEC command.

Beginning in privileged EXEC mode, follow these steps to enable DHCP on interfaces:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type interface_number*	Enter interface configuration mode.
Step 3	**ip address dhcp**	Enable DHCP client on the interface to allow automatic assignment of IP addresses to the specified interface.
Step 4	**description** [*interface_description*]	Enter description for the interface.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ip default-gateway** *ip-address*	Configure default gateway. **Note** The default gateway may be learned from DHCP.
Step 7	Use the following commands to verify the configuration: • **show interfaces** *interface_type interface_number* • **show ip interfaces** *interface_type interface_number* • **show ip route**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Manually Assigning IP Information

Beginning in privileged EXEC mode, follow these steps to manually assign IP information to multiple interfaces:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface_type interface_number*	Enter interface configuration mode.
Step 3	**ip address** *ip-address subnet-mask*	Enter the IP address and subnet mask.

	Command or Action	Purpose
Step 4	**description** [*interface_description*]	Enter description for the interface.
Step 5	**exit**	Return to global configuration mode.
Step 6	**ip default-gateway** *ip-address*	Configure default gateway.
Step 7	Use the following commands to verify the configuration: • **show interfaces** *interface_type interface_number* • **show ip interfaces** *interface_type interface_number* • **show ip route**	Verify the configuration.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To remove the IP address, use the **no ip address** interface configuration command. If you are removing the address through SSH, your connection to the LoRaWAN Gateway will be lost.

Configuring DNS

DNS Client

When your network devices require connectivity with devices in networks for which you do not control the name assignment, you can assign device names that uniquely identify your devices within the entire internetwork using the domain name server (DNS). DNS uses a hierarchical scheme for establishing host names for network nodes, which allows local control of the segments of the network through a client-server scheme. The DNS system can locate a network device by translating the hostname of the device into its associated IP address.

On the Internet, a domain is a portion of the naming hierarchy tree that refers to general groupings of networks based on the organization type or geography. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that the Internet identifies by a com domain, so its domain name is cisco.com. A specific hostname in this domain, the File Transfer Protocol (FTP) system, for example, is identified as ftp.cisco.com.

Name Servers

Name servers keep track of domain names and know the parts of the domain tree for which they have complete information. A name server might also store information about other parts of the domain tree. To map domain names to IP addresses on the LoRaWAN Gateway, you must identify the hostnames, specify a name server, and enable the DNS service.

You can configure the LoRaWAN Gateway to use one or more domain name servers to find an IP address for a host name.

DNS Operation

A name server handles client-issued queries to the DNS server for locally defined hosts within a particular zone as follows:

An authoritative name server responds to DNS user queries for a domain name that is under its zone of authority by using the permanent and cached entries in its own host table. When the query is for a domain name that is under its zone of authority but for which it does not have any configuration information, the authoritative name server replies that no such information exists.

A name server that is not configured as the authoritative name server responds to DNS user queries by using information that it has cached from previously received query responses.

Configuring DNS Server

To configure the DNS server, use the **ip name-server** privileged EXEC command

Beginning in privileged EXEC mode, follow these steps to configure DNS:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip name-server** *ip-address*	Configure DNS server.
Step 3	**exit**	Return to global configuration mode.
Step 4	**show hosts**	Verify the configuration.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Mapping Hostnames to IP Addresses

This section provides configuration of hostname to IP address mapping, so that host can be reached by name without DNS.

Beginning in privileged EXEC mode, follow these steps to map hostnames to IP addresses:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip host** *hostname ip-address*	Define a static hostname-to-address mapping. You can define up to 5 mapping entires. Use the **no** form of the command to delete the mapping entry.

	Command or Action	Purpose
		Note You can also use this command to set the LXC /etc/hosts entries from the CLI.
Step 3	**exit**	Return to global configuration mode.
Step 4	**show ip host**	Verify the configuration.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
Gateway#config terminal
Gateway(config)#ip host thinkpark.com 122.23.12.1


Gateway#show ip host
IP                              Hostname
--                              -------
11.11.11.1                      apple.com
11.11.11.2                      apple2.com
11.11.11.3                      apple3.com
11.11.11.4                      apple4.com
```

CHAPTER 3

Administering the Cisco LoRaWAN Gateway

This chapter describes how to perform one-time operations to administer the Cisco LoRaWAN Gateway.

Managing the System Time and Date

You can manage the system time and date on your LoRaWAN Gateway using automatic configuration, such as the Network Time Protocol (NTP).

The NTP is designed to time-synchronize a network of devices. NTP runs over User Datagram Protocol (UDP), which runs over IP. NTP is documented in RFC 1305 and RFC 5905.

An NTP network usually gets its time from an authoritative time source, such as a radio clock or an atomic clock attached to a time server. NTP then distributes this time across the network. NTP is extremely efficient; no more than one packet per minute is necessary to synchronize two devices to within a millisecond of one another.

The communications between devices running NTP (known as *associations*) are usually statically configured; each device is given the IP address of all devices with which it should form associations. Accurate timekeeping is possible by exchanging NTP messages between each pair of devices with an association. However, in a LAN environment, NTP can be configured to use IP broadcast messages instead. This alternative reduces configuration complexity because each device can simply be configured to send or receive broadcast messages. However, in that case, information flow is one-way only.

NTP Version 4

NTP version 4 is implemented on the modem. NTPv4 is an extension of NTP version 3. NTPv4 supports both IPv4 and IPv6 and is backward-compatible with NTPv3.

NTPv4 provides these capabilities:

- Suppport for IPv6. (Note that IXM supports only IPv4.)

- Improved security compared to NTPv3. The NTPv4 protocol provides a security framework based on public key cryptography and standard X509 certificates.
- Automatic calculation of the time-distribution hierarchy for a network. Using specific multicast groups, NTPv4 automatically configures the hierarchy of the servers to achieve the best time accuracy for the lowest bandwidth cost. This feature leverages site-local IPv6 multicast addresses.

Configuring NTP Server

Beginning in privileged EXEC mode, follow these steps to configure the NTP server:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ntp server** {**ip** *name* | **address** *address* }	Defines the NTP server that provides the clocking source for the modem.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show ntp status**	(Optional) Show NTP status to verify the configuration.
Step 5	**show ntp associations**	(Optional) Show the NTP associations with upstream servers.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To disable the NTP service, use the **no ntp server** *hostname* global configuration command.

Configuring a System Name and Prompt

You configure the system name on the LoRaWAN Gateway to identify it. By default, the system name and prompt are *Router* .

Beginning in privileged EXEC mode, follow these steps to manually configure a system name:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**hostname** *name*	Manually configure a system name. The default setting is *Router* .

	Command or Action	Purpose
		The name must follow the rules for ARPANET hostnames. They must start with a letter, exit with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names can be up to 63 characters.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-confi**g	(Optional) Save your entries in the configuration file.

What to do next

When you set the system name, it is also used as the system prompt.

To return to the default hostname, use the **no hostname** global configuration command.

Configuring UBX Support for GPS

The UBX protocol is the communication convention used by certain GPS receiver chips. The UBX format is binary as opposed to text-based. UBX Protocol messages operate over an asynchronous serial connection following the RS-232 standard. Messages are classified into different categories such as Configuration, Timing, Informative, Monitor, and Navigation. Messages sent to the chip are either commands or enquiries.

Beginning in privileged EXEC mode, follow these steps to configure the UBX support for GPS.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**gps ubx enable**	Enable the UBX protocol to UART output. To disable the UBX support, use the **no** form of the command.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Checking and Saving the Running Configuration

You can check the configuration settings that you entered or changes that you made by entering this privileged EXEC command:

```
Router# show running-config
```

To store the configuration or changes you have made to your startup configuration in flash memory, enter this privileged EXEC command:

```
Router# copy running-config startup-config
```

This command saves the configuration settings that you made. If you fail to do this, your configuration will be lost the next time you reload the system. To display information stored in the NVRAM section of flash memory, use the **show startup-config** privileged EXEC command.

Reloading IXM

The **reload** command halts the system. If the system is not set to manually boot up, it reboots itself. Use the **reload** command after you save the LoRaWAN Gateway configuration information to the startup configuration (**copy running-config startup-config**).

Using Reset Button

A Cisco Wireless Gateway for LoRaWAN that has already been configured can be reset to the manufacturing configuration by pressing the **Reset** button located at the side of the Console port on the device.

If you press the **Reset** button and release it in less than 5 seconds, the system will reboot immediately with the last saved configuration.

If you press the **Reset** button and release it after more than 5 seconds, the system will reboot immediately and restore to the factory default.

CHAPTER 4

Configuring VLAN

This chapter describes how to configure VLAN on the Cisco LoRaWAN Gateway. The LoRaWAN Gateway supports IEEE 802.1Q encapsulation. You can configure the fastethernet port as a trunk port that enables tagging of outgoing traffic from the Cisco LoRaWAN Gateway.

Configuring IP Address for VLAN

Beginning in privileged EXEC mode, follow these steps to configure IP address for the VLAN:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface vlan** *vlan-id*	Enter interface configuration mode, and enter the VLAN to which the IP information is assigned. The VLAN range is 1 to 4094.
Step 3	**ip address** {*ip-address subnet-mask* | **dhcp**}	Configure the IP address.
Step 4	**exit**	Return to global configuration mode.
Step 5	**show interfaces vlan** *vlan-id*	Verify the configured IP address.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Configuring VLAN Trunks

A trunk is a point-to-point link between one or more Ethernet interfaces and another networking device such as a router or a switch. Ethernet trunks carry the traffic of multiple VLANs over a single link, and you can extend the VLANs across an entire network.

You can configure the FastEthernet port as a trunk port that enables tagging of outgoing traffic from the Cisco LoRaWAN Gateway.

Configuring a Trunk Port

Beginning in privileged EXEC mode, follow these steps to configure a trunk port:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface** *interface-id*	Specify the port to be configured for trunking, and enter interface configuration mode.
Step 3	**switchport mode trunk**	Set the interface in permanent trunking mode and negotiate to convert the link to a trunk link even if the neighboring interface is not a trunk interface.
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To reset all trunking characteristics of a trunking interface to the defaults, use the **no switchport trunk** interface configuration command.

Defining the Allowed VLANs on a Trunk

By default, a trunk port sends traffic to and receives traffic from all VLANs. All VLAN IDs, 1 to 4094, are allowed on each trunk. However, you can remove VLANs from the allowed list, preventing traffic from those VLANs from passing over the trunk.

Beginning in privileged EXEC mode, follow these steps to modify the allowed list of a trunk:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 2	**interface** *interface-id*	Specify the port to be configured, and enter interface configuration mode.
Step 3	**switchport mode trunk**	Configure the interface as a VLAN trunk port.
Step 4	**switchport trunk allowed vlan** *vlan-id*	(Optional) Configure the VLAN allowed on the trunk.
Step 5	**exit**	Return to privileged EXEC mode.
Step 6	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To return to the default allowed VLAN list of all VLANs, use the **no switchport trunk allowed vlan** interface configuration command.

Enabling Sending and Receiving Tagged Packet on Ethernet Port

To enable sending and receiving of tagged packets on the Ethernet port, the following needs to be configured on the Cisco LoRaWAN Gateway:

```
interface FastEthernet 0/1
switchport mode trunk
switchport trunk allowed vlan <vlan id 1-4094>
exit
!
interface Vlan <vlan-id>
ip address <dhcp | ip mask>
```

Note Only a single vlan tag is allowed on the trunk port. All traffic destined for network specified by interface vlan IP address will go out of the Ethernet port with that vlan tag.

The port will also expect incoming packets (with its own ip address or broadcast address) to be tagged with the same vlan tag. In order for the peer switch or router to send tagged packets to the Cisco LoRaWAN Gateway, they need to be configured as trunk ports as well.

Here is a configuration example on a Cisco Me3400 switch:

```
interface FastEthernet0/23
switchport trunk allowed vlan 220
switchport mode trunk
```

Note The uplink to the rest of the network from this switch also needs to include this vlan.

On a Catalyst 3750 it would be:

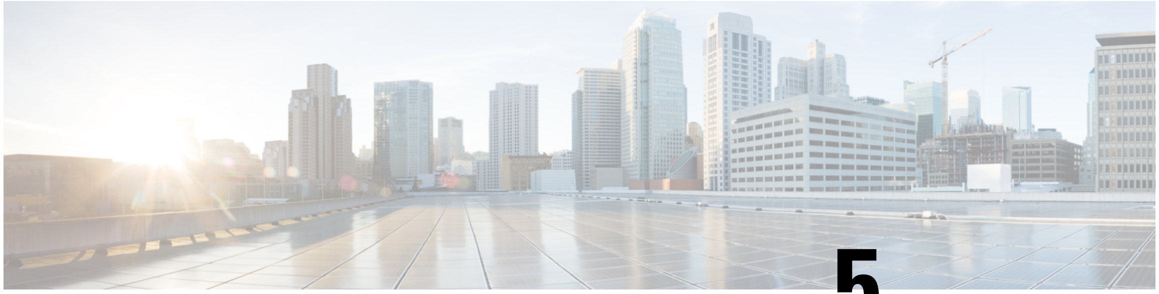
```
interface GigabitEthernet 1/0/1
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan <vlan_id>
  switchport mode trunk
```

If you need to use Vlan 1, remember that Cisco switches treat Vlan 1 as the native vlan on trunk ports by default. That is, incoming "untagged" packets will be treated as they belong to Vlan 1. And similarly when Vlan 1 packets untagged are sent. These packets will not be picked up on the Cisco LoRaWAN Gateway Vlan interface. To avoid this, a different native vlan must be chosen on the peer switch. See the following example:

```
interface GigabitEthernet 1/0/1
  switchport trunk encapsulation dot1q
  switchport trunk native vlan <vlan id other than 1>
  switchport trunk allowed vlan 1
  switchport mode trunk
```

Examples of Show Commands

```
Router# show vlan
 VLAN Name                             Status    Ports
 ---- -------------------------------- --------- --------------------------------
  220 VLAN0220                         Active     Fa0/1

Router# show interfaces
Vlan220 is up
        address is 00:50:43:24:1F:4A
        MTU is 1500 bytes
FastEthernet0/1 is up
        Hardware is Fast Ethernet, address is 00:5F:86:5C:27:78
        MTU is 1500 bytes

Router# show interfaces Vlan 220
Vlan220 is up
        address is 00:50:43:24:1F:4A
        MTU is 1500 bytes

Router# show ip interface
  FastEthernet  FastEthernet IEEE 802.3
  Vlan          Vlan IEEE 802.1q

Router# show ip interface Vlan 220
Vlan220  is up
  Internet address is 172.27.165.208
  Netmask is 255.255.255.128
  Broadcast address is 172.27.165.255
  MTU is 1500 bytes
```



CHAPTER 5

Configuring CDP

This chapter describes how to configure Cisco Discovery Protocol (CDP) on the Cisco LoRaWAN Gateway.

Understanding CDP

CDP is a device discovery protocol that runs over Layer 2 (the data link layer) on all Cisco-manufactured devices (routers, bridges, access servers, and switches) and allows network management applications to discover Cisco devices that are neighbors of already known devices. With CDP, network management applications can learn the device type and the Simple Network Management Protocol (SNMP) agent address of neighboring devices running lower-layer, transparent protocols. This feature enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP). Because CDP runs over the data-link layer only, two systems that support different network-layer protocols can learn about each other.

Each CDP-configured device sends periodic messages to a multicast address, advertising at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime information, which is the length of time a receiving device holds CDP information before discarding it. Each device also listens to the messages sent by other devices to learn about neighboring devices.

Configuring CDP

These sections include CDP configuration information and procedures.

Enabling and Disabling CDP

Beginning in privileged EXEC mode, follow these steps to enable or disable the CDP device discovery capability:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 2	**(no) cdp run**	Enable or disable CDP.
Step 3	**exit**	Return to privileged EXEC mode.

Configuring the CDP Characteristics

Beginning in privileged EXEC mode, follow these steps to configure the CDP timer and holdtime.

You can configure the frequency of CDP updates, and the amount of time to hold the information before discarding it.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**cdp timer** *seconds*	(Optional) Set the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.
Step 3	**cdp holdtime** *seconds*	(Optional) Specify the amount of time a receiving device should hold the information sent by your device before discarding it. The range is 10 to 255 seconds; the default is 180 seconds.
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**show cdp**	Verify configuration by displaying global information about CDP on the device.
Step 6	**show cdp neighbors**	Display information about neighbors.
Step 7	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Use the **no** form of the CDP commands to return to the default settings.

CHAPTER 6

Configuring Authentication

This chapter describes how to configure authentication on the Cisco LoRaWAN Gateway.

Preventing Unauthorized Access

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

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

Protecting Access to Privileged EXEC Commands

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

Configuring Enable Secret Passwords with Encryption

To provide an additional layer of security, particularly for passwords that cross the network or that are stored on a Trivial File Transfer Protocol (TFTP) server, you can use the **enable secret** global configuration commands.

The command allows you to establish an encrypted password that users must enter to access privileged EXEC mode (the default).

Beginning in privileged EXEC mode, follow these steps to configure encryption for enable secret passwords:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**enable secret** {*password* | **5** *encrypted_passwd*|**8** *encrypted_passwd*}	Define a secret password for access to privileged EXEC mode. Specify 5 to indicate md5 encryption. Specify 8 to indicate SHA512 password. **Note** Special characters cannot be used for the plain password. **Note** While upgrading to Release 2.0.20, admin has to reconfigure the passwords for SHA512 to be effective and downgrade is not supported.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To remove a password, use the **no enable secret** global configuration command.

Configuring Username and Password for Local Authentication

You can configure username and password pairs, which are locally stored on the LoRaWAN Gateway. These pairs are assigned to lines or ports and authenticate each user before that user can access the LoRaWAN Gateway.

Beginning in privileged EXEC mode, follow these steps to establish a username-based authentication system that requests a login username and a password:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**username** *name* {*password* | **5** *encrypted_passwd* |**8** *encrypted_passwd*}	Enter the username and password for each user. Specify 5 to indicate md5 encryption. Specify 8 to indicate SHA512 password.

	Command or Action	Purpose
		Note Special characters cannot be used for the plain password. **Note** While upgrading to Release 2.0.20, admin has to reconfigure the passwords for SHA512 to be effective and downgrade is not supported.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To disable username authentication for a specific user, use the **no username** *name* global configuration command.

Note For enable secret, username, and system admin, use the following characters for the password:

- Lowercase alphabet: [a-z]
- Uppercase alphabet: [A-Z]
- Numbers: [0-9]
- Special Character: [$%{}+_:]

Configuring Secure Shell

This section describes how to configure the Secure Shell (SSH) feature.

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

Beginning in privileged EXEC mode, follow these steps to configure SSH on the LoRaWAN Gateway.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

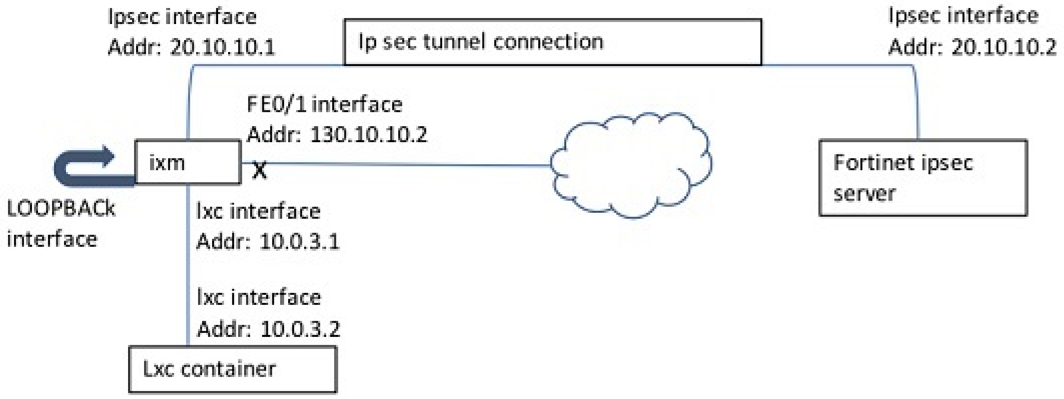
	Command or Action	Purpose
Step 2	**hostname** *hostname*	Configure a hostname for your LoRaWAN Gateway.
Step 3	**ip domain name** *domain_name*	Configure a host domain for your LoRaWAN Gateway.
Step 4	**ip ssh** {**port**|**session**|**authentication-retries**| **time-out**|**admin-access**|**local**| **limit-local**}	Configure the SSH control parameters: • **port** – Configure SSH port. • **session** – Configure number of SSH session. • **authentication-retries** – Configure number of authentication retries. • **time-out** – Configure timeout interval. • **admin-access** – Allow admin access via SSH. • **local** – Restrict user to container and reverse-tunnel SSH access only. • **limit-local** – Permit SSH on local only. Limit the listening address to local address only (for example, 127.0.0.1 or 10.0.3.1). Not listen on LAN interface.
Step 5	**crypto key generate rsa**	Enable the SSH server for local and remote authentication on the LoRaWAN Gateway and generate an RSA key pair. Generating an RSA key pair automatically enables SSH.
Step 6	**exit**	Return to privileged EXEC mode.
Step 7	Do one of the following: • **show ip ssh** • **show ssh**	Show and configuration information for your SSH server. Show the status of the SSH server on the LoRaWAN Gateway.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

To delete the RSA key pair, use the **crypto key zeroize rsa** global configuration command. After the RSA key pair is deleted, the SSH server is automatically disabled.

Configuring IP SSH Limit Local

The following figure shows an example of the **IP SSH limit local** command behavior.



When **IP SSH limit local disabled** is configured, the SSH connections to all innterfaces are allowed. When **IP SSH limit local enabled** is configured, the SSH connection to FE0/1 (130.10.10.2) is not allowed.

Note When **IP SSH limit local** is enabled on the IXM, the SSH access from outside is disabled for the unit. The **uboot console disable** option only checks whether SSH is enabled or not, and does not factor the **IP SSH limit local** option. If both commands are configured, it is possible that both the console conntecvity and SSH connectivity are lost. In that case, the only way to access the unit is through container via Thing park.

Displaying the SSH Configuration and Status

To display the SSH server configuration and status, use one or more of the privileged EXEC commands in Table 1: Commands for Displaying the SSH Server Configuration and Status , on page 27:

Table 1: Commands for Displaying the SSH Server Configuration and Status

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

Using SCP to Upload Files

To copy a local file to a remote location, use the following **scp** EXEC command:

scp local *src_filename username host dst_filename*

To copy a remote file to local flash, use the following **scp** EXEC command:

scp remote *username host src_filename dst_filename*

SSH Access Over IPSec Tunnel

From the primary server and secondary server, you can SSH to IXM over the tunnel.

Example from IR800:

```
IR800# ssh -v 2 -l via 172.27.170.71
```

Configuring Reverse SSH and Connecting to Container

To open a shell to the container for user, use the **request shell container-console** EXEC command. Password is needed when you request shell container. If you have changed the system admin password, you need to use the new password.

Note Admin can change the password by using the **sysadmin security password** command.

Configuring Reverse SSH

Beginning in privileged EXEC mode, follow these steps to create a reverse SSH tunnel.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**secure-tunnel create** *<port-no> <user-id> <remote-host>*	Create a reverse SSH tunnel.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show secure-tunnel**	Show the secure tunnel status.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
configure terminal
 secure tunnel create 30000 vnallamo 10.28.29.226
```

From the 10.28.29.226 server, execute the following command to reverse SSH:

```
ssh -l vik localhost -p 30000
```

Note When IPSec is enabled, secure tunnel may not be working due to gateway reachability. This is a known issue.

Copying Files From the Container

Beginning in privileged EXEC mode, follow these steps to copy files from the container to the host.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**container copy** *<filename> <path>*	Copy files from the container to the host.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Changing Private Network Between Host and Container

Beginning in privileged EXEC mode, follow these steps to change the private network between the host and the container.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**container private-network** *<chosen-private-network-option-from-the-list>*	Change the private network between the host and the container. You can choose one of the following options: 10.0.0.0/28, 172.16.0.0/28, or 192.168.0.0/28. By default, the private network is 10.0.3.0/24, which is configured on startup. To restore the default, use the no form of the command.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show container private-network**	Verify the configuration.

	Command or Action	Purpose
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
Gateway#show container private-network
Container private network: 172.16.0.0/2
```

User Accounts

This section describes the user accounts and their usages.

Use the **request shell host** command to enter the Linux shell and use the **request shell exit** command to exit.

Table 2: User Accounts

userID	SSH connection	Shell	Linux shell access via request shell host	Notes
system	no (default)	/bin/sh	yes	• Use the **ip ssh admin-access** CONF command to allow SSH access. • Use the **admin security password** EXEC command to change system password.
user1	yes	clish	no	-
user2	yes	clish	no	-

Table 3: Linus Shell Access

Request Shell	Exit	Host
SSH	Exit from host	Go into console
console	Go into console	Go into console

Table 4: Password Change on Switchover

Switchover Type	Description
From virtual mode to standalone mode	The virtual mode root password is assigned to the standalone mode system password.
From standalone mode to virtual mode	The standalone mode system password is lost during the switchover, and the virtual mode root password remains.

Configuring Logging in Container

Beginning in privileged EXEC mode, follow these steps to configure logging in the container.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**container log all**	Enable logging through syslog-ng in the container. To restore the default, use the **no** form of the command.
Step 3	**exit**	Return to privileged EXEC mode.

After the is command is enabled, you can view the logs by logging into the container. The logs are located in **/var/run**.

Example

```
Gateway(config)#container log all
Container syslog has started.
```

CHAPTER 7

Configuring IPSec

This chapter provides information about IPSec configuration on the Cisco LoRaWAN Gateway.

Understanding IPSec

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (site-to-site), or between a security gateway and a host (remote-access).

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection.

IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at Application layer. Hence, only IPsec protects any application traffics over an IP network. Applications can be automatically secured by its IPsec at the IP layer. Without IPsec, the protocols of TLS/SSL must be inserted under each of applications for protection.

Configuring IPsec

Beginning in privileged EXEC mode, follow these steps to configure IPsec on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**crypto ipsec profile** {**common**|**primary**|**secondary**}	Configure parameters used by tunnel. **Note** The primary profile MUST be configured. Common and secondary are optional. For more information, see Configuring Crypto IPSec Profile Common, on page 35 and Configuring Crypto IPSec Profile Individual , on page 36.
Step 3	Do one of the following: • **ipsec isakmp** *username password* **group** *group_id* **psk** • **ipsec cert install** {**usb** |**local**}**enable** • **ipsec cert scep** *<url> <country_code> <state> <locality> <organization> <unit> <name> <device-id>* {**ndes**|**xpki**} *<persistency> <key-length>*	These commands are exclusive. • Configure PSK. • Enable downloading certificates from USB or local flash. **Note** If SCEP is enabled, the **ipsec cert install local enable** command will fail. Disable SCEP and then execute this command. • Configure SCEP. From Release 2.0.20, xpki is supported as well as ndes. • xpki - Use a Cisco Router as the CA server • ndes - Use a Window server as the CA server **Example** `Gateway(config)#`**`ipsec cert scep http://172.27.163.69/cgi-bin/pkiclient.exe US CA Milpitas Cisco iot CSR1K true`**
Step 4	**ipsec enable**	Enable IPSec.
Step 5	**ipsec subnet lock**	Lock the device traffic with IPsec subnet. Traffic outside of the subnet will not be accepted.
Step 6	**exit**	Return to global configuration mode.
Step 7	**show ipsec certs**	(Optional) Display details about certificates (RSA only).

	Command or Action	Purpose
Step 8	**show ipsec status** {**info**|**detail**}	(Optional) Display details about IPsec status.
Step 9	**debug ipsec**	(Optional) Enable logging for IPsec. This command should be executed after the **ipsec enable** command is configured. To disable the logging for IPsec, use the **no debug ipsec** command. **Note** This command should be used ONLY for debugging purpose as it can impact performance.
Step 10	**show ipsec log**	(Optional) Display the IPsec logs on the screen.
Step 11	**clear ipsec log**	(Optional) Clear the existing IPsec logs.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

What to do next

Before PSK or PKI can be configured, you must configure the primary crypto ipsec profile at the minimum. For more information, see Configuring Crypto IPSec Profile Common, on page 35 and Configuring Crypto IPSec Profile Individual , on page 36..

Note No spaces are allowed in any DNs (or IDs) or ca parameters.

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

Configuring Crypto IPSec Profile Common

This section contains configurations of attributes shared by all the tunnels.

Note The crypto ipsec profile common command can only configure attributes shared by tunnels for RSA only, but not for PSK.

Beginning in privileged EXEC mode, follow these steps to configure crypto IPSec profile common on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**crypto ipsec profile common**	Configure parameters used by all tunnels.
Step 3	**leftid** <*left_id*>	(Optional) Configures the ID of the LoRaWAN module. • *left_id* - Full subject distinguished name (DN) of the certificate, including IP address, domain name, or e-mail address
Step 4	**leftca** <*left_ca_issuer*>	(Optional) Configures the DN of the CA the LoRaWAN module received its certificates from. • *left_ca_issuer* - CA DN of the Cisco LoRaWAN Gateway
Step 5	**rightca** <*right-ca-issuer*>	(Optional) Configures the DN of the CA the corresponding IPSec server received its certificates from. • *right-ca-issuer* - CA DN of the IPSec server
Step 6	**exit**	Exit the crypto ipsec profile common block and updates the IPSec configuration.
Step 7	**exit**	Return to global configuration mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

Example of Common Profile Block

```
crypto ipsec profile common
leftid C=CN,ST=Nanning, L=Nanning, O=Cisco,OU=iot,CN=cisco-iot
leftca cn=LASSI-ROOT-CA,dc=LASSI,dc=example,dc=com
```

Configuring Crypto IPSec Profile Individual

This section contains configuration of the parameters of the individual tunnels between the IPSec server and the Cisco LoRaWAN Gateway. The primary block MUST be configured before any other IPSec configurations are implemented.

Note Adding the subnet parameter enforces a subnet-only tunnel. Any packets within that subnet will travel through the tunnel and any packets outside of that subnet will not travel within the tunnel. If all packets need to go through the tunnel, do not configure any subnet. This will establish a host-only tunnel.

Note Primary configurations will override secondary configurations, so if no subnet is configured in primary (default, host-only tunnel) and subnet is configured in the secondary tunnel, then packets will not be able to go through the secondary tunnel.

Beginning in privileged EXEC mode, follow these steps to configure crypto IPSec profile individual on the Cisco LoRaWAN Gateway:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**crypto ipsec profile** {**primary**|**secondary**}	Configure parameters used by individual tunnel.
Step 3	**ipaddr** <*ip-address*> **iketime** <*ike-lifetime*> **keytime** <*key-life*> **aes** <*ike-encryption*>	Configures the required parameters of the tunnel. • *ip-address* - IP address or hostname of the IPSec server. • *ike-lifetime* - Lifetime of ISAKMP or IKE SA in seconds. • *key-life* - Lifetime of one tunnel connection instance in seconds. • *ike-encryption* – Encryption method of ike directive in strongSwan; 128 or 256 for aes128-sha256-ecp256 or aes256-sha256-ecp256 by default.
Step 4	**rightid** <*right_id*>	(Optional) Configure the ID of the IPSec server. • *right-id* - IPSec server's certificate's full subject DN, IP address, domain name, or e-mail address.
Step 5	**subnet** <subnet/mask>	(Optional) Configures the subnet and mask of IP addresses the IPSec server will accept in the tunnel. • *subnet/mask* - Subnet and mask, for example, 10.0.0.0/8.

	Command or Action	Purpose
Step 6	**exit**	Exit the crypto ipsec profile individual block and update the IPSec configuration.
Step 7	**exit**	Return to global configuration mode.
Step 8	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

Examples of Primary and Secondary Profile blocks:

```
crypto ipsec profile primary
ipaddr 192.168.3.4 iketime 86400 keytime 86400 aes 128
subnet 10.10.0.0/8
rightid SN=FTX2103Z05B, unstructuredName=CRS829.cisco.com
exit
!
crypto ipsec profile secondary
ipaddr 192.168.3.1 iketime 86400 keytime 86400 aes 128
subnet 10.10.0.0/8
rightid
unstructuredName=IR829_CH.cisco.com,C=CN,ST=Nanning,L=Nanning,O=Cisco,OU=IR829,CN=ndes.com
exit
```

Basic Configuration for RSA to Connect to Primary and Secondary

```
172.27.170.71 LoRaWAN Module <——————————> Primary 172.27.170.77
                                 <——————————> Secondary 172.27.170.72

   crypto ipsec profile primary
   ipaddress 172.27.170.77 iketime 86400 keytime 86400 yes 256
   exit
   crypto ipsec profile secondary
   ipaddress 172.27.170.77 iketime 86400 keytime 86400 yes 256
   exit
   ipsec cert scep http://172.27.126.60/CertSrv/mscep/mscep.dll US CA Milpitas Cisco iot
LORA ndes true 2048
   ipsec enable
```

Locking Traffic to IPSec Tunnels

When subnets are configured, only the packets destined for that subnet pass through the IPsec tunnel. To make sure that all traffic passes through IPsec tunnels when subnets are configured, use the **ipsec subnet lock** command to allow only the traffic between the IXM and its designated subnets.

Erasing IPSec Certificates and Key

To erase IPSec certificates and key, use the **ipsec cert erase** EXEC command.

Uploading Certificates from USB or Local Flash

To upload certificates from USB, use the following EXEC command:

ipsec install usb <*pfx-file* > <cr> | <*password* >

To upload certificates from local flash, use the following EXEC command:

ipsec install local *path*: *file password*

Example

```
ipsec install local flash:ndes2.pfx cisco
```

Disabling LXC Restart During IPSec Reauthentication

To disable LXC to restart during the IPSec reauthentication, use the **ipsec lxc-restart-disable** command.

CHAPTER 8

Configuring PPPoE

This section describes how to configure the Point-to-Point over Ethernet (PPPoE) client on the Cisco LoRaWAN Gateway.

PPPoE Client Overview

The Point-to-Point over Ethernet (PPPoE) is a network protocol for encapsulating PPP frames inside Ethernet frame. PPPoE combines Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems.

The Cisco Wireless Gateway for LoRaWAN can be configured as a PPPoE client, so that a tunnel can be established for the router to access the WAN.

At system initialization, the PPPoE client establishes a session with the access concentrator by exchanging a series of packets. Once the session is established, a PPP link is set up, which includes authentication using Password Authentication protocol (PAP). Once the PPP session is established, each packet is encapsulated in the PPPoE and PPP headers.

Configuring the Dialer Interface

Beginning in privileged EXEC mode, follow these steps to configure the dialer interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface dialer** *number*	Enter interface configuration mode for the dialer interface.

	Command or Action	Purpose
Step 3	**ip address negotiated**	Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.
Step 4	**ip mtu** *number*	Configure the maximum transmission unit (MTU) of the PPPoE interface. Default is 1492. *number* - PPPoE MTU
Step 5	**ip tcp adjust-mss** *number*	Configure the Maxitum Segment Size (MSS) of the PPPoE interface. Default is 1412. *number* - PPPoE MSS
Step 6	**ppp authentication chap**	Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).
Step 7	**ppp chap hostname** <*hostname*>	Define an interface-specific CHAP hostname.
Step 8	**ppp chap password** <*password*>	Define an interface-specific CHAP password.
Step 9	**dialer-group** *name*	Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.
Step 10	**dialer-pool** *name*	Specify the dialer pool to use to connect to a specific destination subnetwork.
Step 11	**exit**	Return to global configuration mode.
Step 12	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
config terminal
interface Dialer 1
 ip address negotiated
 dialer-group 1
 ppp authentication chap
 ppp chap hostname alice
 ppp chap password 1234
 dialer-pool 1
 exit
```

Configuring the Ethernet Interface

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**interface FastEthernet** *number*	Enter interface configuration mode for the Ethernet interface.
Step 3	**pppoe-client dial-pool-number** *number*	Configure the PPPoE client and specifies the dialer pool.
Step 4	**exit**	Return to global configuration mode.
Step 5	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
config terminal)
interface FastEthernet 0/1
 pppoe-client dial-pool-number 1
 exit
```

Enabling the PPPoE Service

Beginning in privileged EXEC mode, follow these steps to enable the PPPoE service:

Procedure

	Command or Action	Purpose
Step 1	**pppoe** *profile_number*	Connect to the PPPoE service. For *profile_number*, specify the target tunnel profile.
Step 2	**copy running-config startup-config**	(Optional) Save your entries in the configuration file.

Example

```
# pppoe 1
```

Monitoring and Debugging the PPPoE Configuration

Use the following global configuration commands to display the PPPoE session statistics:

```
#show pppoe session [status|packets|log]
```

```
#show ip interface pppoe
```

Use the following global configuration command to debug the PPPoE configuragion:

```
# [no] debug pppoe detail
```

Examples

```
Gateway#show pppoe session status
pppoe-status: Link is up and running on interface ppp1
ppp1      Link encap:Point-to-Point Protocol
          inet addr:13.13.1.10  P-t-P:13.13.13.1  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1492  Metric:1
          RX packets:310 errors:0 dropped:0 overruns:0 frame:0
          TX packets:439 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:76623 (74.8 KiB)  TX bytes:128214 (125.2 KiB)

Gateway#show pppoe session packets
      IN   PACK VJCOMP  VJUNC  VJERR  |      OUT   PACK VJCOMP  VJUNC NON-VJ
   76623    310      0      0      0  |   128214    439      0      0    439

Gateway#show ip interface PPPoE
PPP1 is up
  Internet address is 13.13.1.10
  Netmask is 255.255.255.255
  Server address is 13.13.13.1
  MTU is 1492 bytes

Gateway#show ip route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         0.0.0.0         0.0.0.0         U     0      0        0 ppp1
10.0.3.0        0.0.0.0         255.255.255.0   U     0      0        0 lxcbr0
13.13.13.1      0.0.0.0         255.255.255.255 UH    0      0        0 ppp1
```

PPPoE Configuration Examples on IXM and IR829

The following is an example of PPPoE client configuration on IXM:

```
!
interface FastEthernet 0/1
 pppoe-client dial-pool-number 1
 exit
!
interface Dialer 1
 ip address negotiated
 dialer-group 1
 ppp authentication chap
 ppp chap hostname alice
 ppp chap password 1234
 dialer-pool 1
 exit
!
pppoe 1

ipsec enable
```

The folowing is an example of PPPoE server configuration on IR829:

```
IR800#show running-config
*Jul 31 23:55:30.118: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...

Current configuration : 3713 bytes
!
! Last configuration change at 23:55:30 UTC Mon Jul 31 2017
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname IR800
!
boot-start-marker
boot system flash:ir800-universalk9-mz.SPA.156-3.M2
boot-end-marker
!
!
!
aaa new-model
!
!
aaa authentication login default local enable
aaa authentication login IKE1_IKE2_AUTHEN_LOCAL local
aaa authorization network IKE1_IKE2_AUTHOR_LOCAL local
!
!
!
!
!
aaa session-id common
service-module wlan-ap 0 bootimage autonomous
!
```

```
ignition off-timer 900
!
ignition undervoltage threshold 9
!
no ignition enable
!
!
!
!
!
!
!
!
!
!
!


!
!
!
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
!
!
license udi pid IR829GW-LTE-VZ-AK9 sn FTX2124Z04Z
!
!
username cisco privilege 15 password 0 cisco
username alice password 0 1234
!
redundancy
!
!
!
!
!
controller Cellular 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
!
!
!
!
!
!
!
!
!
bba-group pppoe ALTAMEER
 virtual-template 33
!
!
interface Loopback3
```

```
 ip address 13.13.13.1 255.255.255.0
!
interface GigabitEthernet0
 no ip address
 shutdown
!
interface GigabitEthernet1
 no ip address
!
interface GigabitEthernet2
 no ip address
!
interface GigabitEthernet3
 no ip address
 pppoe enable group ALTAMEER
!
interface GigabitEthernet4
 switchport access vlan 10
 no ip address
!
interface Wlan-GigabitEthernet0
 no ip address
!
interface Wpan2
 no ip address
 ieee154 txpower 25
 no ieee154 fec-off
!
interface GigabitEthernet5
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Cellular0
 no ip address
 encapsulation slip
 dialer in-band
 dialer string lte
!
interface Cellular1
 no ip address
 encapsulation slip
!
interface Virtual-Template33
 mtu 1492
 ip unnumbered Loopback3
 ip nat inside
 ip virtual-reassembly in
 peer default ip address pool ALTAMEER
 ppp authentication chap
!
interface wlan-ap0
 no ip address
 shutdown
!
interface Vlan1
 no ip address
 ip nat outside
 ip virtual-reassembly in
 pppoe enable group ALTAMEER
!
interface Vlan10
 ip address 172.27.170.119 255.255.255.128
 ip nat outside
 ip virtual-reassembly in
!
interface Async0
 no ip address
 encapsulation scada
!
interface Async1
 no ip address
 encapsulation scada
!
!
ip local pool ALTAMEER 13.13.1.10 13.13.1.20
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface Vlan10 overload
ip route 0.0.0.0 0.0.0.0 Vlan10 172.27.170.1
ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
!
ipv6 ioam timestamp
!
!
access-list 10 permit any
!
!
!
control-plane
!
!
!
!
line con 0
 exec-timeout 0 0
 stopbits 1
line 1 2
 stopbits 1
line 3
 script dialer lte
 modem InOut
 no exec
 transport preferred lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 transport input all
 transport output all
 rxspeed 2400000
 txspeed 153000
line 4
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line 8
 no exec
 transport preferred lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
line 1/3 1/6
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
```

```
 exec-timeout 0 0
 privilege level 15
 password cisco
 transport input all
 transport output all
!
no scheduler max-task-time
iox client enable interface GigabitEthernet5
!
!
!
!
!
!
end
```

CHAPTER 9

Managing Packet Forwarder

This chapter describes how to configure and manage the LoRaWAN packet forwarder (LRR) based on Thingpark implementation. Note that other 3rd party LoRaWAN packet forwarder may have different file structure. All examples in this section are based on Thingpark.

You can use the packet forwarder upload command to upload any *.ini files to the LXC container /etc/ folder.

LRR package can be copied to flash or usb and installed using packet forwarder command.

Note LRR ID is the key information required to register a LoRaWAN Gateway on Thingpark Network Manager.

Uploading or Downloading Packet Forwarder

Beginning in privileged EXEC mode, follow these steps to upload or download configuration files to host or USB from LRR.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**packet-forwarder** {**upload normal** <*path*> | **download normal** <*filename*>	Upload or download configuration files to host or USB from LRR.
Step 3	**exit**	Return to privileged EXEC mode.
Step 4	**show packet-forwarder uploads** [**detail**]	Display details about uploaded files.

Managing Packet Forwarder

Beginning in privileged EXEC mode, follow these steps to manage the packet forwarder.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**packet-forwarder** [**install** | **uninstall**] [**firmware**| **pubkey**]	Install or uninstall the packet forwarder. The packet forwarder can be installed from a file in USB drive or in flash.
Step 3	**packet-forwarder** [**start** | **restart** | **stop**]	Start, restart, or stop the packet forwarder.
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**show packet-forwarder** [**info**|**status**|**log** [**list**|**name**]]	Show packet forwarder details.

Example

- The following commands install the LRR package:

```
(config)#packet-forwarder install pubkey flash:lrr-opk.pubkey
(config)#packet-forwarder install firmware flash:lrr-1.8.23-ciscoms_noconfig.cpkg
```

- The following commands show the packet forwarder information and status:

```
#show packet-forwarder info
PublicKeyStatus : Installed
FirmwareStatus : Installed
PacketFwdVersion : 1.8.23
LRRID : 6596c32a
PartnerID : 0001
#
#show packet-forwarder status
Status : Running
```

- When the packet-forwarder is shown as “running”, the LRR log files can be displayed IXM through the by using the **show packet-forwarder log list** command:

```
#show packet-forwarder log list
Log file     Description
======================================
lrr.ini      lrr.ini information
config       Get the detail config
radio        Radio status
trace        LRR Trace log
```

- The following command specifies the numbers of log to be displayed.

```
#show packet-forwarder log name config 10
11:37:41.696  (3168) sortchan frhz=913900000 index=58
11:37:41.696  (3168) sortchan frhz=914100000 index=59
```

```
11:37:41.696  (3168) sortchan frhz=914200000 index=71
11:37:41.696  (3168) sortchan frhz=914300000 index=60
11:37:41.696  (3168) sortchan frhz=914500000 index=61
11:37:41.696  (3168) sortchan frhz=914700000 index=62
11:37:41.696  (3168) sortchan frhz=914900000 index=63
$ROOTACT /tmp/mdm/pktfwd/firmware
ConfigDefault '/tmp/mdm/pktfwd/firmware/lrr/config'
ConfigCustom '/tmp/mdm/pktfwd/firmware/usr/etc/lrr'
```

- The following command displays the lrr.ini file.

```
#show packet-forwarder log name lrr.ini
port_crypted_k=0
ftpaddr=[58ba93ec55edaf7b8d43c8fb34bc96652abf5db92b0b675a405ad3abf93289d2]
ftpaddr_crypted_k=0
ftpuser=[df09087afa773c3dde7994ee50ab0ad9]
ftpuser_crypted_k=0
ftppass=[ed37881434753d194bbe66a8bc2de5ba]
ftppass_crypted_k=0
ftpport=[2ab6268fa568f91eaa80c4e531aabe80]
ftpport_crypted_k=0
use_sftp=0
```

CHAPTER 10

Working with Configuration Files and Software Images

This chapter describes how to copy configuration files and how to download software images to a Cisco LoRaWAN Gateway.

Managing Files

You can manage the files system in USB or flash.

Copying Files

To copy a file from a source to a destination, use the **copy** *source-url destination-url* privileged EXEC command. For the source and destination URLs, you can use **running-config** and **startup-config** keyword shortcuts. For example, the **copy running-config startup-config** command saves the currently running configuration file to the NVRAM section of flash memory to be used as the configuration during system initialization.

Network file system URLs include **ftp:** and **tftp:** and have these syntaxes:

- FTP—**ftp:**[[//*username* [**:***password*]@*location*]/*directory*]/*filename*
- TFTP—**tftp:**[[//*location*]/*directory*]/*filename*

Local writable file systems include flash:.

Some invalid combinations of source and destination exist. Specifically, you cannot copy these combinations:

- From a running configuration to a running configuration
- From a startup configuration to a startup configuration
- From a device to the same device (for example, the **copy flash: flash:** command is invalid)

You can copy from remote to local, local to remote, and local to local. However, copying from remote to remote is not supported. During the copying process, one symbol ! printed on the screen indicates 100 blocks (512 bytes per block) transferred.

For specific examples of using the **copy** command with configuration files, see Working with Configuration Files, on page 56.

To copy software images either by downloading a new version or by uploading the existing one, use the **archive download-sw** or the **archive upload-sw** privileged EXEC command. For more information, see Working with Software Images, on page 57.

File Management Commands

You can use the commands in the following table to manage the file system.

Table 5: File Management Commands

Command	Description
cd	Change current directory.
copy	Copy from one file to another.
delete	Delete a file.
dir	List files on a filesystem.
format	Format a filesystem. **Note** Only flash can be formatted.
mkdir	Create a new directory.
more	Display the contents of a file.
pwd	Display the current working directory.
rename	Rename a file.

Working with Configuration Files

This section describes how to download or maintain configuration files.

You can copy (*download*) configuration files from a TFTP or FTP server to the running configuration or startup configuration of the Cisco LoRaWAN Gateway. You might perform this task to back up a current configuration file to a server before changing its contents so that you can later restore the original configuration file from the server.

The protocol you use depends on which type of server you are using. The FTP transport mechanisms provide faster performance and more reliable delivery of data than TFTP. These improvements are possible because FTP is built on and uses the TCP/IP stack, which is connection-oriented.

Configuration File Types and Location

Startup configuration files are used during system startup to configure the software. Running configuration files contain the current configuration of the software. The two configuration files can be different. For example, you might want to change the configuration for a short time period rather than permanently. In this case, you would change the running configuration but not save the configuration by using the **copy running-config startup-config** privileged EXEC command.

Displaying Configuration Files

To display the configuration of the device, use the **show** [**running-config** | **startup-config**] EXEC command.

Removing Configuration Files

To remove the configuration of the device, use the **no configuration** command in global configuration mode.

Reloading the System

To reboot the system, use the **reload** EXEC command.

The reload command will first check if the running configuration has been saved and prompt user if not. You can enter **yes** to save the configuration or **no** to skip this step. Then, you will be prompted to reload the system.

Working with Software Images

This section describes how to download software image files, which is stored as a *.tar.gz* file and contains the kernel and root file system.

You can download a Cisco LoRaWAN Gateway image file from a TFTP or FTP server, or from a USB device, to upgrade the Cisco LoRaWAN Gateway software.

Downloading an Image File

Note When upgrading from any version prior to Release 1.0.20 to Release 2.0, you must perform a factory upgrade for proper behavior.

Note To download the firmware from an USB device, you should first enable the USB support by executing the **usb enable** command.

Beginning in privileged EXEC mode, follow these steps to download a new image file.

Procedure

	Command or Action	Purpose
Step 1	—	Log into the Cisco LoRaWAN Gateway through through SSH or Console. **Note** The console port is 115.2kbs.
Step 2	**archive download-sw firmware** {**/factory** | **/normal** | **/uboot-only** | **/uboot-normal** | **/uboot-factory** [**/save-reload** | **/force-reload**]} *path*	Download the image file to the Cisco LoRaWAN Gateway. • **/factory** – Upgrade the firmware and delete user data. **Note** Avoid using the **/factory** option with this command, because it erases everything and brings back to factory default. • **/factory** - Upgrade the firmware and delete the user data • **/normal** - Upgrade the firmware and keep the user data • **/uboot-only** - Upgrade the uboot and keep the user data • **/uboot-normal** - Upgrade the uboot and firmware, and keep the user data • **/uboot-factory** - Upgrade the uboot and firmware, and delete the user data • **/save-reload** – Save the current configuration if required and reload the system after successful upgrade. • **/force-reload** – Do not save the current configuration and reload the system after successful upgrade. • *path* - The location of the file, which can be usb:, tftp, ftp, or flash:

What to do next

Example

```
#archive download-sw firmware /normal /save-reload
tftp://172.27.74.9/corsica_i_k9-2.0.0015.tar.gz
```

USB Support

After the USB is plugged in:

- To enable USB, use the following command:

```
Router# usb enable
```

- To display the USB content, use the following command:

```
Router# dir usb:
```

- To disable USB, use the following command:

```
Router# usb disable
```

The USB partition should be formatted to FAT//ms-dos. Other file system types are not supported.

- For the formatting on Windows 7 and Windows 10, choose **Fat** (default) for the format option, and **4096 bytes** for the allocation size; or choose **Fat32** for the format option, and **2048 bytes** for the allocation size.
- For the formatting on MAC OS, choose **MS-Dos (FAT)**.

Note To make sure that the USB is detected and usable on the IXM:

1. If any error is shown during the formatting, try to format it again or use another USB.
2. Do not unplug the USB directly after formatting. Use the **Eject** command provided by the host OS.

Configuring U-boot

U-boot is a universal bootloader for embedded boards based on PowerPC, ARM, MIPS and several other processors, which can be installed in a boot ROM and used to initialize and test the hardware or to download and run OS and application code.

Bootloader version requirement for the u-boot feature is “Bootloader Version: 20170515_cisco”.

Beginning in privileged EXEC mode, follow these steps to configure U-boot option.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enter global configuration mode.

	Command or Action	Purpose
Step 2	**uboot console** {**disable**|**restore**}	Configure U-boot console. • **disable** - Disable U-boot console (and System console if SSH is enabled). **Note** When **IP SSH limit local** is enabled on the IXM, the SSH access from outside is disabled for the unit. The **uboot console disable** option only checks whether SSH is enabled or not, and does not factor the **IP SSH limit local** option. If both commands are configured, it is possible that both the console conntecvity and SSH connectivity are lost. In that case, the only way to access the unit is through container via Thing park. • **restore** - Restore U-boot console (and System console if it was disabled).
Step 3	**uboot protection** *word*	Enable U-boot password protection. • *word* - 8 to 30 alphanumeric or special characters. To disable U-boot password protection, use the **no uboot protection** command.
Step 4	**exit**	Return to privileged EXEC mode.
Step 5	**show uboot console** **Example:** `show uboot protection`	Show U-boot console status. Show U-boot password protection status.

CHAPTER 11

FND Configuration for IXM

The Cisco IoT Field Network Director (IoT FND) is a software platform that manages a multi-service network and security infrastructure for IoT applications, such as smart grid applications, including Advanced Metering Infrastructure (AMI), Distribution Automation (DA), distributed intelligence, and substation automation. IoT FND is a scalable, highly-secure, modular, and open platform with an extensible architecture. IoT FND is a multi-vendor, multi-service, communications network management platform that enables network connectivity to an open ecosystem of power grid devices.

For more information about FND, see the FND documentation at the following URL: https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/tsd-products-support-series-home.html.

IoT FND supports the following configurations for the Cisco Wireless Gateway for LoRaWAN:

- Firmware upgrade
- Hardware monitoring and events report
- IP networking configuration and operations (for example, IP address and IPsec)
- Zero Touch provisioning, including initial installation of the Thingpark LRR software

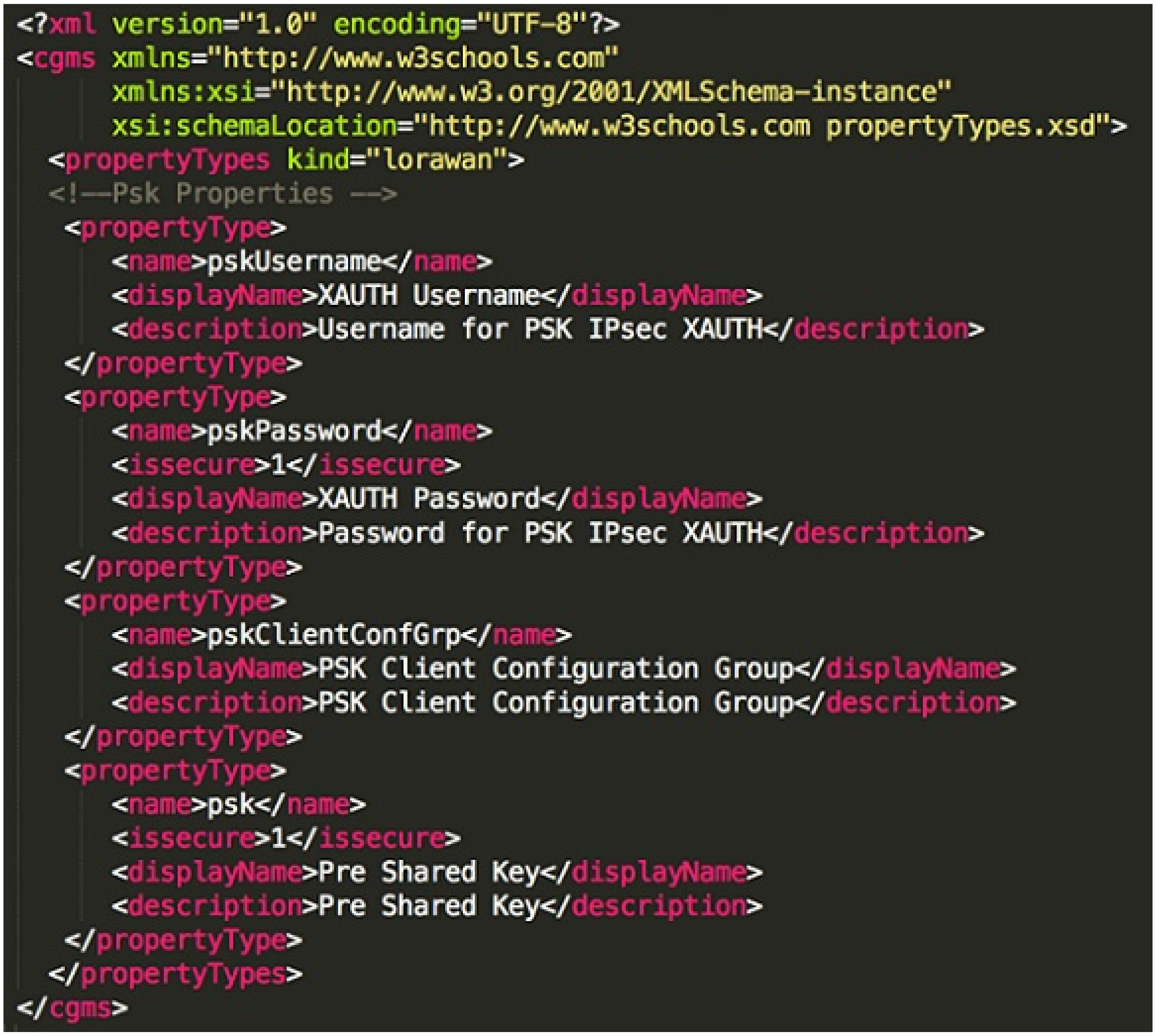
This chapter contains the following topics.

Preparing FND for IXM ZTD

Follow these steps to prepare FND for IXM ZTD:

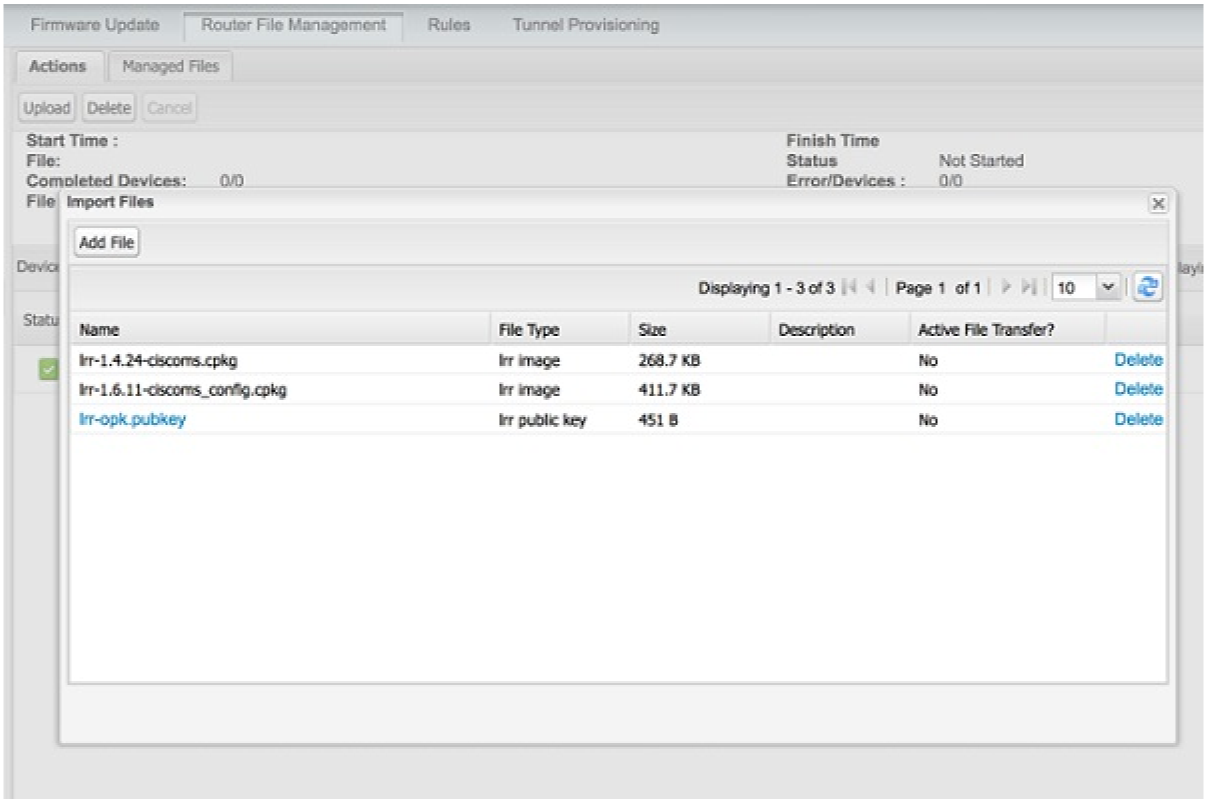
Procedure

Step 1 If you are using PSK authentication for tunneloing, add the **userPropertyTypes.xml** file to the FND server under **/opt/cgms/server/cgms/conf**. Restart the FND service after adding the following. If you are using RSA, ignore this step.



```
<?xml version="1.0" encoding="UTF-8"?>
<cgms xmlns="http://www.w3schools.com"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://www.w3schools.com propertyTypes.xsd">
  <propertyTypes kind="lorawan">
  <!--Psk Properties -->
   <propertyType>
      <name>pskUsername</name>
      <displayName>XAUTH Username</displayName>
      <description>Username for PSK IPsec XAUTH</description>
   </propertyType>
   <propertyType>
      <name>pskPassword</name>
      <issecure>1</issecure>
      <displayName>XAUTH Password</displayName>
      <description>Password for PSK IPsec XAUTH</description>
   </propertyType>
   <propertyType>
      <name>pskClientConfGrp</name>
      <displayName>PSK Client Configuration Group</displayName>
      <description>PSK Client Configuration Group</description>
   </propertyType>
   <propertyType>
      <name>psk</name>
      <issecure>1</issecure>
      <displayName>Pre Shared Key</displayName>
      <description>Pre Shared Key</description>
   </propertyType>
  </propertyTypes>
</cgms>
```

Step 2 Add the Actility LRR and public key to FND by clicking the **import** button on the File Management page.



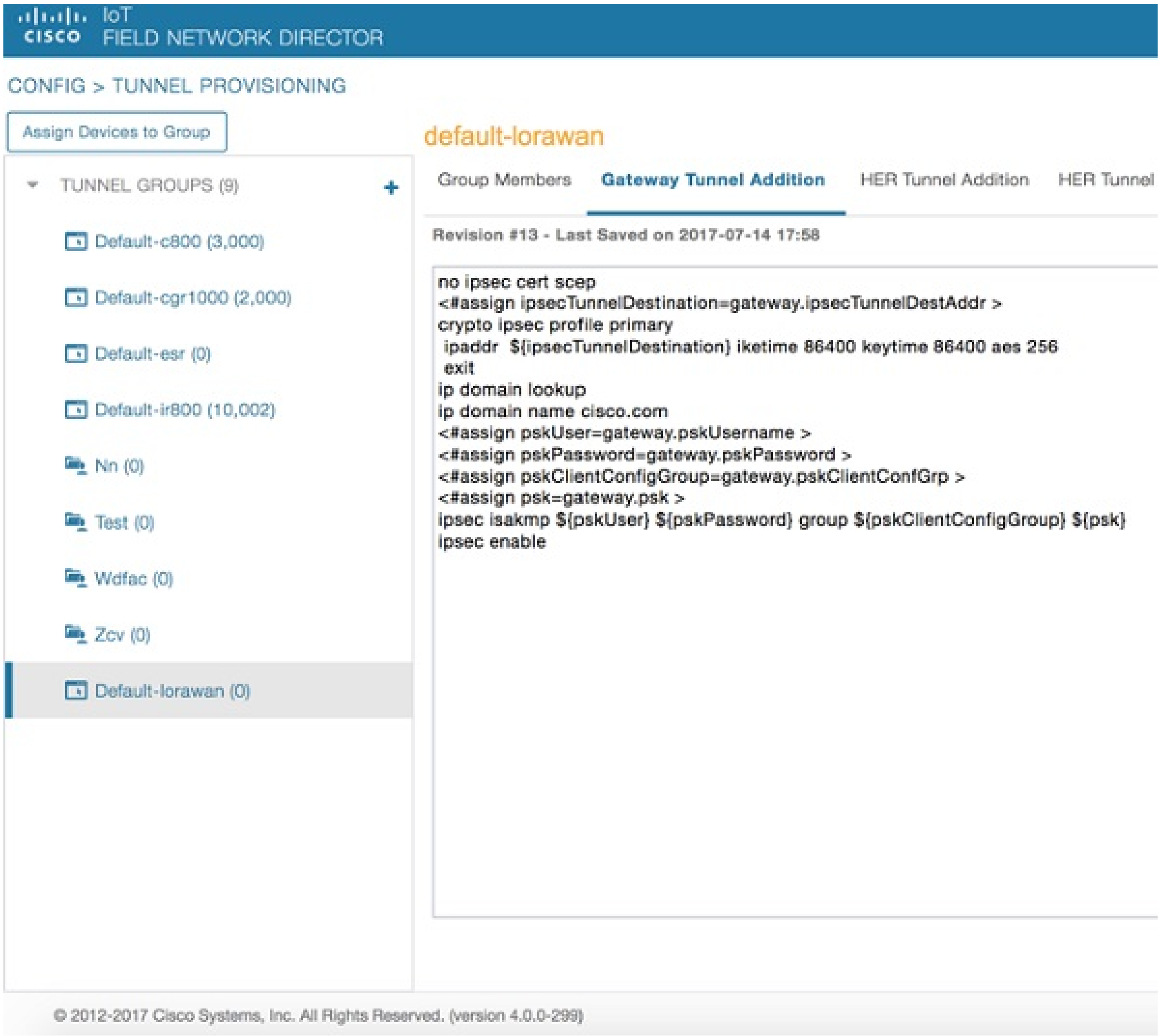
Start Time :
File:
Completed Devices: 0/0
File

Finish Time
Status Not Started
Error/Devices : 0/0

Displaying 1 - 3 of 3 | Page 1 of 1 | 10

Name	File Type	Size	Description	Active File Transfer?	
lrr-1.4.24-ciscoms.cpkg	lrr image	268.7 KB		No	Delete
lrr-1.6.11-ciscoms_config.cpkg	lrr image	411.7 KB		No	Delete
lrr-opk.pubkey	lrr public key	451 B		No	Delete

Step 3 Update the Tunnel Configuration group with the following parameters and save the changes. The following figure shows an example for PSK.

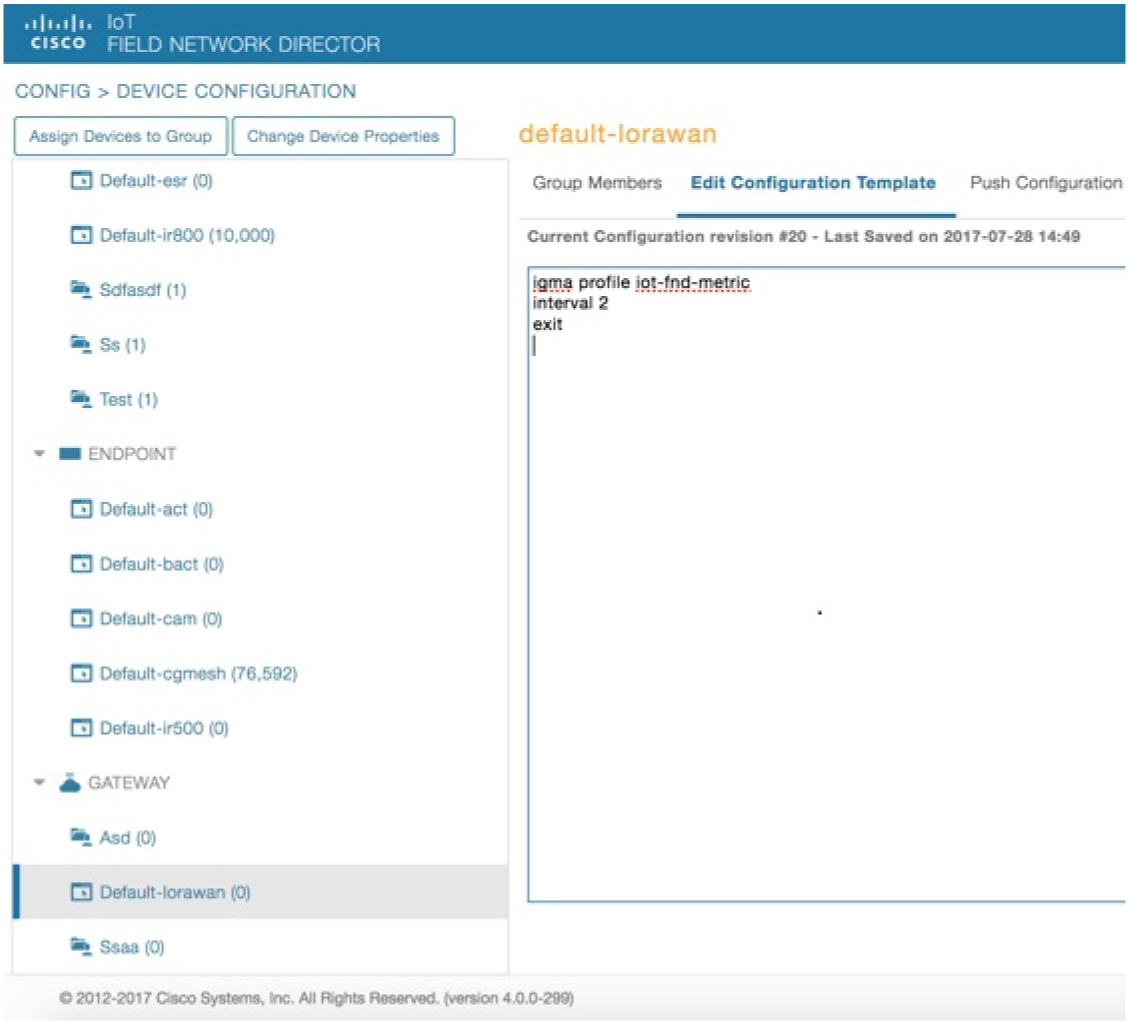


Revision #13 - Last Saved on 2017-07-14 17:58

```
no ipsec cert scep
<#assign ipsecTunnelDestination=gateway.ipsecTunnelDestAddr >
crypto ipsec profile primary
 ipaddr  ${ipsecTunnelDestination} iketime 86400 keytime 86400 aes 256
 exit
ip domain lookup
ip domain name cisco.com
<#assign pskUser=gateway.pskUsername >
<#assign pskPassword=gateway.pskPassword >
<#assign pskClientConfigGroup=gateway.pskClientConfGrp >
<#assign psk=gateway.psk >
ipsec isakmp ${pskUser} ${pskPassword} group ${pskClientConfigGroup} ${psk}
ipsec enable
```

© 2012-2017 Cisco Systems, Inc. All Rights Reserved. (version 4.0.0-299)

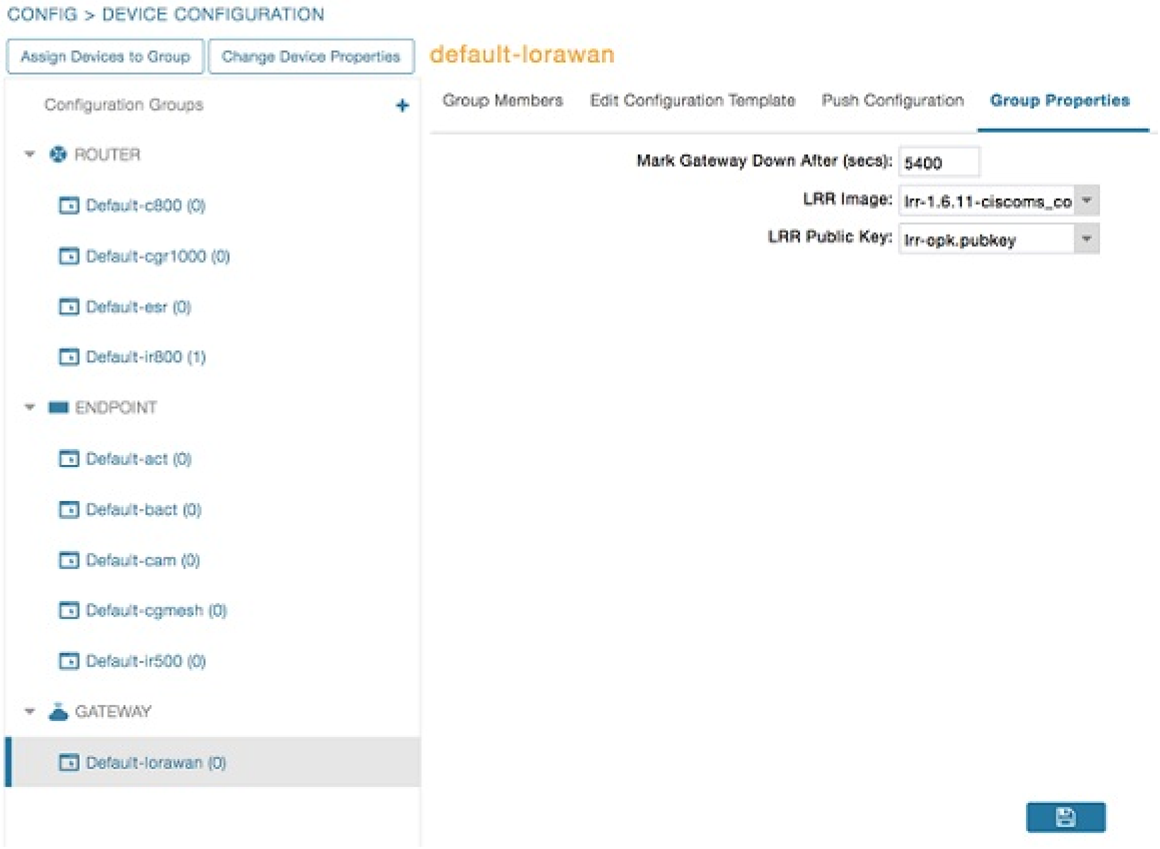
Step 4 Update the Device Configuration group with the following parameters and save the changes. The following figure shows a sample configuration.



Current Configuration revision #20 - Last Saved on 2017-07-28 14:49

```
igma profile iot-fnd-metric
interval 2
exit
```

Update the Device Configuration Group properties with the following parameters and save the changes.

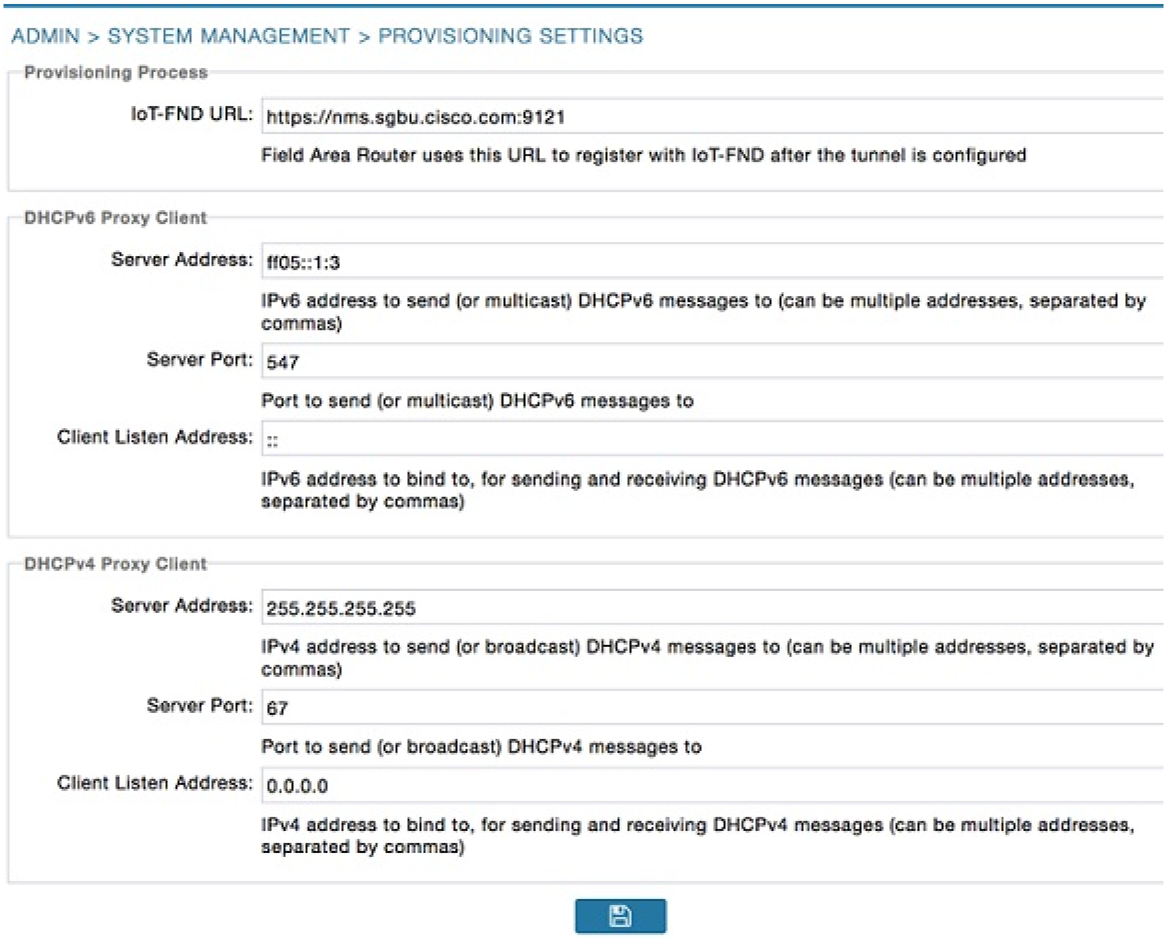


Mark Gateway Down After (secs): 5400

LRR Image: lrr-1.6.11-ciscoms_co

LRR Public Key: lrr-opk.pubkey

The Tunnel Provisioning settings page will have the FND common name populated as the following figure shows.



Provisioning Process

IoT-FND URL: https://nms.sgbu.cisco.com:9121

Field Area Router uses this URL to register with IoT-FND after the tunnel is configured

DHCPv6 Proxy Client

Server Address: ff05::1:3

IPv6 address to send (or multicast) DHCPv6 messages to (can be multiple addresses, separated by commas)

Server Port: 547

Port to send (or multicast) DHCPv6 messages to

Client Listen Address: ::

IPv6 address to bind to, for sending and receiving DHCPv6 messages (can be multiple addresses, separated by commas)

DHCPv4 Proxy Client

Server Address: 255.255.255.255

IPv4 address to send (or broadcast) DHCPv4 messages to (can be multiple addresses, separated by commas)

Server Port: 67

Port to send (or broadcast) DHCPv4 messages to

Client Listen Address: 0.0.0.0

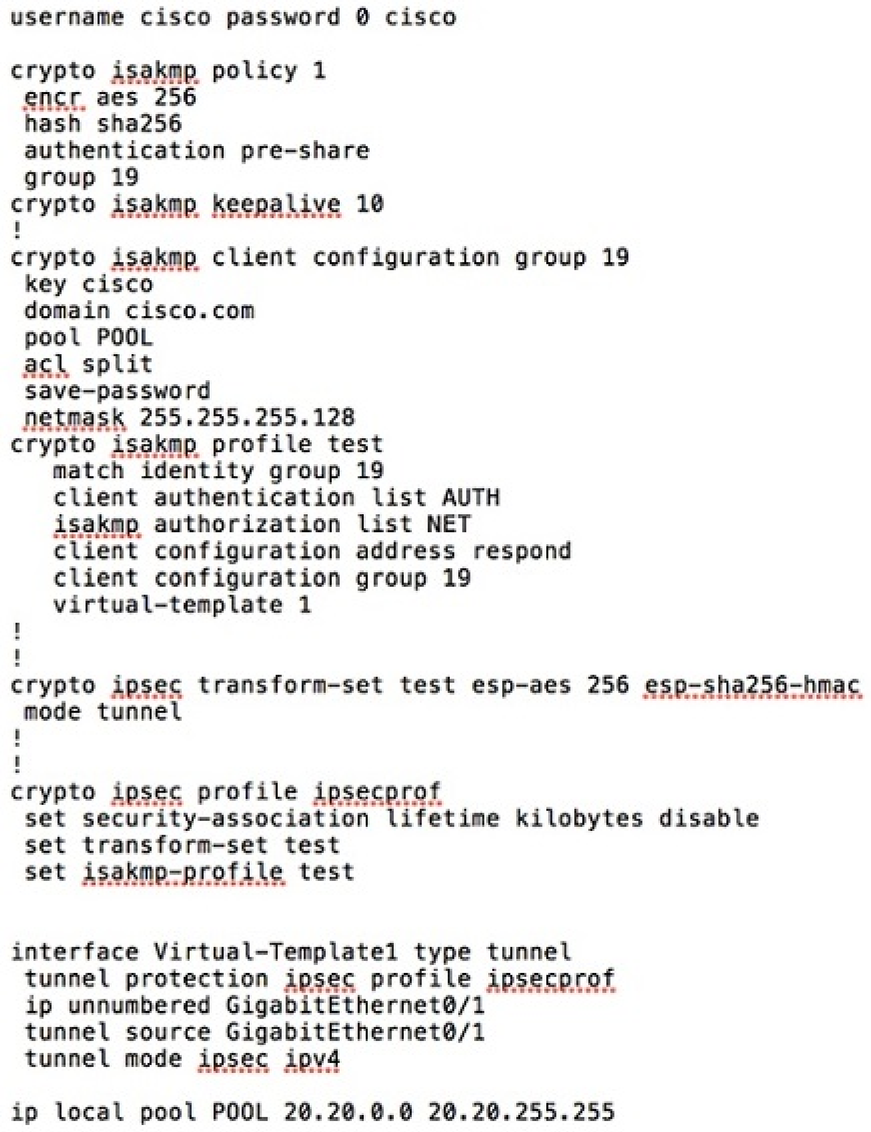
IPv4 address to bind to, for sending and receiving DHCPv4 messages (can be multiple addresses, separated by commas)

Step 5 Make sure you have obtained certificates from the CA (the same ones used to issue certs for FND). Execute the **show ipsec certs** command to verify. Make sure the firewall allows ports 9120, 9121, 9122, and all the SSH, telnet, and DHCP ports. Make sure the TPS name is pingable. Then execute the **copy running express-setup-config** command.

```
Hostname IXM
!
ip domain lookup
ip domain name cisco.com
!
ip name-server 55.55.0.15
!
interface FastEthernet 0/1
 description interface
 ip address 4.4.4.2 255.255.255.0
 exit
!
ip default-gateway 4.4.4.1
!
ntp server ip 55.55.0.1
!
clock timezone America/Los_Angeles
!
igma profile iot-fnd-tunnel
```

```
 active
 add-command show fpga
 interval 5
 url https://ps.sgbu.cisco.com:9120/igma/tunnel
 exit

ipsec cert scep https://55.55.0.15/csertsrv/msecp.dll us ca mil cisco iot test true ndes
true 2048
```

You need to add the HER configuration manually, for example, the tunnel crypto profiles and transform sets. The following easyVPN example uses PSK as authentication.

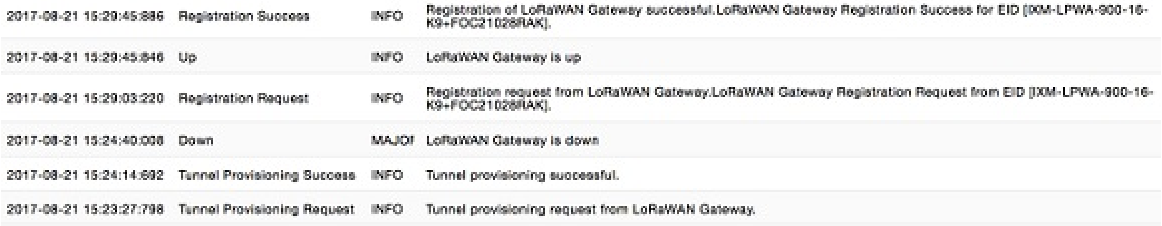


```
username cisco password 0 cisco

crypto isakmp policy 1
 encr aes 256
 hash sha256
 authentication pre-share
 group 19
crypto isakmp keepalive 10
!
crypto isakmp client configuration group 19
 key cisco
 domain cisco.com
 pool POOL
 acl split
 save-password
 netmask 255.255.255.128
crypto isakmp profile test
   match identity group 19
   client authentication list AUTH
   isakmp authorization list NET
   client configuration address respond
   client configuration group 19
   virtual-template 1
!
!
crypto ipsec transform-set test esp-aes 256 esp-sha256-hmac
 mode tunnel
!
!
crypto ipsec profile ipsecprof
 set security-association lifetime kilobytes disable
 set transform-set test
 set isakmp-profile test


interface Virtual-Template1 type tunnel
 tunnel protection ipsec profile ipsecprof
 ip unnumbered GigabitEthernet0/1
 tunnel source GigabitEthernet0/1
 tunnel mode ipsec ipv4

ip local pool POOL 20.20.0.0 20.20.255.255
```

Step 6 Encrypt the PSK passwords using the signature-tool under **/opt/cgms-tools/bin**. Add the encrypted passwords in the CSV file and prepare it for upload. Add the modem to FND as the following sample CSV shows. Add ISR4K using the following CSV.

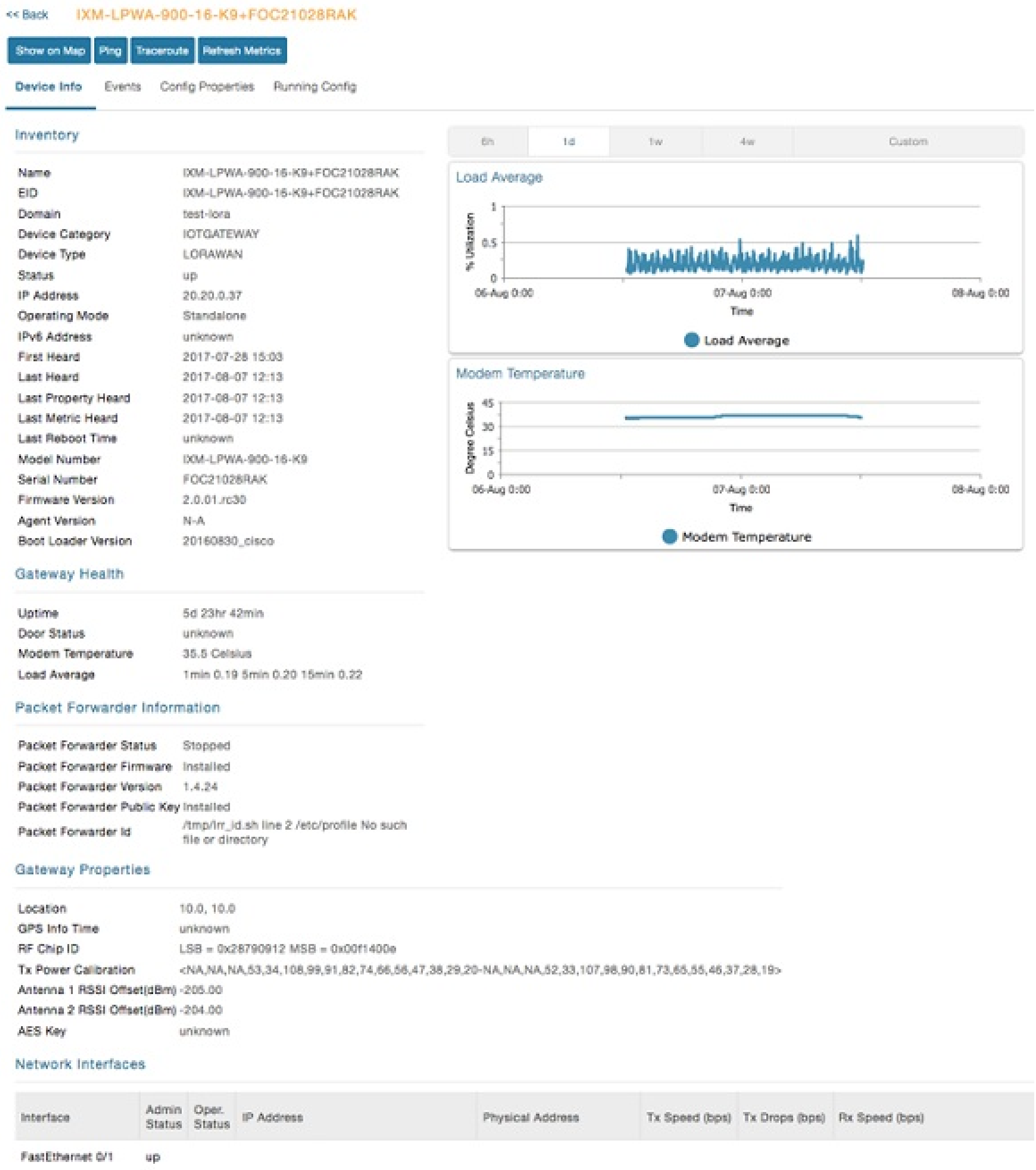
```
eid,netconfUsername,netconfPassword,ip,deviceType,lat,domain,lng,ipsecTunnelDestAddr,tunnelHerEid,
pskUsername,pskPassword,pskClientConfGrp,psk
IXM-LPWA-900-16-K9+FOC21028RAK,,,,lorawan,10,root,10,4.4.4.1,C3900-SPE250/K9+FOC172417YT,cisco,
ki8OjEO5Pr+krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uXs8JRuSPOfojMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThiLERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFxarakJsfo/zd69EpzrI8Hsic/QmMzA==,19,
ki8OjEO5Pr+krJTtUooUMD0GoqmOAznc2JObiUUr4ismXyP0uXs8JRuSPOfojMDavGIHiO8unUUJm3zdxv0LP8b6fe5G+
oshy76A6IqX1jk7ymSFOaVPQBT8fUS6onjsuSThiLERS0B6Brn2gRx/KpQMk9IdYQMOSsHh4khvtxbqBZy6j++pIjeG4+
dPz/v52DmJR+DOrE7ZQpfvS9PSHkJoaqC2o6PrKN5YZ50G9+Tm+diPmbyv/PdHKtXn1ny3qBAdbfDwOjlA+NtJPld3/
06vq6WhHsgujYwMJWs7Cuu3rR0/FVHF/5wFxarakJsfo/zd69EpzrI8Hsic/QmMzA==
C3900-SPE250/K9+FOC172417YT,nms,sgbu123!,55.55.0.18,isr3900,,,,,,,,,
```

Step 7 Once the Modem is registered, the IXM will show as up in the FND. Please check the following events if there are issues during ZTD.



2017-08-21 15:29:45:886	Registration Success	INFO	Registration of LoRaWAN Gateway successful.LoRaWAN Gateway Registration Success for EID [IXM-LPWA-900-16-K9+FOC21028RAK].
2017-08-21 15:29:45:846	Up	INFO	LoRaWAN Gateway is up
2017-08-21 15:29:03:220	Registration Request	INFO	Registration request from LoRaWAN Gateway.LoRaWAN Gateway Registration Request from EID [IXM-LPWA-900-16-K9+FOC21028RAK].
2017-08-21 15:24:40:008	Down	MAJOI	LoRaWAN Gateway is down
2017-08-21 15:24:14:692	Tunnel Provisioning Success	INFO	Tunnel provisioning successful.
2017-08-21 15:23:27:798	Tunnel Provisioning Request	INFO	Tunnel provisioning request from LoRaWAN Gateway.

Step 8 Detailed IXM modem information can be viewed by clicking on the modem link.



IXM-LPWA-900-16-K9+FOC21028RAK

Inventory

Name	IXM-LPWA-900-16-K9+FOC21028RAK
EID	IXM-LPWA-900-16-K9+FOC21028RAK
Domain	test-lora
Device Category	IOTGATEWAY
Device Type	LORAWAN
Status	up
IP Address	20.20.0.37
Operating Mode	Standalone
IPv6 Address	unknown
First Heard	2017-07-28 15:03
Last Heard	2017-08-07 12:13
Last Property Heard	2017-08-07 12:13
Last Metric Heard	2017-08-07 12:13
Last Reboot Time	unknown
Model Number	IXM-LPWA-900-16-K9
Serial Number	FOC21028RAK
Firmware Version	2.0.01.rc30
Agent Version	N-A
Boot Loader Version	20160830_cisco

Gateway Health

Uptime	5d 23hr 42min
Door Status	unknown
Modem Temperature	35.5 Celsius
Load Average	1min 0.19 5min 0.20 15min 0.22

Packet Forwarder Information

Packet Forwarder Status	Stopped
Packet Forwarder Firmware	Installed
Packet Forwarder Version	1.4.24
Packet Forwarder Public Key	Installed
Packet Forwarder Id	/tmp/lrr_id.sh line 2 /etc/profile No such file or directory

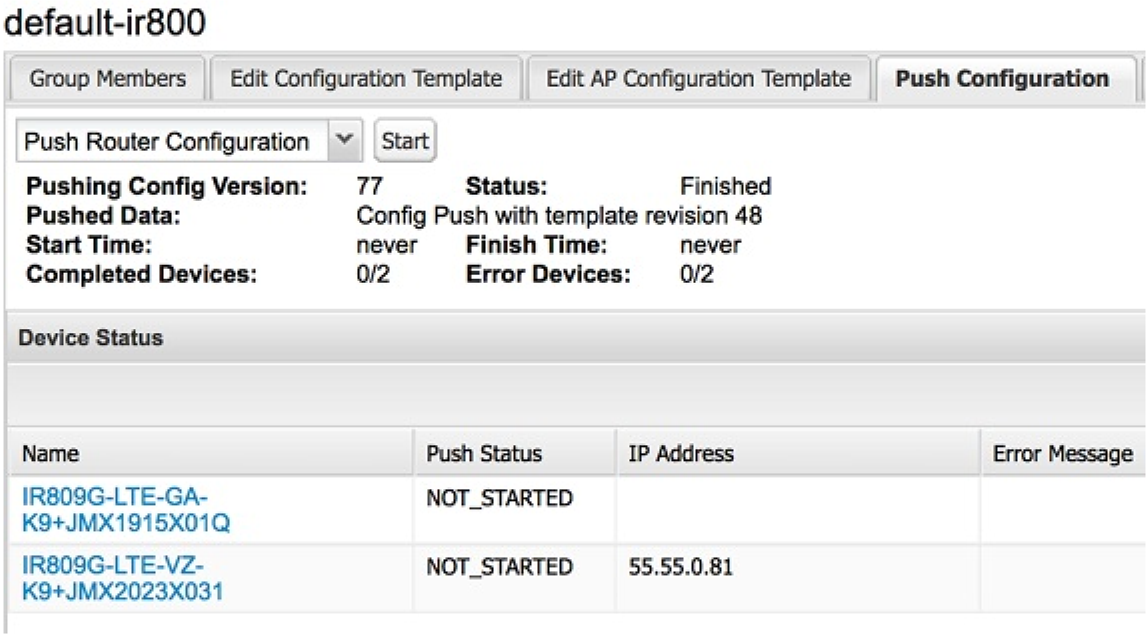
Gateway Properties

Location	10.0, 10.0
GPS Info Time	unknown
RF Chip ID	LSB = 0x28790912 MSB = 0x00f1400e
Tx Power Calibration	<NA,NA,NA,53,34,108,99,91,82,74,66,56,47,38,29,20-NA,NA,NA,52,33,107,98,90,81,73,65,55,46,37,28,19>
Antenna 1 RSSI Offset(dBm)	-205.00
Antenna 2 RSSI Offset(dBm)	-204.00
AES Key	unknown

Network Interfaces

Interface	Admin Status	Oper. Status	IP Address	Physical Address	Tx Speed (bps)	Tx Drops (bps)	Rx Speed (bps)
FastEthernet 0/1	up						

Step 9 If configuration update is required or a new modem is added to the router, follow the same procefure from Step 1. But in this case you invoke a configuration push.


default-ir800
Group Members
Edit Configuration Template
Edit AP Configuration Template
Push Configuration
Push Router Configuration
Start
Device Status

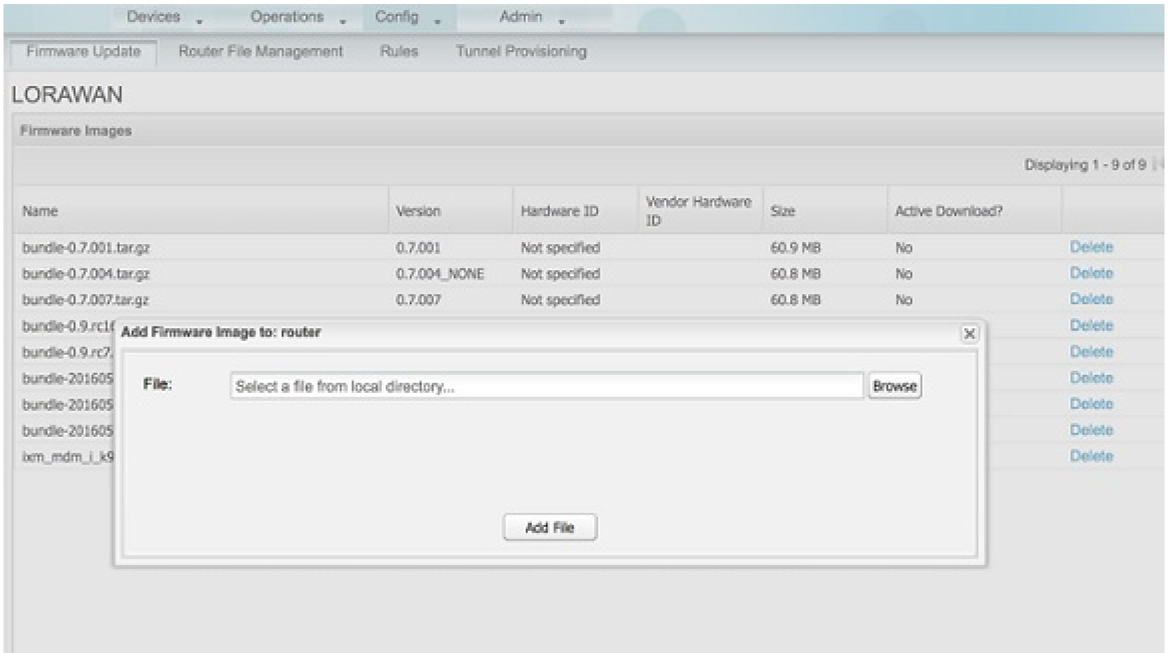
Pushing Config Version: 77 **Status:** Finished
Pushed Data: Config Push with template revision 48
Start Time: never **Finish Time:** never
Completed Devices: 0/2 **Error Devices:** 0/2

Name	Push Status	IP Address	Error Message
IR809G-LTE-GA-K9+JMX1915X01Q	NOT_STARTED		
IR809G-LTE-VZ-K9+JMX2023X031	NOT_STARTED	55.55.0.81	

IXM modem Firmware Update

Procedure

Step 1 Load the firmware file to FND.



LORAWAN

Firmware Images

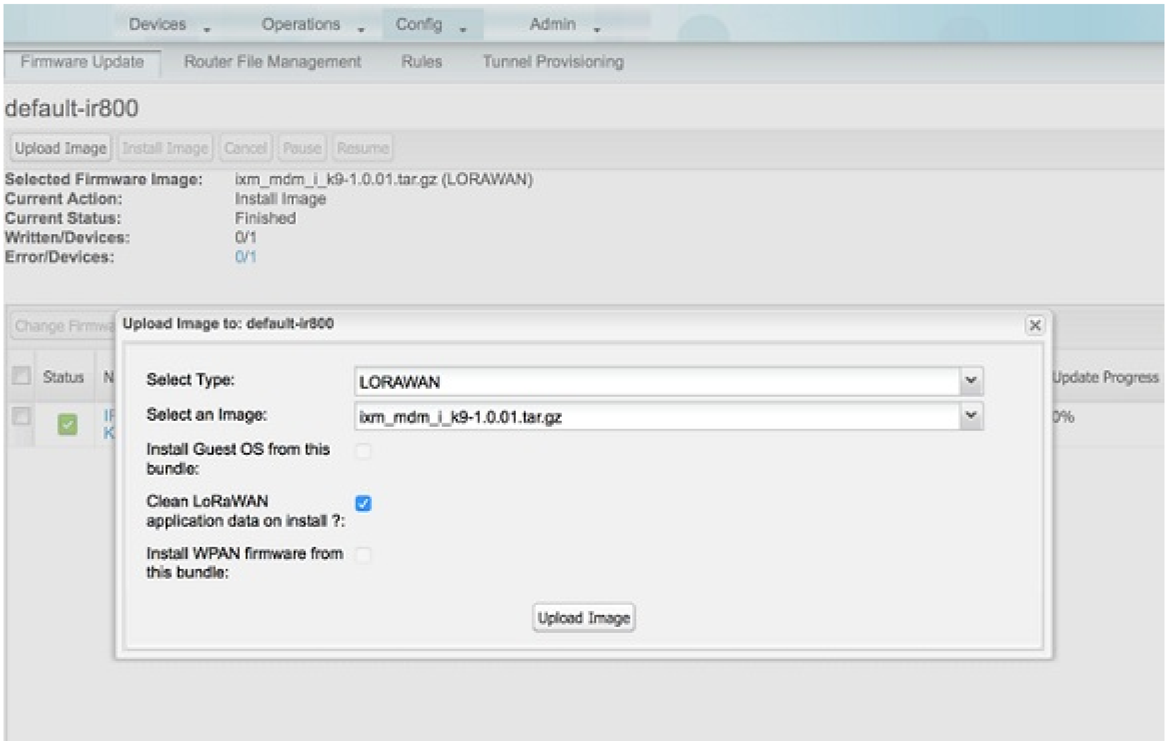
Displaying 1 - 9 of 9

Name	Version	Hardware ID	Vendor Hardware ID	Size	Active Download?	
bundle-0.7.001.tar.gz	0.7.001	Not specified		60.9 MB	No	Delete
bundle-0.7.004.tar.gz	0.7.004_NONE	Not specified		60.8 MB	No	Delete
bundle-0.7.007.tar.gz	0.7.007	Not specified		60.8 MB	No	Delete
bundle-0.9.rc1(						Delete
bundle-0.9.rc7.						Delete
bundle-201605						Delete
bundle-201605						Delete
bundle-201605						Delete
ixm_mdm_i_k9						Delete

Add Firmware Image to: router

File: Select a file from local directory...

Step 2 Push the firmware to the IXM modem. If you want to erase the LRR or pubkey, select the clean install option as shown below.



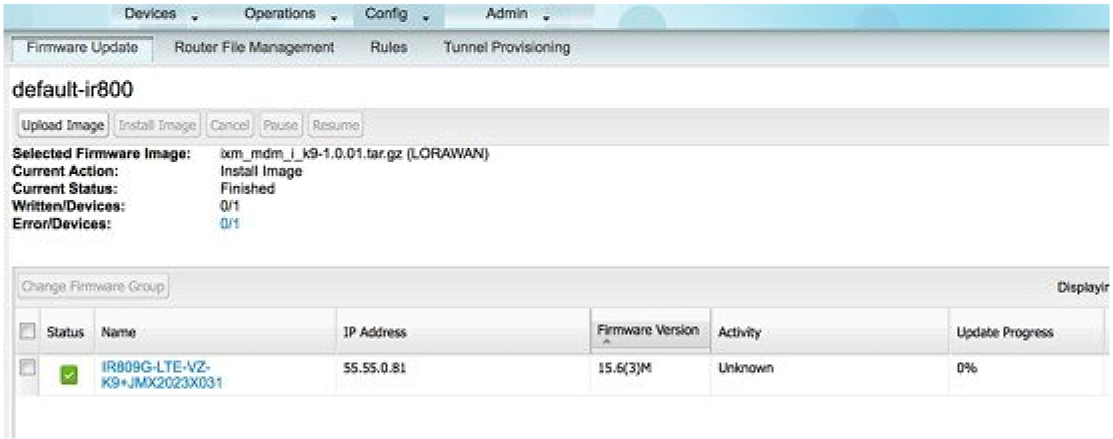
default-ir800

Selected Firmware Image: ixm_mdm_i_k9-1.0.01.tar.gz (LORAWAN)
Current Action: Install Image
Current Status: Finished
Written/Devices: 0/1
Error/Devices: 0/1

Upload Image to: default-ir800

Select Type: LORAWAN
Select an Image: ixm_mdm_i_k9-1.0.01.tar.gz
Install Guest OS from this bundle: □
Clean LoRaWAN application data on install ?: ☑
Install WPAN firmware from this bundle: □

Step 3 When upload is complete, install the image by clicking the **install** button.



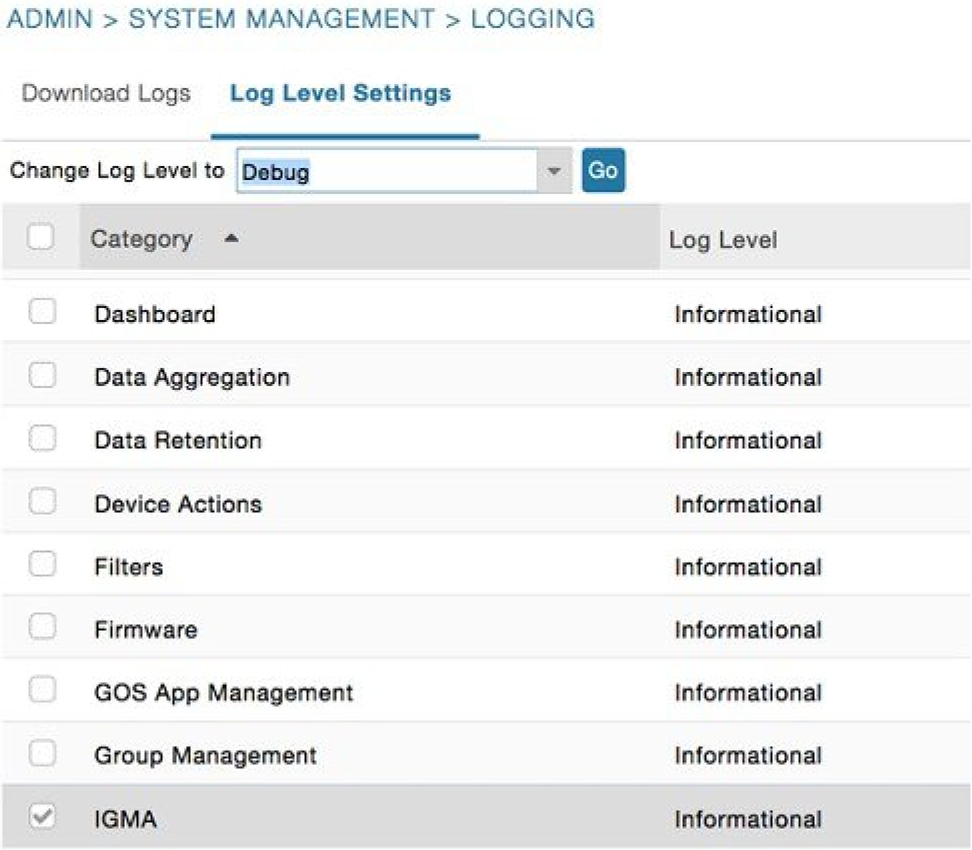
default-ir800

Selected Firmware Image: ixm_mdm_i_k9-1.0.01.tar.gz (LORAWAN)
Current Action: Install Image
Current Status: Finished
Written/Devices: 0/1
Error/Devices: 0/1

□	Status	Name	IP Address	Firmware Version	Activity	Update Progress
□	✓	IR809G-LTE-VZ-K9+JMX2023X031	55.55.0.81	15.6(3)M	Unknown	0%

Troubleshooting

Enable the following debug categories on FND before troubleshooting:



Change Log Level to Debug

□	Category	Log Level
□	Dashboard	Informational
□	Data Aggregation	Informational
□	Data Retention	Informational
□	Device Actions	Informational
□	Filters	Informational
□	Firmware	Informational
□	GOS App Management	Informational
□	Group Management	Informational
☑	IGMA	Informational

- TPS does not have any messages from IXM.

  - Check if the certs are installed correctly on IXM and from the same CA as the FND certs.
  - Make sure the IGMA profile is pointing to the correct tunnel profile and the proxy name resolution is correct.
  - Make sure the proxy can be pinged.
  - Make sure the IGMA profile has the correct commands.

- FND does not have any messages from the IXM.
  - Check if the tunnel network is reachable from the FND cluster.
  - Make sure the IGMA profile is pointing to the correct FND profile and the name resolution is correct.
  - Make sure the FND can be pinged.

- Tunnel provisioning request failed.
  - Check the FND tunnel template for command accuracy.

- FND Registration failed.
  - Check the FND configuration template for command accuracy.
  - Tunnel issues (for example, flapping or disconnect).