CONTENTS

Full Cisco Trademarks with Software License  ?

Preface  ix

Conventions  ix

Related Publications  x

Obtaining Documentation and Submitting a Service Request  x

CHAPTER 1

Overview  1

Overview  1

Switching to Virtual Mode  2

Displaying System Information  2

Displaying Version Information  2

Displaying Platform Status  3

Displaying AES Key  3

Displaying GPS Information  3

Displaying FPGA Information  4

Displaying Inventory Information  5

Displaying Radio Information  5

Displaying Certificate Information  6

CHAPTER 2

Assigning IP Address and Domain Name Server  7

Assigning IP Address  7

Configuring DHCP  7

Understanding DHCP  7

Enabling DHCP on Interfaces  8

Manually Assigning IP Information  8
Configuring DNS 9
  DNS Client 9
  Name Servers 9
  DNS Operation 10
  Configuring DNS Server 10

Mapping Hostnames to IP Addresses 10

CHAPTER 3

Administering the Cisco LoRaWAN Gateway 13
  Managing the System Time and Date 13
  Network Time Protocol (NTP) 13
  NTP Version 4 13
  Configuring NTP Server 14
  Configuring a System Name and Prompt 14
  Configuring GPS as the Clock Source 15
  Configuring UBX Support for GPS 15
  Checking and Saving the Running Configuration 16
  Reloading IXM 16
  Using Reset Button 16

CHAPTER 4

Configuring VLAN 17
  Configuring IP Address for VLAN 17
  Configuring VLAN Trunks 18
  Configuring a Trunk Port 18
    Defining the Allowed VLANs on a Trunk 18
  Enabling Sending and Receiving Tagged Packet on Ethernet Port 19
  Examples of Show Commands 20

CHAPTER 5

Configuring CDP 21
  Understanding CDP 21
  Configuring CDP 21
    Enabling and Disabling CDP 21
    Configuring the CDP Characteristics 22

CHAPTER 6

Configuring Authentication 23
<table>
<thead>
<tr>
<th>Chapter 7</th>
<th>Configuring IPSec</th>
<th>33</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Understanding IPSec</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Configuring IPsec</td>
<td>33</td>
</tr>
<tr>
<td></td>
<td>Configuring Crypto IPSec Profile Common</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Configuring Crypto IPSec Profile Individual</td>
<td>36</td>
</tr>
<tr>
<td></td>
<td>Basic Configuration for RSA to Connect to Primary and Secondary</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Locking Traffic to IPSec Tunnels</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>Erasing IPSec Certificates and Key</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Uploading Certificates from USB or Local Flash</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Disabling LXC Restart During IPSec Reauthentication</td>
<td>39</td>
</tr>
<tr>
<td></td>
<td>Resetting Secure-Storage for Certificate Download</td>
<td>39</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 8</th>
<th>Configuring PPPoE</th>
<th>41</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PPPoE Client Overview</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Configuring the Dialer Interface</td>
<td>41</td>
</tr>
<tr>
<td></td>
<td>Configuring the Ethernet Interface</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Enabling the PPPoE Service</td>
<td>43</td>
</tr>
<tr>
<td></td>
<td>Monitoring and Debugging the PPPoE Configuration</td>
<td>44</td>
</tr>
</tbody>
</table>
## Contents

### Chapter 9

**Managing Packet Forwarder**

- Uploading or Downloading Packet Forwarder 51
- Managing Packet Forwarder 52
- Managing Common Packet Forwarder (CPF) 53
  - Understanding Common Packet Forwarder 53
  - Configuring Common Packet Forwarder 53
  - Debugging Common Packet Forwarder 57

### Chapter 10

**Managing Plug-n-Play (PnP)**

- Understanding Plug-n-Play 59
- Configuring Plug-n-Play 59
- Debugging Plug-n-Play 61

### Chapter 11

**Smart Licensing Using Policy**

- Overview of Smart Licensing Using Policy 63
  - Smart Account 64
  - Virtual Account 64
  - Architecture 64
    - Product Instance 64
    - Cisco Smart Software Manager (CSSM) 65
    - Cisco Smart Licensing Utility (CSLU) 65
  - Concepts 65
    - License Enforcement Types 66
    - License Duration 66
    - Authorization Code 66
    - Policy 66
      - Understanding Policy Selection 67
      - RUM Report and Report Acknowledgement 68
      - Trust Code 68
  - Supported Topologies 68
  - Workflow for Topology: Full Offline Access 70
  - Workflow for Topology: CSLU Has Access to CSSM 71
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.

---

Note

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

---

Conventions

This document uses the following conventions.

<table>
<thead>
<tr>
<th>Conventions</th>
<th>Indication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong> font</td>
<td>Commands and keywords and user-entered text appear in <strong>bold</strong> font.</td>
</tr>
<tr>
<td><strong>italic</strong> font</td>
<td>Document titles, new or emphasized terms, and arguments for which you supply values are in <strong>italic</strong> font.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Elements in square brackets are optional.</td>
</tr>
<tr>
<td>{x</td>
<td>y</td>
</tr>
<tr>
<td>[ x</td>
<td>y</td>
</tr>
<tr>
<td>string</td>
<td>A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.</td>
</tr>
<tr>
<td>courier font</td>
<td>Terminal sessions and information the system displays appear in courier font.</td>
</tr>
<tr>
<td>&lt; &gt;</td>
<td>Nonprinting characters such as passwords are in angle brackets.</td>
</tr>
<tr>
<td>[ ]</td>
<td>Default responses to system prompts are in square brackets.</td>
</tr>
<tr>
<td>!, #</td>
<td>An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.</td>
</tr>
</tbody>
</table>
**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.
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, on page 1
- Switching to Virtual Mode, on page 2
- Displaying System Information, on page 2

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:

For the information of software installation procedure, see the release notes of Cisco LoRaWAN Gateway at:

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
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.

- 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.

- 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:
• 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
Unknown

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*7S
$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,1,00*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,A,................,N*4D
$GNVTG,
##PASS: GPS I2C interface check OK

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*7S
$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,1,00*65
$GNGLL,3725.12517,N,12155.20795,W,231503.00,A,A*6B
$GNZDA,231503.00,04,05,2017,00,00*7B
```

• 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
```
Displaying Inventory Information

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

<table>
<thead>
<tr>
<th>Gateway#show inventory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>ImageVer</td>
</tr>
<tr>
<td>BootloaderVer</td>
</tr>
<tr>
<td>SerialNumber</td>
</tr>
<tr>
<td>PID</td>
</tr>
<tr>
<td>UTCTime</td>
</tr>
<tr>
<td>IPv4Address</td>
</tr>
<tr>
<td>IPv6Address</td>
</tr>
<tr>
<td>FPGAVersion</td>
</tr>
<tr>
<td>FPGAStatus</td>
</tr>
<tr>
<td>ChipID</td>
</tr>
<tr>
<td>TimeZone</td>
</tr>
<tr>
<td>LocalTime</td>
</tr>
<tr>
<td>ACT2 Authentication</td>
</tr>
</tbody>
</table>

Displaying Radio Information

The show radio command displays the radio information.

<table>
<thead>
<tr>
<th>Gateway#show radio</th>
</tr>
</thead>
<tbody>
<tr>
<td>LORA_SN:</td>
</tr>
<tr>
<td>LORA_PN:</td>
</tr>
<tr>
<td>LORASKU:</td>
</tr>
<tr>
<td>LORA_CALC:</td>
</tr>
<tr>
<td>CAL_TEMP_CELSIUS:</td>
</tr>
<tr>
<td>CAL_TEMP_CODE_AD9361:</td>
</tr>
<tr>
<td>RSSI_OFFSET:</td>
</tr>
<tr>
<td>LORA_REVISION_NUM:</td>
</tr>
<tr>
<td>RSSI_OFFSET_AUS:</td>
</tr>
</tbody>
</table>

radio status: off

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
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, on page 7
- Configuring DNS, on page 9
- Mapping Hostnames to IP Addresses, on page 10

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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface_type interface_number</code></td>
<td>Enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip address dhcp</code></td>
<td>Enable DHCP client on the interface to allow automatic assignment of IP addresses to the specified interface.</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>description [interface_description]</code></td>
<td>Enter description for the interface.</td>
</tr>
<tr>
<td>Step 5</td>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6</td>
<td><code>ip default-gateway ip-address</code></td>
<td>Configure default gateway. Note: The default gateway may be learned from DHCP.</td>
</tr>
</tbody>
</table>

*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`

*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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure terminal</code></td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td><code>interface interface_type interface_number</code></td>
<td>Enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td><code>ip address ip-address subnet-mask</code></td>
<td>Enter the IP address and subnet mask.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 4 description [interface_description]</td>
<td>Enter description for the interface.</td>
<td></td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 6 ip default-gateway ip-address</td>
<td>Configure default gateway.</td>
<td></td>
</tr>
<tr>
<td>Step 7 Use the following commands to verify the configuration:</td>
<td>Verify the configuration.</td>
<td></td>
</tr>
<tr>
<td>• show interfaces interface_type interface_number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• show ip interfaces interface_type interface_number</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• show ip route</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

**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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip name-server ip-address</td>
<td>Configure DNS server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show hosts</td>
<td>Verify the configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ip host hostname ip-address</td>
<td>Define a static hostname-to-address mapping. You can define up to 5 mapping entries. Use the <code>no</code> form of the command to delete the mapping entry.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>You can also use this command to set the LXC /etc/hosts entries from the CLI.</td>
<td></td>
</tr>
</tbody>
</table>

**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, on page 13
• Configuring a System Name and Prompt, on page 14
• Configuring GPS as the Clock Source, on page 15
• Configuring UBX Support for GPS, on page 15
• Checking and Saving the Running Configuration, on page 16
• Reloading IXM, on page 16
• Using Reset Button, on page 16

Managing the System Time and Date

You can manage the system time and date on your LoRaWAN Gateway, either by using automatic configuration, such as the Network Time Protocol (NTP), or by using the GPS as a source for the clock.

Network Time Protocol (NTP)

Network Time Protocol (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:

- Support 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>ntp server {ip name</td>
<td>address address }</td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>show ntp status</td>
<td>(Optional) Show NTP status to verify the configuration.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show ntp associations</td>
<td>(Optional) Show the NTP associations with upstream servers.</td>
</tr>
<tr>
<td>Step 6</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
### Configuring GPS as the Clock Source

Beginning in privileged EXEC mode, follow these steps to configure GPS as the gateway clock source:

**Procedure**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 clock gpstime enable</td>
<td>Use the GPS as the modem clock source.</td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

### 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:
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.
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, on page 17
- Configuring VLAN Trunks, on page 18
- Enabling Sending and Receiving Tagged Packet on Ethernet Port, on page 19
- Examples of Show Commands, on page 20

Configuring IP Address for VLAN

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

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface interface-id</td>
<td>Specify the port to be configured for trunking, and enter interface configuration mode.</td>
</tr>
<tr>
<td>Step 3</td>
<td>switchport mode trunk</td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
### 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>
```

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
```

---

**Purpose**

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

**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.
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
```
Configuring CDP

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

- Understanding CDP, on page 21
- Configuring CDP, on page 21

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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>cdp timer <em>seconds</em></td>
<td>(Optional) Set the transmission frequency of CDP updates in seconds. The range is 5 to 254; the default is 60 seconds.</td>
</tr>
<tr>
<td>Step 3</td>
<td>cdp holdtime <em>seconds</em></td>
<td>(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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show cdp</td>
<td>Verify configuration by displaying global information about CDP on the device.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show cdp neighbors</td>
<td>Display information about neighbors.</td>
</tr>
<tr>
<td>Step 7</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**What to do next**

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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`enable secret {password</td>
<td>5 encrypted_passwd</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td><code>exit</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

**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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>`username name {password</td>
<td>5 encrypted_passwd</td>
</tr>
</tbody>
</table>
### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>

**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: [$%{}+_:.]
<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 2</strong></td>
<td><strong>hostname hostname</strong></td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>ip domain name domain_name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>ip ssh {port|session|authentication-retries|time-out|admin-access|local|limit-local}</td>
</tr>
<tr>
<td></td>
<td>• port – Configure SSH port.</td>
</tr>
<tr>
<td></td>
<td>• session – Configure number of SSH session.</td>
</tr>
<tr>
<td></td>
<td>• authentication-retries – Configure number of authentication retries.</td>
</tr>
<tr>
<td></td>
<td>• time-out – Configure timeout interval.</td>
</tr>
<tr>
<td></td>
<td>• admin-access – Allow admin access via SSH.</td>
</tr>
<tr>
<td></td>
<td>• local – Restrict user to container and reverse-tunnel SSH access only.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>crypto key generate rsa</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>exit</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Do one of the following:</td>
</tr>
<tr>
<td></td>
<td>• show ip ssh</td>
</tr>
<tr>
<td></td>
<td>• show ssh</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>copy running-config startup-config</td>
</tr>
</tbody>
</table>

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

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

### 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

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

**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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 container copy &lt;filename&gt; &lt;path&gt;</td>
<td>Copy files from the container to the host.</td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 container private-network &lt;chosen-private-network-option-from-the-list&gt;</td>
<td>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.</td>
</tr>
<tr>
<td>Step 3 exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 4 show container private-network</td>
<td>Verify the configuration.</td>
</tr>
</tbody>
</table>
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>
<thead>
<tr>
<th>User ID</th>
<th>SSH connection</th>
<th>Shell</th>
<th>Linux shell access via request shell host</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 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>
<thead>
<tr>
<th>Request Shell</th>
<th>Exit</th>
<th>Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>Exit from host</td>
<td>Go into console</td>
</tr>
<tr>
<td>console</td>
<td>Go into console</td>
<td>Go into console</td>
</tr>
</tbody>
</table>
### Table 4: Password Change on Switchover

<table>
<thead>
<tr>
<th>Switchover Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From virtual mode to standalone mode</td>
<td>The virtual mode root password is assigned to the standalone mode system password.</td>
</tr>
<tr>
<td>From standalone mode to virtual mode</td>
<td>The standalone mode system password is lost during the switchover, and the virtual mode root password remains.</td>
</tr>
</tbody>
</table>

## Configuring Logging in Container

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

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>container log all</td>
<td>Enable logging through syslog-ng in the container.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>To restore the default, use the <strong>no</strong> form of the command.</td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

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, on page 33
- Configuring IPsec, on page 33
- Configuring Crypto IPSec Profile Common, on page 35
- Configuring Crypto IPSec Profile Individual, on page 36
- Basic Configuration for RSA to Connect to Primary and Secondary, on page 38
- Locking Traffic to IPSec Tunnels, on page 38
- Erasing IPSec Certificates and Key, on page 39
- Uploading Certificates from USB or Local Flash, on page 39
- Disabling LXC Restart During IPSec Reauthentication, on page 39
- Resetting Secure-Storage for Certificate Download, on page 39

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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 2</strong> crypto ipsec profile {common</td>
<td>primary</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Do one of the following: These commands are exclusive.</td>
</tr>
<tr>
<td>• ipsec isakmp username password group group_id psk</td>
<td>• Configure PSK.</td>
</tr>
<tr>
<td>• ipsec cert install {usb</td>
<td>local} enable</td>
</tr>
<tr>
<td>• ipsec cert scep &lt;url&gt; &lt;country_code&gt; &lt;state&gt; &lt;locality&gt; &lt;organization&gt; &lt;unit&gt; &lt;name&gt; &lt;device-id&gt; {ndes</td>
<td>xpi} &lt;persistency&gt; &lt;key-length&gt;</td>
</tr>
<tr>
<td>• xpki - Use a Cisco Router as the CA server</td>
<td></td>
</tr>
<tr>
<td>• ndes - Use a Windows server as the CA server</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ipsec enable</td>
<td>Enable IPSec.</td>
</tr>
<tr>
<td><strong>Step 5</strong> ipsec subnet lock</td>
<td>Lock the device traffic with IPsec subnet. Traffic outside of the subnet will not be accepted.</td>
</tr>
<tr>
<td><strong>Step 6</strong> exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 7</strong> show ipsec certs</td>
<td>(Optional) Display details about certificates (RSA only).</td>
</tr>
</tbody>
</table>
### Configuring IPSec

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

**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

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

### 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.
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.

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>crypto ipsec profile {primary</td>
<td>secondary}</td>
</tr>
<tr>
<td>Step 3</td>
<td>ipaddr &lt;ip-address&gt; iketime &lt;ike-lifetime&gt; keytime &lt;key-life&gt; aes &lt;ike-encryption&gt;</td>
<td>Configures the required parameters of the tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>ip-address</em> - IP address or hostname of the IPSec server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>ike-lifetime</em> - Lifetime of ISAKMP or IKE SA in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>key-life</em> - Lifetime of one tunnel connection instance in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>ike-encryption</em> – Encryption method of ike directive in strongSwan; 128 or 256 for aes128-sha256-ecp256 or aes256-sha256-ecp256 by default.</td>
</tr>
<tr>
<td>Step 4</td>
<td>rightid &lt;right_id&gt;</td>
<td>(Optional) Configure the ID of the IPSec server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>right-id</em> - IPSec server’s certificate’s full subject DN, IP address, domain name, or e-mail address.</td>
</tr>
<tr>
<td>Step 5</td>
<td>subnet &lt;subnet/mask&gt;</td>
<td>(Optional) Configures the subnet and mask of IP addresses the IPSec server will accept in the tunnel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <em>subnet/mask</em> - Subnet and mask, for example, 10.0.0.0/8.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Step 6 exit</td>
<td>Exit the crypto ipsec profile individual block and update the IPSec configuration.</td>
<td></td>
</tr>
<tr>
<td>Step 7 exit</td>
<td>Return to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td>Step 8 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

**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=FTX2103205B, 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.

Resetting Secure-Storage for Certificate Download

For gateways with a minimum Release 2.1.0.1, if the box is downgraded to an older image, certificates are inaccessible while the older image is loaded. If you want to download new certificates in the older image, run the `pki secure-storage reset` EXEC command before downgrading. This command deletes all currently installed certificates and restructure secure storage. If you do not want to install new certificates in the older image, it is recommended not to run this command.
Resetting Secure-Storage for Certificate Download

Configuring IPSec
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, on page 41
- Configuring the Dialer Interface, on page 41
- Configuring the Ethernet Interface, on page 43
- Enabling the PPPoE Service, on page 43
- Monitoring and Debugging the PPPoE Configuration, on page 44
- PPPoE Configuration Examples on IXM and IR829, on page 45

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:

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>interface dialer number</td>
<td>Enter interface configuration mode for the dialer interface.</td>
</tr>
<tr>
<td>Command or Action</td>
<td>Purpose</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Step 3</strong> ip address negotiated</td>
<td>Specify that the IP address for a particular interface is obtained via PPP/IPCP address negotiation.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 4</strong> ip mtu number</td>
<td>Configure the maximum transmission unit (MTU) of the PPPoE interface. Default is 1492.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>number</em> - PPPoE MTU</td>
<td></td>
</tr>
<tr>
<td><strong>Step 5</strong> ip tcp adjust-mss number</td>
<td>Configure the Maximum Segment Size (MSS) of the PPPoE interface. Default is 1412.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><em>number</em> - PPPoE MSS</td>
<td></td>
</tr>
<tr>
<td><strong>Step 6</strong> ppp authentication chap</td>
<td>Set the PPP authentication method to Challenge Handshake Authentication Protocol (CHAP).</td>
<td></td>
</tr>
<tr>
<td><strong>Step 7</strong> ppp chap hostname &lt;hostname&gt;</td>
<td>Define an interface-specific CHAP hostname.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 8</strong> ppp chap password &lt;password&gt;</td>
<td>Define an interface-specific CHAP password.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 9</strong> dialer-group name</td>
<td>Assign the dialer interface to a dialer group. This command applies the interesting traffic definition to the interface.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 10</strong> dialer-pool name</td>
<td>Specify the dialer pool to use to connect to a specific destination subnetwork.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 11</strong> exit</td>
<td>Return to global configuration mode.</td>
<td></td>
</tr>
<tr>
<td><strong>Step 12</strong> copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
<td></td>
</tr>
</tbody>
</table>

**Example**

```
cfg 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

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

### Example

```bash
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

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>pppoe profile_number</td>
<td>Connect to the PPPoE service. For profile_number, specify the target tunnel profile.</td>
</tr>
<tr>
<td>Step 2</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
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 configuration:

```
# [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
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 txqueue len:3
RX bytes:76623 (74.8 KiB) TX bytes:128214 (125.2 KiB)

Gateway\# `show pppoe session packets`
<table>
<thead>
<tr>
<th>IN</th>
<th>PACK</th>
<th>VJCOMP</th>
<th>VJUNC</th>
<th>VJERR</th>
<th>OUT</th>
<th>PACK</th>
<th>VJCOMP</th>
<th>VJUNC</th>
<th>NON-VJ</th>
</tr>
</thead>
<tbody>
<tr>
<td>76623</td>
<td>310</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>128214</td>
<td>439</td>
<td>0</td>
<td>0</td>
<td>439</td>
</tr>
</tbody>
</table>

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
<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>Metric</th>
<th>Ref</th>
<th>Use</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ppp1</td>
</tr>
<tr>
<td>10.0.3.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>lxcbr0</td>
</tr>
<tr>
<td>13.13.13.1</td>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
<td>UH</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>ppp1</td>
</tr>
</tbody>
</table>
The following is an example of PPPoE client configuration on IXM:

```plaintext
! 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 following is an example of PPPoE server configuration on IR829:

```plaintext
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
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
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 ieeel54 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
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, on page 51
- Managing Packet Forwarder, on page 52
- Managing Common Packet Forwarder (CPF), on page 53

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**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>packet-forwarder {upload normal &lt;path&gt;</td>
<td>Upload or download configuration files to host or USB from LRR.</td>
</tr>
<tr>
<td></td>
<td>download normal &lt;filename&gt;</td>
<td></td>
</tr>
<tr>
<td>Step 3</td>
<td>exit</td>
<td>Return to privileged EXEC mode.</td>
</tr>
</tbody>
</table>
Managing Packet Forwarder

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

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td><code>configure</code> terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>`packet-forwarder [install</td>
<td>uninstall] [firmware</td>
</tr>
<tr>
<td>Step 3</td>
<td>`packet-forwarder [start</td>
<td>restart</td>
</tr>
<tr>
<td>Step 4</td>
<td><code>exit</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>`show packet-forwarder [info</td>
<td>status</td>
</tr>
</tbody>
</table>

### 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=[58ba95ec55edaf7b8d43c8fb34bc96652abf5db92b0b675a405ad3abf93289d2]
  ftpaddr_crypted_k=0
  ftpuser=[df09087afa773c3dde7994ee50ab0ad9]
  ftpuser_crypted_k=0
  ftppass=[ed37881434753d194bbe66a8bc2de5ba]
  ftppass_crypted_k=0
  ftpport=[2ab6268fa568f91eaa80c4e531aabe80]
  use_sftp=0

Managing Common Packet Forwarder (CPF)

This section describes how to configure and manage the common packet forwarder (CPF) on the Cisco LoRaWAN Gateway.

Understanding Common Packet Forwarder

CPF is an agent running on the host of a LoRa gateway, forwarding RF packets received by the concentrator (uplinks) to a LoRaWAN Network Server (LNS) through secured IP links and transmitting RF packets sent by the LNS (downlinks) through the same secured IP links to some device.

Configuring Common Packet Forwarder

If the LRR packages are installed, CPF cannot be enabled. Uninstall any LRR packages before configuring CPF.

When CPF is enabled, it will perform a GPS check on bootup. This GPS check will use the currently recorded coordinates to verify that the given channel plans are valid in that location. Once a location fix is achieved, the location is stored in non-volatile memory. The location fix status can be viewed using the show gps history command. After this point, GPS is no longer required and the antenna does not need to be connected.

Note

Factory defaulting the IXM deletes this stored location information, in which case, a location fix will need to be achieved again.

Refer to the respective Release Notes for countries supported by the IXM.

Beginning in privileged EXEC mode, follow these steps to configure common packet forwarder on the Cisco LoRaWAN Gateway:
## Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 2    | common-pack-forwarder cert install gw path-to-cert path-to-key | Install IXM gateway's certification and key (mandatory if auth-mode is client-server):  
*path-to-cert* – file path to the gateway’s cert  
*path-to-key* – file path to the gateway’s key |
| 3    | common-pack-forwarder cert install srv path-to-cert | Install IXM LNS’ CA certificate (mandatory if auth-mode is other than none):  
*path-to-cert* – file path to the LNS’ CA cert |
| 4    | common-pack-forwarder cert erase gw | Erase IXM LoRa gateway's certification and key. |
| 5    | common-pack-forwarder cert erase srv | Erase LNS server's certification. |
| 6    | common-packet-forwarder profile | Configure parameters for the CPF. |
| 7    | ipaddr ip-address port | Configure network server IP address and port.  
*ip-address* – Network server IP address  
*port* – Network server port number |
| 8    | auth-mode mode | Authentication mode.  
- none: use websocket (ws), default  
- client-server: authenticate both client and server with secure websocket (wss)  
- server: server authentication, only |
| 9    | gps enable | Enable CPF to utilize GPS signal. |
| 10   | aeskey key | Configure AES key used for CPF.  
*key* – AES key used for CPF |
| 11   | gatewayid gateway-id | Configure gateway id used for CPF.  
*gateway-id* – Gateway ID used for CPF |
| 12   | antenna antenna-number type antenna-type gain antenna-gain loss cable-loss | Configure individual antenna properties.  
*antenna-number* – Antenna ID <1,2>  
*antenna-type* – Antenna type <omni, sector>  
*antenna-gain* – Antenna gain  
*cable-loss* – Cable loss |
<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td><code>region-cp lora-region-name</code></td>
<td>Configure LoRa region channel plan code per naming convention defined in LoRa Alliance RP2-1.0.2 (for example: EU868, AU915, AS923-1, AS923-2, AS923-3, IN65, RU864). <em>lora-region-name</em> – LoRa region code name (optional if default one is used)</td>
</tr>
<tr>
<td>14</td>
<td><code>board-bw bandwidth</code></td>
<td><code>bandwidth</code> – Manually setup the board rx bandwidth if you need to change the default.</td>
</tr>
<tr>
<td>15</td>
<td><code>board-freq freq</code></td>
<td><code>freq</code> – Manually setup the board rx frequency if you need to change the default.</td>
</tr>
<tr>
<td>16</td>
<td><code>tls-sni enable</code></td>
<td><code>enable</code> – Connect to LNS to compare the configured LNS server name with the one embedded in the LNS server's certificate.</td>
</tr>
<tr>
<td>17</td>
<td><code>cpf enable</code></td>
<td>Start the CPF. If prompted about a Smart License, answer &quot;yes&quot;.</td>
</tr>
<tr>
<td>18</td>
<td><code>exit</code></td>
<td>Exit the CPF profile block and update the CPF configuration.</td>
</tr>
<tr>
<td>19</td>
<td><code>exit</code></td>
<td>Return to privileged EXEC mode.</td>
</tr>
<tr>
<td>20</td>
<td><code>show common-packet-forwarder info</code></td>
<td>(Optional) Show CPF configuration and information.</td>
</tr>
<tr>
<td>21</td>
<td><code>show common-packet-forwarder status</code></td>
<td>(Optional) Show current state of CPF and if registration with NS was successful.</td>
</tr>
<tr>
<td>22</td>
<td><code>show common-packet-forwarder log list</code></td>
<td>(Optional) List available log options such as CPF configuration or trace.</td>
</tr>
<tr>
<td>23</td>
<td><code>show common-packet-forwarder log name trace number-of-lines</code></td>
<td>(Optional) Display the CPF trace log. <em>number-of-lines</em> – Number of lines in log to display from end of file.</td>
</tr>
<tr>
<td>24</td>
<td><code>show common-packet-forwarder log name config number-of-lines</code></td>
<td>(Optional) Display the current CPF configuration. <em>number-of-lines</em> – Number of lines in config to display from end of file.</td>
</tr>
</tbody>
</table>
| 25   | `debug cpf` | (Optional) Change CPF trace log level to "DEBUG". *Note* The default log level is "WARNING". This command is to change CPF log level to "DEBUG".
1. Usually the country configuration is not needed and is not used by the gateway. The resident country is determined by the gps location information automatically. It is used only when the LoRa gateway is managed by Cisco IDA agent in privileged mode.

2. Region-cp is only needed when the resident country supports multiple LoRa region channel plans and a non-default one is used (for example, in US, default channel plan is US915. If AU915 is wanted, set region-cp to AU915).

3. Class B is supported. Refer to https://doc.sm.tc/station/tcpo.html# for more information about Class B requirements on LoRa Server side (time sync and beacon configurations).

---

**Example**

- Example of Common Packet Forwarder Profile Block:

```
common-packet-forwarder profile
ipaddr A.B.C.D port XXXX
gps enable
aeskey 00AEAEFFFE000000
antenna 1 omni gain 1.5 loss 0.2
antenna 2 sector gain 1.5 loss 0.2
gatewayid ::1
cpf enable
exit
```

- Example of showing Common Packet Forwarder information and status:

```
# show common-packet-forwarder info
FirmwareStatus : Installed
FirmwareVersion : 2.1.0.1
Gateway ID : ::1
Region : US915
IPAddress:Port : A.B.C.D:XX
TXLut :
GPS : Enabled
AESKey : 00AEAEFFFE000000
Antenna 1 : enabled, type omni, gain 1.5, loss 0.2
Antenna 2 : enabled, type sector, gain 1.5, loss 0.2

# show common-packet-forwarder status
Enabled : Yes
Running : Yes
NS Registration : Successful
```

---

**Note**

The **Enabled** status simply means that CPF has been configured successfully. **Running** status depicts whether CPF has started successfully or not. Note that GPS signal should be available for the CPF to run correctly.
Debugging Common Packet Forwarder

When the CPF is running, the CPR trace log file can be displayed through the IXM by using the `show common-packet-forwarder log name trace` command:

```
# show common-packet-forwarder log list
Log file Description
----------------------------------------
config CPF Configuration
trace CPF Trace log
```

```
# show common-packet-forwarder log name trace 15
2019-04-16 09:38:40.625 [SYS:INFO] prefix EUI : ::0 (station.conf)
2019-04-16 09:38:40.625 [SYS:INFO] Station EUI : ::1
2019-04-16 09:38:40.625 [SYS:WARN] Station in NO-CUPS mode
2019-04-16 09:38:40.828 [TCE:INFO] INFOS reconnect backoff 10s (retry 1)
2019-04-16 09:38:41.821 [TCE:INFO] INFOS reconnect backoff 10s (retry 1)
```

```
# show common-packet-forwarder log name config 15
    "log_size": 10000000,
    "log_rotate": 3,
    "gps": "/dev/ttyS1",
    "TX_AM_GAP": "90ms",
    "pps": "fuzzy"
},
"gps_conf": {
    "gw_latitude": 0,
    "gw_longitude": 0,
    "gw_altitude": 0,
    "fixed_altitude": false
}
```

```
station channel plan
```

The command `debug cpf` can also be executed to increase the log level of CPF logging.
CHAPTER 10

Managing Plug-n-Play (PnP)

This chapter describes how to configure and manage the Plug-n-Play (PnP) on the Cisco LoRaWAN Gateway.

• Understanding Plug-n-Play, on page 59
• Configuring Plug-n-Play, on page 59
• Debugging Plug-n-Play, on page 61

Understanding Plug-n-Play

The PnP agent is an embedded software application running on Cisco routers, switches, wireless access points, and sensors. It enables zero-touch provisioning by automatically starting on boot up for new or factory reset devices and by automatically discovering the PnP server. Once a secure channel communication is established with the PnP server through one of the secure PnP discovery mechanisms, the PnP agent is capable of performing different operations on a Cisco device, such as image upgrading, configuration upgrading, and CLI executing.

Configuring Plug-n-Play

Note

The PnP agent will be trigged only by doing a factory reset on an existing device or on a completely new device.

The PnP agent on the IXM supports the following DHCP, DNS, and CCO discovery mechanisms:

• DHCP/DNS discovery: The precondition of using DHCP and DNS discovery is to setup DHCP server first. Refer to http://pnp.cisco.com/index.php/solutions/training/agent-discovery for information on configuring the DHCP server.

• CCO discovery:

This configuration is only for PnP CCO discovery use. If IXM needs NTP server, it still needs to go through CLIs.

1. Log in to https://software.cisco.com/#

2. Choose Plug and Play Connect under Network Plug and Play.
3. Add the device information.
4. You will see status "Pending Redirection."
5. When device connects to CCO status will be "Contacted" and after some time "Redirected."
6. After successful PNP, a Redirection Successful message appears.

For more information, see the following document: http://pnp.cisco.com/index.php/solutions/pnp-connect.

Follow these steps to configure pnp on the LoRaWAN gateway:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>pnp enable</td>
<td>Start the PnP agent.</td>
</tr>
<tr>
<td>Step 3</td>
<td>pnp disable</td>
<td>Stop the PnP agent.</td>
</tr>
<tr>
<td>Step 4</td>
<td>exit</td>
<td>Exit the global configuration mode.</td>
</tr>
<tr>
<td>Step 5</td>
<td>show pnp profiles</td>
<td>(Optional) Show PnP version.</td>
</tr>
<tr>
<td>Step 6</td>
<td>show pnp status</td>
<td>(Optional) Show PnP status.</td>
</tr>
</tbody>
</table>
| Step 7 | show pnp log name trace **number-of-lines** | (Optional) Display the PnP trace log.  
**number-of-lines** – Number of lines in the log to display from end of file.  
**number-of-lines** – Number of lines in config to display from end of file. |

**Example**

Example of showing PnP profiles and status

```
#show pnp profiles
Created by UDI
DHCP Discovery PID:POSIX-Reference,VID:V01,SN:23336985067

Primary transport: http
Address: 10.154.201.104
Port: 9455
CA file:

Work-Request Tracking:
  Pending-WR: Correlator=
Cisco-PnP-POSIX-reference-1.8.1.dev19-2-7013f6f5-ac52-4a96-b589-ac35d91c499b-1
  Last-WR: Correlator=
Cisco-PnP-POSIX-reference-1.8.1.dev19-1-c9aadc77-760b-42b6-b6c7-859093ab5e09-1

PnP Response Tracking:
  Last-PR: Correlator=
Cisco-PnP-POSIX-reference-1.8.1.dev19-1-c9aadc77-760b-42b6-b6c7-859093ab5e09-1
```
Debugging Plug-n-Play

When the PnP is running, the PnP trace log file can be displayed through the IXM using the `show pnp log name trace` command:

```
#show pnp log name trace 15
2016-08-06 17:43:56,023 - pnp.infra.network.HTTPConnClient - DEBUG - PNP requests with url:
http://10.154.201.104:9455/pnp/HELLO
2016-08-06 17:43:56,040 - pnp.discovery.infra.discovery_manager - DEBUG - Existing profile config found valid.
2016-08-06 17:43:56,041 - pnp.discovery.infra.discovery_manager - DEBUG - Discovery skipped upon existing profile configs presence
2016-08-06 17:43:56,043 - pnp.infra.utils.pnp_utils - DEBUG - PnP config read: Connection Info:
Transport: http
Address: 10.154.201.104
Port: 9455
Remote CA File: Core Trust Enabled? False
2016-08-06 17:43:56,056 - pnp.agent - INFO - platform_dict: {'hardwareInfo': {'platformName': 'reference', 'hostname': 'Gateway', 'vendor': 'Network-PnP', 'processorT
2016-08-06 17:43:56,058 - pnp.agent - DEBUG - Unsuccessful attempt to get reason code from msg: INVALID_REASON_CODE
2016-08-06 17:43:56,058 - pnp.agent - DEBUG - Agent not using reload reason.
2016-08-06 17:43:56,061 - pnp.infra.utils.pnp_utils - DEBUG - PnP config read: Connection Info:
Transport: http
Address: 10.154.201.104
```
Overview of Smart Licensing Using Policy

Smart Licensing Using Policy is supported on Cisco Wireless Gateway for LoRaWAN Release 2.2 and later, for the subscription of Common Packet Forwarder (CPF).

Smart Licensing Using Policy is an enhanced version of Smart Licensing, with the overarching objective of providing a licensing solution that does not interrupt the operations of your network, rather, one that enables a compliance relationship to account for the hardware and software licenses you purchase and use. Smart Licensing Using Policy provides a seamless experience with the various aspects of licensing.

- Purchase licenses: Purchase licenses through the existing channels and use the Cisco Smart Software Manager (CSSM) portal to view product instances and licenses.

Note

To simplify your implementation of Smart Licensing Using Policy, provide your Smart Account and Virtual Account information when placing an order for new hardware or software. This allows Cisco to install applicable policies and authorization codes (terms explained in the Concepts, on page 65 section below), at the time of manufacturing.

- Use: All licenses on your devices are unenforced. This means that you do not have to complete any licensing-specific operations, such as registering or generating keys before you start using the software and the licenses that are tied to it. License usage is recorded on your device with timestamps and the required workflows can be completed at a later date.

- Report license usage to CSSM: Multiple options are available for license usage reporting. You can use the Cisco Smart Licensing Utility (CSLU), or report usage information directly to CSSM. For air-gapped
networks, a provision for offline reporting where you download usage information and upload it to CSSM, is also available. The usage report is in plain text XML format.

- Reconcile: For situations where delta billing applies (purchased versus consumed).

The primary benefits of this enhanced licensing model are:

- Seamless day-0 operations
  After a license is ordered, no preliminary steps, such as registration or generation of keys etc., are required unless you use an export-controlled or enforced license.

- Visibility and manageability
  Tools, telemetry and product tagging, to know what is in-use.

- Flexible, time series reporting to remain compliant
  Easy reporting options are available, whether you are directly or indirectly connected to Cisco Smart Software Manager (CSSM), or in an air-gapped network.

Smart Account

To use Smart Licensing, you must first set up a Cisco Smart Account at Cisco Software Central.

A Smart Account provides a single location for all Smart-enabled products and entitlements. It helps speed procurement, deployment, and maintenance of Cisco Software. When creating a Smart Account, you must have the authority to represent the requesting organization. After submitting, the request goes through a brief approval process.

Virtual Account

A Virtual Account exists as a sub-account within the Smart Account. Virtual Accounts are a customer-defined structure based on organizational layout, business function, geography or any defined hierarchy. They are created and maintained by the Smart Account administrator.

Architecture

This section explains the various components that can be part of your implementation of Smart Licensing Using Policy.

Product Instance

A product instance is a single instance of a Cisco product, identified by a Unique Device Identifier (UDI). A product instance records and reports license usage (RUM reports), and provides alerts and system messages about overdue reports, communication failures, etc. The RUM reports and usage data are also stored securely in the product instance.
Cisco Smart Software Manager (CSSM)

CSSM is a portal that enables you to manage all your Cisco software licenses from a centralized location. CSSM helps you manage current requirements and review usage trends to plan for future license requirements.

You can access CSSM at https://software.cisco.com. Under the License tab, click the Smart Software Licensing link.

In CSSM you can:

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


Click on the View Video button.

Cisco Smart Licensing Utility (CSLU)

CSLU is a Windows-based reporting utility that provides aggregate licensing work-flows. This utility performs the following key functions:

• Provides the options relating to how work-flows are triggered. The work-flows can be triggered by CSLU or by the product instance.

• Collects usage reports from the product instance and upload these usage reports to the corresponding smart account or virtual account – online, or offline, using files. Similarly, the RUM report ACK is collected online, or offline, and provided back to the product instance.

• Sends authorization code requests to CSSM and receives authorization codes from CSSM.

CSLU can be part of your implementation in the following ways:

• Install the windows application, to use CSLU as a standalone tool and connect it to CSSM.

• Install the windows application, to use CSLU as a standalone tool and not connect it to CSSM. With this option, the required usage information is downloaded to a file and then uploaded to CSSM. This is suited to air-gapped networks.

Concepts

This section explains the key concepts of Smart Licensing Using Policy.
License Enforcement Types

A given license belongs to one of three enforcement types. The enforcement type indicates if the license requires authorization before use, or not.

- **Unenforced or Not Enforced**
  
  Unenforced licenses do not require authorization before use in air-gapped networks, or registration, in connected networks. The terms of use for such licenses are as per the end user license agreement (EULA).

- **Enforced**

  Licenses that belong to this enforcement type require authorization before use. The required authorization is in the form of an authorization code, which must be installed in the corresponding product instance.

  An example of an enforced license is the Media Redundancy Protocol (MRP) Client license, which is available on Industrial Ethernet Switches.

- **Export-Controlled**

  Licences that belong to this enforcement type are export-restricted by U.S. trade-control laws and these licenses require authorization before use. The required authorization code must be installed in the corresponding product instance for these licenses as well. Cisco may pre-install export-controlled licenses when ordered with hardware purchase.

  An example of an export-controlled license is the High Speed Encryption (HSECK9), which is available on certain Cisco Routers.

License Duration

This refers to the duration or term for which a purchased license is valid. A given license may belong to any one of the enforcement types mentioned above and be valid for the following durations:

- **Perpetual**: There is no expiration date for such a license.
- **Subscription**: The license is valid only until a certain date.

Authorization Code

The Smart Licensing Authorization Code (SLAC) allows activation and continued use of a license that is export-controlled or enforced.

If you are upgrading from an earlier licensing model to Smart Licensing Using Policy, you may have a Specific License Reservation (SLR) with its own authorization code. The SLR authorization code is supported after upgrade to Smart Licensing Using Policy.

Policy

A policy provides the product instance with these reporting instructions:

- **License usage report acknowledgement requirement (Reporting ACK required)**: The license usage report is known as a RUM Report and the acknowledgement is referred to as an ACK (See RUM Report and Report Acknowledgement, on page 68). This is a yes or no value which specifies if the report for this product instance requires CSSM acknowledgement or not. The default policy is always set to “yes”.
• First report requirement (days): The first report must be sent within the duration specified here.
• Reporting frequency (days): The subsequent report must be sent within the duration specified here.
• Report on change (days): In case of a change in license usage, a report must be sent within the duration specified here.

Understanding Policy Selection

CSSM determines the policy that is applied to a product instance. Only one policy is in use at a given point in time. The policy and its values are based on a number of factors, including the licenses being used.

Cisco default is the default policy that is always available in the product instance. If no other policy is applied, the product instance applies this default policy. The table below shows the Cisco default policy values.

While you cannot configure a policy, you can request for a customized one, by contacting the Cisco Global Licensing Operations team. Go to Support Case Manager. Click OPEN NEW CASE > Select Software Licensing. The licensing team will contact you to start the process or for any additional information. Customized policies are also made available through your Smart account in CSSM.

To know which policy is applied (the policy in-use) and its reporting requirements, enter the `show license all` command in privileged EXEC mode.

Table 5: Policy: Cisco default

<table>
<thead>
<tr>
<th>Policy</th>
<th>Default Policy Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export (Perpetual/Subscription)</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td>Note</td>
<td>First report requirement (days): 90</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 90</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 90</td>
</tr>
<tr>
<td>Enforced (Perpetual/Subscription)</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td>Note</td>
<td>First report requirement (days): 90</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 90</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 90</td>
</tr>
<tr>
<td>Unenforced/Non-Export Perpetual</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td></td>
<td>First report requirement (days): 365</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 0</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 90</td>
</tr>
<tr>
<td>Policy: Cisco default</td>
<td>Default Policy Values</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Unenforced/Non-Export Subscription</td>
<td>Reporting ACK required: Yes</td>
</tr>
<tr>
<td></td>
<td>First report requirement (days): 90</td>
</tr>
<tr>
<td></td>
<td>Reporting frequency (days): 90</td>
</tr>
<tr>
<td></td>
<td>Report on change (days): 90</td>
</tr>
</tbody>
</table>

1 For Unenforced/Non-Export Perpetual: the default policy’s first report requirement (within 365 days) applies only if you have purchased hardware or software from a distributor or partner.

**RUM Report and Report Acknowledgement**

A Resource Utilization Measurement report (RUM report) is a license usage report, which the product instance generates, to fulfill reporting requirements as specified by the policy.

An acknowledgement (ACK) is a response from CSSM and provides information about the status of a RUM report.

The policy that is applied to a product instance determines the following reporting requirements:

- Whether a RUM report is sent to CSSM and the maximum number of days provided to meet this requirement.
- Whether the RUM report requires an acknowledgement (ACK) from CSSM.
- The maximum number of days provided to report a change in license consumption.

A RUM report may be accompanied by other requests, such as a trust code request, or a SLAC request. So in addition to the RUM report IDs that have been received, an ACK from CSSM may include authorization codes, trust codes, and policy files as well.

**Trust Code**

A UDI-tied public key with which the product instance signs a RUM report. This prevents tampering and ensures data authenticity.

**Supported Topologies**

This section describes the various ways in which you can implement Smart Licensing Using Policy. Cisco Wireless Gateway for LoRaWAN supports the following topologies:

- Full Offline Access
In this topology, devices do not have connectivity to CSSM (software.cisco.com). You must copy and paste information between Cisco products and CSSM to manually check in and out licenses.

To implement this topology, see Workflow for Topology: Full Offline Access, on page 70.

- CSLU (Cisco Smart Licensing Utility) mode

CSLU mode has two different kind of CSLU modes depending on the topology between the CSLU and CSSM.

- CSLU has access to CSSM

In this topology the devices are connected to CSLU controller. There is connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco products send usage information to a locally installed CSLU. There is online transmission between CSLU and CSSM to check-in and check-out licenses and data.

To implement this topology, see Workflow for Topology: CSLU Has Access to CSSM, on page 71.

- CSLU has No Access to CSSM.
In this topology the devices are connected to CSLU. There is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco products send usage information to a locally installed CSLU. You need to copy and paste information between CSLU and CSSM to manually check-in and check-out licenses.

To implement this topology, see Workflow for Topology: CSLU Has No Access to CSSM, on page 74.

Workflow for Topology: Full Offline Access

This procedure requires a manual exchange of required information between the router and CSSM.

Procedure

Step 1 Set license transport method to “off”.
In configuration mode, perform the following:
Example:
Gateway#configure terminal
Gateway(config)#license smart transport off

Step 2 Start license service through enabling common-packet-forwarder.
In configuration mode, perform the following:
Example:
Gateway(config)#common-packet-forwarder profile
Gateway(config-cpf-profile)#ipaddr A.B.C.D port X
Gateway(config-cpf-profile)#cpf enable

Step 3 Generate a license usage (RUM reports) file from the device and export the license usage file to your host laptop/PC.
Enter the license smart save usage command in privileged EXEC mode.
Example:
Gateway#license smart save usage all flash:report

Step 4 Copy the usage report from IXM using the SCP command in privileged EXEC mode.
Example:
Gateway#scp local flash:report user1 171.69.181.77 /ws/user1/report

Step 5 Import the license usage file to CSSM on Cloud.
a) Log in to the CSSM Web UI at https://software.cisco.com, using the username and password provided by Cisco.
b) Select the Smart Account (upper left-hand corner of the screen) that will receive the report.
c) Select Smart Software Licensing → Reports → Usage Data Files.
d) The Upload Usage Data window appears. Click Browse, and navigate to where the file is. Click on Upload Data.
e) From the **Select Virtual Accounts** pop-up, select the Virtual Account that will receive the uploaded file. The file is uploaded to Cisco and is listed in the Usage Data Files table in the Reports screen showing the File Name, time it was reported, which Virtual Account it was uploaded to, the Reporting Status, Number of Product Instances reported, and the Acknowledgement status.

f) In the Acknowledgement column, click **Download** to save the .txt ACK file for the report you uploaded. Wait for the ACK to appear in the Acknowledgement column.

g) Check under the **Product Instances** tab to verify your device is listed.

**Step 6**

Download the ACK file, using the SCP command in privileged EXEC mode.

**Example:**

```
Gateway#scp remote user 171.69.181.77 /ws/ACK_report flash:ACK_report
```

**Step 7**

Import the ACK file from CSSM to your device, using the **license smart import file** command in privileged EXEC mode.

**Example:**

```
Gateway#license smart import file flash: ACK_report
```

**Step 8**

Verify the Product Instance has imported the data. Use the following command to display license authorization, policy and reporting information for the product instance.

**Example:**

```
Gateway#show license usage
```

**Step 9**

Verify the license is in use.

**Example:**

```
Gateway#show license summary
```

---

**Workflow for Topology: CSLU Has Access to CSSM**

Tasks for Product Instance-Initiated Communication:

- Ensure network reachability (SSH).
- Check NTP status is in sync.
- Ensure the transport type is set to **cslu** (default).

```
Device(config)#license smart transport cslu
```

- Specify the CSLU information to be used.

  Configure a specific URL for CSLU by using the following CLI:

```
Device(config)#license smart url cslu http://<HOST or IP>:<port-num>/cslu/v1/pi
```

  - **HOST or IP** – Hostname / IP address of the windows (where CSLU is installed)
  - **port-num** – use 8180 or 8182.

- Verify the license policy is successfully installed by running the CLI command and verifying the time/date stamp.
Gateway# show common-packet-forwarder status
   Enabled : Yes
   Running : Yes
   NS Registration : Successful
   License Status: Reported - Yes, Acknowledged - Yes

Gateway# show license status
   Utility:
      Status: DISABLED
   Smart Licensing Using Policy:
      Status: ENABLED
   Data Privacy:
      Sending Hostname: yes
      Callhome hostname privacy: DISABLED
      Smart Licensing hostname privacy: DISABLED
      Version privacy: DISABLED
   Transport:
      Type: cslu
      Cslu address: http://172.27.164.116:8182/cslu/v1/pl
      Proxy: Not Configured
   Policy:
      Policy in use: Installed On Feb 23 2021 02:14:41 UTC
      Policy name: Test Policy
      Reporting ACK required: no (Customer Policy)
      Unenforced/Non-Export Perpetual Attributes:
         First report requirement (days): 94 (Customer Policy)
         Reporting frequency (days): 100 (Customer Policy)
         Report on change (days): 100 (Customer Policy)
      Unenforced/Non-Export Subscription Attributes:
         First report requirement (days): 120 (Customer Policy)
         Reporting frequency (days): 100 (Customer Policy)
         Report on change (days): 100 (Customer Policy)
      Enforced (Perpetual/Subscription) License Attributes:
         First report requirement (days): 0 (CISCO default)
         Reporting frequency (days): 204 (Customer Policy)
         Report on change (days): 100 (Customer Policy)
      Export (Perpetual/Subscription) License Attributes:
         First report requirement (days): 0 (CISCO default)
         Reporting frequency (days): 100 (Customer Policy)
         Report on change (days): 100 (Customer Policy)
   Miscellaneous:
      Custom Id: <empty>
   Usage Reporting:
      Last ACK received: Feb 23 2021 02:14:41 UTC
      Next ACK deadline: <none>
      Reporting push interval: 0 (no reporting)
      Next ACK push check: <none>
      Next report push: <none>
      Last report push: Feb 23 2021 02:10:41 UTC
      Last report file write: <none>

   Trust Code Installed: <none>

Gateway#
Gateway# configure terminal
Gateway(config)# interface FastEthernet 0/1
Gateway(config-if)# ip address 172.27.170.104 255.255.255.128
Gateway(config-if)# exit
Gateway(config)# ip default-gateway 172.27.170.1
Gateway(config)#
Gateway(config)# exit
*Feb 20 02:37:17: Configured from console by console
Gateway# configure terminal
Gateway(config)# crypto key generate rsa
Gateway(config)# ip ssh admin-access
Gateway(config)# exit
*Feb 20 02:37:31: Configured from console by console
Gateway# configure terminal
Gateway(config)# common-packet-forwarder profile
Gateway(config-cpf-profile)# ipaddr 172.27.166.121 port 6070
Gateway(config-cpf-profile)# cpf enable
By typing 'y' below, I agree that to abide to SMART LICENSING subscription royalty agreement with Cisco on this unit
Do you agree the above statement? [y/n] y
common-packet-forwarder started successfully
Gateway(config-cpf-profile)# exit
Gateway(config)# exit
Gateway# configure terminal
Gateway(config)# license smart transport cslu
Gateway(config)# license smart url cslu http://172.27.164.116:8182/cslu/v1/pi
Gateway(config)# exit
%SMART_LIC-6-POLICY_INSTALL_SUCCESS:A new licensing policy was successfully installed
Check the status of the device on CSLU as shown below:

*Figure 1: Verify the status of the device on CSLU*

Check updated information on CSSM as shown below:
Workflow for Topology: CSLU Has No Access to CSSM

In this topology, the devices are connected to CSLU. There is no connectivity between CSLU and CSSM (Cisco Smart Software Manager – software.cisco.com). Cisco products send usage information to a locally installed CSLU. You need to copy and paste information between CSLU and CSSM to manually check-in and check-out licenses.

Procedure

**Step 1** In the CSLU Preferences tab, click the **Cisco Connectivity** toggle switch to **off**. The field switches to “Cisco Is Not Available”.

**Step 2** Download tar file from CSLU.
Step 3  Select the PID and choose **Download All for Cisco** from CSLU.

Step 4  Save the file from CSLU.
Step 5  Upload the tar file downloaded from CSLU to CSSM.

Step 6  Check the status on CSSM and download the file from CSSM.

Step 7  Upload the file downloaded file from CSSM on the CSLU.
Step 8

Upload the specified tar file.

Step 9

Verify the status on CSLU.

Gateway# show license usage

License Authorization:
Status: Not Applicable
LORAWAN_CPF (LORAWAN_CPF):
  Description: LORAWAN_CPF
  Count: 1
  Version: v01
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: LORAWAN_CPF
  Feature Description: LORAWAN_CPF
  Enforcement type: NOT ENFORCED
  License type: Invalid

Gateway#show license status

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

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

Transport:
  Type: cslu
  Cslu address: http://172.27.164.116:8182/cslu/v1/pi
  Proxy: Not Configured

Policy:
  Policy in use: Installed On Feb 24 2021 00:04:10 UTC
  Policy name: Test Policy
  Reporting ACK required: no (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 94 (Customer Policy)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 120 (Customer Policy)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 204 (Customer Policy)
    Report on change (days): 100 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 100 (Customer Policy)
    Report on change (days): 100 (Customer Policy)

Miscellaneous:
  Custom Id: <empty>

Usage Reporting:
  Last ACK received: Feb 24 2021 00:04:10 UTC
  Next ACK deadline: <none>
  Reporting push interval: 0 (no reporting)
  Next ACK push check: <none>
  Next report push: <none>
  Last report push: Feb 23 2021 23:04:11 UTC
  Last report file write: <none>
Removing the Product Instance from CSSM

Procedure

Step 1  Log in to the CSSM Web UI at https://software.cisco.com and click Smart Software Licensing. Log in using the username and password provided by Cisco.
Step 2  Click the Inventory tab.
Step 3  From the Virtual Account drop-down list, choose your virtual account.
Step 4  Click the Product Instances tab. The list of product instances that are available is displayed.
Step 5  Locate the required product instance from the product instances list. Optionally, you can enter a name or product type string in the search tab to locate the product instance.
Step 6  Click the required product instance to expand the same. The Overview window is displayed.
Step 7  From the Actions drop-down list, choose Remove. The Remove Product Instance window is displayed.
Step 8  In the Reservation Return Code field, enter the return code.
Step 9  Click Remove Product Instance. The license is returned to the license pool.
CHAPTER 12

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, on page 81
- Working with Configuration Files, on page 82
- Working with Software Images, on page 83
- USB Support, on page 85
- Configuring U-boot, on page 85

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 82.

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 83.

### File Management Commands

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

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cd</td>
<td>Change current directory.</td>
</tr>
<tr>
<td>copy</td>
<td>Copy from one file to another.</td>
</tr>
<tr>
<td>delete</td>
<td>Delete a file.</td>
</tr>
<tr>
<td>dir</td>
<td>List files on a filesystem.</td>
</tr>
<tr>
<td>format</td>
<td>Format a filesystem.</td>
</tr>
<tr>
<td>mkdir</td>
<td>Create a new directory.</td>
</tr>
<tr>
<td>more</td>
<td>Display the contents of a file.</td>
</tr>
<tr>
<td>pwd</td>
<td>Display the current working directory.</td>
</tr>
<tr>
<td>rename</td>
<td>Rename a file.</td>
</tr>
</tbody>
</table>

### 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

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Log into the Cisco LoRaWAN Gateway through through SSH or Console.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Download the image file to the Cisco LoRaWAN Gateway.</td>
</tr>
</tbody>
</table>

### Step 2

archive download-sw firmware 

<table>
<thead>
<tr>
<th>Path</th>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>/factory</td>
<td></td>
<td>Download the firmware and delete user data.</td>
</tr>
<tr>
<td>/normal</td>
<td></td>
<td>Avoid using the /factory option with this command, because it erases everything and brings back to factory default.</td>
</tr>
<tr>
<td>/uboot-only</td>
<td></td>
<td>Upgrade the boot and keep the user data</td>
</tr>
<tr>
<td>/uboot-normal</td>
<td></td>
<td>Upgrade the boot and firmware, and keep the user data</td>
</tr>
<tr>
<td>/uboot-factory</td>
<td></td>
<td>Upgrade the boot and firmware, and delete the user data</td>
</tr>
<tr>
<td>/save-reload</td>
<td></td>
<td>Save the current configuration if required and reload the system after successful upgrade.</td>
</tr>
<tr>
<td>/force-reload</td>
<td></td>
<td>Do not save the current configuration and reload the system after successful upgrade.</td>
</tr>
<tr>
<td>path</td>
<td>The location of the file, which can be usb:, tftp, ftp, or flash:</td>
<td></td>
</tr>
</tbody>
</table>

### What to do next

**Example**

```bash
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**

<table>
<thead>
<tr>
<th>Command or Action</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>configure terminal</td>
</tr>
<tr>
<td></td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| 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 connectivity 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.
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:

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, on page 87
- IXM modem Firmware Update, on page 97
- Configuring IGMA, on page 99
- Troubleshooting, on page 100

Preparing FND for IXM ZTD

Follow these steps to prepare FND for IXM ZTD:

Procedure

Step 1
If you are using PSK authentication for tunneling, 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.
Step 2  Add the Actility LRR and public key to FND by clicking the **import** button on the File Management page.
Step 3  Update the Tunnel Configuration group with the following parameters and save the changes. The following figure shows an example for PSK.
Step 4  Update the Device Configuration group with the following parameters and save the changes. The following figure shows a sample configuration.
Update the Device Configuration Group properties with the following parameters and save the changes.
The Tunnel Provisioning settings page will have the FND common name populated as the following figure shows.
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
```
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
  encri aes 256
  hash sha256
  authentication pre-share
  group 19

crypto isakmp keealive 10

.crypto isakmp client configuration group 19
  key cisco
  domain cisco.com
  pool POOL


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


crypto ipsec profile ipsecpof
  set security-association lifetime kilobytes disable
  set transform-set test
  set isakmp-profile test


tunnel protection ipsec profile ipsecpof
  ip unnumbered GigabitEthernet0/1
tunnel source GigabitEthernet0/1
tunnel mode ipsec ipv4

tunnel 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.
FND Configuration for IXM

Preparing FND for IXM ZTD

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.

<table>
<thead>
<tr>
<th>Date/Time</th>
<th>Event Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-21 15:29:45</td>
<td>Success</td>
<td>Registration Success</td>
</tr>
<tr>
<td>2017-08-21 15:29:45</td>
<td>Up</td>
<td>INFO LoRaWAN Gateway is up</td>
</tr>
<tr>
<td>2017-08-21 15:29:52</td>
<td>Request</td>
<td>INFO Registration request from LoRaWAN Gateway</td>
</tr>
<tr>
<td>2017-08-21 15:24:00</td>
<td>Down</td>
<td>MAJOR LoRaWAN Gateway is down</td>
</tr>
<tr>
<td>2017-08-21 15:24:14</td>
<td>Success</td>
<td>INFO Tunnel provisioning successful</td>
</tr>
<tr>
<td>2017-08-21 15:23:27</td>
<td>Request</td>
<td>INFO Tunnel provisioning request from LoRaWAN Gateway</td>
</tr>
</tbody>
</table>

Step 8

Detailed IXM modem information can be viewed by clicking on the modem link.
Step 9 If configuration update is required or a new modem is added to the router, follow the same procedure from Step 1. But in this case you invoke a configuration push.
default-ir800

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

Device Status

<table>
<thead>
<tr>
<th>Name</th>
<th>Push Status</th>
<th>IP Address</th>
<th>Error Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>IR809G-LTE-GA-K9+JMX1915X01Q</td>
<td>NOT_STARTED</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IR809G-LTE-VZ-K9+JMX2023X031</td>
<td>NOT_STARTED</td>
<td>55.55.0.81</td>
<td></td>
</tr>
</tbody>
</table>

IXM modem Firmware Update

Procedure

Step 1  Load the firmware file to FND.
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.

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

IoT Gateway Management Agent (IGMA) is for management in conjunction with FND.

The IGMA configuration commands are as following:

- To start IGMA, use the following command:

  IXM#igma start
  IGMA Starting...

- To configure IGMA, use the following command:

  IXM#configure terminal
  IXM(config)#igma
  event IGMA Event Configuration
  local-trustpoint Set IGMA local-trustpoint configuration
  profile IGMA Profile Configuration
  secure Set igma secure mode

- To check the status of IGMA:

  IXM#request shell container-console
  Enter System Password:

  Connected to tty 0
  Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a itself

  bash-3.2#
  bash-3.2#
  bash-3.2#
  bash-3.2# ps -ef | grep igma
  7151 root 0:00 grep igma
  bash-3.2#

- Regarding ports, trustpoints and security, Apache web server should be running with the port 443.
  Also the following CLI will activate igma using SUDI:

  igma local-trustpoint sudi
- Configuration in combination with CPF
  
  Sample Configuration along with CPF
  
  !
  igma secure enable
  
  !
  igma event destination https://us-int.ciscoiot.com 5683
  
  igma profile iot-fnd-metric
  active
  add-command show common-packet-forwarder info
  add-command show common-packet-forwarder status
  add-command show fpga
  add-command show inventory
  add-command show ip interface FastEthernet 0/1
  add-command show ipsec status info
  add-command show led status
  add-command show platform status
  add-command show radio
  add-command show version
  interval 15
  url https://us-int.ciscoiot.com/cgna/igma/metric
  exit

  igma profile iot-fnd-register
  add-command show fpga
  add-command show inventory
  add-command show ip interface FastEthernet 0/1
  add-command show ipsec status info
  add-command show platform status
  add-command show radio
  add-command show version
  interval 5
  url https://us-int.ciscoiot.com:443/cgna/igma/register
  exit
  !
  common-packet-forwarder profile
  ipaddr us-int.ciscoiot.com port 3001
  antenna 1 omni gain 1.5 loss 0.0
  gatewayid 1000000000000031
  auth-mode none
  country UnitedStates
  cpf enable
  exit
  !
  igma local-trustpoint sudi

Troubleshooting

Enable the following debug categories on FND before troubleshooting:
• 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).