Release Notes for the Cisco LoRaWAN Gateway, Release 2.1.0.2

First Published: 2020-09-04

Last Modified: 2020-10-01

Introduction

The Cisco LoRaWAN Gateway is one of the Cisco Internet of Things (IoT) extension module series. It can be connected to the Cisco 809 and 829 Industrial Integrated Services Routers (IR800 series) for virtual mode or standalone for low-power wide-area (LPWA) access and is positioned as a carrier-grade gateway for 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.

Note Currently, Cisco LoRa IXM only supports Actility's proprietary "Packet Forwarder", long range relay (LRR), in production. This release will add support of Common Packet Forwarder (CPF). CPF will enable LoRaWAN gateway as an open platform to operate with the open source LoRa Network Servers. CPF is pre-installed in the latest software image of IXM and can be managed via CLI from IXM. The Basic Station (Station for short), an implementation of the LoRa packet forwarder, has been officially released and supported by Semtech. For more details, refer to https://doc.sm.tc/station/.

Note The Cisco LoRaWAN Gateway was previously named Cisco LoRaWAN Interface Module.

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

You can configure the LoRaWAN IXM running on virtual interface mode or standalone mode through CLI or IoT FND. For more information, see the Cisco Wireless Gateway for LoRaWAN Software Configuration Guide.

Note The Common Packet Forwarder (CPF) feature is only supported in standalone mode.

System Requirements

Hardware Supported

Model No.	Description
IXM-LPWA-800-16-K9	Cisco LoRaWAN Gateway, IoT extension module series, radio spectrum from 863–870 MHz, 16 LoRa channels, IP67
IXM-LPWA-900-16-K9	Cisco LoRaWAN Gateway, IoT extension module series, radio spectrum from 902–928 MHz, 16 LoRa channels, IP67

Software Images

Filename	Description
ixm_mdm_i_k9-2.1.0.2.tar.gz	Cisco LoRaWAN Gateway OS Image Version 2.1.0.2 with Semtech Basic Station Release Version 2.0.5 FPGA Version 61 HAL Version 5.1.0

Installation of a New Software Release

For both standalone mode and virtual mode, after you upgrade the LoRaWAN gateway to Release 2.0.30, you can only downgrade to Release 2.0.20. Downgrading to releases earlier than 2.0.20 is not supported. For example, from Release 2.0.30 to Release 2.0.11, or from Release 2.0.30 to Release 2.0.10, is not supported..

To upgrade to Release2.0.x, any older versions must first be upgraded to Release 1.0.20. For example, Release 1.0.4, 1.0.5, or 1.0.6 has to be upgraded to 1.0.20 first and then upgraded to Release 2.0.x. From 2.0.x, the gateway can be upgraded to 2.1.0.2.

Firmware Upgrade From Standalone Mode

Note We assume that you have the latest FPGA v61. If you have loaded any recent release on the IXM, use the **show inventory** command to check the FPGA status. If the FPGA version is not 61, upgrade first with an image that has FPGA v61.

Refer to the release support matrix on various FPGA version and LRR version support.

Follow these steps to install a new software image on the standalone mode LoRaWAN Gateway:

Procedure

Step 1 Log into the Cisco LoRaWAN Gateway through the console port, or SSH if configured.

Note The console port is 115.2kbs.

Step 2 Check the current version before upgrade.

Example:

```
IXM#show version
Cisco LoRaWAN Gateway Software, Version 2.1.0.2, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012-2018 by Cisco Systems, Inc.
Compiled by Cisco LoRaWAN Gateway Team

ROM: Bootstrap program is Cisco LoRaWAN Gateway boot loader
Firmware Version : 2.1.0.2, RELEASE SOFTWARE
Bootloader Version: 20180130_cisco

Hostname:IXM uptime is 1 hour, 45 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 1026516K bytes of memory.
Last reset from power-on

Base ethernet MAC Address : 00:50:43:6D:3C:28
Model revision number: : E0
System serial number: : FOC23126GCP

IXM#
```

Step 3 Download the image file to the Cisco LoRaWAN Gateway from a TFTP server or from a USB device, and install the image.

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

Use the following command to download and install the firmware.

```
#archive download-sw firmware{/factory|/normal [/save-reload|/force-reload]}
 path
```

- **/factory** – Upgrade the firmware and delete user data.

Note Avoid using the **/factory** option with this command, because it erases everything and brings back to factory default.

- **/normal** – Upgrade the firmware and keep user data.
- **/save-reload** – Save the current configuration if required and reload the system after successful upgrade.
- **/force-reload** – Do not save the current configuration and reload the system after successful upgrade.
- *path* - The location of the file, which can be usb:, tftp, ftp, or flash:

Note When upgrading from 2.0.32 or prior to 2.1.0.2 with **/normal** option, you need to upgrade it TWICE, which will synchronize the primary and backup images to the same version. Same method applies to downgrading from 2.1.0.2 to 2.0.32 or prior as well to keep the primary and backup images in sync.

Note If the factory upgrade option is used, the twice upgrade is not required.

Example:

```
IXM#archive download-sw firmware /factory /force-reload usb:ixm_mdm_i_k9-2.1.0.2.tar.gz
Unsaved configuration will not be saved
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Copy 87337565 bytes took 00:00:03 [hh:mm:ss]
Validating archive...
Validation successful
Extracting images...
Extracted images successfully
Verifying images...
Cross checking versions...
Performing secure image validation...
```

Step 4 After the image is installed successfully, verify the status.

Example:

```
IXM#show version
Cisco LoRaWAN Gateway Software, Version 2.1.0.2, RELEASE SOFTWARE
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2012-2018 by Cisco Systems, Inc.
Compiled by Cisco LoRaWAN Gateway Team

ROM: Bootstrap program is Cisco LoRaWAN Gateway boot loader
Firmware Version : 2.1.0.2, RELEASE SOFTWARE
Bootloader Version: 20180130_cisco
```

```
Hostname:IXM uptime is 1 hour, 39 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 1026516K bytes of memory.
Last reset from power-on

Base ethernet MAC Address : 00:50:43:6D:3C:28
Model revision number: : E0
System serial number: : FOC23126GCP
```

Step 5 Check the FPGA status using the following command:

Example:

```
IXM#show inventory
Name : IXM
ImageVer : 2.1.0.2
BootloaderVer : 20180130_cisco
SerialNumber : FOC23126GCP
PID : IXM-LPWA-800-16-K9
UTCTime : 01:46:14.173 UTC Sat Aug 15 2020
FPGAVersion : 61
FPGAStatus : Ready
ChipID : LSB = 0x286c070c MSB = 0x00f14492
TimeZone : UTC
LocalTime : Sat Aug 15 01:46:14 UTC 2020
ACT2 Authentication: PASS
IXM#
```

Virtual Mode Installation

Note Before upgrading to Release 2.0.x from Release 1.0.x, make sure you have the FPGA v58 properly installed. The FPGA upgrade will be triggered once the IXM boots up with the image version 1.0.20. After 10 - 15 minutes, you can use the following command to check the FPGA version. Do not install the packet forwarder software or perform radio related configuration while the FPGA is upgrading or downgrading.

```
IR829_1#show virtual-lpwa 3 modem info
Name : Virtual-LPWA 3
ModemImageVer : 2.1.0.2
BootloaderVer : 20180130_cisco
```

```
ModemAgentVer : 1.02
SerialNumber : FOC23126GDH
PID : IXM-LPWA-800-16-K9
UTCTime : 02:16:14.332 UTC Wed Aug 19 2020
IPv4Address : 192.168.100.2
IPv6Address : none
FPGAVersion : 61
TimeZone : PDT
LocalTime : Tue Aug 18 19:16:14 PDT 2020
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x306b0a14 MSB = 0x00f14200
LoRaSerialNumber : FOC22433QLK
LoRaCalc :
<135,122,114,106,98,94,90,86,77,69,60,52,43,39,35,31-142,130,122,114,106,102,98,94,85,77,69,60,52,48,44,40>
CalTempCelsius : 40
CalTempCodeAD9361 : 97
RSSIOffset : -202.16,-202.99
AESKey : Unknown
IR829_1#
```

Follow this procedure to upgrade to Release 2.1.0.2:

Procedure

Step 1 Log in to the IR809 or IR829 system with terminal through SSH or Console.

Step 2 Copy the image file into IR809 or IR829 from your host, and the image will be stored in flash.

Example:

```
IR829_1#copy scp: flash:
Address or name of remote host [172.27.74.9]?
Source username [admin]?
Source filename [/tftpboot/ixm_mdm_i_k9-2.1.0.2.tar.gz]?
Destination filename [ixm_mdm_i_k9-2.1.0.2.tar.gz]?
WARNING!!!
READ THIS BEFORE ATTEMPTING TO LOGON
This System is for the use of authorized users only. Individuals
using this computer without authority, or in excess of their
authority, are subject to having all of their activities on this
system monitored and recorded by system personnel. In the course
of monitoring individuals improperly using this system, or in the
course of system maintenance, the activities of authorized users
may also be monitored. Anyone using this system expressly
consents to such monitoring and is advised that if such
monitoring reveals possible criminal activity, system personnel
may provide the evidence of such monitoring to law enforcement
officials.
Cisco Acceptable Use Policy:
http://wwwin.cisco.com/infosec/policies/acceptableuse.shtml
Password:
Sending file modes: C0777 14 ixm_mdm_i_k9-2.1.0.2.tar.gz
87347295 bytes copied in 128.345 secs (571314 bytes/sec)
IR829_1#
IR829_1#
IR829_1#dir | include ixm_mdm_i_k9-2.1.0.2.tar.gz
91 -rw- 87347295 Aug 18 2020 17:27:32 -07:00 ixm_mdm_i_k9-2.1.0.2.tar.gz
IR829_1#
```

Step 3 (Optional) If you are upgrading from an older version to Release 1.0.20, the upgrade will result in updating the FPGA to version 61. After upgrading the image, no action should be taken while the FPGA is upgrading. You must wait until you get the upgrade status of Ready, as the following example shows.

Example:

```
IR829_1#show virtual-lpwa 10 modem status
Name : Virtual-LPWA 10
Status : Running
Uptime : 6:27:03.500000
Door : DoorClose
Upgrade Status : Ready

IR829_1#

IR829_1#show virtual-lpwa 3 modem info
Name : Virtual-LPWA 3
ModemImageVer : 2.1.0.2
BootloaderVer : 20180130_cisco
ModemAgentVer : 1.02
SerialNumber : FOC23126GDH
PID : IXM-LPWA-800-16-K9
UTCTime : 02:16:12.770 UTC Wed Aug 19 2020

IPv4Address : 192.168.100.2
IPv6Address : none
FPGAVersion : 61
TimeZone : PDT
LocalTime : Tue Aug 18 19:16:12 PDT 2020
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x306b0a14 MSB = 0x00f14200
LoRaSerialNumber : FOC22433QLK
LoRaCalc :
<135,122,114,106,98,94,90,86,77,69,60,52,43,39,35,31-142,130,122,114,106,102,98,94,85,77,69,60,52,48,44,40>
CalTempCelsius : 40
CalTempCodeAD9361 : 97
RSSIOffset : -202.16,-202.99
AESKey : Unknown

IR829_1#
```

Step 4 Upgrade the firmware to Release 2.1.0.2 using the following factory install CLI:

```
IR829_1#virtual-lpwa 10 modem install firmware factory flash:ixm_mdm_i_k9-2.1.0.2.tar.gz
```

Step 5 After the image is installed successfully, verify the status. As shown in the following output, **ModemImageVer** has been updated, but **BootloaderVer** remains the same.

Example:

```
IR829_1#show virtual-lpwa 3 modem info
Name : Virtual-LPWA 3
ModemImageVer : 2.1.0.2
BootloaderVer : 20180130_cisco
ModemAgentVer : 1.02
SerialNumber : FOC23126GDH
PID : IXM-LPWA-800-16-K9
UTCTime : 02:16:14.332 UTC Wed Aug 19 2020
IPv4Address : 192.168.100.2
IPv6Address : none
```

```
FPGAVersion : 61
TimeZone : PDT
LocalTime : Tue Aug 18 19:16:14 PDT 2020
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x306b0a14 MSB = 0x00f14200
LoRaSerialNumber : FOC22433QLK
LoRaCalc :
<135,122,114,106,98,94,90,86,77,69,60,52,43,39,35,31-142,130,122,114,106,102,98,94,85,77,69,60,52,48,44,40>
CalTempCelsius : 40
CalTempCodeAD9361 : 97
RSSIOffset : -202.16,-202.99
AESKey : Unknown

IR829_1#
```

Step 6 Upgrade the firmware to Release 2.1.0.2 using the same CLI with uboot or uboot-only option:

```
IR829_1#virtual-lpwa 10 modem install firmware factory flash:ixm_mdm_i_k9-2.1.0.2.tar.gz ?
  no-uboot    install without uboot
  only-uboot  install uboot only
  uboot       install uboot together
  <cr>
```

Note This step is to upgrade the uboot options if the device is upgraded to Release 2.0.x for the first time, because the uboot options are not available for Release 1.0.20. Additionally, to use these uboot options in IR8x9, you must upgrade the IOS image of IR8x9 to Release 15.7(3)M2.

Note If certificates for IPSec have been persistently stored in the module in any image before 2.0, follow this procedure during an upgrade to image 2.0 and later. This applies to both factory and normal upgrades and must be done for proper behavior of the module.

a. Erase the certificates.

b. Upgrade the image.

c. Re-download the new certificates.

Step 7 After the image is installed successfully, verify the status. You will find from the output that both **ModemImageVer** and **BootloaderVer** have been upgraded.

Example:

```
IR829#show virtual-lpwa 3 modem info
Name : Virtual-LPWA 3
ModemImageVer : 2.1.0.2
BootloaderVer : 20180130_cisco
ModemAgentVer : 1.02
SerialNumber : FOC23126GDH
PID : IXM-LPWA-800-16-K9
UTCTime : 02:16:12.770 UTC Wed Aug 19 2020
IPv4Address : 192.168.100.2
IPv6Address : none
FPGAVersion : 61
TimeZone : PDT
LocalTime : Tue Aug 18 19:16:12 PDT 2020
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x306b0a14 MSB = 0x00f14200
LoRaSerialNumber : FOC22433QLK
```

```
LoRaCalc :
<135,122,114,106,98,94,90,86,77,69,60,52,43,39,35,31-142,130,122,114,106,102,98,94,85,77,69,60,52,48,44,40>
CalTempCelsius : 40
CalTempCodeAD9361 : 97
RSSIOffset : -202.16,-202.99
AESKey : Unknown

IR829_1#
```

Switching Between Standalone Mode and Virtual Mode

When the LoRaWAN gateway is in standalone mode, use the **switchover** EXEC command to switch to the virtual mode.

```
#switchover
```

You can switch the LoRaWAN gateway from virtual mode to standalone mode through IR8x9, using the following command.

```
IR800#virtual-lpwa 1 modem standalone mode enable
```

New and Changed Information

This section contains new and changed information for this release.

New Features In This Release

The following new features are introduced in this release:

- Common Packet Forwarder (CPF) on IXM standalone mode.

Note The CPF feature is intended to operate only when a GPS fix is actively available or has been stored from an earlier fix. The location derived from the GPS fix must be in one of the countries listed in the table below. If not, the radio will not turn on.

- Semtech Basic Station Mode to interoperate with LoRaWAN Network Server (LNS) implementing the corresponding backend side.
- Class B device is supported in CPF on IXM in standalone mode.
- Plug-n-Play (PnP) is supported for IXM provisioning (for example, Cisco PnP cloud).
- GPS check for verification of channel plans is also included in this release. Countries supported by this GPS check include:

Code	Name	Channel plan
AL	Albania	EU868
AD	Andorra	EU868
AM	Armenia	EU868
AR	Argentina	AU915-928
AT	Austria	EU868
AU	Australia	AU915 (default) AS923
AZ	Azerbaijan	EU868
BY	Belarus	EU868
BE	Belgium	EU868
BA	Bosnia	EU868
BN	Brunei	EU868
BG	Bulgaria	EU868
KH	Cambodia	EU868
CA	Canada	US915 (default) AU915
CN	China	AS923
HR	Croatia	EU868
CY	Cyprus	EU868
CZ	Czech Republic	EU868
DK	Denmark	EU868
EE	Estonia	EU868
FI	Finland	EU868
FR	France	EU868
DE	Germany	EU868
GR	Greece	EU868
HK	Hongkong	EU868
HU	Hungary	EU868
IS	Iceland	EU868
IE	Ireland	EU868

Code	Name	Channel plan
IN	India	IN865
IT	Italy	EU868
JP	Japan	AS923
LA	Laos	EU868
LV	Latvia	EU868
LI	Liechtenstein	EU868
LT	Lithuania	EU868
LU	Luxembourg	EU868
MK	Macedonia	EU868
MY	Malaysia	EU868
MX	Mexico	US915
MD	Moldova	EU868
ME	Montenegro	EU868
NL	Netherlands	EU868
NZ	New Zealand	AS923 AU915
NO	Norway	EU868
PL	Poland	EU868
PT	Portugal	EU868
PR	Puerto Rico	US915
RO	Romania	EU868
RS	Serbia	EU868
RU	Russia	RU864
SG	Singapore	EU868
SK	Slovakia	EU868
SI	Slovenia	EU868
ZA	South Africa	EU868
ES	Spain	EU868
SE	Sweden	EU868

Code	Name	Channel plan
CH	Switzerland	EU868
TH	Thailand	EU868
TR	Turkey	EU868
GB	United Kingdom	EU868
UA	Ukraine	EU868
US	United States	US915 (default) AU915
VA	Vatican City	EU868
VN	Vietnam	EU868

Note Refer to the LoRa Alliance RF region specifications for more information.

New Commands In This Release

This section contains new commands in this release.

Standalone Mode Commands

The following table provides the standalone mode commands.

Command	Purpose
clock gpstime enable	Enables the GPS as the modem clock source. Executed from global configuration prompt.
pki secure-storage reset	Resets secure storage infrastructure for certificate download in releases 2.1.0.2 and prior. Run this command on the 2.1.0.2 image and downgrade to the prior images. Executed from the Exec prompt.

Common-Packet-Forwarder (CPF) Commands

The following table provides the Common-Packet-Forwarder (CPF) Exec commands (executed from # prompt):

Command	Purpose
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 **Note** Files will automatically be deleted from the source location after import.
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 **Note** Files will automatically be deleted from the source location after import.
common-pack-forwarder cert erase gw	Erase IXM LoRa gateway's certification and key.
common-pack-forwarder cert erase srv	Erase LNS server's certification.

The following table provides the Common-Packet-Forwarder profile configuration commands.

1. Type "configure terminal" at the exec prompt.
2. Type "common-packet-forwarder profile" at the global configuration prompt.

Command	Purpose
ipaddr *ip-address* **port** *port*	Configure network server IP address and port. *ip-address* – Network server IP address *port* – Network server port number
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
gps enable	Enable CPF to utilize GPS signal.
aeskey *key*	Configure AES key used for CPF. *key* – AES key used for CPF
gatewayid *gateway-id*	Configure gateway id used for CPF. *gateway-id* – Gateway ID used for CPF

Command	Purpose
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
region-cp *lora-region-name*	Configure LoRa region channel plan code: EU868, US915, AU915, AS923, IN865, RU864. *lora-region-name* – LoRa region code name (optional if default one is used)
board-bw *bandwidth*	*bandwidth* – Manually setup the board rx bandwidth if you need to change the default.
board-freq *freq*	*freq* – Manually setup the board rx frequency if you need to change the default.
tls-sni *enable*	*enable* – Connect to LNS to compare the configured LNS server name with the one embedded in the LNS server's certificate.
cpf enable	Start the CPF. If prompted about a Smart License, answer "yes".
exit	Exits the CPF profile block and updates the configuration.
exit	Exits the global configuration mode.

Show and Debug Commands

Command	Purpose
show common-packet-forwarder info	(Optional) Show CPF configuration and information.
show common-packet-forwarder status	(Optional) Show current state of CPF and if registration with NS was successful.
show common-packet-forwarder log list	(Optional) List available log options such as CPF configuration or trace.
show common-packet-forwarder log name trace *number-of-lines*	(Optional) Display the CPF trace log. *number-of-lines* – Number of lines in log to display from end of file.
show common-packet-forwarder log name config *number-of-lines*	(Optional) Display the current CPF configuration. *number-of-lines* – Number of lines in config to display from end of file.

Command	Purpose
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".

CPF configuration example:

```
IXM#show running-config

!
hostname IXM
!

interface FastEthernet 0/1
ip address dhcp
exit
!
common-packet-forwarder profile
ipaddr 172.27.166.13 port 6090
gps enable
gatewayid 0000000000000001
auth-mode client-server
cpf enable
exit
IXM#
```

Plug-n-Play (PnP) Commands

The following table provides the Plug-n-Play (PnP) commands.

Command	Purpose
pnp enable	Start the PnP agent.
pnp disable	Stop the PnP agent.
show pnp profiles	(Optional) Show PnP version.
show pnp status	(Optional) Show PnP status.
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.

Known Issues

This section contains the known issues in this release.

- **Problem:** Container logging takes about 40 seconds to configure for the first time.
- **Problem:** Starting the packet forwarder takes about 30 seconds for the first time.

- **Problem:** On downgrade from 2.1.0.2 to images 2.0.32 and prior, installed certificates disappear, or after downgrade to 2.0.32, certificates do not persist.

  Workaround:

  1. Certificates will safely remain in secure-storage and will show up again once the device is upgraded to an image later than Release 2.0.32.
  2. Standalone mode only—If you want to download new certificates in images 2.0.32 and earlier, run the command **pki secure-storage reset** (in release 2.1.0.2) to clean secure-storage beforehand. Then, downgrade the image.

  

  Note Using this procedure deletes all certificates currently stored on the device.

- **Problem:** For 2.1.0.2 image,when falling back to backup image due to the boot failures (which is very rare), installed certificates disappear.

  Workaround: When upgrading from 2.0.32 or prior to 2.1.0.2 with **/normal** option, you need to upgrade it TWICE, which will synchronize the primary and backup images to the same version. Same method applies to the downgrading from 2.1.0.2 to 2.0.32 or prior as well to keep the primary and backup images in sync.

  If upgrading or downgrading with **/factory** option, you don't need to do the same. The primary image and backup images are already synchronized.

Caveats

You can use the Bug Search Tool to find information about caveats, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To use the Bug Search Tool:

1. Go to https://tools.cisco.com/bugsearch/.
2. Log in with your Cisco.com user ID and password.
3. Enter information in the Search For, Product, and Releases field as needed, then press **Enter**.

For more information about the Bug Search Tool, click **Help** on the main Bug Search Tool page.

Open Caveats

This section contains open caveats for this release.

- **CSCvv45171**

  Symptom: After the common packet forwarder (CPF) is enabled and the connection to LoRa network server is not ready, the CPF log repeatedly shows "[S2E:ERRO] Failed to send gps event, no buffer space" messages.

  Workaround: Fix the connection issue. The messages do not affect the functionalities of CPF.

- **CSCvv95216**

Symptom: Setting "user" as a username using "username user password xxxx" will cause the following two issues:

1. Inability to login to the container.
2. If you issue **config ntp**, the following messages appear in the console: "Starting ntpd: FAIL" and "ntpq: read: Connection refused"

Only "user" causes this issue. Other usernames, for example "user1", "user2", "cisco" are OK to use.

Workaround: Do a factory reset.

Related Documentation

These documents provide detailed information about the Cisco LoRaWAN Gateway and are available at: www.cisco.com/go/lorawanmodule

- Getting Started and Product Document of Compliance for the Cisco LoRaWAN Interface Module
- Cisco LoRaWAN Gateway Hardware Installation Guide
- Cisco LoRaWAN Gateway Software Configuration Guide
- Release Notes for IoT Field Network Director
- Release Notes for Cisco IR800 Industrial Integrated Services Routers and Cisco 1000 Series Connected Grid Routers
- Cisco IR800 Integrated Services Router Software Configuration Guide
- Cisco IoT Field Network Director User Guide