Cisco IR800 Integrated Services Router Software Configuration Guide

First Published: 2016-12-20

Last Modified: 2022-11-14

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

CONTENTS

Preface

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

Preface

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

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

It contains the following sections:

Objective

This guide provides an overview of the software features and explains how to perform the configuration steps for the Cisco IR800 Integrated Services Routers.

Audience

This guide is intended for people who have a high level of technical ability, although they may not have experience with Cisco software.

Conventions

This section describes the conventions used in this guide.

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

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

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

Searching Cisco Documents

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

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

CHAPTER 1

Product Overview

This chapter provides an overview of the features available for the Cisco IR800 Integrated Services Routers (ISRs).

General Description

The 800 Series Industrial Integrated Services Routers are compact, ruggedized, Cisco IOS Software routers. They offer support for integrated 4G LTE wireless WAN (both 809 and 829 models) and wireless LAN capabilities (829 model only). The IR829 offers an Internal WLAN Access Point which runs on-board the router. The AP803 runs its own IOS software independently from the IR829 IOS, and requires configuring. The AP803 works as a standalone access point or with a wireless controller.

They offer:

- Easily and rapidly deployable
- Highly available, highly secure, and reliable
- Designed for machine-to-machine (M2M) communication and for mobile vehicle communication in harsh environmental conditions
- Designed to withstand hostile environments, tolerating a wide temperature range

These industrialized routers deliver enterprise-class features, including highly secure data, voice, and video communications to stationary and mobile network nodes across wired and wireless links. They can deliver enterprise-grade, wireline-like functionality.

The routers also support Cisco IOx Software, providing an open, extensible environment for hosting additional operating systems and applications directly at the network edge. They can enhance other Cisco IoT System products across multiple industries, including transportation, manufacturing, electrical utilities, and others.

For a complete listing of the routers capabilities, see the Cisco 829 Industrial Integrated Services Routers Product Information .

Hardware Overview

This section covers the overview of the IR809 and IR829.

IR829 Product Overview

Figure 1: Cisco IR829 Integrated Services Router, on page 2 shows the IR829.

Figure 1: Cisco IR829 Integrated Services Router

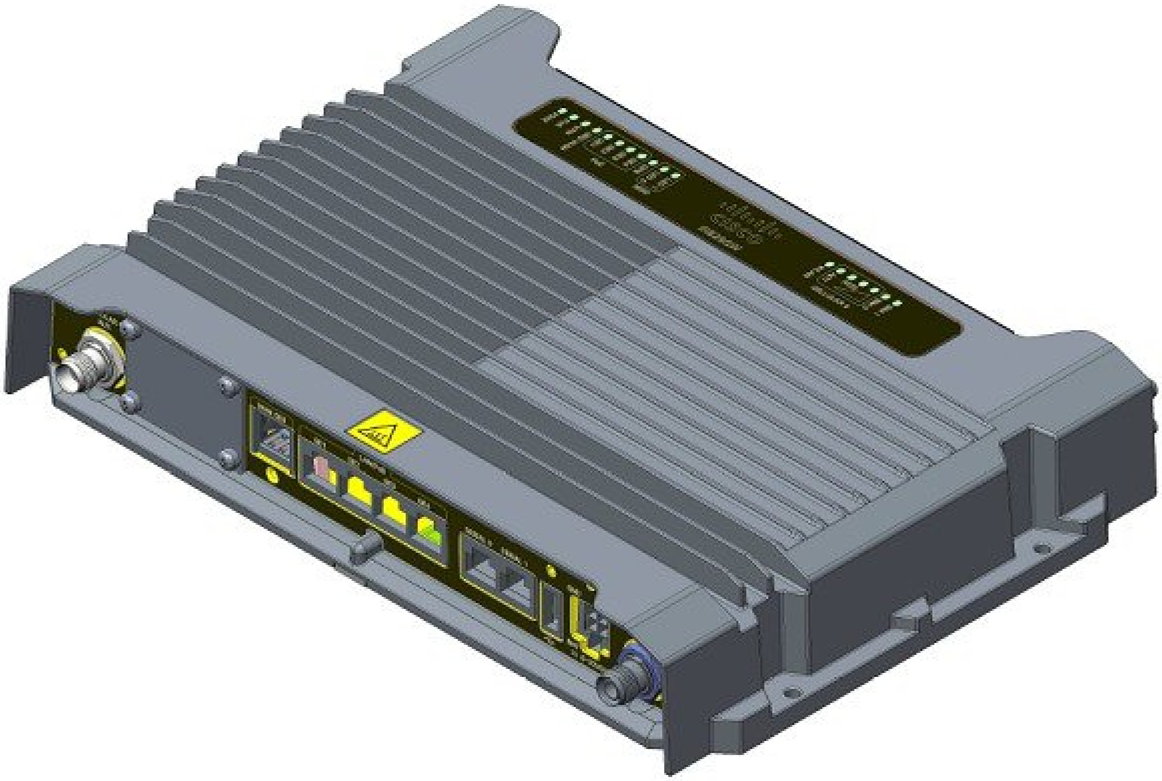
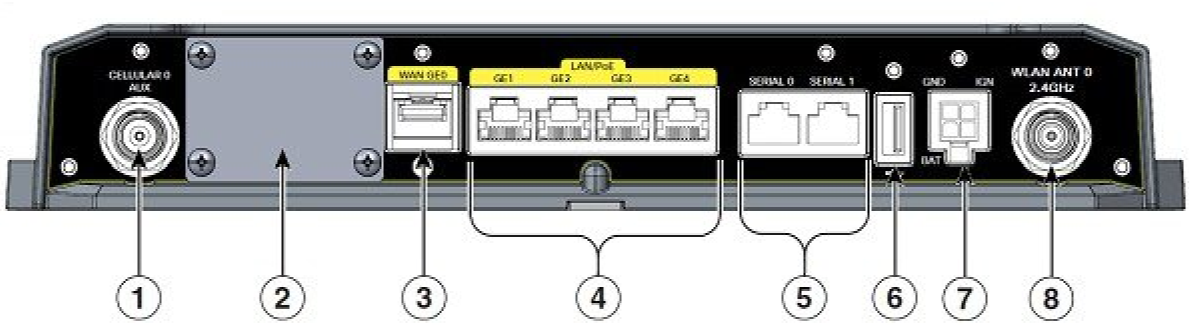


Figure 2: Cisco IR829 Front Panel Single Modem, on page 3 shows the front panel details of the Cisco IR829 Single Modem.

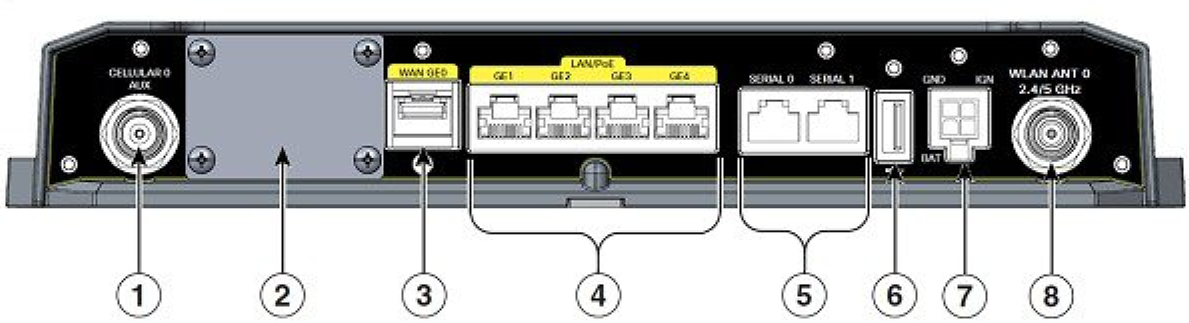
Figure 2: Cisco IR829 Front Panel Single Modem



1	CELLULAR 0 AUX	5	Serial Ports
2	mSATA Slot	6	USB-A Port
3	Gigabit WAN (SFP)	7	Power Input, Battery, and Ignition connector. Refer to the DC Power section for pin-outs.
4	Gigabit Ethernet LAN/PoE (RJ45)	8	WLAN ANT 0 2.4GHz

Figure 3: Cisco IR829 Front Panel Duel Modem, on page 3 shows the front panel details of the Cisco IR829 Dual Modem.

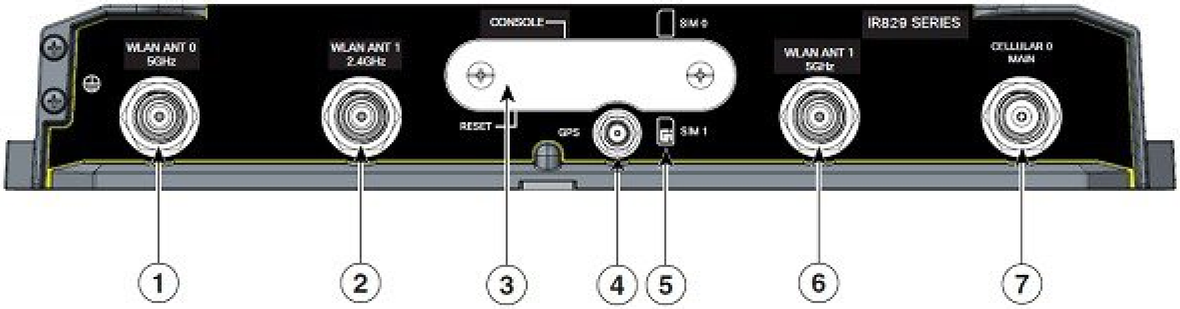
Figure 3: Cisco IR829 Front Panel Duel Modem



1	CELLULAR 0 AUX	5	Serial Ports
2	mSATA Slot	6	USB-A Port
3	Gigabit WAN (SFP)	7	Power Input, Battery, and Ignition connector. Refer to the DC Power section for pin-outs.
4	Gigabit Ethernet LAN/PoE (RJ45)	8	WLAN ANT 0 2.4/5GHz

Figure 4: Cisco IR829 Back Panel Single Modem, on page 4 shows the back panels details of the Cisco IR829 Single Modem.

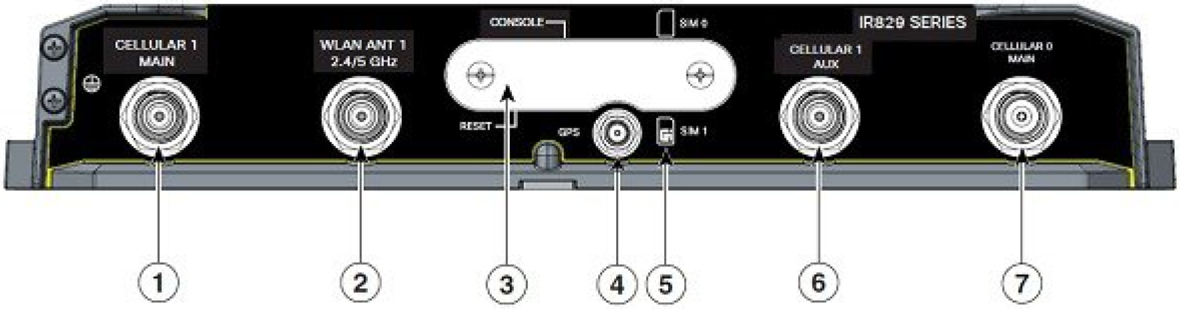
Figure 4: Cisco IR829 Back Panel Single Modem



1	WLAN ANT 0 5GHz	5	Denotes SIM card order, SIM0 on top and SIM1 on bottom.
2	WLAN ANT 1 2.4GHz	6	WLAN ANT 1 5GHz
3	Cover over SIM cards, reset button and console port cover, see Figure 6: Behind the SIM Door, on page 5	7	CELLULAR 0 MAIN
4	GPS SMA		

Figure 5: Cisco IR829 Back Panel Dual Modem, on page 4 shows the back panels details of the Cisco IR829 Dual Modem.

Figure 5: Cisco IR829 Back Panel Dual Modem



1	Cellular 1 Main	5	Denotes SIM card order, SIM0 on top and SIM1 on bottom.
2	WLAN ANT 1 2.4/5GHz	6	Cellular 1 AUX
3	Cover over SIM cards, reset button and console port cover, see Figure 6: Behind the SIM Door, on page 5	7	CELLULAR 0 MAIN
4	GPS SMA		

Note Behind the SIM Door Assembly, there is a reset switch (1), Mini USB console port (2), and Dual SIM slots (3). See Figure 6: Behind the SIM Door, on page 5 for details

Figure 6: Behind the SIM Door

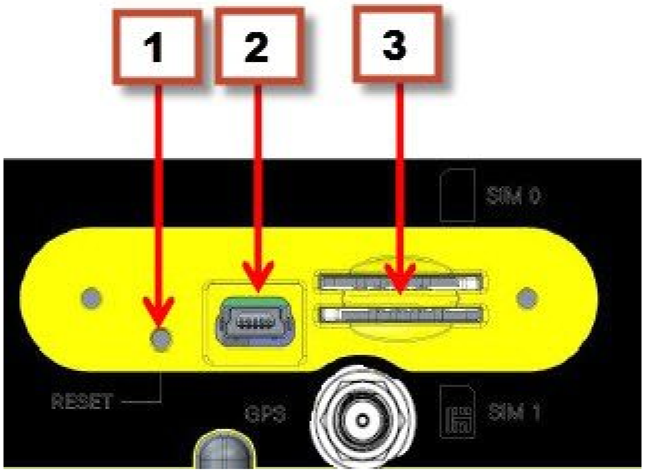


Figure 7: Cisco IR829 Top Cover, on page 6 shows the top of the Cisco IR829.

Figure 7: Cisco IR829 Top Cover

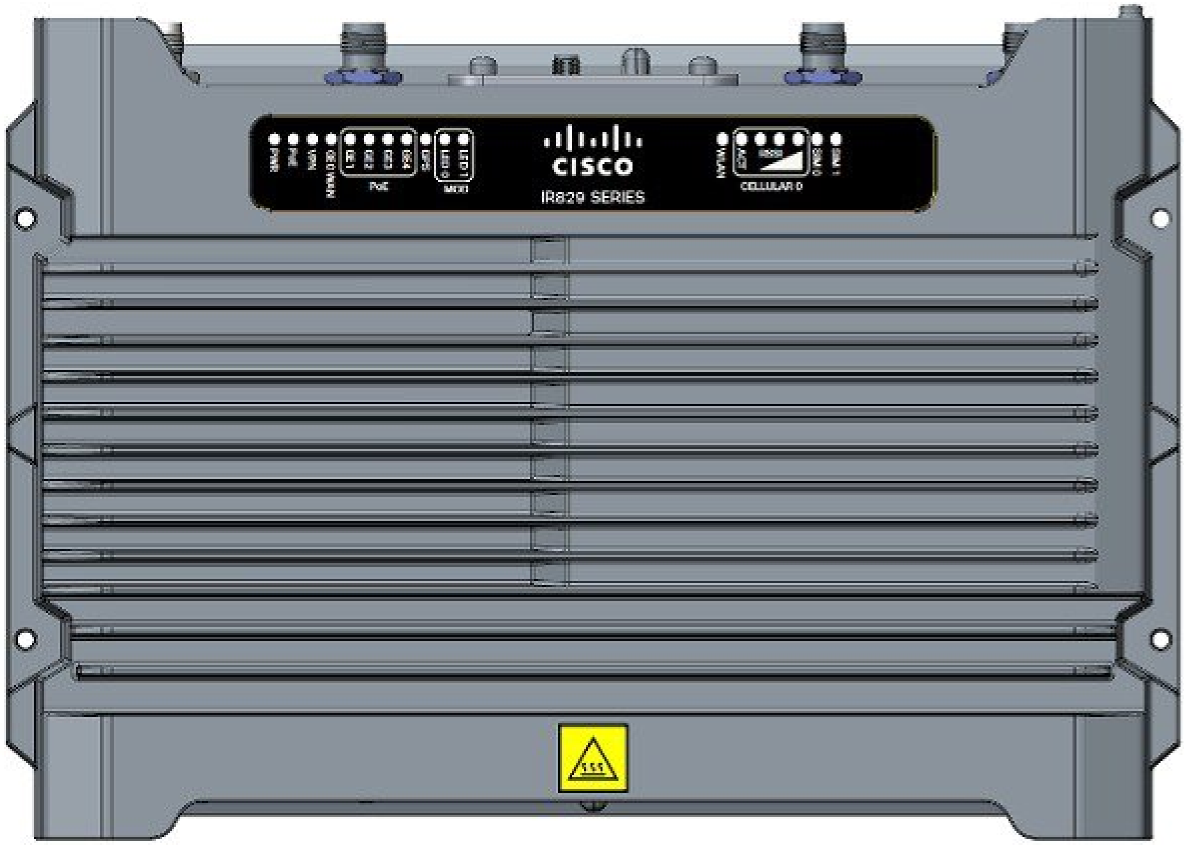
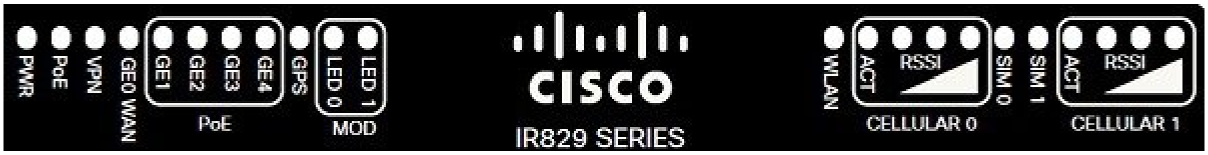


Figure 8: Cisco IR829 LED Detail, on page 6 shows the LED detail from the Dual Modem SKU. Single Modem SKUs will only have Cellular0 LEDs.

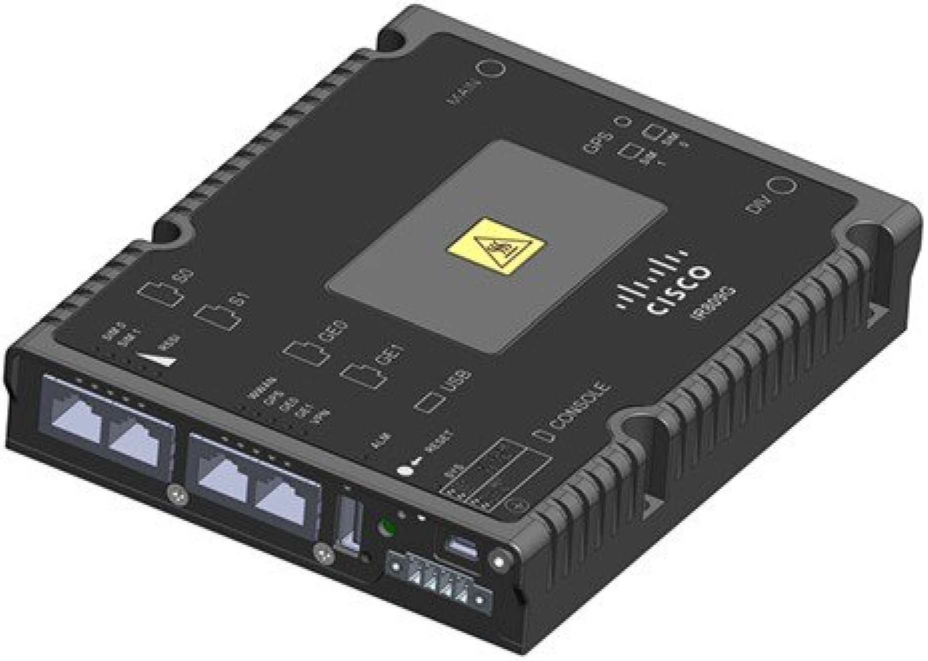
Figure 8: Cisco IR829 LED Detail



IR809 Product Overview

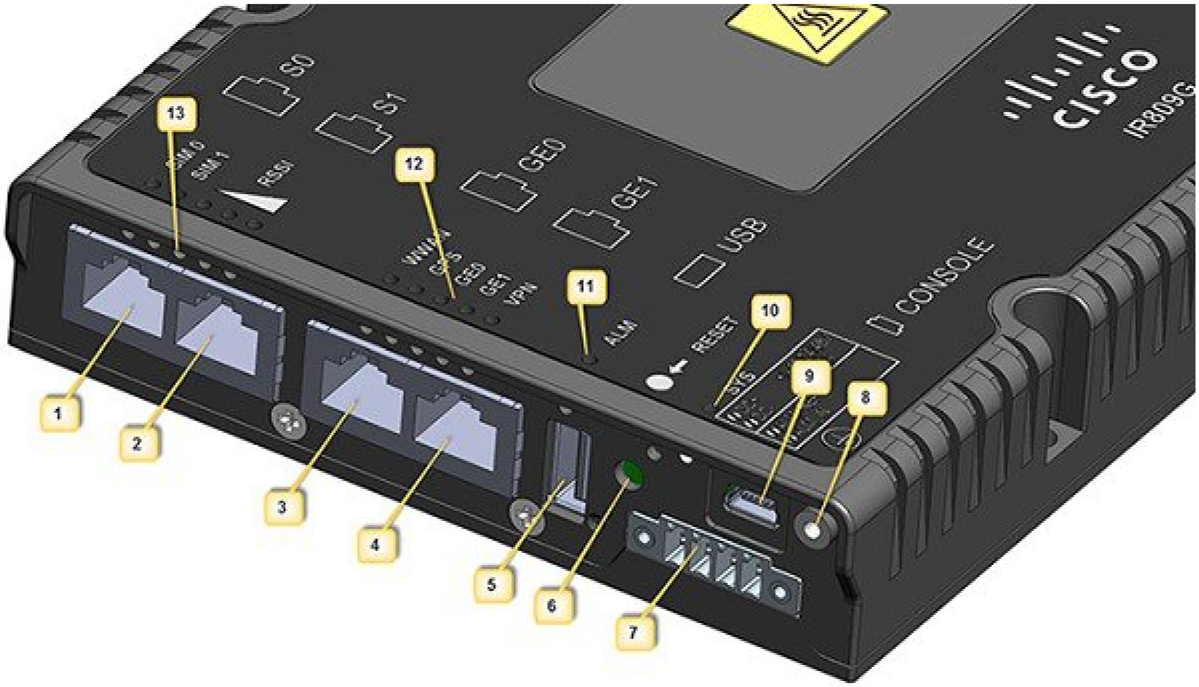
The following figure shows the IR809.

Figure 9: Cisco IR809 Integrated Services Router



The following figure shows the front panel details of the Cisco IR809.

Figure 10: Cisco IR809 Front Panel



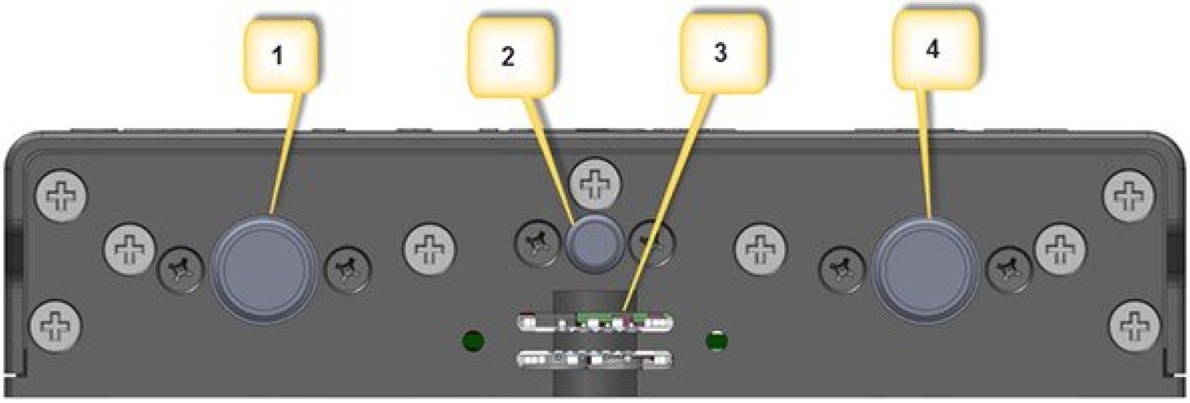
1	S0 RS232 DCE/RS485 Combo Port	8	Grounding Point

2	S1 RS232 DTE only	9	Mini type-B USB console/debug port
3	GE0 (10/100/1000)	10	SYS LED
4	GE1 (10/100/1000)	11	Alarm LED
5	USB 2.0 (Type-A Host Port)	12	WAN/WWAN LEDs
6	RESET Button	13	SIM Card LEDs
7	DC Power/Alarm Connector		

Note LEDs are viewable from the top and from the front of the IR809.

The following figure shows the back panels details of the Cisco IR809.

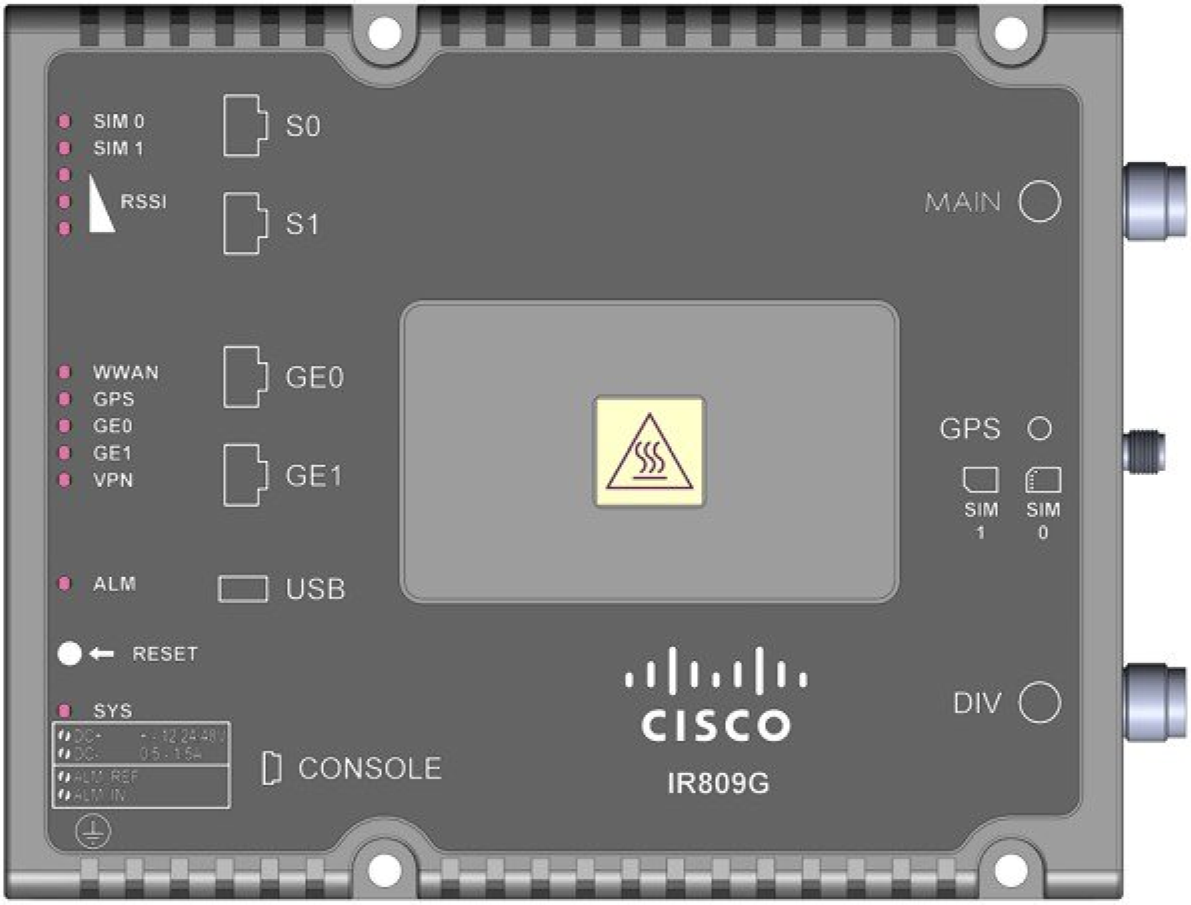
Figure 11: Cisco IR809 Back Panel



1	DIV TNC connector for 4G Modem
2	SMA connector for GPS
3	SIM0 and SIM1 Card Slots
4	MAIN TNC connector for 4G Modem

The following figure shows the top cover details of the Cisco IR809.

Figure 12: Cisco IR809 Top Cover



Note See the respective Hardware Installation Guides for detailed description of the LEDs.

Reset Button

The reset button resets the router configuration to the default configuration set by the factory. To restore the router configuration to the default configuration set by the factory, use a standard size #1 paper clip with wire gauge 0.033 inch or smaller and simultaneously press the reset button while applying power to the router.

Note On the IR829, the rear cover must be removed to expose the reset switch.

Starting with release 15.6(1)T, the IR809 and IR829 have changed the way the reset button works. The IR800 series platforms now perform in the same manner as the C819. The high level description of the functionality works like this:

- Press and hold the reset button while powering up the router

- During warm reboot this button has no impact on performance
- Simply pressing the button at any time does not reset the router
- The router will not react to the reset button if it is pressed after power-up because the button needs to be pushed before turning ON/inserting power – to make sure that the condition is detected.
- The push-button cannot be used to boot a IOS image from network. The golden image has to be on flash: only

Note For the location of the reset button, see the appropriate IR809 or IR829 Hardware Installation Guide.

Perform the following steps to use the reset button:

Procedure

Step 1 Unplug power.

Step 2 Press the reset button on the router.

Step 3 Power up the system while holding down the reset button.

Step 4 Check the “boot system” setting configuration in the default configuration file (prior to saving it to startup-config), and verify that it points to an existing IOS image on the flash: partition. Note: If that particular IOS image is not present, the device will drop in rommon-2 mode and you will need to manually boot an IOS image from there.

Step 5 Copy your desired default config file to the startup-config.

Step 6 Reload the router. Do NOT enter Yes if prompted whether you want to save the running-config to startup-config.

Example

An example of the log activity after a reboot follows:

```
IR800# show log

*Nov 30 19:31:04.925: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down

*Nov 30 19:31:10.651: %PLATFORM-5-RESET_BUTTON: Reset Button pressed during boot up.

*Nov 30 19:31:11.527: %LINK-3-UPDOWN: Interface Async0, changed state to up

*Nov 30 19:31:11.595: %SYS-5-RESTART: System restarted --

Cisco IOS Software, ir800 Software (ir800-UNIVERSALK9-M), Version 15.6(1)T, RELEASE
SOFTWARE (fc1)
```

What to do next

Note To simplify the boot process, the IR800 routers do not support the ROMMON configuration register and the associated CLI commands. The IR800 either boots the pre-configured images, or stops at the ROMMON prompt for user intervention. In the event of a boot failure, see Chapter 3, "Setup Command Facility" for additional information.

Booting a Default IOS Image and Default Configuration - Method 1

The IR800 differs from traditional IOS routers when booting a default IOS image and a default configuration. These steps apply on a device running 15.6(1)T or later.

Method 1:

Procedure

Step 1 Save a copy of your IR800 IOS image with the .default extension on flash. For example: ios-image.default.

Step 2 Save a copy of your IR800 Hypervisor image with the .default extension on bootstrap. For example: hypervisor-image.default.

Step 3 Save your desired default configuration file with the .cfg extension on flash. For example: config.cfg.

Step 4 Reset your IR800 router by powering it down, then press and hold the RESET button while powering up the device.

The IR800 router will automatically boot hypervisor-image.default, then ios-image.default, and load the config.cfg.

Step 5 Make sure there exists only one IOS image with a .default extension, only one configuration file with the .cfg extension on the flash, and only one hypervisor image with the .default extension on bootstrap.

Booting a Default IOS Image and Default Configuration - Method 2

If you do not have a config.cfg on flash, it will boot with the Cisco default configuration (aka: empty) startup-config.

Method 2:

Procedure

Step 1 Check the "boot system" setting configuration in the default configuration file (prior to saving it to startup-config), and verify that it points to an existing IOS image on the flash: partition.

Note If that particular IOS image is not present, the device will drop in rommon-2 mode and you will need to manually boot an IOS image from there.

Step 2 Copy your desired default config file to the startup-config.

Step 3 Reload the router. Do NOT enter Yes if prompted whether you want to save the running-config to startup-config.

What to do next

An example of the log activity after a reboot follows:

```
IR800# show log

*Nov 30 19:31:04.925: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0,
changed state to down
*Nov 30 19:31:10.651: %PLATFORM-5-RESET_BUTTON: Reset Button pressed during boot up.
*Nov 30 19:31:11.527: %LINK-3-UPDOWN: Interface Async0, changed state to up
*Nov 30 19:31:11.595: %SYS-5-RESTART: System restarted --
Cisco IOS Software, ir800 Software (ir800-UNIVERSALK9-M), Version 15.6(1)T, RELEASE SOFTWARE
 (fc1)
```

Configuration Register

To configure the register:

```
IR800#conf t
Enter configuration commands, one per line. End with CNTL/Z.
IR800(config)#config-register 0x?
<0x0-0xFFFF>
IR800(config)#config-register 0x102
IR800(config)#
Jul 26 22:10:22.790: Bootstrap Emulator called with code 62
Jul 26 22:10:22.790: Bootstrap Emulator called with code 61
IR800(config)#
```

To display the register:

```
IR800#sh ver
…..
…..
…..
Configuration register is 0x2101 (will be 0x102 at next reload)
```

The Format for the configuration registers is 0 x _ _ _ _ (4 bytes)

For example:

0x102, 0x2102, 0x2142, 0x142, 0x101, 0x2101

The Configuration Register 1st byte table shows the configuration register 1st byte values and descriptions.

Table 1: Configuration Register 1st byte

Value	Description
0	Boots into rommon 2 on reload. Importance – access to rommon mode and rommon parameters can be changed.

Value	Description
1	Ignores auto-boot and boots first image in flash. In case of failure to boot the first image, it will try a maximum of 3 times to boot the same image and then halt in rommon 2. Importance – Irrespective of auto-boot string it will boot first image from flash. Auto-boot is ignored.
2 to F	Checks auto-boot and if present, the device will boot with auto-boot string. If auto-boot is not present, then the device will boot first image from flash. In case of failure to boot the first image, it will try a maximum of 3 times to boot the same image and then halt in rommon 2. Importance - Auto-boot has the higher priority, and if that fails then the device will boot-up with first image.

The Configuration Register 2nd byte table shows the configuration register 2nd byte values and descriptions.

Table 2: Configuration Register 2nd byte

Value	Description
0	On reload after the device boots up with an image, it will have all the configuration stored in startup config.
4	On reload after the device boots up with an image, it will ignore the startup config and stays on config dialog box for user to enter configuration. **Note** startup-config is still present however not used by router Importance – Used for password recovery.

The Configuration Register 3rd byte table shows the configuration register 3rd byte values and descriptions.

Table 3: Configuration Register 3rd byte

Value	Description
0 or 1	Allows the user to break and get into rommon mode by pressing Ctrl C. Importance – To debug or to set something in rommon mode.

The Configuration Register 4th byte table shows the configuration register 4th byte values and descriptions.

Table 4: Configuration Register4th byte

Value	Description
0 or 2	Doesn’t make any difference, behavior is decided by next 3 bytes.

Auto-recovery of Corrupt Filesystems

On rare occasions, the router could get stuck in ROMMON to flash and bootstrap file system corruption caused by hard reloads. Hard reloads can be a consequence of fluctuating voltage or very low current. The file system (in flash: or bootstrap:) is completely inaccessible at this point.

Starting with 15.8(3)M, on the IR8x9 platforms, software will automatically recover the router if one or more filesystems are corrupt. This feature is enabled once the user executes bundle install, write memory, reload.

For example:

```
IR800#bundle install flash:ir800-universalk9-bundle.SSA.158-3.0m.M
Installing bundle image: /ir800-universalk9-bundle.SSA.158-3.0m.M......
...........................
updating Hypervisor image...
Sending file modes: C0444 25196401 ir800-hv.srp.SPA.3.0.55
SRP md5 verification passed!
updating IOS image...
Sending file modes: C0644 64486377 ir800-universalk9-mz.SSA.158-3.0m.M
IOS md5 verification passed!
Done!
Performing image backup .........Done!
```

During the bundle installation, the user will observe the message "Backup partition successful'. Once the bundle install is complete, the user can also verify if backup is successful using **show platform bundle**.

For example:

```
IR800#show platform bundle
Installed
Backup Success
```

This backup partition is taken from the Guest-OS data partition on the IR809, IR829, IR829GW, IR829B products.

The IR829M products mSATA SSD partition is unaffected.

If a previous user was already using up this extra partition in old software, the new software will NOT proceed with creating a backup partition. This ensures the user data is always intact. If the user wants to trigger a backup, ~300Mb needs to be cleaned up from Guest-OS /dev/sdb. In some routers, Guest-OS /dev/sdb may appear to have ~250Mb lesser, and some ~330Mb. This is due to the two different versions of eMMC on the IR8x9s, and there is no software cli to provide eMMC part number to distinguish.

Files Backed Up to the New Backup Partition

- IOS image
- Hypervisor image
- Guest-OS image (if IOX Recovery is enabled using **conf t** then **iox recovery-enable**)
- Standard Files:
    - Entire eem folder
    - The entire managed folder, except managed/images
    - All pnp* files (all PnP related files)
    - vlan.dat

  - Archive folder

- Field Network Director specific files:
  - express-setup-config
  - before-registration-config
  - before-tunnel-config
- Sample file labeled additional_backup_file (This file is to ensure if a user wants to customize low sized (50 kbytes or less) configuration file copy, they can save it in this name and it will be backed up.

Files NOT Backed Up to the New Backup Partition

- Duplicates of software images in managed/images
- User generated files, folders and configurations
- FW of 4G modems
- IOx application data

Notes:

The backup partition is limited in space and only for basic device recovery, and to load startup -config [as SPI Flash: is intact]. In this manner, remote device reachability is back up again. Remaining files need to be restored again by end user.

If a user running old software would like to increase their current Guest-OS disk space, it is recommended to take a data backup, and execute the following command taking up larger disk space. Starting at IOS release 156(3)M3 and greater, the default disk space allocated to Guest-OS is Option 1 from the example below. For previous releases default used to be Option 6 from the example below.

```
IR800#guest-os 1 disk-repartition ?
1 disk1: 500MB vs disk2: 1800MB
2 disk1: 700MB vs disk2: 1600MB
3 disk1: 900MB vs disk2: 1400MB
4 disk1: 1100MB vs disk2: 1200MB
5 disk1: 1300MB vs disk2: 1000MB
6 disk1: 1500MB vs disk2: 800MB
7 disk1: 1700MB vs disk2: 600MB
```

Note: Actual storage available for applications will be less than the value chosen for all profiles. The disk2 partition displayed in the15.8(3)M release has to account for 300MB less space. For example: option1, disk2 is 1500MB not 1800MB. In future releases, this will be corrected.

Once an auto-recovery is complete, the user will observe a small file in flash called **fs_recovered.ios**. It will contain the timestamp of the last recovery. This file is indication that backup was successful, and that there was indeed a corruption of the filesystem. This file is not persistent on soft reload of the router.

Alternatively, the user can also backup using:

```
IR800#hypervisor backup_images
```

```
WARNING - If you are running this command for the first time, it might delete all application
```

```
 data in IOx. This operation cannot be undone. Continue? [yes/no]: y
Performing image backup........ Done
```

This will ensure the latest sync of vlan.dat, pnp and managed configs.

The first time the command is executed, it will forcibly create the backup. If an IOx user was using up the 300Mb required for backup partition creation from an older IOS release, then it will be carved into backup and the user will loose data. The user can opt for 'no' and perform a manual backup of that data before proceeding with **hypervisor backup_images** command.

Plug and Play Agent (PnP) support over 4G/Ethernet

An option was added to the bundle install command:

bundle install <bundle_image_name> rom-autoboot

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

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

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

PNP using Ethernet can be done in three different ways:

1. Specifying OPTION 43 on DHCP ROUTER

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

2. Specifying DNS on DHCP ROUTER

   Example: domain-name test.com

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

3. Specifying CCO’s address by configuring devicehelper.cisco.com on DHCP ROUTER

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

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

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

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

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

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

Additional Resources for Cisco Plug and Play can be found at the following links:

Plug and Play (PnP) Support on the IR829 LAN

Feature applies to the IR829 product series only

Starting with this release, PnP will be supported over LAN ports (G1 to G4). In previous releases, PnP was supported only over WAN port and 4G LTE.

Similar to WAN port, PnP over LAN Interfaces can be triggered by configuring either DHCP, DNS or CCO details on DHCP/DNS server. Since all the LAN interfaces default to Vlan1, when the router boots up in factory default mode, it acquires an IP address from either DHCP or DNS server through Vlan1. This is how PnP is initiated. Once the initial PnP discovery is successful and the router is discovered on the PnP Server (for example: any Network Management System such as Field Network Director, APIC-EM, DNAC to name a few), it will be in an unclaimed state. From here, the user can 'claim' the device and push required configurations from the PnP server to the router.

Note: Image upgrade from the PnP server is currently not supported.

PnP using Ethernet can be done in three different ways:

1. Specifying OPTION 43 on DHCP router

```
ip dhcp pool IOT_address
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 43 ascii 5A1D;B2;K4;I172.23.165.116;J80
ntp master
```

2. Specifying DNS on DHCP router

```
ip dhcp pool IOT_DNS
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
```

```
domain-name pnp-agent-tb.cisco.com
dns-server 192.168.2.1
ip host pnpserver.pnp-agent-tb.cisco.com 172.23.165.116
ip host pnpntpserver.pnp-agent-tb.cisco.com 172.23.165.116
ip dns server
```

3. Specifying CCO’s address by configuring devicehelper.cisco.com on DHCP router

```
ip dhcp pool IOT_dhcp
network 192.168.3.0 255.255.255.0
default-router 192.168.3.1
dns-server 192.168.3.1
ip host devicehelper.cisco.com 64.101.32.10
ip host time-pnp.cisco.com 192.168.3.1
ntp master
```

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

To verify if PnP is completed or not, verify with the **show run** command. At the bottom of the command output, there should be a PnP profile and the PnP controller IP address. This means the device was redirected to the PnP server and the PnP discovery was successfully done. Once the configuration file is pushed from the PnP server, verify this using the **show pnp task** command and verify the Config-Upgrade Task should show Result: Success.

You can further debug and verify the entire PnP process using the commands **show pnp summary**, **show pnp trace** and **show pnp tech-support**.

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

```
IR800#show running-config | begin pnp profile
pnp profile pnp_redirection_profile
transport https ipv4 128.107.248.237 port 443
!
end
IR800#show pnp task
------------------ show pnp tasks ---------------------
Certificate-Install Task - Last Run ID:5, ST:7201, Result:Success,
LT:117562, ET:4 ms
Src:[-], Dst:[-]
Device-Auth Task - Never Run
Device-Info Task - Last Run ID:9, ST:5301, Result:Success, LT:200634, ET:1 ms Src:[udi],
Dst:[pnp-zero-touch]
Image-Install Task - Never Run
SMU Task - Never Run
Config-Upgrade Task - Last Run ID:10, ST:5202, Result:Success, LT:267420, ET:984 ms
Src:[https://192.168.1.1:443/api/v1/file/onetimedownload/1530b4e5-beb8-4db3-b4df-28dc016464fc],
 Dst:[running]
CLI-Config Task - Never Run
Licensing Task - Never Run
File-Transfer Task - Never Run
Redirection Task - Never Run
CLI-Exec Task - Last Run ID:12, ST:5401, Result:Success, LT:279464, ET:1 ms
Src:[cli-exec request], Dst:[running-exec]
Script Task - Never Run
```

Password Recovery

Use the following procedure in the event you have lost the router password.

Procedure

Step 1 Copy a ".cfg" configuration file in the router flash memory without any "username", "password", or "AAA" statements.

Example:

```
IR800# copy usb:default-config flash:default-config.cfg
Destination filename [default-config.cfg]?
```

In the router flash memory you must have only one ".cfg" at a time. If there are two or more the system will be confused resulting in unexpected behavior.

Step 2 Make a copy of the "startup-config" file in the router flash memory without an extension.

Example:

```
IR800# copy startup-config flash:startup-config
Destination filename [startup-config.cfg]?
```

Step 3 Power-off the router. Press the "Reset Button" and power-on the router, holding the button for 30sec. The router should boot with the new ".cfg" file.

Step 4 Copy the "startup-config" file over the "running-config".

Example:

```
IR800# copy flash:startup-config running-config
Destination filename [startup-config.cfg]?
```

Step 5 Change only the passwords necessary for your configuration. You can remove individual passwords by using the no in front of each statement. For example, entering the no enable secret command removes the enable secret password.

Step 6 Save the configuration changes.

Example:

```
IR800# write
building configuration...
```

No Service Password Recovery

The No Service Password-Recovery feature is a security enhancement, that when enabled, prevents anyone with console access from using a break sequence (Control+C) during bootup to enter into rommon.

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

- There is a corrupt or missing IOS image in the flash: directory

- Manual boot setting was done in IOS mode
- IOS bootup was disrupted 20 consecutive times

In an upcoming release, Cisco will lock the environment variable in rommon mode to further secure the device.

Prerequisites:

Ensure bundle install process is used to upgrade to this image. Same as with all other features.

Enabling No Service Password Recovery

To enable the feature, use the steps in the following table.

Step	Command or Action	Purpose
Step 1	**enable** Example: `IR800>`**`enable`**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show version** Example: `IR800#`**`show version`**	Displays information about the system software, including configuration register settings.
Step 3	**configure terminal** Example: `IR800#`**`configure terminal`**	Enters global configuration mode.
Step 4	**config-register** <*value*> Example: `IR800(config)#`**`config-register 0x102`**	(Optional) Changes the configuration register setting.
Step 5	**no service password-recovery** Example: `IR800(config)#`**`no service password-recovery`**	Disables the password-recovery capability at the system console.
Step 6	**exit** Example: `IR800(config)#`**`exit`**	Exits global configuration mode and returns to EXEC mode.
Step 7	**write memory** Example: `IR800#`**`write memory`**	Save the configs in NVRAM.

Disabling No Service Password Recovery

The **no service password-recovery** feature is disabled by configuring **service password-recovery**.

```
IR800(config)#service password-recovery
```

Known Limitations:

Always disable the feature by performing **service password-recovery**, before downgrading to an image that does not support this feature.

Software Overview

The IR800 series offers a rich IOS feature set. This section provides a brief overview of these features.

Note Features may be dependent of platform and releases

Feature	Description
Cellular Connectivity	• 4G LTE, 3.7G, 3.5G, or 3G Cellular WAN link • External, dual 4G antennas with main and receive diversity for maximum signal strength connectivity • Dual subscriber identity module (SIM) capability • Auto-Sim • MPDN • Assisted GPS [for specific modems] • Dual-SIM • Dual-LTE (on dual LTE SKUs only) • Concurrent connections to two cellular networks for high reliability, enhanced data throughputs for mission critical services.
Wi-Fi (829 only)	• Dual radio 802.11n concurrent 2.4 GHz and 5.0 GHz with embedded 2X3 MIMO • Up to 300 Mbps data rate per radio
Cisco IOx Application Support	Provides an open, extensible environment for hosting OS and applications at the network edge. Application Hosting on Guest Operation System.

Feature	Description
Security	Advanced security features that support: - Access control - Data confidentiality and data privacy - Threat detection and mitigation - Device and platform integrity
Cisco IOT Field Network Director	Available as the optional Cisco Industrial Operations Kit. This is a software platform that manages a multiservice network and security infrastructure for IoT applications such as transportation, smart grid, services, distribution automation and substation automation.
Cisco IOS Mobile IP Features	- Mobile IP offers transparent roaming for mobile networks, establishing a transparent Internet connection regardless of location or movement. This enables mission-critical applications to stay connected even when roaming between networks. - Assigned IP addresses to the home network are maintained in private or public networks.
Cisco IOS Mobile Network Features	Allows an entire subnet or mobile network to maintain connectivity to the home network while roaming.
QoS Features	- Provides traffic precedence to delay-sensitive or prioritized applications. - Facilitates low-latency routing of delay-sensitive industrial applications.
Management and Manageability	- Network managers can remotely manage and monitor networks with SNMP, Telnet, or HTTP/HTTPS/SSH, and locally through a console port. - Support for extensive 3G and 4G LTE-based MIBs allows for centralized management of remote devices and gives network managers visibility into and control over the network configuration at the remote site. - Network managers can reset to a predesignated golden image, as well as configure an 829 through Cisco IOS Software or through an external reset button. - Network managers can upgrade 3G, 3.5G, 3.7G, and 4G LTE firmware and router configurations remotely. The tight integration with Cisco IOS Software enables router to self-monitor the LTE WAN link and automatically recover from a radio link failure.
Cisco IOS Software Requirement	- Cisco IOS Software feature set: Universal Cisco IOS Software - Cisco IOS Software Release - 15.5(3)M, or later, and modem firmware - 5.5.58, or later. (several features require later IOS releases)

Hardware Differences Between IR809, IR829, and C819HG

The IR809s are very compact cellular (3G and 4G/LTE) industrial routers for remote deployment in various industries. They enable reliable and secure cellular connectivity for remote asset monitoring and machine-to-machine (M2M) solutions such as distribution automation, pipeline monitoring, and roadside infrastructure monitoring.

The IR829s are highly ruggedized compact cellular (3G and 4G LTE with GPS and dual SIM) and WLAN (2.4/5GHz) industrial routers supporting for scalable, reliable, and secure management of fleet vehicles and mass transit applications.

The 819HG-LTE-MNA-K9: Multimode Cisco LTE 2.0 for carriers that operate LTE 700 MHz (band 17), 1900 MHz (band 2 PCS), 850 MHz (band 5), 700 MHz (band 13), 1900 MHz (band 25 extended PCS) networks; or 1700/2100 MHz (band 4 AWS) networks; backward-compatible with UMTS and HSPA+: 850 MHz (band 5), 900 MHz (band 8), 1900 MHz (band 2 PCS), and 1700/2100 MHz (band 4 AWS), with EVDO Rev A/CDMA 1x BC0, BC1, BC10.

Hardware Comparison

Feature	IR809	IR829	C819HG
OIR of SIM	Yes	Yes	Yes
Guest OS Support	Yes	Yes	Yes
2G/3G/4G Support	Yes, dual SIM support, SKUs available per region See Cellular Interface Modules, on page 53 for additional information.		819(H)G-4G supports dual-SIM Different SKU's per region. SW MC 7750,7700,7710
USB Flash	Yes	Yes	No
USB type A Interface	Yes	Yes	No
Console Port	Mini USB	Mini USB	RJ-45
Alarm Port	One Alarm input on IR809	No	No
IEEE 802.11a/b/g/n WiFi	No	Yes, depending on the platform type.	No

Feature	IR809	IR829	C819HG
Power Requirements	Nominal voltage: 12-48V DC Min/max voltage: 9.6 – 60V DC input Max, Min current: 3A, 0.5A	Nominal voltage: 12V, 24V DC Min/max voltage: 9-32V DC input Max/Min current: 7.8 A, 2.8 A Maximum power consumption: 40 W (no PoE) and 70W (PoE)	Nominal voltage: 12V, 24V DC Min/max voltage: 10-36V DC Maximum power consumption: 26W
Ethernet Ports	2 x RJ45 10/100/1000Mbs	4 x RJ45 10/100/1000Mbs 1 x SFP 1000Mbs	4 x RJ45 10/100 Mbs 1 x GE 10/100/1000Mbs
Serial Ports	2 x RJ45 (1xRS-232 and 1xRS232/RS-485)		12 in 1 Smart Serial
Antenna: Main, Diversity and GPS	Yes	Yes	819(H)G-4G has Active GPS SMA Connector and option for 2 4G antennas

Antenna Recommendations

Neither the IR809 or IR829 is shipped with antennas. These antennas must be ordered separately. The IR829 must be installed with 2 antennas (Main & Aux) to guarantee the best performance level. Using a single antenna may impact the downlink performance by a minimum 3dB, and can be much greater (10-20dB) due to multipath fading (destructive interference between direct and reflected radio waves).

In case of 3G UMTS, a solo antenna would not be able to switch to the diversity port.

With the IR829, it must be guaranteed >15dB isolation between the WiFi and LTE antennas at all frequencies of 4G LTE and WiFi operation, for minimum impact to performance. This is ideally 20-25dB.

The Sierra Wireless MC73xx modem series supports MIMO on LTE. WCDMA UMTS HSPA DC-HSPA+ is diversity only, without MIMO.

Note Poorly installed MIMO antennas, such that the two (or more in case of 3x3, 4x4 MIMO) antennas have a strong correlation coefficient. This may cause the two streams to interfere with each other (otherwise known as lack of diversity), since the system has trouble separating the two. The multi-element antennas (5-in-1, 3-in-1, 2-in-1) have good diversity

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

Cisco Industrial Routers Antenna Guide:

http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/antennas/installing-combined/industrial-routers-antenna-guide.html

Cisco Aironet Antennas and Accessories Reference Guide

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

Features Supported in Different IOS Releases

The IR800 series was originally released with IOS software version 15.5(3)M. The following lists the software releases with the features added.

15.5(3)M (initial release)

- Software based Crypto

15.5(3)M*x*

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/IR8xx-Release-Notes.html

- Hardware based Crypto

15.6(1)T

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-1TIR8xx-Release-Notes.html

- IR809 Input alarm port, including SNMP Trap support
- SLIP & PPP serial encapsulation on serial interfaces
- Reset button behavior changed to match other 800 series
- IOX phase 2 CAF, 64 bits Linux, IR800-IOXVM image
- Guest OS Serial port access

15.6(2)T

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-2TIR8xx-Release-Notes.html

- Ignition power management on the IR829
- Performance improvements on IR800s

15.6(3)M

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M-Release-Notes.html

- Boot time reduction
- Copper SFP support on the IR829
- Serial Baud Rate configuration support
- USB EHCI emulation to GOS Support
- Memory allocation optimization between VDS, IOS and GOS

15.6(3)M0a

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M0a-Release-Notes.html

- Support added for the Sierra Wireless MC7430 series modems on the IR829.

15.6(3)M1

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M1-Release-Notes.html

- 4G LTE IPv6 Support
- Accelerometer and Gyroscope Support
- IOXVM Storage Partition Enhancement
- IOXVM Graceful Shutdown
- Sierra Wireless MC7430 modem support on the IR809.

15.6(3)M1b

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M1b-Release-Notes.html

- 4G LTE IPv6 Support
- Accelerometer and Gyroscope Support
- IOXVM Storage Partition Enhancement
- IOXVM Graceful Shutdown
- Support for New Modems and Dual Modems.

15.6(3)M2

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M2-Release-Notes.html

- 100Mbs SFP Support on the IR829
- Bridge Virtual Interface Support for IR800 Guest-OS
- New Features for LTE Modems
  - Assisted-GPS support on IR800 MC73xx modems
  - Multi-PDN support on IR800 MC73xx and MC74xx modems
  - 2000B MTU support on cellular interface for MC73xx modems

15.6(3)M3

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-6-3M3-Release-Notes.html

- Bug Fixes Only

15.7(3)M

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-7-3M-Release-Note.html

- IOx Radius authentication

- IOx IPv6 Networking Option
- Cellular Backoff

15.7(3)M1

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-7-3M1-Release-Note.html

- Guest OS persistent logging through reload
- Guest OS file system corruption detection and recovery
- Plug and Play Agent (PnP) support over 4G/Ethernet
- AutoSim and Firmware Based Switching
- Battery Back Up (BBU) Support

15.7(3)M2

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-7-3M2-Release-Note.html

- Virtual LPWA support for LoRaWAN
- IOS APIs to Enable Native IOx Applications
- Support for mSATA Module

15.8(3)M

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-8-3M-Release-Note.html

- Plug and Play (PnP) Support on the IR829 LAN Interfaces
- Auto-Negotiation Support for the IR829 Gigabit-Ethernet 0 Interface
- Ignition Undervoltage Threshold in Double Decimal
- Auto-recovery of Corrupt Filesystems
- Radio Frequency Band Select
- Modem Low Power Mode
- Enhancement to Modem Crash Action
- Displaying the Wear Leveling Data for the mSATA SSD on the IR829
- Improvements in IOS and Guest-OS Clock Time Synchronization

15.8(3)M1

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-8-3M1-Release-Note.html

- GPS NMEA Multiple Stream
- Display digital signature and software authenticity-related information for a specific image file from image header

- Client Information Signaling Protocol (CISP)
- Dot1x Supplicant Support on the L2 interface on the IR829
- LLDP (Link Layer Discovery Protocol) Support for 3rd party PoE devices on the IR829

15.8(3)M2

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-8-3M2-Release-Note.html

- IR809 and IR829: MIB support for Gyroscope and Accelerometer
- IR829M: MIB support for mSATA Wear Ratio and Usage
- IR809 and IR829: PNP Image Upgrade from FND

15.9(3)M

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-9-3M-Release-Note.html

- IR829 - MIB Support for Ignition Power Management
- IR829 - Ignition Off Timer Range Limitation
- IR829 - Ignition Undervoltage Setting

15.9(3)M1

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-9-3M1-Release-Note.html

- Guest-OS Kernel Migration

15.9(3)M2

https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/15-9-3M2-Release-Note.html

- AT&T FirstNet Support for the IR829
- No Service Password Recovery on the IR809 and IR829

Related Documentation

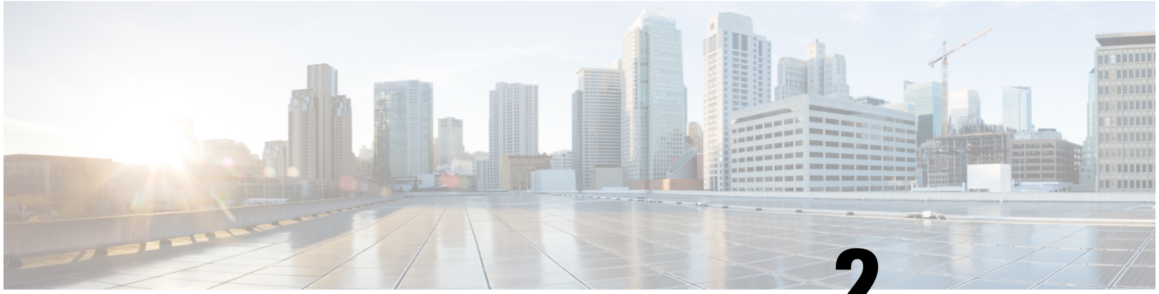
The following documentation is available:

- Cross-Platform Release Notes for Cisco IOS Release 15.9M:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-9m/release/notes/15-9-3-m-rel-notes.html

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

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



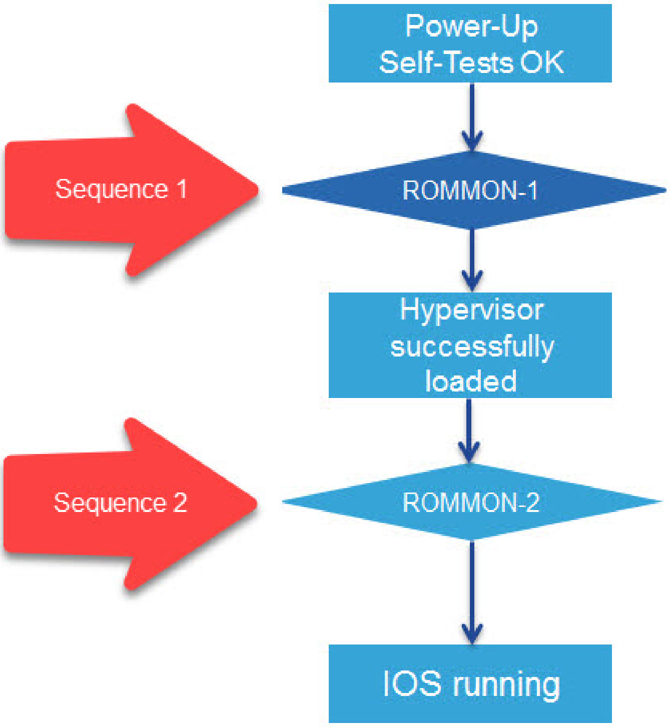
CHAPTER 2

Initial Configuration

This chapter provides instructions for initial configuration of the Cisco IR800 series Integrated Services Routers (ISRs). To create the initial configuration, the setup command facility prompts you for basic information about your router and network.

IR800 Bootstrap Sequence and Troubleshooting

The typical power up sequence on the IR800 is as follows:



These next sections describe actions that can be taken during the bootup.

Sequence 1

ROMMON 1 has a networking capability, so you can perform a tftp copy. You may also copy a file from USB to flash or bootstrap while in ROMMON 1.

Example from a tftp server:

```
rommon-1>
rommon-1> set ip 192.0.2.218 255.255.255.0
rommon-1> set gw 192.0.2.1
rommon-1> set
-------------------------- TABLE -------------------
CONSOLE_SPEED=9600
MAC_ADDRESS=00:00:00:00:00:00
LICENSE_SERIAL_NUMBER=FGL192423V4
LICENSE_PRODUCT_ID=IR829GW-LTE-LA-EK9
LICENSE_SUITE=
BOOT=
LICENSE_BOOT_LEVEL=securityk9,securityk9:ir800;datak9,datak9:ir800;
BOOT_STRING_IOS=ir800-uk9.br.sub
BOOT_IOS_SEQUENCE=0
BSI=0
RANDOM_NUM=877834120
RET_2_RTS=17:30:02 UTC Mon Jul 18 2016
RET_2_RCALTS=1468863103
SB_CORE_VER=F01047X15.01ada48ab2015-04-03
SB_ML_VER=MA0061R06.0404022015
```

```
SB_BOOT_SRC=upgrade
IP_ADDRESS=192.0.2.218
IP_MASK=255.255.255.0
IP_GW=192.0.2.1
-------------------------- END TABLE -------------------
rommon-1> ping 192.0.2.1
PING 192.0.2.1 (192.0.2.1): 56 data bytes
64 bytes from 192.0.2.1: seq=0 ttl=64 time=0.242 ms
64 bytes from 192.0.2.1: seq=1 ttl=64 time=0.276 ms
64 bytes from 192.0.2.1: seq=2 ttl=64 time=0.293 ms
64 bytes from 192.0.2.1: seq=3 ttl=64 time=0.279 ms
64 bytes from 192.0.2.1: seq=4 ttl=64 time=0.280 ms
--- 192.0.2.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.242/0.274/0.293 ms
rommon-1>
rommon-1> copy tftp://192.0.2.1/<directory>/ir800-universalk9-bundle.SSA.ipv6 flash:
Copying image ... p://192.0.2.1/<directory>
/ir800-universalk9-bundle.SSA.ipv6 flash:
rommon-1>
```

Example from USB to IOS flash:

```
rommon-1> dir
flash:
        30616 May 24 21:54 CyUSBSerialTestUtility
        16384 Jul  1 22:03 ORPHAN1
        16384 Jul  1 22:44 ORPHAN2
        16384 Jul  1 22:57 ORPHAN3
      7700480 Jun 24 00:20 apimage.tar
        16384 Jun 12  2015 eem
     67713096 Jun 29  2015 gemboa.V5.2.2.efi.SSA
     24448133 Jul  9 00:29 ir800-hv.srp.SPA.0.37.ipv6.a
     25140565 Apr 11 23:54 ir800-hv.srp.SPA.1.1.4
     25246549 May 24 21:43 ir800-hv.srp.SPA.1.1.7.gyro
     62404334 Jul 14 05:07 ir800-uk9.br.sub
     62399648 May 24 21:44 ir800-uk9.video1
    166676220 Jul  9 05:16 ir800-universalk9-bundle.SSA.ipv6
     62419759 Jun 23 22:47 ir800-universalk9-mz.SSA.156-2.10.13.GB
     62346125 Jul  9 05:49 ir800-universalk9-mz.SSA.156-20160709_012039
         9424 Jul  2 00:24 ir800_gyro_accel_ctrld
         3211 Jul  1 18:54 lll-1.6.11-ciscoms_config.cpkg
        16384 Jun 12  2015 managed
         2968 Jun  2 00:54 no_usb_emul
bootstrap:
     23750485 Oct  9  2015 ir800-hv.srp.SPA.0.29
usb:
     24448133 Jul  8 17:17 ir800-hv.srp.SPA.0.37.ipv6.a
     24447317 Jul  8 19:41 ir800-hv.srp.SPA.CCO.PI30
     62321081 Jul  8 19:42 ir800-uk9.CCO.PI30
     62346125 Jul  8 18:23 ir800-universalk9-mz.SSA
rommon-1> copy usb:ir800-universalk9-mz.SSA flash:
rommon-1> dir
flash:
        30616 May 24 21:54 CyUSBSerialTestUtility
        16384 Jul  1 22:03 ORPHAN1
        16384 Jul  1 22:44 ORPHAN2
        16384 Jul  1 22:57 ORPHAN3
      7700480 Jun 24 00:20 apimage.tar
        16384 Jun 12  2015 eem
     67713096 Jun 29  2015 gemboa.V5.2.2.efi.SSA
     24448133 Jul  9 00:29 ir800-hv.srp.SPA.0.37.ipv6.a
     25140565 Apr 11 23:54 ir800-hv.srp.SPA.1.1.4
     25246549 May 24 21:43 ir800-hv.srp.SPA.1.1.7.gyro
     62404334 Jul 14 05:07 ir800-uk9.br.sub
     62399648 May 24 21:44 ir800-uk9.video1
    166676220 Jul  9 05:16 ir800-universalk9-bundle.SSA.ipv6
     62346125 Jul 18 17:34 ir800-universalk9-mz.SSA
     62419759 Jun 23 22:47 ir800-universalk9-mz.SSA.156-2.10.13.GB
     62346125 Jul  9 05:49 ir800-universalk9-mz.SSA.156-20160709_012039
         9424 Jul  2 00:24 ir800_gyro_accel_ctrld
         3211 Jul  1 18:54 lll-1.6.11-ciscoms_config.cpkg
        16384 Jun 12  2015 managed
         2968 Jun  2 00:54 no_usb_emul
bootstrap:
     23750485 Oct  9  2015 ir800-hv.srp.SPA.0.29
usb:
     24448133 Jul  8 17:17 ir800-hv.srp.SPA.0.37.ipv6.a
     24447317 Jul  8 19:41 ir800-hv.srp.SPA.CCO.PI30
     62321081 Jul  8 19:42 ir800-uk9.CCO.PI30
     62346125 Jul  8 18:23 ir800-universalk9-mz.SSA
rommon-1>
```

Problems that may occur during ROMMON-1 are:

- Hypervisor was uninstalled, but not re-installed
- BOOT_HV variable missing

Resolution would be to **boot ir800-hv.srp.SPA.<version>**

Note USB memory stick or PEN drive can be used as storage at ROMMON-1, i.e. copying HPV and IOS files.

Sequence 2

Problems that may occur during ROMMON-2 are:

- IOS bundle was installed but “write mem” was not performed.
- BOOT or BOOT_STRING_IOS variables missing

Resolution would be to **boot flash:ir800-universalk9-mz.SPA.<version>**

Note USB can not be used as storage at ROMMON-2

Show the NVRAM status:

```
IR829# show platform nvram
....
---------------------------------------------
LICENSE_SERIAL_NUMBER=FGL194520W0
LICENSE_PRODUCT_ID=IR829GW-LTE-GA-EK9
BOOT_HV=bootstrap:ir800-hv.srp.SPA.0.37
BOOT=flash:ir800-universalk9-mz.SPA.156-2.T,12;
EULA_ACCEPTED=TRUE
```

```
RET_2_RTS=18:47:19 PST Wed Feb 24 2016
RANDOM_NUM=1610696746
LICENSE_SUITE=
LICENSE_BOOT_LEVEL=
BSI=0
RET_2_RCALTS=
BOOT_IOS_SEQUENCE=4
BOOT_STRING_IOS=flash:ir800-universalk9-mz.SPA.156-2.T
SB_CORE_VER=F01047X15.01ada48ab2015-04-03
SB_ML_VER=MA0061R06.0404022015
SB_BOOT_SRC=upgrade
```

In the NVRAM status shown above, the default BOOT_IOS_SEQUNCE value is 4. Starting with IOS version 15.7(3)M2, the value has increased to 20.

Setup Command Facility

The setup command facility guides you through the configuration process by prompting you for the specific information that is needed to configure your system. Use the setup command facility to configure a hostname for the router, to set passwords, and to configure an interface for communication with the management network.

To use the setup command facility, you must set up a console connection with the router and enter the privileged EXEC mode.

To configure the initial router settings by using the setup command facility, follow these steps:

Procedure

Step 1 Set up a console connection to your router, and enter privileged EXEC mode.

Step 2 In privileged EXEC mode, at the prompt, enter **setup**.

Example:

```
IR800# setup
```

The following message is displayed:

Example:

```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]:
```

You are now in the setup command facility.

The prompts in the setup command facility vary, depending on your router model, on the installed interface modules, and on the software image. The following steps and the user entries (in **bold**) are shown as examples only.

Note If you make a mistake while using the setup command facility, you can exit and run the setup command facility again. Press Ctrl-C and enter the setup command at the privileged EXEC mode prompt (Router#). To proceed using the setup command facility, enter **yes.**

Example:

```
Would you like to enter the initial configuration dialog? yes
```

Step 3 When the following messages appear, enter **yes** to enter basic management setup.

Example:

```
At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system
Would you like to enter basic management setup? [yes/no]: yes
```

Step 4 Enter a hostname for the router (this example uses Router).

Example:

```
Configuring global parameters:
Enter host name [Router]: Router
```

Step 5 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration.

Example:

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

Step 6 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration.

Example:

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

Step 7 Enter the virtual terminal password, which prevents unauthenticated access to the router through ports other than the console port.

Example:

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

Step 8 Respond to the following prompts as appropriate for your network:

Example:

```
Configure SNMP Network Management? [yes]:
    Community string [public]:
```

A summary of the available interfaces is displayed. The following is an example summary and may not reflect your configuration:

Example:

```
Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           10.1.0.165      YES DHCP   up                    up
GigabitEthernet1           unassigned      NO  unset  up                    up
Async0                     unassigned      YES unset  up                    down
Async1                     unassigned      YES unset  up                    down
GigabitEthernet2           unassigned      NO  unset  up                    up
Cellular0                  unassigned      NO  unset  down                  down
Cellular1                  unassigned      NO  unset  down                  down
```

Step 9 Choose one of the available interfaces for connecting the router to the management network.

Example:

```
Enter interface name used to connect to the
management network from the above interface summary: GigabitEthernet0
```

Step 10 Respond to the following prompts as appropriate for your network:

Example:

```
Configuring interface GigabitEthernet0:
 Configure IP on this interface? [yes]: yes
Use the 100 Base-TX (RJ-45) connector? [yes]: yes
Operate in full-duplex mode? [no]: yes
Configure IP on this interface? [yes]: yes
    IP address for this interface: 172.16.2.3
    Subnet mask for this interface [255.255.0.0] : 255.255.0.0
    Class B network is 172.16.0.0, 26 subnet bits; mask is /16
```

The configuration is displayed:

Example:

```
The following configuration command script was created:
hostname Router
enable secret 5 $1$D5P6$PYx41/lQIASK.HcSbfO5q1
enable password xxxxxx
line vty 0 4
password xxxxxx
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0
no shutdown
speed 100
duplex auto
ip address 172.16.2.3 255.255.0.0
!
```

Step 11 Respond to the following prompts. Enter 2 to save the initial configuration.

Example:

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

```
Use the enabled mode 'configure' command to modify this configuration.
Press RETURN to get started! RETURN
The user prompt is displayed.
Router>
```

Step 12 Verify the initial configuration. See the Verifying the Initial Configuration, on page 38 for verification procedures.

What to do next

After the initial configuration file is created, you can use the Cisco IOS CLI to perform additional configuration.

FirstNet Support

Feature Overview

For the FirstNet specified routers, the user is prompted to configure strong enable secret after factory default boot up, along with the below default security features:

- Telnet and HTTP - Disabled by Default
- SSH and HTTPS - Enabled by Default
    - To configure SSH, refer tohttps://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960x/software/15-0_2_EX/security/configuration_guide/b_sec_152ex_2960-x_cg/b_sec_152ex_2960-x_cg_chapter_01001.html#d43017e591a1635
    - To configure HTTPS, refer tohttps://www.cisco.com/c/en/us/td/docs/ios-xml/ios/https/configuration/15-mt/https-15-mt-book/nm-https-sc-ssl3.html#GUID-3501A644-E52A-40F4-A5D2-E7D4853B96B7
- Login delay and login block - Enabled by Default
- This feature is supported only in releases above 15.9(3)M2

Enabling Login Delay and Login Block

To enable the feature, refer to the following table.

Command or Action	Purpose
login delay *seconds* Example: `IR800>`**`login delay 3`**	When the user authentication fails in Telnet/SSH/HTTP, the next login prompt will appear to the user after a specified amount of time in seconds. The feature is enabled after factory default boot up. The default value is 3 seconds.

Command or Action	Purpose
login block-for *seconds* **attempts** *tries* **within** *seconds* Example: `IR800#login block-for 60 attempts 3 within 30`	When the user authentication fails in Telnet/SSH/HTTPS for a specific number of attempts within a period a time in seconds, then further connection attempts are refused for a particular amount of time. The feature is enabled after factory default boot up. The default behavior is when the user authentication fails in SSH/Telnet/HTTP for 3 attempts within 30 seconds, then the connection request to that service is blocked for 60 seconds.

Strong Enable Secret

When the router boots up in factory default mode, the user is prompted to configure a strong enable secret with below strength checks:

- Minimum length of 10 characters
- Have at least one lower case, one upper case and one numerical digit
- Should not contain the word cisco

If the user ignores the Initial configuration dialog box by entering NO, or presses CTRL+C at the dialog box to quit, the enable secret configuration is displayed until the user configures the strong enable secret.

Verifying the enable secret Prompt

```
         --- System Configuration Dialog ---

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

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

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

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:

  Enter host name [IR800]: IR800

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

  -------------------------------------------------
  secret should be of minimum 10 characters with
  at least 1 upper case, 1 lower case, 1 digit and
  should not contain [cisco]
  -------------------------------------------------
  Enter enable secret: ***********
  Confirm enable secret: ***********
  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.

  Enter enable password: <password>

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

  Enter virtual terminal password: <password>

  The iox hypervisor password is used to protect access to
  the VDS. This password will be ENCRYPTED.
  Enter VDS root password []:

Current interface summary

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES unset  administratively down down
GigabitEthernet1           unassigned      YES unset  down                  down
GigabitEthernet2           unassigned      YES unset  down                  down
GigabitEthernet3           unassigned      YES unset  down                  down
GigabitEthernet4           unassigned      YES unset  down                  down
Wlan-GigabitEthernet0      unassigned      YES unset  up                    up
Async0                     unassigned      YES unset  up                    down
Async1                     unassigned      YES unset  up                    down
GigabitEthernet5           unassigned      YES unset  administratively down down
Cellular0/0                unassigned      YES TFTP   down                  down

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

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

Verifying the Status of SSH

```
IR800#show ip ssh
SSH Enabled - version 2.0
Authentication methods:publickey,keyboard-interactive,password
```

Verifying the status of HTTPS

```
IR800#show ip http server status
HTTP secure server status: Enabled
HTTP secure server port: 443
```

Verifying the Initial Configuration

To verify that the new interfaces are operating correctly, perform the following tests:

- To verify that the interfaces and line protocol are in the correct state—up or down—enter the **show interfaces** command.

- To display a summary status of the interfaces configured for IP, enter the **show ip interface brief** command.

- To verify that you configured the correct hostname and password, enter the **show configuration** command.

After you complete and verify the initial configuration, you can configure your Cisco router for specific functions.

Note The QoS Input Service Policy can only be configured on the WAN interface, not on the SVI interface.

Note To ensure product security, even though the use of Hypervisor is not discussed in this guide, a proper password should be set. Only IOS priv15 users will be able to configure the password. The commands are shown as follows:

```
Router:(config)#iox hypervisor password ?
  0     Specifies an UNENCRYPTED password will follow
  7     Specifies a HIDDEN password will follow
  LINE  The UNENCRYPTED (cleartext) password
```

LEDs

The Cisco IR800 has LEDs that are discussed in the Hardware Configuration Guide for each model. There is also a command that will show you the status of the LEDs if you are not near the device. Use the show platform led command with options to view the different output.

Note The following examples are from the IR829. The IR809 differs slightly.

Single Modem

```
IR829#show platform led
LED STATUS:
==================================================
GE PORTS :  GE0      GE1      GE2      GE3      GE4
LINK LED :  OFF      GREEN    OFF      GREEN    GREEN
==================================================
PoE LED   : OFF
Cellular PORTS: Cellular0
RSSI LED 1  : Green
RSSI LED 2  : Green
RSSI LED 3  : Off
GPS LED     : Off
SIM0 LED    : Green
SIM1 LED    : Off
==================================================
VPN LED   : OFF
System LED: green, on
IR829#
IR829#show platform led summary
Ports  LINK/ENABLE
-------+---------------
GE0     OFF
GE1     GREEN
GE2     OFF
GE3     GREEN
```

```
GE4     GREEN
-------+---------------
PoE LED   : OFF
         RSSI 1        RSSI 2       RSSI 3        GPS
-----+------------+------------+------------+-------------
Ce0      Green         Green        Off           Off
-----+------------+------------+------------+-------------
Cellular   SIM0   SIM1
--------+-------+-------
Ce0        Green  Off
--------+-------+-------
VPN LED   : OFF
System LED: green, on
IR829#
IR829#show platform led system
System LED: green, on
Summary of the LED status providers:
            Client                Type     Status
------------------------------  --------  --------
GigabitEthernet0                critical  OK
GigabitEthernet1                critical  OK
GigabitEthernet3                critical  OK
GigabitEthernet4                critical  OK
Cellular0                       critical  OK
--------------------------------------------------
```

Dual Modem

```
IR829#show platform led
LED STATUS:
==================================================
GE PORTS :  GE0      GE1      GE2      GE3      GE4
LINK LED :  OFF      OFF      OFF      OFF      OFF
==================================================
PoE LED   : GREEN
Cellular PORTS: Cellular0/0
RSSI LED 1  : Green
RSSI LED 2  : Off
RSSI LED 3  : Off
GPS LED     : Off
SIM LED     : Off
==================================================
Cellular PORTS: Cellular1/0
RSSI LED 1  : Green
RSSI LED 2  : Green
RSSI LED 3  : Off
GPS LED     : Unknown
SIM LED     : Off
==================================================
VPN LED     : OFF
System LED: amber, blinking
IR829#show platform led
LED STATUS:
==================================================
GE PORTS :  GE0      GE1      GE2      GE3      GE4
LINK LED :  OFF      OFF      OFF      OFF      OFF
==================================================
PoE LED   : GREEN
Cellular PORTS: Cellular0/0
RSSI LED 1  : Green
RSSI LED 2  : Off
RSSI LED 3  : Off
GPS LED     : Off
```

```
SIM LED     : Off
==================================================
Cellular PORTS: Cellular1/0
RSSI LED 1  : Green
RSSI LED 2  : Green
RSSI LED 3  : Off
GPS LED     : Unknown
SIM LED     : Off
==================================================
VPN LED   : OFF
System LED: amber, blinking
IR829#show platform led summary
Ports  LINK/ENABLE
-----+-----------------
GE0     OFF
GE1     OFF
GE2     OFF
GE3     OFF
GE4     OFF
-----+-----------------
PoE LED   : GREEN
        RSSI 1        RSSI 2       RSSI 3         GPS
-----+------------+------------+------------+-------------
Ce0/0   Green         Off          Off            Off
-----+------------+------------+------------+-------------
Cellular   SIM0   SIM1
--------+-------+-------
Ce0/0       Off      Off
--------+-------+-------
VPN LED   : OFF
System LED: amber, blinking
IR829#
IR829#show platform led system
System LED: amber, blinking
Summary of the LED status providers:
            Client                Type     Status
------------------------------  --------  --------
GigabitEthernet0                critical  OK
GigabitEthernet1                critical  failed
GigabitEthernet2                critical  failed
GigabitEthernet3                critical  failed
GigabitEthernet4                critical  failed
Cellular0/0                     critical  OK
Cellular1/0                     critical  OK
--------------------------------------------------
```

The system LED is physically labeled SYS on IR809 and PWR on IR829. However, the software logic for the system LED status works in the same way for both IR809 and IR829.

Note By definition, amber blinking means the system has an error, but has network connectivity. For most of the time, this amber blinking condition is seen because one or more of the Ethernet ports on your IR829 is in administrative un-shut state, but there’s no actual link (e.g. cable disconnected or peer port is down etc.)

To make the status show solid green, ensure that the link on each administrative un-shut port connects a device that is up, or you can put all disconnected ports in administrative shut state.

```
IR800#show platform led system
```

```
System LED: amber, blinking
Summary of the LED status providers:
            Client                Type     Status
------------------------------  --------  --------
GigabitEthernet5                critical  OK
```

Unconnected ports in an un-shut state

```
IR800#sh platform led system

System LED: amber, blinking
Summary of the LED status providers:
            Client                Type     Status
------------------------------  --------  --------
GigabitEthernet5                critical  OK
GigabitEthernet0                critical  OK
GigabitEthernet1                critical  OK
GigabitEthernet2                critical  failed
GigabitEthernet3                critical  failed
GigabitEthernet4                critical  failed
```

Un-connected ports in “shutdown” state

```
(config)#int range gigabitEthernet 2-4
(config-if-range)#shut
IR800#sh platform led system

System LED: green, on
Summary of the LED status providers:
            Client                Type     Status
------------------------------  --------  --------
GigabitEthernet5                critical  OK
GigabitEthernet0                critical  OK
GigabitEthernet1                critical  OK
```

Note There may be a lag time between the LED indication on the router and what the show led commands return.

Software Bundle Installation

The Cisco IR800 ships with the latest software available with the configuration that was ordered. There should be no reason to have to upgrade unless a failure occurs, or you wish to install a new bundle to benefit from new features. Should the need arise, the following steps will assist in performing a bundle installation.

Note The bundle install will fail if “ip ssh source-interface” is configured. Make sure that none of the interfaces have ssh running on them before performing the installation.

```
IR829#show run | inc ip ssh source
ip ssh source-interface GigabitEthernet0
IR829#
```

Displaing Digital Signature and Software Authenticity

Feature is new for release 15.8(3)M1 and applies to the IR8x9

Updates have been made to CLI commands due to unsupported file format errors:

- show software authenticity file *<IOS image/SRP image/bundle image/GOS image>*
- verify *<IOS image/SRP image/bundle image/GOS image>*

These commands would return the error:

```
IR800#show software authenticity file flash:ir800-universalk9-mz.SSA
%Error processing flash:ir800-universalk9-mz.SSA: Unsupported file format
```

With this feature enhancement, users will now be able to run these CLIs to display and verify digital signature and software authenticity information for these types of signed files present in flash: partition only (IOS image, Hypervisor image, bundle image and Guest-OS image) supported on the IR8x9

show software authenticity file command

Command Syntax:

show software authenticity file flash:*<bundle image>* | *<ios image>* | *<srp image>* | *<gos image>*

Description:

Displays digital signature and software authenticity-related information for a specific image file from image header.

Field	Description
File Name	Name of the file
Image Type	States the type of image
Signer Information	
Common Name	CiscoSystems
Organizational Unit	Gemini-Balboa
Organizational Name	CiscoSystems
Certificate Serial Number	Number assigned to the certificate
Hash Algorithm	Type of algorithm used for hashing
Signature Algorithm	Type of algorithm used to sign this image
Key Version	The version of the key used to generate the signature

For additional information on this command, please see:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/command/cf_command_ref/show_protocols_through_showmon.html#wp9122926510

Expected output example:

```
Router# show software authenticity file ?

  flash:           Image to be authenticated
 nvram:         Image to be authenticated
Router#show software authenticity file flash: ir800-universalk9-mz.SSA
File Name                      :flash:ir800-universalk9-mz.SSA
Image type                     :Special
Signer Information
Common Name                    :CiscoSystems
Organization Unit              :Gemini-Balboa
Organization Name              :CiscoSystems
Certificate Serial Number      :563ACCAA
Hash Algorithm                 :SHA512
Signature Algorithm            :2048-bit RSA
Key Version                    :A
```

Note: It may take several minutes for the command to perform the image authentication.

verify command

Syntax:

verify flash:*<bundle image>* | *<ios image>* | *<srp image>* | *<gos image>*

Description:

Verify the digital signature for specific image.

Expected output example:

```
Router#verify ?
  /md5           Compute an md5 signature for a file
  flash:         File to be verified
 nvram:         File to be verified
Router#verify flash:ir800-universalk9-mz.SSA
Starting image verification
Hash Computation:    100%Done!
Computed Hash   SHA2: e89c7108ea9fdac90ea6eb4a28ed4d87
                      D5d61a30cb29a4d1b33a2ec49a0e8f73
                      653e1c4add30e8f8659214c6befcede0
                      4339366eff3018baeb811971303d9fd9

Embedded Hash   SHA2: e89c7108ea9fdac90ea6eb4a28ed4d87
                      D5d61a30cb29a4d1b33a2ec49a0e8f73
                      653e1c4add30e8f8659214c6befcede0
                      4339366eff3018baeb811971303d9fd9
CCO Hash             MD5: BAE76E54A55E42B5E68531A5FA39ADF0
Digital signature successfully verified in file flash:ir800-universalk9-mz.SSA
```

Bundle Installation Steps

Overview:

1. Download the bundle to flash memory from a TFTP server.

2. Install the bundle from the Command Line Interface.
3. Save the configuration, and reload the router to use the new image.
4. Download the 4G firmware upgrade.

Example:

Procedure

Step 1 Copy the bundle from a TFTP server to your router.

Example:

```
IR800#copy tftp flash

Address or name of remote host [192.168.254.254]? your ip address here
Source filename [path to file/ir800-universalk9-bundle.SSA.156-2.10.62.GB]? <enter>
Destination filename [ir800-universalk9-bundle.SSA.156-2.10.62.GB]? <enter>
Accessing tftp://192.168.254.254/tachen/ir800-universalk9-bundle.SSA.156-2.10.62.GB...
Loading tachen/ir800-universalk9-bundle.SSA.156-2.10.62.GB from 192.168.254.254 (via Vlan1):
 !
*Jun 25 18:28:45.685: %ARP-4-NULL_SRC_MAC: NULL MAC address from 172.16.0.1 on
wl0!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 161162048 bytes]
161162048 bytes copied in 466.054 secs (345801 bytes/sec)
```

Step 2 The bundle download is complete, and now needs to be installed. Perform the *bundle install flash: < bundle iOS image name>* command.

Note The Bundle and Hypervisor installation will fail if SSH is not properly configured.

Example:

```
IR800#bundle install flash:ir800-universalk9-bundle.SSA.156-2.10.62.GB
Installing bundle image:
/ir800-universalk9-bundle.SSA.156-2.10.62.GB..............................................
updating Hypervisor image...
Sending file modes: C0444 25160429 ir800-hv.srp.SPA.2.6.9
    SRP md5 verification passed!
updating IOS image...
Sending file modes: C0644 63827874 ir800-universalk9-mz.SSA.156-2.10.62.GB
    IOS md5 verification passed!
Done!
IR800#
*Nov 16 18:54:39.456: %SYS-5-CONFIG_I: Configured from console by bundle install command
*Nov 16 18:54:39.456: %IR800_INSTALL-6-SUCCESS_BUNDLE_INSTALL: Successfully installed bundle
 image.
```

Step 3 Once the bundle installation has completed, verify with the **show platform bundle installed** command.

Step 4 (Optional) View which version of Hypervisor you are running.

Example:

```
IR800# show platform hypervisor
version: 2.5.5.2
```

Step 5 Verify the boot system parameter before reloading the router.

Step 6 Save the configuration and reload the router.

Example:

```
IR800#reload
Do you want to reload the internal AP ? [yes/no]: yes
System configuration has been modified. Save? [yes/no]: yes
Building configuration...
  [OK]
Proceed with reload? [confirm] <enter>
*Jun 25 19:03:13.685: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
```

Step 7 Download the 4G firmware or AP image. Instructions for uploading firmware are located here:

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

Search for “Upgrading the Modem Firmware”.

Additional Software Bundle Installation Options

The bundle install command has additional options.

Command Option	Description
exclude	Used to one of the components of the bundle. Example: Install only hypervisor and IOS from the bundle. IR800#bundle install flash:bundle_image exclude GOS
delete	Used to automatically delete the bundle and free up flash: memory after installation is complete.
rom-autoboot	Used to save autoboot information in rommon. This configuration was exclusively introduced for PnP feature. Setting this will ensure that even if there is 'no boot system', the router will bootup with IOS image available in the flash: file system. The IOS image picked will be the one that matches with the bundle, not the first or any random IOS image in the flash: file system. If a 'write erase' command is executed followed by reload, the router will boot back into an IOS prompt, and not be stuck at rommon2.

The following items are important to remember when using bundle install:

- The default bundle install flash: ensures that the boot system flash: is set each time. The default will bootup all three images - hypervisor, native IOS and guest-os alike.
- Software mix-and-match between the three images is not supported. The router can only be fully functional if all three images are from the same bundle.
- Cellular modem firmware upgrade is not inclusive in a bundle installation.

- In IOS mode, verify show platform nvram does not have BOOT_MCU_FW_UPGRADE=NEVER and BOOT_FPGA_FW_UPGRADE=NEVER.
- After a bundle installation, it is mandatory the router be reloaded. Prior to a reload, most operations will be non-functional.

Power Over Ethernet (PoE)

The IR829 has an optional PoE accessory (IR800-IL-POE). When installed, it supplies a maximum of 30.8W shared between the 4 GE LAN ports (GI1-GI4). The Power can be distributed among the ports in the following manner:

- If one port supports PoE+ (30W), then the other ports have no PoE.
- If 2 ports support PoE (15.4 W), then the other ports have no PoE.
- All 4 ports can support 7.7 W per port.

Note The router cannot be upgraded for PoE in the field.

IOS supports bi-directional inline power negotiations with Cisco devices through the use of CDP. Cisco Power Devices (PDs) may signal increase or decrease in their demand for power through CDP. Decrease in demand will result in returning unused power to the pool of available power. Increase in demand will be accommodated, subject to the available unused power and the port power limit (and 802.3at classification where applicable). If the PDs do not support CDP, the inline power allocation is based on the classification if they are 802.3at devices or 15.4W if not 802.3at compliant.

Command Examples

```
IR829(config)#interface gi2
IR829(config-if)#power inline ?
  auto   Automatically detect and power inline devices
  never  Never apply inline power
  port   Configure Port Power Level
IR829(config-if)#power inline port ?
  max  Maximum power configured on this interface
IR829(config-if)#power inline port max ?
  <4000-30800>  milli-watts
IR829#show power inline

PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
EXT-PS           0        30.800    30.000          PS GOOD
Interface   Config   Device   Powered    PowerAllocated   State
---------   ------   ------   -------    --------------   -----
Gi1         auto     IEEE-4   On        30.000 Watts      PHONE
Gi2         auto     Unknown  Off        0.000 Watts      UNKNOWN
Gi3         auto     Unknown  Off        0.000 Watts      UNKNOWN
Gi4         never    Unknown  Off        0.000 Watts      NO_POWER
```

LLDP (Link Layer Discovery Protocol) Support for 3rd party PoE devices

This feature applies to the IR829 only.

Previously, the IR829 supported PoE allocation/negotiation only for the PD (Powered Devices) which communicate using CDP (Cisco Discovery Protocol). With this release, support is added for Link Layer Discovery Protocol.

LLDP is a vendor-neutral CDP like neighbor discovery protocol that is used by network devices to advertise information about themselves to other devices on the network. LLDP supports a set of attributes that it uses to discover neighbor devices. These attributes contain type, length, and value descriptions and are referred to as TLVs. LLDP supported devices can use TLVs to receive and send information to their neighbors.

Details such as configuration information, device capabilities, and device identity can be advertised using this protocol. LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones and network devices such as switches. LLDP-MED specifically provides support for voice over IP (VoIP) applications and provides additional TLVs for capabilities discovery, network policy, power over Ethernet (PoE), inventory management, and location information. LLDP-MED contains power management TLV which allows PD (power device) to request power. Power TLV defines the format for power request.

Once power is applied to the port, LLDP-MED (Power TLV) is used to determine the actual power requirement of PDs and the system power budget is adjusted accordingly. The router processes the request and either grants or denies power based on the current power budget. If the request is granted, then the router simply updates the power budget. If the request is denied, the router turns OFF power to the port, generates a syslog message, and updates the power budget and LEDs.

If LLDP-MED is disabled or if the PD does not support the LLDP-MED power TLV, then the initial allocation value is used throughout the duration of the connection. No new CLIs are added and the following commands can be used to troubleshoot.

show power inline *interface [detail]*

Used in exec mode, this command show sinline power settings and status per interface or all respectively.

```
IR800>show power inline

PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
EXT-PS           0        30.800    14.389          PS GOOD
Interface   Config   Device   Powered    PowerAllocated   State
---------   ------   ------   -------    --------------   -----
Gi1         auto     Unknown  Off         0.000 Watts      NOT_PHONE
Gi2         auto     Unknown  Off         0.000 Watts      UNKNOWN
Gi3         auto     IEEE-4   On         14.389 Watts      PHONE
Gi4         auto     Unknown  Off         0.000 Watts      UNKNOWN
```

[no] lldp tlv-select power-management

Used in interface config mode, this command configures inline power support and optionally specifies a maximum inline power level in milliwatts.

```
IR800(config-if)#power inline auto

IR800(config-if)#power inline never

IR800(config-if)#power inline port max 30000
```

show lldp *{entry | interface | neighbors | traffic}*

Used in exec mode, this command shows information for LLDP running status, specific neighbor entry, interface status and configuration, neighbor entries, and statistics.

```
IR800# show lldp entry *

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Total entries displayed: 0
Switch#show lldp entry *

Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
------------------------------------------------
Chassis id: 192.168.1.11
Port id: 002584184414:P1
Port Description: SW PORT
System Name: SEP002584184414.DMSBU.com
System Description:
Cisco IP Phone 9971, V1, sip9971.9-3-0RT1-100dev

Time remaining: 154 seconds
System Capabilities: B,T
Enabled Capabilities: B,T
Management Addresses:
    IP: 192.168.1.11
Auto Negotiation - supported, enabled
Physical media capabilities:
    1000baseT(HD)
    1000baseX(FD)
    Symm, Asym Pause(FD)
    Symm Pause(FD)
    Other/unknown
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

    MED Codes:
          (NP) Network Policy, (LI) Location Identification
          (PS) Power Source Entity, (PD) Power Device
          (IN) Inventory

    H/W revision: 1
    F/W revision: sboot9971.031610R1-9-3-0RT1-100d
    S/W revision: sip9971.9-3-0RT1-100dev
    Serial number: FCH1321927B
    Manufacturer: Cisco Systems, Inc.
    Model: CP-9971
    Capabilities: NP, PD, IN
    Device type: Endpoint Class III
    Network Policy(Voice): VLAN data, untagged, Layer-2 priority: 5, DSCP: 46
    Network Policy(Voice Signal): VLAN data, untagged, Layer-2 priority: 4, DSCP: 32
    PD device, Power source: PSE, Power Priority: High, Wattage: 10.6
    Location - not advertised


Total entries displayed: 1
```

Note: PoE port power priority (Critical, High, Low, default) and Power policing are not supported.

Serial Port Configuration

Before you begin

Serial Port configuration on the IR800 series depends on having proper cabling to start with. Before you configure the serial port of the IR809 or IR829, make sure to read the serial port section of the IR829 Hardware Installation Guide:https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/hardware/install/guide/829hwinst/pview.html#85723

Note The serial port can be used either by IOS, or through an IOx application.

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

interface async ?

To configure the serial port:

Procedure

Perform the steps in the following example.

Example

```
IR800#sh run int async 0
Building configuration...

Current configuration : 62 bytes
!
interface Async0
 no ip address
 encapsulation raw-tcp
end
```

Configuring Accelerometer and Gyroscope

Ensure that your router is running IOS version 15.6(3)M1 or above.

Accelerometer and Gyroscope functionality tracks the speed and angular movement of the device.Two configuration CLIs and one show CLI are available:

```
IR829(config)#[no] gyroscope-reading enable
```

Once this is enabled, gyroscope reading will start by the frequency currently set. Prior to IOS release 15.7(3)M1, the format of the command was:

```
IR829 (config)#gyroscope-reading frequency ?
1/min Reading 1 times per minute
1/sec Reading 1 time per second
10/min Reading 10 times per minute
```

From IOS release 15.7(3)M1 going forward, the format has been modified to:

```
IR829 (config)#gyroscope-reading frequency ?
one/min Reading 1 times per minute
one/sec Reading 1 time per second (default value)
ten/min Reading 10 times per minute
```

Note After upgrading to IOS release 15.7(3)M1, the router will have to be reconfigured.

Default frequency is 1/sec. If this is configured, it would overwrite default frequency and any later reading would be according to the newly set frequency.

```
IR829 #show platform gyroscope-data
Starting Entry = 0, next_entry = 1003, start time = , wrap_around = 0
Date Time G-X G-Y G-Z XL-X XL-Y XL-Z
2016:09:19 18:23:09.26 -1636.25 -367.50 1400.00 -5.795 16.470 1026.203
2016:09:19 18:24:09.23 -2073.75 -481.25 1382.50 -10.309 24.705 1016.504
2016:09:19 18:25:09.28 2152.50 -253.75 1496.25 -7.564 27.267 1016.443
2016:09:19 18:26:08.83 402.50 -647.50 1295.00 -8.113 43.493 1030.046
2016:09:19 18:27:08.90 -1706.25 -1058.75 1295.00 -6.771 41.724 1017.419
2016:09:19 18:28:08.85 253.75 -498.75 1452.50 -4.819 31.110 1030.168
```

This CLI would only show data if "gyroscope-reading" is enabled. All readings since start (unless wrap-around occurs, which means table is full), would be shown in the order from the most recent to the oldest.

Each entry shows G-X, Y, Z(3D gyroscope data) in mdps (Milli Degrees Per Second) and XL-X,Y, Z (3D accelerator data) in unit mg (milli g forces) where g is ≈ 9.81 m/s 2 .

Note Configurations would be in running-config and would stay over reload if saved.

A new MIB/OID is available to support the following SNMP operations:

- SNMPwalk: snmpwalk is used to fetch all values of a sub tree under the MIB table or value of particular OID.
- SNMPget: snmpget is used to fetch the value of a particular OID.

The entity OID value is iso.3.6.1.4.1.9.12.3.1.8.230.

The **show platform gyroscope** command gives information about this MIB.

Auto-Negotiation Support for Gigabit-Ethernet 0 on the IR829

The IR829 product series (with a 1000Base-T SFP) only supported a fixed speed of 1000Mbps. To enable multiple speed support Cisco introduced auto-negotiation as the default speed on Gigabit-Ethernet 0.

It is highly recommended to use auto-negotiation on both sides of the network for best performance results. Once auto-negotiation is initiated, the device (PHY) determines whether or not the remote device has auto-negotiation capability. If so, the device and the remote device negotiate the speed and duplex with which to operate. If the remote device does not have auto-negotiation capability, the device uses the parallel detect function to determine the speed of the remote device for 100BASE-TX and 10BASE T modes. If the link is established based on the parallel detect function, then it is required to establish the link at half duplex mode only. Refer to IEEE 802.3 clauses 28 and 40 for a full description of auto-negotiation.

Note: Auto-Negotiation is enabled by default. There is no CLI configuration.

Where To Go From Here

There are a wide variety of configuration options available on the Cisco IR800. This guide provides information on the most common options. Use the following resources for additional information:

Cisco 800 Series Industrial Integrated Services Routers

Cisco Firmware Upgrade Guide for Cellular Modems

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

Cisco 4G LTE Software Installation Guide

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

Cisco 3G and 4G Serviceability Enhancement User Guide

http://www.cisco.com/c/en/us/td/docs/routers/access/800/819/user/guide/3G4G-enhancements-userguide.html

CHAPTER 3

Cellular Interface Modules

This chapter provides configuration details for the cellular interface modules used in the IR800 series routers.

It is important to understand the architecture of the IR800 series and the relationship between Modems, SIMs, Interface and Controller. The following table helps to illustrate these relationships.

Router	Controller	SIM	Modem Slot	PDN Interface	Line
IR829	0	0|1	0	Cellular 0	3
IR829	0	0|1	0	Cellular 1	8
IR829 (dual modem) *	0	0	0	Cellular 0/0	3
IR829 (dual modem) *	0	0	0	Cellular 0/1	8
IR829 (dual modem) *	1	1	1	Cellular 1/0	9
IR829 (dual modem) *	1	1	1	Cellular 1/1	15
IR809	0	0|1	0	Cellular 0	3
IR809	0	0|1	0	Cellular 1	8

Note Check the Product Marketing Data Sheet for updated modem information.

With the introduction of the next generation SKUs, some functionality has changed. Refer to the following table for details.

Description	IR829GW-[LA/GA/NA/VZ]-*K9	IR829-2LTE-EA-*K9
North American	Yes	Yes
APJC	Yes	No

Description	IR829GW-[LA/GA/NA/VZ]-*K9	IR829-2LTE-EA-*K9
EMER	Yes	Yes
EMEA	Yes	Yes
2G Support	Yes	No
3G Support	Yes	Yes
LTE Support	Yes	Yes
GPS	Yes	Yes **Note** Only available from the first LTE Modem.
Wi-Fi (2.4/5 GHZ)	2.4 GHz and 5GHz use separate antenna connector	2.4 GHz + 5GHz coexist on the same antenna connector
Dual SIM	Yes	No
Band 30	No	No
LTE category supported	cat4	cat4

This chapter contains the following sections:

Cellular Interface

The Cisco IR800 series Industrial routers use the Sierra Wireless MC73XX and MC74XX series modems supporting MIMO on LTE. WCDMA UMTS HSPA DC-HSPA+ is diversity only, without MIMO.

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

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

The software download page can be found here:

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

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

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

Cisco 4G LTE Software Installation Guide http://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/software/feature/guide/EHWIC-4G-LTESW.html

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

4G LTE Dual SIM

Dual Subscriber Identity Module (SIM) provides reliability and multihoming capabilities over LTE and HSPA-based networks. With two LTE modems, the IR829 enables concurrent connectivity to two cellular networks for high reliability, enhanced data throughputs, load balancing and differentiated services.

Note Dual SIM active/backup mode is supported only on single LTE models of the IR829.

The following features are provided:

- The two SIMs operate in active/backup mode on the single LTE models of the IR829, and active/active mode with each of the two SIMs assigned to a specific cellular radio on the dual LTE models. Both mobile provider networks must be supported by the given IR829 SKU, and it must be in an applicable region.
- By default, SIM slot 0 is the primary, and SIM slot1 is the backup. Behavior may be changed using the **lte sim primary** command.
- Profiles for each SIM are assigned by using the **lte sim profile** command. Each SIM has an associated Internet profile and an IMS profile in the CLI.
- Dual-SIM behavior is managed under Cellular 0 CLI configuration.
- The fail over occurs when there is no signal from the current carrier, and generally happens depending on the fail over timer value that is set. The default value is 5 minutes. The range is from 0-7 minutes..
- Dual active LTE radios providing Multi-carrier support for active and backup use cases. Newer cellular modems have been added (MC74xx) with FDD/TDD LTE on LA and EA 829 models.

Note The 7455 modems do not support dual SIM capabilities.

AutoSim and Firmware Based Switching

The advantages of the AutoSim feature are:

- Ease of Ordering Carrier Specific SKUs
- Quicker failover times in dual-sim deployments
- Ease of switchover from other service providers to Telstra network

Auto-SIM is supported in Sierra wireless firmware Version 02.20.03. A new CLI is added in the cellular controller to enable/disable Auto-SIM. The modem in Auto-SIM mode selects the right carrier firmware after a SIM slot switch and an automatic modem reset. Auto-SIM is supported on the MC7455, MC7430, EM7430, and EM7455 modems. During bootup, if the Auto-SIM configuration on the modem doesn't match to the IOS configuration, the corresponding Auto-SIM or manual mode is pushed to the modem.

After an Auto-SIM configuration change, the modem is automatically reset; the default is "auto-sim" enabled.

Enable Auto-SIM:

```
router(config)#controller cellular <slot>
router(config-controller)#lte firmware auto-sim  #default is auto-sim enabled
```

Note After enabling auto-sim, wait for 5 minutes until the radio comes up. Once the radio is up, issue a modem power-cycle and wait for 3 minutes for the radio to come up again. Modem Power-Cycle is mandatory for auto-sim configuration to take effect.

Disable Auto-SIM:

```
router(config)#controller cellular <slot>
router(config-controller)#no lte firmware auto-sim
```

Note After disabling auto-sim, wait for 5 minutes until the radio comes up. Once the radio is up, issue a modem power-cycle and wait for 3 minutes for the radio to come up again. Modem Power-Cycle is mandatory for auto-sim configuration to take effect.

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

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

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

```
router#show cellular <slot> firmware
```

For additional information, see the following guide:https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/NIM/software/configuration/guide/4GLTENIM_SW.html

Dual Radio Configuration and Single Radio Configuration

The following examples are of an IR800 cellular configuration using dual modems. A single modem example will look much the same, without the *Cellular1/0* and *Cellular1/1* entries.

```
DUAL-Modem> enable
DUAL-Modem# show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0           unassigned      YES NVRAM  administratively down down
GigabitEthernet1           unassigned      YES unset  down                  down
GigabitEthernet2           unassigned      YES unset  down                  down
GigabitEthernet3           unassigned      YES unset  down                  down
GigabitEthernet4           unassigned      YES unset  down                  down
Wlan-GigabitEthernet0      unassigned      YES unset  up                    up
Async0                     unassigned      YES unset  up                    down
Async1                     unassigned      YES unset  up                    down
GigabitEthernet5           unassigned      YES NVRAM  administratively down down
Cellular0/0                192.168.43.237  YES IPCP   up                    up
Cellular1/0                10.61.25.231    YES IPCP   up                    up
Second Modem
Cellular0/1                unassigned      YES TFTP   down                  down
```

```
Cellular1/1                unassigned      YES TFTP   down                  down
Second Modem
Vlan1                      unassigned      YES unset  up                    up
wlan-ap0                   unassigned      YES NVRAM  up                    up
DUAL-Modem# show running-config

Building configuration...
Current configuration : 4021 bytes
!
! Last configuration change at 18:31:06 UTC Mon Oct 24 2016
!
version 15.6
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
!
hostname DUAL-Modem
!
boot-start-marker
boot system flash:/ir800-universalk9-mz.SPA.156-3.M0a
boot-end-marker
!
no aaa new-model
ethernet lmi ce
service-module wlan-ap 0 bootimage autonomous
!
ignition off-timer 900
!
ignition undervoltage threshold 9
!
no ignition enable
!
no ip domain lookup
ip inspect WAAS flush-timeout 10
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
chat-script lte "" "AT!CALL" TIMEOUT 20 "OK"
!
license udi pid IR829-2LTE-EA-BK9 sn FGL2032219N
!
redundancy
notification-timer 120000
controller Cellular 0
lte sim data-profile 3 attach-profile 1

    #When using Verizon, use data profile 3 and attach to profile 1
    #When using AT&T, use data profile 1 and attach to profile 1

lte modem link-recovery rssi onset-threshold -110
lte modem link-recovery monitor-timer 20
lte modem link-recovery wait-timer 10
lte modem link-recovery debounce-count 6
!
controller Cellular 1
lte modem link-recovery rssi onset-threshold -110
lte modem link-recovery monitor-timer 20
lte modem link-recovery wait-timer 10
lte modem link-recovery debounce-count 6
interface GigabitEthernet0
no ip address
```

```
shutdown
!
interface GigabitEthernet1
no ip address
!
interface GigabitEthernet2
no ip address
!
interface GigabitEthernet3
no ip address
!
interface GigabitEthernet4
no ip address
!
interface Wlan-GigabitEthernet0
no ip address
!
interface GigabitEthernet5
no ip address
shutdown
duplex auto
speed auto
!
interface Cellular0/0
  #Both interfaces need to be configured in the IOS software

ip address negotiated
ip virtual-reassembly in
encapsulation slip
load-interval 30
dialer in-band
dialer string lte
dialer-group 1
no peer default ip address
async mode interactive
routing dynamic
!
interface Cellular1/0
  #Both interfaces need to be configured in the IOS software
ip address negotiated
ip virtual-reassembly in
encapsulation slip
load-interval 30
dialer in-band
dialer string lte
dialer-group 1
no peer default ip address
async mode interactive
routing dynamic
!
interface Cellular0/1
no ip address
encapsulation slip
!
interface Cellular1/1
no ip address
encapsulation slip
!
interface wlan-ap0
no ip address
!
interface Vlan1
no ip address
!
```

```
interface Async0
no ip address
encapsulation scada
!
interface Async1
no ip address
encapsulation scada
!
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Cellular1/0
ip route 8.8.8.8 255.255.255.255 Cellular0/0

Route values added
!
dialer-list 1 protocol ip permit
ipv6 ioam timestamp
!
access-list 1 permit any
!
control-plane
!
!
line con 0
stopbits 1
line 1 2
stopbits 1
line 3
script dialer lte
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
rxspeed 150000000
txspeed 50000000
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
l
ine 8
script dialer lte
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
rxspeed 150000000
txspeed 50000000
line 9
script dialer lte
no exec
transport preferred lat pad telnet rlogin lapb-ta mop udptn v120 ssh
transport input all
transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
rxspeed 236800
txspeed 118000
line 15
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
```

```
rxspeed 236800
txspeed 118000
line 1/3 1/6
transport preferred none
transport output none
stopbits 1
line vty 0 4
login
transport input none
!
no scheduler max-task-time
!!
End
```

Test the modem configuration with a ping command:

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

The following two examples show a Verizon profile followed by an AT&T profile.

Verizon Profile

```
DUAL-Modem# show cellular 0/0 profile

Profile 1 = INACTIVE **
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwims
Authentication = None
Profile 2 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwadmin
Authentication = None
Profile 3 = ACTIVE*

Profile 3 is used for Verizon
--------
PDP Type = IPv4v6
PDP address = 166.140.43.237
Access Point Name (APN) = we01.VZWSTATIC
Authentication = None
        Primary DNS address = 198.224.173.135
        Secondary DNS address = 198.224.174.135
Profile 4 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwapp
Authentication = None
Profile 5 = INACTIVE
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzw800
Authentication = None
Profile 6 = INACTIVE
```

```
--------
PDP Type = IPv4v6
Access Point Name (APN) = vzwenterprise
Authentication = None
  * - Default profile
 ** - LTE attach profile
```

AT&T Profile

```
DUAL-Modem# show cellular 1/0 profile

Profile 1 = ACTIVE* **

Profile 1 is used for AT&T
--------
PDP Type = IPv4
PDP address = 10.61.25.231
Access Point Name (APN) = m2m.com.attz
Authentication = None
        Primary DNS address = 8.8.8.8
        Secondary DNS address = 8.8.4.4
  * - Default profile
 ** - LTE attach profile
DUAL-Modem# show cellular 0/0 hardware
Modem Firmware Version = SWI9X30C_02.20.03.00
Modem Firmware built = 2016/06/30 10:54:05
Hardware Version = 1.0
Device Model ID: MC7455MOBILE
International Mobile Subscriber Identity (IMSI) = 311480166946902
International Mobile Equipment Identity (IMEI) = 352009080050110
Integrated Circuit Card ID (ICCID) = 89148000001653263375
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) = 6692200807
Modem Status = Online
Current Modem Temperature = 34 deg C
PRI SKU ID = 1103084, PRI version = 002.024, Carrier = Verizon
Carrier identified as Verizon
OEM PRI version = 000.001
```

Creating a Cellular Profile for Verizon.

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

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

```
Enter configuration commands, one per line.  End with CNTL/Z.
DUAL-Modem(config)# controller cellular 0
DUAL-Modem(config-controller)# lte sim data-profile 3 attach-profile 1
DUAL-Modem(config-controller)# end
DUAL-Modem#
DUAL-Modem# show

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

Creating a Cellular Profile for AT&T

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

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

Note: Please issue a modem reset for the modified attach-profile to take effect.
DUAL-Modem(config-controller)# end
DUAL-Modem#
```

Controller Cellular 0 and NAT Configuration

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

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

Procedure

Step 1 Show the controller cellular 0

Example:

```
IR800#show run | begin controller
controller Cellular 0
 lte sim data-profile 1 attach-profile 1 slot 0 !
Value set-up for configuration example
 lte sim max-retry 0
 lte failovertimer 0
 lte modem link-recovery rssi onset-threshold -110
 lte modem link-recovery monitor-timer 20
 lte modem link-recovery wait-timer 10
 lte modem link-recovery debounce-count 6
!
```

Step 2 If the cellular interface obtains an IPv4 private address, NAT should be configured.

Example:

```
IR800#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#inter cellular 0
IR800(config-if)#ip nat outside
IR800(config)#inter vlan 4
IR800(config-if)#ip nat inside
IR800(config)#access-list 10 permit 10.20.20.0 0.0.0.255
!
IPv4 subnet to be NATed
IR800(config)# ip nat inside source list 10 interface Cellular0 overload
!
NAT interface association
```

Step 3 Once the Cellular configuration is done, ping a well-known IP address to test the connectivity.

Example:

```
IR800#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 340/472/740 ms
IR800#
```

Step 4 Attached Cellular 0 profile must become “active” and “connection” shows IP address and traffic.

Example:

```
IR800#show cellular 0 profile
Profile 1 = ACTIVE* **
--------
PDP Type = IPv4
PDP address = 10.60.159.255
Access Point Name (APN) = LTE
Authentication = None
 Primary DNS address = 212.27.40.240
 Secondary DNS address = 212.27.40.241
  * - Default profile
 ** - LTE attach profile
Configured default profile for active SIM 0 is profile 1.
IR800#show cellular 0 connection
Profile 1, Packet Session Status = ACTIVE
 Cellular0:
```

```
 Data Transmitted = 700 bytes, Received = 600 bytes
 IP address = 10.60.159.255
 Primary DNS address = 212.27.40.240
 Secondary DNS address = 212.27.40.241
Profile 2, Packet Session Status = INACTIVE
```

What to do next

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

```
IR800#show interfaces cellular 0
Cellular0 is up, line protocol is up
  Hardware is 4G WWAN Modem - Global (Europe & Australia) Multimode LTE/DC-HSPA+/HSPA+/HSPA/U

  Internet address is 10.123.161.59/32
  MTU 1500 bytes, BW 384 Kbit/sec, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SLIP, loopback not set
  Keepalive not supported
  Last input 00:22:41, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/10 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     12 packets input, 1128 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     51 packets output, 3364 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
     0 carrier transitions
     DCD=up  DSR=up  DTR=up  RTS=up  CTS=up
IR800#
```

If the negotiated IP address in not operational:

```
IR800#show interfaces cellular 0
Cellular0 is up (spoofing), line protocol is up (spoofing)
  Hardware is 4G WWAN Modem - Global (Europe & Australia) Multimode LTE/DC-HSPA+/HSPA+/HSPA/U


Internet address will be assigned dynamically by the network
```

Other Useful Commands

```
IR800# show cell 0 hardware
Modem Firmware Version = SWI9X15C_05.05.58.00
Modem Firmware built = 2015/03/04 21:30:23
Hardware Version = 1.0
Device Model ID: MC7304
Package Identifier ID: 1102029_9903299_MC7304_05.05.58.00_00_Cisco_005.010_000
International Mobile Subscriber Identity (IMSI) = 208150103324395
International Mobile Equipment Identity (IMEI) = 352761060206340
```

```
Integrated Circuit Card ID (ICCID) = 8933150112100222053
Mobile Subscriber Integrated Services
Digital Network-Number (MSISDN) = 33695764790
Current Modem Temperature = 47 deg C
PRI SKU ID = 9903299, PRI version = 05.10, Carrier = 1

IR800# show cell 0 security
Active SIM = 0  !
SIM slot #0 active
SIM switchover attempts = 0
Card Holder Verification (CHV1) = Disabled
SIM Status = OK
SIM User Operation Required = None
Number of CHV1 Retries remaining = 3

IR800# cellular 0 lte sim unlock XXXX
     !
XXXX = PIN code

IR800# show cell 0 radio
Radio power mode = ON
Channel Number = 3037
Current Band = Unknown
Current RSSI(RSCP) = -99 dBm
Current ECIO = -10 dBm
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = UMTS ( UMTS/WCDMA )

IR800# show cell 0 network
Current System Time = Sat Oct 10 9:12:59 2015
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = LTE
Mobile Country Code (MCC) = 208
Mobile Network Code (MNC) = 15
Packet switch domain(PS) state = Attached
Location Area Code (LAC) = 3910
Cell ID = 222094374

IR800# show cell 0 all
```

Note The output to the **show cell 0 all** command is extensive, and omitted from this guide for brevity.

Accessing 4G Modem AT Commands

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

Get the line number associated to Cellular 0:

```
IR800#show line
 Tty Line Typ   Tx/Rx   A Modem  Roty AccO AccI  Uses  Noise Overruns  In
 I   3    3 TTY  -       -        -    -    -     1      0    4/0      Ce0
```

Use one of the IR800 IP address along with 2000 + line number (2003)

```
IR800#10.15.15.1 2003
Trying 10.15.15.1, 2003 ... Open
```

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

```
AT!GSTATUS?
!GSTATUS:
Current Time:  213353  Temperature: 38
Bootup Time:   0  Mode:        ONLINE
System mode:   WCDMA       PS state:    Attached
WCDMA band:    WCDMA 900
WCDMA channel: 3037
GMM (PS) state:REGISTERED      NORMAL SERVICE
MM (CS) state: IDLE            NORMAL SERVICE
WCDMA L1 state:L1M_PCH_SLEEP   LAC:         0F46 (3910)
RRC state:   DISCONNECTED    Cell ID:     0D3CE428 (222094376)
RxM RSSI C0:   -90  RxD RSSI C0: -106
RxM RSSI C1:   -106  RxD RSSI C1: -106
```

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

```
IR800#disc
Closing connection to 10.2.2.2 [confirm]enter
IR800#
```

Checking 4G Modem Firmware through AT Commands

To check the IR800 4G modem firmware, execute the 4G modem AT commands after connecting to the modem. The following example is for an IR809G-LTE-GA-K9 loaded with FW-MC7304-LTE-GB Global firmware.

Note On the IR809, the PRI SKU ID= 9903299 is not representative of the GB firmware

```
at!priid?
PRI Part Number: 9903299
Revision: 05.10
Carrier PRI: 9999999_9902674_SWI9X15C_05.05.58.00_00_GENEU-4G_005.026_000
OK
at!package?
1102029_9903299_MC7304_05.05.58.00_00_Cisco_005.010_000
at!gobiimpref?
!GOBIIMPREF:
 preferred fw version:   05.05.58.00
 preferred carrier name: GENEU-4G
 preferred config name:  GENEU-4G_005.026_000
 current fw version:     05.05.58.00
 current carrier name:   GENEU-4G
 current config name:    GENEU-4G_005.026_000
```

Radio Frequency Band Select

This new feature allows the user to configure and lock down the modem to a specific RF band, or set of bands. The preference can be set to be equal to, or a sub-set of the capability supported by the modem/carrier combination.

The following examples show the controller configuration commands:

```
router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#controller cell interface number


router(config-controller)#lte modem ?
  band-select      Modem band select
  dm-log           Modem DM logging configuration
  fota-poll-timer  Set poll timer for AVMS to do Firmware upgrade over the air
  link-recovery    Cellular Link Recovery
  mtu              Modem mtu
  nas-log          Modem NAS logging configuration

router(config-controller)#lte modem band-select ?
  all-lte-only     Choose all LTE bands only
  all-nonlte-only  Choose all non-LTE bands only
  band-indices     Specify the lte and non-lte band indices

router(config-controller)#lte modem band-select band-indices ?
  WORD  Band index(es) in string format "<band index#>, <band index#>, ...".
        (supported band indices are listed under 'show cellular radio band'.)

router(config-controller)#lte modem band-select band- indices "2 4 5" ?
  slot  primary SIM slot

router(config-controller)#lte modem band-select band- indices "2 4 5" slot ?

  <0-1>  Slot number

router(config-controller)#lte modem band-select band- indices "2 4 5" slot 0

router#show run | sec controller
controller Cellular 0
 lte sim max-retry 0
 lte failovertimer 4
 lte modem dm-log rotation
 lte modem link-recovery disable
 lte modem band-select band- indices "2,4,5" slot 0
```

The following examples show the controller show commands:

```
router#show cellular interface number radio ?

  band     Show Radio band settings
  history  Show Radio history in graph format
  |        Output modifiers
  <cr>     <cr>

router#show cellular interface number radio band
```

```
LTE bands supported by modem:
- Bands 2 4 5 12.
LTE band Preference settings for the active sim(slot 0):
- Bands 2 4 5 12.
Non-LTE bands supported by modem:
Index:
  88 - WCDMA US PCS 1900 band
  90 - WCDMA US 1700 band
  91 - WCDMA US 850 band
Non-LTE band Preference settings for the active sim(slot 0):
Index:
  88 - WCDMA US PCS 1900 band
  90 - WCDMA US 1700 band
  91 - WCDMA US 850 band

IR807#show run | sec controller
controller Cellular 0
no lte gps enable
lte modem crash-action boot-and-hold
lte modem fota-poll-timer 15
lte modem mtu 1700
lte modem link-recovery disable
IR800#
```

Low Power Mode

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

```
router# show cellular <interface number> radio

Radio power mode = OFF, Reason = User Request
Channel Number = 0
Current Band = Unknown
Current RSSI = -128 dBm
Current ECIO = -2 dBm
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = AUTO
```

```
router# show cellular <interface number> radio details

 Radio turned off under cellular controller configuration.
router#
```

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

Enhancement to Modem Crash Action

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

:
https://www.cisco.com/c/en/us/support/docs/interfaces-modules/lte-wireless-wan-interfaces/200463-Generate-4G-modem-crash-dump.html
or

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

A new CLI has been added to set the crash action on the modem upon a crash. The CLI is **lte modem crash-action ?**. The device can be set to either reset, or to boot and hold.

The following example shows the new functionality of the configuration CLI:

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

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

The following example shows the new functionality of the exec CLI:

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

This CLI will show the current state the modem is set to. This is the same as AT command **at!eroption=?**.

IR800 Cellular Technology Selection

The cellular interface supports a seamless hand off between LTE and 3G networks when the LTE cell becomes weak in certain spots and vice versa. But it may also be disable to lock the cellular interface in a given technology, for example. LTE.

The cellular interface supports 3G and 2.5G technologies. The IOS CLI can be used to select a particular technology that is most desirable in your local zone.

Use the cellular 0 lte technology command:

```
IR829# cellular 0 lte technology ?
  !
Blue
 values available on Global SKU

auto   Automatic LTE Technology Selection
  cdma-1xrtt   CDMA 1xRTT
  cdma-evdo    CDMA EVDO Rev A
  cdma-hybrid  HYBRID CDMA

  gsm   GSM
  lte   LTE
  umts  UMTS
```

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

Show the completed configuration: (output edited for brevity)

```
IR800#show run
Building configuration...
Current configuration : 4365 bytes
!
! Last configuration change at 09:53:09 UTC Sat Oct 10 2015 by cisco
!
version 15.5
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.155-3.M0a
boot-end-marker
!
enable password cisco
!
aaa new-model
!
aaa session-id common
ethernet lmi ce
!
ip dhcp pool GuestOS
 network 10.16.16.0 255.255.255.0
 default-router 10.16.16.1
 dns-server 8.8.8.8
!
ip domain name local.cisco.com
ip cef
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
chat-script LTE "" "AT!CALL" TIMEOUT 20 "OK‟
!
license udi pid IR809G-LTE-GA-K9 sn JMX1915X00Q
license accept end user agreement
license boot module ir800 technology-package securityk9
license boot module ir800 technology-package datak9
!
username cisco password 0 cisco
!
redundancy
!
controller Cellular 0
 lte sim data-profile 1 attach-profile 1 slot 0
 lte sim max-retry 0
 lte failovertimer 0
 lte modem link-recovery rssi onset-threshold -110
 lte modem link-recovery monitor-timer 20
 lte modem link-recovery wait-timer 10
 lte modem link-recovery debounce-count 6
!
interface GigabitEthernet0
 description backhaul
 ip address dhcp
 duplex auto
 speed auto
 ipv6 address autoconfig default
!
interface GigabitEthernet1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet2
 ip address 10.16.16.1 255.255.255.0
 duplex auto
 speed auto
 ipv6 address autoconfig
!
interface Cellular0
 ip address negotiated
 encapsulation slip
 dialer in-band
 dialer idle-timeout 0
 dialer string LTE
 dialer-group 1
 async mode interactive
!
interface Cellular1
 no ip address
 encapsulation slip
!
interface Async0
 no ip address
 encapsulation scada
!
interface Async1
 no ip address
 encapsulation scada
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 Cellular0
ip ssh time-out 60
!
dialer-list 1 protocol ip permit
!
control-plane
!
line con 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 telnet
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 speed 384000
line 8
 script dialer LTE
 modem InOut
 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
 speed 384000
line 1/3 1/6
 transport preferred none
 transport output none
 stopbits 1
line vty 0 4
 password cisco
 transport input telnet ssh
!
no scheduler max-task-time
!
end
IR800#
```

GPS

The IR800 series can be configured to enable real-time location tracking of remote assets and geo-fence when used with IOT Field Network Director. Field Network Director receives GPS data directly from IOS, not NMEA.

Key Points:

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

Note On the IR829 dual-LTE model, GPS can only be configured on cellular 0/0.

For information about the GPS LED indications and locations of the GPS connectors, see IR829 Product Overview and IR809 Product Overview .

To configure GPS on the IR800 series, refer to the following examples.

```
IR829# conf term
IR829(config)#controller cellular 0
IR829(config-controller)#lte gps ?
  enable  enable GPS feature
  mode    select GPS mode
  nmea    enable NMEA data
IR829(config-controller)#lte gps mode standalone

IR829(config-controller)#lte gps nmea ip
IR829#show cellular 0 gps

GPS Info
-------------
GPS Feature: enabled
GPS Port Selected: Dedicated GPS port
GPS State: GPS enabled
GPS Mode Configured: standalone
Latitude: 48 Deg 38 Min 31.2114 Sec North
Longitude: 2 Deg 13 Min 47.3992 Sec East
Timestamp (GMT): Wed Jul 22 08:05:28 2015
```

```
Fix type index: 0, Height: 94 m
Satellite Info
----------------
Satellite #14, elevation 28, azimuth 310, SNR 31 *
Satellite #15, elevation 22, azimuth 171, SNR 39 *
Satellite #17, elevation 25, azimuth 45, SNR 34 *
Satellite #18, elevation 8, azimuth 248, SNR 25
Satellite #22, elevation 12, azimuth 281, SNR 24
Satellite #24, elevation 78, azimuth 90, SNR 35 *
Satellite #25, elevation 23, azimuth 241, SNR 27
Satellite #1, elevation 0, azimuth 0, SNR 0
Satellite #2, elevation 0, azimuth 0, SNR 0
Satellite #6, elevation 6, azimuth 85, SNR 0
Satellite #12, elevation 62, azimuth 241, SNR 0
Satellite #26, elevation 0, azimuth 0, SNR 0
Satellite #29, elevation 0, azimuth 0, SNR 0
IR829#
```

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

For example:

```
IR829#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IR829(config)#controller cellular 0
IR829(config-controller)#lte gps nmea ?
  ip      NMEA over IP interface
  serial  NMEA over serial interface
IR829(config-controller)#lte gps nmea ip ?
  udp  UDP Transport
  <cr>
IR829(config-controller)#lte gps nmea ip udp ?
  A.B.C.D  Source address
IR829config-controller)#lte gps nmea ip udp 10.3.4.5 ?
  A.B.C.D  Destination address
IR829(config-controller)#lte gps nmea ip udp 10.1.1.1 10.3.4.5 ?
  <0-65535>  Destination port
IR829(config-controller)#lte gps nmea ip udp 10.1.1.1 10.3.4.5 3456
Cellular Modem in HWIC slot 0/0 is still in reset, we recommend to re-execute this cmd after
 60 seconds
IR829(config-controller)#
```

The Command Line Interface for the gyroscope feature has been changed in IOS Release 15-7-3M1 in order to be compatible with the CCP Express NMS. The old CLI format was:

```
IR829(config)#gyroscope-reading frequency ?
1/min Reading 1 times per minute
1/sec Reading 1 time per second (default value)
10/min Reading 10 times per minute
```

From this release going forward, the format has been modified to:

```
IR829(config)#gyroscope-reading frequency ?
one/min Reading 1 times per minute
one/sec Reading 1 time per second (default value)
ten/min Reading 10 times per minute
```

After upgrading to this release, the router will have to be reconfigured.

GPS NMEA Multiple Stream

Feature is new for release 15.8(3)M1 and applies to the IR809 and IR829.

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

Setting up the Configuration

To Enable GPS NMEA Multiple Stream:

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

To Disable GPS NMEA Multiple Stream:

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

Examples for Enabling/Disabling GPS NMEA Multiple Stream

Enable Example:

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

Disable Example:

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

GPS Multiple NMEA Stream Information

Use the show controller and show run configuration CLIs:

Sample Output

```
Router#sh cont cel 0 | inc NMEA
NMEA Stream no: 1 Configured
NMEA Stream no: 2 Configured
NMEA Stream no: 3 Not Configured
NMEA Stream no: 4 Configured
NMEA Stream no: 5 Configured
NMEA Stream no: 6 Not Configured
Router#sh run | sec cont
controller Cellular 0
```

```
lte gps nmea ip udp 10.10.0.1 10.10.0.10 2067 stream 1
lte gps nmea ip udp 20.20.0.1 20.25.0.20 2047 stream 2
lte gps nmea ip udp 20.27.0.1 20.27.0.20 2047 stream 4
lte gps nmea ip udp 20.20.0.1 20.20.0.20 2023 stream 5
```

Warning Messages

If the destination ip address and port number already exists:

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

Please use different destination ip address and port number.

If the stream number already exists:

```
Router#sh run | sec cont
controller Cellular 0
 lte gps mode standalone
 lte gps nmea ip udp 10.10.0.1 10.10.0.10 2067 stream 1
Router(config-controller)#lte gps nmea ip udp 20.20.0.1 20.20.0.10 2057 stream 1
Stream number 1 is already active.
```

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

Troubleshooting the Cellular Interface

These procedures are to capture information to share with support in order to assist them in helping to troubleshoot an issue with the cellular interface. In order to capture logs, DM logs must be enabled. Refer to the following:https://www.cisco.com/c/en/us/td/docs/routers/access/800/819/user/guide/3G4G-enhancements-userguide.html#pgfId-1063363

The following are steps to capture Linux logs for the cellular interface.

Procedure

Step 1 Set up the fetch command.

Example:

```
# conf t
# service internal
# exit
# vds fetch-log
```

These steps will generate a directory on flash:vds-log.

Step 2 Capture the logs.

Example:

```
IR800# vds fetch-log
fetch: 4gmodem.log
    Sending file modes: C0644 510 4gmodem.log
fetch: auth.log
    Sending file modes: C0640 162330 auth.log
fetch: auth.log.1
    Sending file modes: C0640 262215 auth.log.1
fetch: auth.log.2.gz
    Sending file modes: C0640 11297 auth.log.2.gz
fetch: auth.log.3.gz
    Sending file modes: C0640 11296 auth.log.3.gz
fetch: cwan_modem0.log
    Sending file modes: C0644 3875716 cwan_modem0.log
fetch: cwan_modem1.log
    Sending file modes: C0644 791629 cwan_modem1.log
fetch: daemon.log
    Sending file modes: C0640 1404 daemon.log
fetch: dmesg
    Sending file modes: C0644 13740 dmesg
fetch: dmesg.0
    Sending file modes: C0644 0 dmesg.0
fetch: ios_cs_verify.log
    Sending file modes: C0644 1091 ios_cs_verify.log
fetch: ios_vds_com.log
    Sending file modes: C0644 219169 ios_vds_com.log
fetch: ios_vds_com.log.1
    Sending file modes: C0644 262207 ios_vds_com.log.1
fetch: ios_vds_com.log.2.gz
    Sending file modes: C0644 7859 ios_vds_com.log.2.gz
fetch: ios_vds_com.log.3.gz
    Sending file modes: C0644 7894 ios_vds_com.log.3.gz
fetch: kern.log
    Sending file modes: C0640 38608 kern.log
fetch: messages
    Sending file modes: C0640 174064 messages
fetch: messages.1
    Sending file modes: C0640 262364 messages.1
fetch: messages.2.gz
etch: messages.2.gz
    Sending file modes: C0640 18434 messages.2.gz
fetch: messages.3.gz
    Sending file modes: C0640 25027 messages.3.gz
fetch: udev
    Sending file modes: C0644 124266 udev
fetch: vdscli-acpid.log
    Send
```

Step 3 Stop the logging after 10 minutes.

Step 4 View the flash directory, and you will see the vds-log directory.

Example:

```
IR800# dir flash:
Directory of flash:/
16  -rw-         660  Nov 11 2016 19:25:20 +00:00  vlan.dat
1   drw-           0   Jan 1 2014 16:27:44 +00:00  7455_02.18.02.00_Verizon_002.022_000
17  -rw-   160368465  Nov 11 2016 19:35:30 +00:00  ir800-universalk9-bundle.SPA.156-3.M0a
18  -rw-    63753008  Nov 11 2016 19:45:34 +00:00  ir800-universalk9-mz.SPA.156-3.M0a
19  -rw-    64381598  Nov 11 2016 19:50:24 +00:00  74XX_02.20.03.00.cwe
```

```
20  -rw-        9143  Nov 11 2016 19:59:30 +00:00  7455_02.20.03.00_ATT_002.019_000.nvu
4   drw-           0   Jan 1 2014 16:17:58 +00:00  managed
14  drw-           0   Jan 1 2014 16:17:58 +00:00  eem
15  -rw-    62582707   Jan 1 2014 16:27:24 +00:00 ir800-universalk9-mz.SSA.156-20160701_225522
21  -rw-   161162048  Nov 16 2016 18:41:46 +00:00  ir800-universalk9-bundle.SSA.156-2.10.62.GB
22  -rw-    63827874  Nov 16 2016 18:54:30 +00:00  ir800-universalk9-mz.SSA.156-2.10.62.GB
23  drw-           0  Nov 16 2016 19:06:34 +00:00  vds-log
```

Step 5 The flash:/vds-log directory contains the log files captured.

Example:

```
   24  -rw-         510  Nov 16 2016 19:06:44 +00:00  4gmodem.log
   25  -rw-      162330  Nov 16 2016 19:06:54 +00:00  auth.log
   26  -rw-      262215  Nov 16 2016 19:07:04 +00:00  auth.log.1
   27  -rw-       11297  Nov 16 2016 19:07:16 +00:00  auth.log.2.gz
   28  -rw-       11296  Nov 16 2016 19:07:24 +00:00  auth.log.3.gz
   29  -rw-     3875716  Nov 16 2016 19:07:42 +00:00  cwan_modem0.log
   30  -rw-      791629  Nov 16 2016 19:07:54 +00:00  cwan_modem1.log
   31  -rw-        1404  Nov 16 2016 19:08:04 +00:00  daemon.log
   32  -rw-       13740  Nov 16 2016 19:08:14 +00:00  dmesg
   33  -rw-           0  Nov 16 2016 19:08:24 +00:00  dmesg.0
   34  -rw-        1091  Nov 16 2016 19:08:32 +00:00  ios_cs_verify.log
   35  -rw-      219169  Nov 16 2016 19:08:42 +00:00  ios_vds_com.log
   36  -rw-      262207  Nov 16 2016 19:08:54 +00:00  ios_vds_com.log.1
   37  -rw-        7859  Nov 16 2016 19:09:04 +00:00  ios_vds_com.log.2.gz
   38  -rw-        7894  Nov 16 2016 19:09:14 +00:00  ios_vds_com.log.3.gz
   39  -rw-       38608  Nov 16 2016 19:09:24 +00:00  kern.log
   40  -rw-      174064  Nov 16 2016 19:09:34 +00:00  messages
   41  -rw-      262364  Nov 16 2016 19:09:44 +00:00  messages.1
   42  -rw-       18434  Nov 16 2016 19:09:54 +00:00  messages.2.gz
   43  -rw-       25027  Nov 16 2016 19:10:04 +00:00  messages.3.gz
   44  -rw-      124266  Nov 16 2016 19:10:14 +00:00  udev
   45  -rw-         292  Nov 16 2016 19:10:24 +00:00  vdscli-acpid.log
   46  -rw-         909  Nov 16 2016 19:10:34 +00:00  vdscli-eventd.log
   47  -rw-         467  Nov 16 2016 19:10:44 +00:00  vdscli-vdscli-bde-gos.log
   48  -rw-         479  Nov 16 2016 19:10:54 +00:00  vdscli-vdscli-bde-ir800.log
   49  -rw-          81  Nov 16 2016 19:11:04 +00:00  vdscli-wiredd.log
   50  -rw-      140382  Nov 16 2016 19:11:14 +00:00  vdscli-wirelessd.log
   51  -rw-        1192  Nov 16 2016 19:11:24 +00:00  vdscli.log
994918400 bytes total (34735718
```

What to do next

Other command output that will be helpful to collect for your business unit contact:

```
# Show platform hypervisor
# Show platform led
# Show tech
# Show cellular 0/0 all
# Show controller 0/0
# Show interface cellular 0/0
# Show ip interface brief
# Show running-config
```

CHAPTER 4

IR829 AP803 Access Point Module

This chapter provides background on the Internal WLAN Access Point which runs on-board the IR829 router. The AP803 runs its own IOS software independently from the IR829 IOS, and requires configuring. The AP803 works as a standalone access point or with a wireless controller.

Hardware Overview

Highlights of the Access Point are:

- Atheros QCA9550 SoC + AR9592 radio
- 256MB DDR2 RAM + 128MB NAND Flash + 1MB Boot flash and configuration/calibration storage
- Dual simultaneous 2.4GHz and 5Ghz 802.11 radios
    - Supports 2 x 2 802.11a/n MIMO and 2 x 2 802.11b/g/n MIMO
    - Packet aggregation: A-MPDU (Tx/Rx), A-MSDU (Tx/Rx)
    - 802.11 dynamic frequency selection (DFS)
    - Cyclic shift diversity (CSD) support
    - 20- and 40-MHz channels
    - 802.11 dynamic frequency selection (DFS) – is applicable to IR829 AP803 and is available in IOS release 8.1MR2

Software Overview

This Embedded AP supports a default Autonomous mode and a Unified mode. Both the Autonomous and Unified images are pre-loaded from Cisco on the access point's flash memory.

The image name describes what each image is for. **w7** is Autonomous Image, while **w8** is the Unified mode (LWAP) Image. For example:

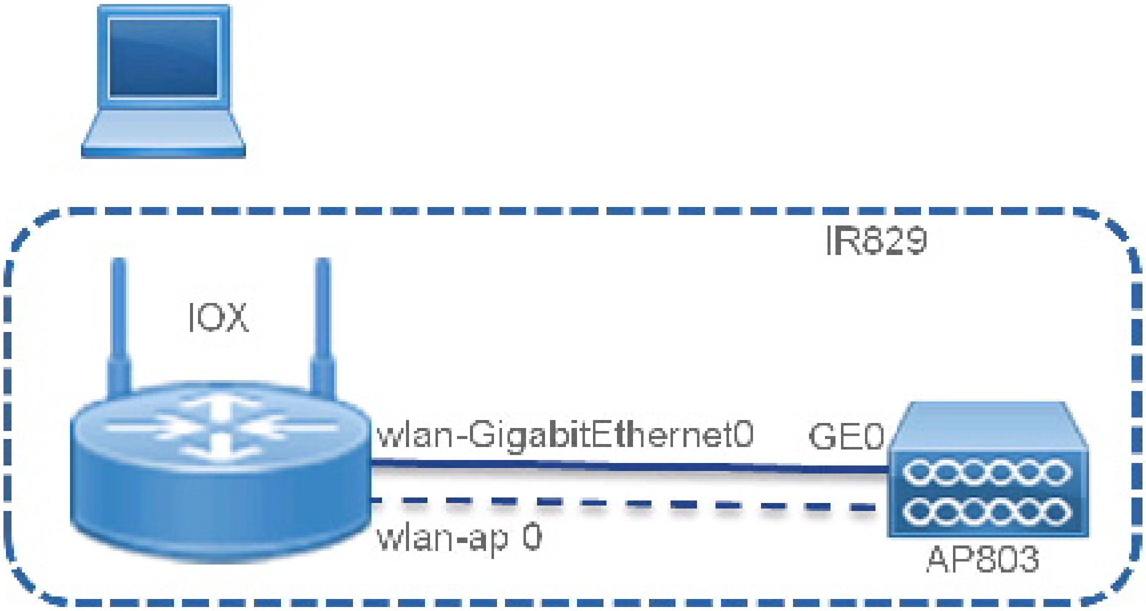
- Autonomous image – ap1g3-k9**w7**-tar.153-3.JBB1.tar
- Unified mode (LWAP) image – ap1g3-k9**w8**-tar.153-3.JBB1.tar
- To select the Autonomous or Unified image use the IOS CLI:

```
IR829(config)#service-module wlan-ap 0 bootimage autonomous
IR829(config)#service-module wlan-ap 0 bootimage unified
```

Note The initial release for the IR829 with the AP803 access point is 8.1 MR1 - 15.3(3)JBB1 - Cisco Wireless Release 8.1.111.0.

IOS Internal Interfaces

The IR829 and AP803 are connected through IOS internal interfaces. Refer to the following graphic as a conceptual guide.



AP803 IOS Gigabit Ethernet0 Interface

This interface is internally connected to the IR829 WLAN-GigabitEthernet0 switch-port.

The Access Point GE0 interface is always up. Neither the Access Point GE0 or the IR829 WLAN-GigabitEthernet0 switch-port interfaces can be shutdown. This is in order to prevent traffic disruption to the internal Access Point.

Note Access Point GE0 can NOT be configured by network operators. It always operates in 1000M/full-duplex mode.

AP803 IOS – BVI 1 (in autonomous mode only)

This is the management interface which bridges the Dot11 radio0, Dot11 radio1 and GE0 interfaces.

IR829 IOS WLAN-GigabitEthernet0

This interface connects internally to the Access Point's GE0 interface and carries all data packets between the Access Point and the Router.

The default configuration for WLAN-GigabitEthernet0 is in switch-port access mode, with native VLAN 1 (Layer-3 interface). You can configure the switch-port in trunk mode as well.

IR 829 IOS wlan-ap 0

This is the interface representing the embedded Access Point on the Router. It requires an IP address and is used only to reverse telnet into the Access Point console. This interface does not carry any data packets between the Router and the Access Point.

IR829 IOS – AP803 Console Access

Connecting to the console of the AP803 allows for monitoring Warning and informational messages. You can configure wlan-ap 0 so that a dedicated IP address is not needed, and wlan-ap 0 can share its IP address with another interface. Use the following steps:

Configuring

```
# conf term
IR829(config)#inter wlan-ap 0
The wlan-ap 0 interface is used for managing the embedded AP.
Please use the "service-module wlan-ap 0 session" command to console into the embedded AP
IR829(config-if)# ip address 10.1.1.1 255.255.255.255
IR829#service-module wlan-ap 0 session
Trying 10.1.1.1, 2004 ... Open
User Access Verification
Username: cisco
Password: <password>
ap>ena
Password: <password>
ap#
```

Connecting

```
IR829#service-module wlan-ap 0 session
Trying 10.1.1.1, 2004 ... Open
User Access Verification
Username: cisco
Password: <password>
ap>ena
Password: <password>
ap#
```

Monitoring

```
IR829#service-module wlan-ap 0 status

Service Module is Cisco wlan-ap0
Service Module supports session via TTY line 4
Service Module is in Steady state
Service Module reset on error is disabled
Service Module heartbeat-reset is enabled
Getting status from the Service Module, please wait..
  Image path       =
flash:ap1g3-k9w7-mx.wnbu_bt.201505140911/ap1g3-k9w7-mx.wnbu_bt.201505140911
  System uptime    = 0 days, 5 hours, 43 minutes, 7 seconds
```

Disconnecting

Key in the following sequence:

ctrl-^

X

This suspends the console and returns you to the command line.

IR829#

Next use one of the following two options:

```
Router> disconnect
```

-or

```
Router > service-module wlan-ap 0 session clear
[confirm]
[OK]
```

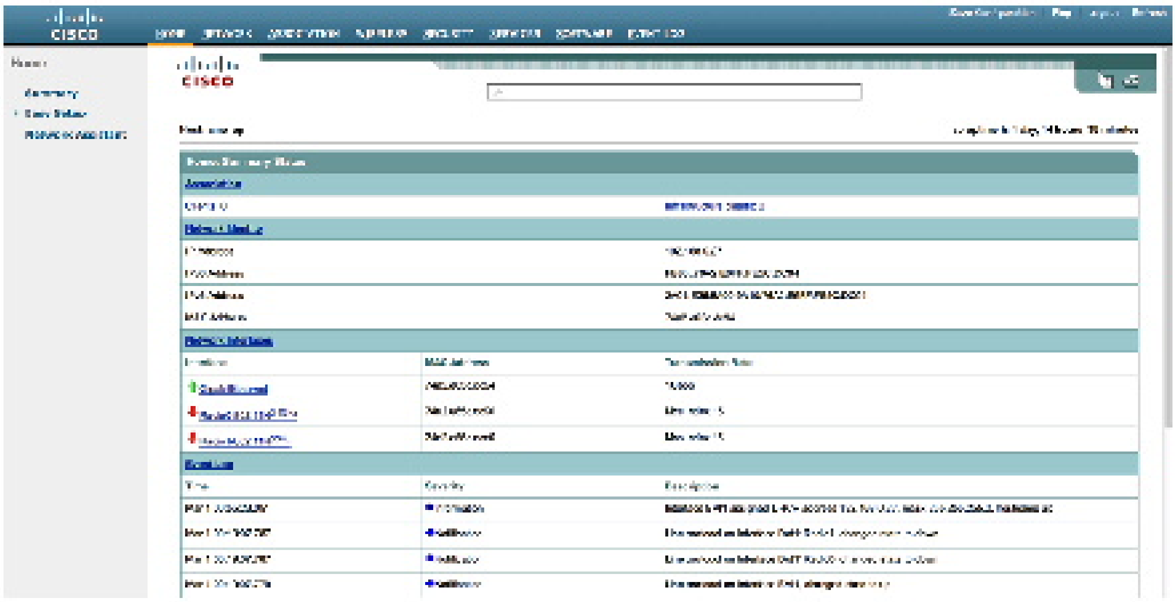
IR829 Service Module

The AP803 Access Point is managed by the IR829 Service Module Monitor. It communicates with the AP803 through layer-2 RBCP (Router Blade Configuration Protocol). The AP803 is managed through the service-module wlan-ap 0 CLI.

```
IR829#service-module wlan-ap 0 ?
  heartbeat-reset  Enable/disable Heartbeat failure to reset Service Module
  reload           Reload service module
  reset            Hardware reset of Service Module
  session          Service module session
  statistics       Service Module Statistics
  status           Service Module Information
  upgrade          Service Module Upgrade

IR829#service-module wlan-ap 0 reset ?
bootloader      Reset service-module to bootloader !
Reset to boot loader prompt
 default-config  Reset service-module to default-config !
Reset to default configuration
 - flash:cpconfig-ap803.cfg to flash:config.txt,
Only valid for Autonomous mode
<cr> !
Reset Access Point only

IR829# conf term
!
to configure Access Point boot image type

IR829(config)#service-module wlan-ap 0 bootimage ?
autonomous  Set AP boot image to autonomous
unified     Set AP boot image to unified
```

AP803 Embedded Web Manager

The IR829 AP803 has an embedded web manager. To access the web manager, open your browser to the IP address of the AP803 BV1 interface. For example:



The feature set for the AP803 is aligned with the Cisco Aironet 1532. More information can be found at:

Cisco Aironet 1530 Series

Upgrading the Firmware on the AP803

The AP803 image is not included in the IR829 IOS bundle. The AP803 image must be installed separately after obtaining the new AP803 release from Cisco.com.

1. Log onto the AP803.
2. Install the new AP803 image using the archive command. Alternately, this can be accomplished through the embedded web interface.
    - archive download-sw ! Software download.
    - /overwrite ! Overwrites the software image in Flash with the downloaded image.
    - /reload ! Reloads the system after downloading the image unless the configuration has been changed and not saved.

The ftp protocol to download the image is:

ftp://username:password@ipaddress/directory/file

For example:

```
IR829#service-module wlan-ap 0 session

Trying 10.1.1.1, 2004 ... Open

ap#archive download-sw /over /reload
 ftp://username:password@192.168.0.90/Temp/ap1g3-k9w7-tar.153-3.JBB1.tar

examining image...
extracting info (285 bytes)!
Image info:
    Version Suffix: k9w7-.153-3.JBB1
    Image Name: ap1g3-k9w7-mx.153-3.JBB1
    Version Directory: ap1g3-k9w7-mx.153-3.JBB1
    Ios Image Size: 12114432
    Total Image Size: 13179392
    Image Feature: WIRELESS LAN
    Image Family: ap1g3
    Wireless Switch Management Version: 8.1.111.0
MwarVersion:08016F00.First AP Supported Version:08010000.
Image version check passed
Extracting files...
ap1g3-k9w7-mx.153-3.JBB1/ (directory) 0 (bytes)...
```

CHAPTER 5

Configuring Virtual-LPWA

This chapter describes the details of configuring virtual-LPWA (VLPWA) interface on the IR800 series for the configuration of the Cisco LoRaWAN Gateway.

This chapter contains the following sections:

Configuring Virtual-LPWA Interface on the IR800 Series

The Cisco LoRaWAN Gateway is connected to IR800 series via an Ethernet cable with PoE+ to work as a LoRaWAN gateway. By creating a VLPWA interface on the IR800 series, you can:

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

Note Cisco IOS Release 15.6(3)M or later is required for the IR800 series to manage the Cisco LoRaWAN Gateway.

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

You can find other documentation for the Cisco LoRaWAN Gateway at: http://www.cisco.com/c/en/us/support/routers/interface-module-lorawan/tsd-products-support-series-home.html

This chapter provides information of configuring virtual interface mode (virtual-lpwa) of the LoRaWAN gateway. For detailed information about standalone mode configuration, see Cisco Wireless Gateway for LoRaWAN Software Configuration Guide.

Configuring Ethernet Interface and Creating VLPWA Interface

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

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

Configuring IR809 for One Cisco LoRaWAN Gateway

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface on IR809, and create the VLPWA interface for one Cisco LoRaWAN Gateway.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface gigabitEthernet** *ID*	Configures the Gigabit Ethernet (GE) port.
Step 3	**ip address** *address mask*	Configures the GE interface IP address. **Note** The IP address should be the default router address in its associated DHCP pool.
Step 4	**ip nat inside**	Identifies the interface as the NAT inside interface.
Step 5	**ip virtual-reassembly in**	Enables virtual fragment reassembly (VFR) on the interface.
Step 6	**exit**	Exits to global configuration mode.
Step 7	**interface Virtual-LPWA** *vlpwa-id*	Creates VLPWA interface. **Note** The value of *vlpwa-id* should be the same as the option 43 hex number which is specified in DHCP pool. See the DHCP section.

	Command or Action	Purpose
Step 8	**end**	Exits to privileged EXEC mode.
Step 9	**write memory**	Saves the configurations.

Configuring IR809 for Multiple Cisco LoRaWAN Gateways

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface on IR809 and create the VLPWA interface for multiple Cisco LoRaWAN Gateways.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface gigabitEthernet** *ID*	Configures the Gigabit Ethernet (GE) port.
Step 3	**no shutdown**	Enables the interface.
Step 4	**exit**	Exits to privileged EXEC mode.
Step 5	**interface gigabitEthernet** *ID.subID*	Configures sub-interface on the GE port.
Step 6	**encapsulation dot1Q** *vlan-id* **native**	Configures IEEE802.1Q encapsulation of traffic on a interface.
Step 7	**ip address** *address mask*	Configures the GE interface IP address. **Note** The IP address should be the default router address in its associated DHCP pool.
Step 8	**ip nat inside**	Identifies the interface as the NAT inside interface.
Step 9	**ip virtual-reassembly in**	Enables virtual fragment reassembly (VFR) on the interface.
Step 10	**exit**	Exits to global configuration mode.
Step 11	**interface Virtual-LPWA** *vlpwa-id*	Creates VLPWA interface. **Note** The value of vlpwa-id should be the same as the option 43 hex number which is specified in DHCP pool. See the DHCP section.
Step 12	**end**	Exits to privileged EXEC mode.
Step 13	**write memory**	Saves the configurations.

Configuring IR829

Each LoRaWAN gateway or virtual-lpwa must be isolated in a dedicated VLAN. If you put it in a VLAN shared with other devices, it may cause the virtual-lpwa interface not being operational.

Beginning in privileged EXEC mode, follow these steps to configure the Ethernet interface on IR829 and create the VLPWA interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface vlan** *vlan-id*	Configures the vlan interface. **Note** The VLAN ID can be different from the vlpwa ID.
Step 3	**ip address** *address mask*	Configures the vlan interface IP address. **Note** IP address should be default router address in its associated DHCP pool.
Step 4	**exit**	Exits to global configuration mode.
Step 5	**interface gigabitEthernet** *ID*	Configures the Gigabit Ethernet port.
Step 6	**switchport mode access**	Sets trunking mode to ACCESS on the given port.
Step 7	**switchport access vlan** *ID*	Sets VLAN when interface is in access mode.
Step 8	**exit**	Exits to global configuration mode.
Step 9	**interface Virtual-LPWA** *vlpwa-id*	Creates VLPWA interface. **Note** The value of vlpwa-id should be the same as the option 43 hex number which is specified in DHCP pool. See the DHCP section.
Step 10	**end**	Exits to privileged EXEC mode.
Step 11	**write memory**	Saves the configurations.

Configuring DHCP Pool for the Cisco LoRaWAN Gateway

The Cisco LoRaWAN Gateway connects to the IR800 series through the Ethernet interface. The communication between Cisco LoRaWAN Gateway firmware and IOS is conducted over IP. Therefore, an IP address must be assigned to the Cisco LoRaWAN Gateway through an IOS local DHCP server pool.

If you connect multiple Cisco LoRaWAN Gateways to a single IR800 router, each interface must have its own DHCP pool.

On the IR800 series, beginning in privileged EXEC mode, follow these steps to configure DHCP pool.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**ip dhcp pool** *pool-name*	Creates a DHCP server address pool and enters DHCP pool configuration mode. **Note** If you have changed the parameters of the DHCP server, you must perform a refresh using the **no service dhcp** *interface-type number* command and **service dhcp** *interface-type number* command.
Step 3	**network** *network-number mask*	Specifies the subnet network number and mask of the DHCP address pool. Make sure to allow only one dhcp address releasable to modem.
Step 4	**`default-router address`**	Specifies the IP address of the default router for a DHCP client. The default router address will be assigned to the associated VLAN interface afterwards.
Step 5	**option 43 hex** *client-ID*	Enables vendor specific option 43 and assign the associated Cisco LoRaWAN Gateway client ID number as the hex value.
Step 6	**dns-server** *address*	Defines DNS services.
Step 7	**exit**	Exits to global configuration mode.
Step 8	**ip dhcp excluded-address** *address*	Masks all redundant addresses including the default router in DHCP pool.
Step 9	**end**	Exits to privileged EXEC mode.
Step 10	**write memory**	Saves the configurations.

Example

The following is an example of configuring DHCP pool on IR809:

```
IR809#configure terminal
IR809(config)#ip dhcp pool modempool
IR809(dhcp-config)#network 192.168.1.0 255.255.255.248
IR809(dhcp-config)#default-router 192.168.1.1
IR809(dhcp-config)#option 43 hex 01
IR809(dhcp-config)#dns-server 192.168.1.1
IR809(dhcp-config)#exit
IR809(config)#
```

```
IR809(config)#ip dhcp excluded-address 192.168.1.1
IR809(config)#ip dhcp excluded-address 192.168.1.3 192.168.1.6
IR809(config)#exit
IR809#
```

The following is an example on IR809 using the sub-interface method:

```
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.3 192.168.1.6
!
ip dhcp pool modempool1
 network 192.168.1.0 255.255.255.248
 default-router 192.168.1.1
 option 43 hex 01
!
interface Virtual-LPWA1
!
interface GigabitEthernet1.101
 encapsulation dot1Q 101 native
 ip address 192.168.1.1 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
!
end
```

The following is an example on IR829 using the VLAN method:

```
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.1.3 192.168.1.6
!
ip dhcp pool modempool1
 network 192.168.1.0 255.255.255.248
 default-router 192.168.1.1
 option 43 hex 01
!
interface Virtual-LPWA1
!
interface GigabitEthernet1
 switchport access vlan 101
!
interface Vlan101
 ip address 192.168.1.1 255.255.255.248
!
end
```

Configuring SNMP TRAP for Modem Notifications

On the IR800 series, beginning in privileged EXEC mode, follow these steps to enable SNMP TRAP notifications for virtual-lpwa interface and its associated Cisco LoRaWAN Gateway.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**snmp-server enable traps vlpwa**	Enables virtual LPWA traps to monitor modem status changing.

	Command or Action	Purpose
Step 3	**snmp-server enable traps snmp linkup linkdown**	Enables linkUp and linkDown traps to monitor modem heartbeat event.
Step 4	**end**	Exits to privileged EXEC mode.
Step 5	**write memory**	Saves the configurations.

What to do next

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

Notification	OID
modem door open/close	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 1 };
modem exceeds maximum temperature threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 2 };
modem temperature returns to normal from overheat	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 3 };
modem falls below minimum temperature threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 4 };
modem temperature returns to normal from undercooling	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 5 };
modem FPGA upgrade starts	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 6 };
modem exceeds maximum CPU threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 7};
modem CPU usage returns to normal	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 8 };
modem exceeds maximum memory threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 9};
modem memory usage returns to normal	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 10 };
modem exceeds maximum storage threshold	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 11};
modem storage usage returns to normal	{ 1, 3, 6, 1, 4, 1, 9, 9, 830, 0, 12 };

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

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

Configuring VLPWA Interface and Associated Cisco LoRaWAN Gateway

On the IR800 series, beginning in privileged EXEC mode, follow these steps to configure one or multiple VLPWA interfaces and associated Cisco LoRaWAN Gateways.

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

Configuring IR809 for One Cisco LoRaWAN Gateway

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface Virtual-LPWA** *vlpwa-id*	Enters the vlpwa interface which is to be configured.
Step 3	**lpwa modem environment** *var1* [*var2*]	Specify the environment variables as the configuration for the LoRaWAN modem. **Note** There are one or two environment variables to be configured.
Step 4	**lpwa packet-forwarder firmware** [**flash:** | **nvram:**] *firmware-name* **auto-install** [*if-not-installed* | *unconditional*]	Configures the packet-forwarder firmware (only Actility LRR is supported) which will be installed on the LoRaWAN modem from the IR800 series. For the values of **auto-install** method: • *if-not-installed* —Automatically install if there is no firmware already installed on modem. • *unconditional* —Automatically install this firmware unconditionally.
Step 5	**lpwa packet-forwarder public-key**[**flash:** | **nvram:**] *public-key file*	Configures the packet-forwarder public-key which will be installed on the LoRaWAN modem from the IR800 series.
Step 6	**end**	Exits to privileged EXEC mode.
Step 7	**write memory**	Saves the configurations.

Example

The following is an example of configuring VLPWA interface on IR809:

```
interface Virtual-LPWA1
no ip address
lpwa packet-forwarder public-key flash:lrr-opk.pubkey
lpwa modem environment PKTFWD_ROOT /tmp/mdm/pktfwd/firmware
lpwa modem environment LXC_STORE_PATH /tmp/mdm/pktfwd/firmware/usr/etc/lrr
lpwa modem password root $1$0822455D0A16
lpwa modem ntp server ip fr.pool.ntp.org
lpwa modem timezone Europe/Paris
```

Configuring Cisco LoRaWAN Gateway Password

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface Virtual-LPWA** *vlpwa-id*	Enters the vlpwa interface which is to be configured.
Step 3	**lpwa modem password** *var1* [*var2*]	Specifies the password variables as the configuration for the LoRaWAN modem. The default account is **root**. **Note** There are one or two environment variables to be configured. But currently only the **root** account is supported.
Step 4	**lpwa modem password root** [*var2*]	Configures the password of the **root** account for LoRaWAN modem. The default password is NULL. The unencrypted (clear text) secret has the minimum length of 4 characters, and the maximum length of 25 characters.
Step 5	**end**	Exits to privileged EXEC mode.
Step 6	**write memory**	Saves the configurations.

Configuring Console Access

Procedure

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

	Command or Action	Purpose
Step 3	**lpwa modem console disable**	Disables the console access.
Step 4	**end**	Exits to privileged EXEC mode.
Step 5	**write memory**	Saves the configurations.

Configuring Clock for the Cisco LoRaWAN Gateway

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

Configuring NTP Server for the Cisco LoRaWAN Gateway

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

Procedure

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

Configuring GPS as the Clock Source

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface Virtual-LPWA** *vlpwa-id*	Enters the vlpwa interface which is to be configured.
Step 3	**lpwa modem clock gpstime**	Use the GPS as the modem clock source.
Step 4	**end**	Exits to privileged EXEC mode.
Step 5	**write memory**	Saves the configurations.

Configuring Cisco LoRaWAN Gateway Timezone

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

Procedure

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

Configuring IPSec on the Cisco LoRaWAN Gateway

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

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

Procedure

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

What to do next

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

Configuring SCEP on the Cisco LoRaWAN Gateway

On the IR800 series, beginning in privileged EXEC mode, use these commands to configure Simple Certificate Enrollment Protocol (SCEP) on the Cisco LoRaWAN Gateway.

Procedure

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

	Command or Action	Purpose

Step 3	Configure SCEP by using a configuration file or profile method. Choose one of the following:
	- **lpwa modem scep** [{**flash:**|**nvram:**} <*SCEP_Configuration_File*>]
	- **lpwa modem scep** [**profile**]
		- To configure by file, enter the SCEP configuration file. This file must be provided with the following formatted:
		`url <SCEP server URL used for enrollment>`
		`country <2 letter country name>`
		`province <Province/State>`
		`locality <Location>`
		`organization <Organization>`
		`unit <Organization Unit>`
		`common-name <Common Name>`
		`type <SCEP server type: NDES>`
		`persistent <Store certificates in modem; default is false>`
		`key-length <Length of keys; 1024, 2048 (default) or 4096>`
		Example:
		`lpwa modem scep flash:scep_conf`
		SCEP Configuration File Example:
		`url http://172.19.234.54:80/certsrv/mscep/mscep.dll`
		`country CN`
		`province Nanning`
		`locality Nanning`
		`organization Cisco`
		`unit iot`
		`common-name cisco-iot`
		`type ndes`
		`persistent false`
		`key-length 1024`
		- To configure the parameters individually, use the profile methord.
		`IR800(config-if)#`**`lpwa modem scep profile`**
		`IR800(config-if-vlpwa-scep)#?`
		`Enter parameters for scep. country, locality, name, org, province, unit & url must all be present.`
		` country       Country server located in`
		` default       Set a command to its defaults`
		` exit          Exit from if-vlpwa-scep sub mode`
		` keylen        Specify key length 1024, 2048 or 4096`
		` locality      Locality of server`
		` name          Name of the certificate`
		` no            Negate a command or set its defaults`
		` organization  Organization of the server`
		` persistent    Specify persistency of the key`

	Command or Action	Purpose

		`province      State or Province`
		`type          Specify type`
		`unit          Business unit within`
		`server`
		`              organization`
		`url           Specify url`
		Note The profile CLI block will only take effect when all parameters are configured. Incomplete parameter set will not be sent to the IXM. Make sure that all parameters in the profile are configured.

Step 4	**end**	Exits to privileged EXEC mode.
Step 5	**write memory**	Saves the configurations.

What to do next

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

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

Configuring Security Protection

On the IR800 series, beginning in privileged EXEC mode, use these commands to configure security protection for the Cisco LoRaWAN Gateway.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal**	Enters global configuration mode.
Step 2	**interface Virtual-LPWA** *vlpwa-id*	Enters the vlpwa interface which is to be configured.
Step 3	**lpwa modem authentication mandatory enable**	Enables mandatory security level in the modem, which is disabled by default. When enabled, IR800 will shut down the corresponding vlan or subinterface for ACT2 authentication failure or version mismatch to prevent further attacking. When disabled, the IR800 will only send notifications to IoT FND when the same

	Command or Action	Purpose
		situations happen, without shutting down vlan or subinterface.
Step 4	**lpwa modem authentication timeout** <*subinterface/vlan name*> <*subinterface/vlan number*> **time** <*time*>	Specifies a timeout protection for a suspended vlpwa interface (one with no traffic up from corresponding vlan or subinterface). You need to set the subinterface or vlan manually with a time (in minute) threshold. If the mandatory security level is also enabled, the corresponding vlan or subinterface will be shut down after the time threshold. If the mandatory security level is disabled, only a notification will be sent to IoT FND.
Step 5	**end**	Exits to privileged EXEC mode.
Step 6	**write memory**	Saves the configurations.

Managing the Cisco LoRaWAN Gateway

On the IR800 series, beginning in privileged EXEC mode, use these commands to manage the Cisco LoRaWAN Gateway.

Note Virtual -lpwa vlpwa-id packet-forwarder install and uninstall at exec level is not supported

Command	Purpose
virtual-lpwa *unit-number* **modem upload pfx** <*url*> **password** <*password*>	Upload files to the LoRaWAN modem: • **normal**—Upload a normal file to the modem. • **pfx**—Upload certification files in pfx format to the modem. Specify the password if any. Specify "N" for no password.
virtual-lpwa *vlpwa-id* [**modem** | **packet-forwarder**]	Management for the LoRaWAN modem virtual-LPWA interface: • **modem**—Manage the modem clock. • **packet-forwarder**—Manage the packet forwarder.

Command	Purpose
virtual-lpwa *vlpwa-id* **modem**[**cacert** | **clock** | **delete** | **install** | **reboot** | **upload**]	Management for the LoRaWAN modem: • **cacert**—Clean the certificates stored in the modem. • **clock**—Manage the modem clock. • **delete**—Delete uploaded file(s) on the modem. • **install**—Install the modem firmware. • **reboot**—Reboot the modem hardware. • **upload**—Upload a file to the modem.
virtual-lpwa *vlpwa-id* **packet-forwarder**[**restart** | **start** | **stop**]	Management for the LoRaWAN modem packet-forwarder: • **restart**—Restart packet-forwarder. • **start**—Start packet-forwarder. • **stop**—Stop packet-forwarder.

virtual-lpwa *vlpwa-id* **modem clock set hh:mm:ss {dd Mon yyyy}**	Management of the clock for the LoRaWAN modem:
	hh:mm:ss:—Current time.
	dd Mon yyyy—Day, month, and year.
	Example:
	`virtual-lpwa`
	`vlpwa-id`
	` modem clock set 20:30:30 31 Mar 2016`

Examples

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

```
IR829#virtual-lpwa 10 modem clock set 12:02:40 15 Apr 2016
Name: Virtual-LPWA 10
```

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

```
IR829#virtual-lpwa 10 modem reboot
Name: Virtual-LPWA 10
Modem reboot initiated.
```

The following is an example of restarting packet-forwarder:

```
IR829#virtual-lpwa 10 packet-forwarder restart
Name: Virtual-LPWA 10
Restarted
```

LoRaWAN Modem Firmware Upgrade

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

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

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

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

Example

- Normal install:

```
IR809#virtual-lpwa 1 modem install firmware normal flash:ixm_mdm_i_k9-1.0.tar.gz
Name: Virtual-LPWA 1
Modem image installed successfully
The modem will reboot in 10 s.
IR809#
```

- TFTP install:

```
IR809(config)#tftp-server flash:ixm_mdm_i_k9-1.0.tar.gz
IR809#virtual-lpwa 1 modem install firmware tftp-normal flash:ixm_mdm_i_k9-1.0.tar.gz
Name: Virtual-LPWA 1
Modem image installed successfully
The modem will reboot in 10 s.
IR809#
```

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

```
IR809(config)#tftp-server flash:ixm_mdm_i_k9-1.0.tar.gz
IR809#virtual-lpwa 1 modem install firmware external-tftp-normal
10.10.10.10:ixm_mdm_i_k9-1.0.tar.gz
Name : Virtual-LPWA 1
Modem image installed successfully
The modem will reboot in 10 s.
IR809#
```

Installing U-boot

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

```
IR829#install firmware factory flash:ixm_mdm_i_k9-1.0.06.tar.gz
{only-uboot|uboot}
  only-uboot  install uboot only
  uboot       install uboot together
  <cr>
```

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

LoRaWAN Gateway FPGA Upgrade

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

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

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

Example

```
IR800#show virtual-lpwa 1 modem info
Name : Virtual-LPWA 1
ModemImageVer : 1.0
BootloaderVer : 20160708_cisco
ModemAgentVer : 1.02
SerialNumber : FOC20133FK0
PID : IXM-LORA-800-H-V2
UTCTime : 00:02:56.492 UTC Sat Aug 06 2016
IPv4Address : 10.20.20.4
IPv6Address : none
FPGAVersion :             ! Blank when FPGA is upgrading
TimeZone : CEST
LocalTime : Sat Aug  6 02:02:56 CEST 2016
ACT2 Authentication : PASS

IR800#show virtual-lpwa 1 modem status
Name : Virtual-LPWA 1
Status : Running
Uptime : 0:04:11.050000
Door : DoorClose
Upgrade Status : Ready  fpga upgrading —14.2%

IR800#show virtual-lpwa 1 modem info | begin IPv6
IPv6Address : none
FPGAVersion : 48           ! Correct FPGA version is displayed when upgrade is complete
TimeZone : CEST
LocalTime : Sat Aug 6 02:32:23 CEST 2016
ACT2 Authentication : PASS
IR809#
```

Uploading a File to the LoRaWAN Gateway

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

Example

```
IR829# virtual-lpwa 1 modem upload flash:lgwx8_us920.ini
Name : Virtual-LPWA 1
Uploaded successfully
```

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

```
IR809#configure terminal
IR809(config)#interface virtual-LPWA 1
IR809(config-if)#lpwa modem environment PKTFWD_ROOT /tmp/mdm/pktfwd/firmware/
IR809(config-if)#lpwa modem environment LXC_STORE_PATH /tmp/mdm/pktfwd/firmware/usr/etc/lrr
IR809(config-if)#exit
```

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

```
IR829# show virtual-lpwa 1 modem uploads
Name : Virtual-LPWA 1
Current folder: '/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr'
_parameters.sh
_system.sh
autoreboot_last
channels.ini
custom.ini
lgw.ini
lrr.ini
sysconfig_done

IR829# show virtual-lpwa 1 modem uploads detail
Name : Virtual-LPWA 1
Current folder: '/mnt/container/rootfs/tmp/mdm/pktfwd/firmware/usr/etc/lrr'
total 32
-rw-r--r-- 1 root root 143 Aug 11 20:26 _parameters.sh
-rw-r--r-- 1 root root 20 Aug 11 20:26 _system.sh
-rw-r--r-- 1 root root 0 Aug 16 09:33 autoreboot_last
-rw-rw-r-- 1 sshd sshd 2000 Aug 5 16:15 channels.ini
-rw-rw-r-- 1 sshd sshd 275 Aug 5 15:35 custom.ini
-rw-rw-r-- 1 sshd sshd 1576 Aug 5 16:18 lgw.ini
-rwxrwxr-x 1 sshd sshd 8017 Aug 24 13:53 lrr.ini
-rw-r--r-- 1 root root 29 Aug 11 20:26 sysconfig_done
IR829#
```

Monitoring the LoRaWAN Gateway

On the IR800 series, beginning in privileged EXEC mode, use these commands to monitor the Cisco LoRaWAN Gateway.

Command	Purpose
show virtual-lpwa *vlpwa-id* **modem**[**gps** | **info** | **ipsec** | **led** | **log** | **statistics** | **status** | **uploads**]	Displays the information of the LoRaWAN modem: • **gps**—Displays modem GPS information. • **info**—Displays modem information. • **ipsec**—Displays modem IPSec status and detailed information. • **led**—Displays modem LED information. • **log**—Displays modem logs. • **statistics**—Displays modem statistics. • **status**—Displays modem status. • **uploads**—Lists uploaded files.
show virtual-lpwa *vlpwa-id* **packet-forwarder** [**info** | **log** | **status**]	Displays the information of the LoRaWAN modem packet-forwarder software: • **info**—Displays packet-forwarder information. • **log**—Displays packet-forwarder logs. • **status**—Displays packet-forwarder status.

Examples

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

```
IR829# show virtual-lpwa 4 modem info
Name : Virtual-LPWA 4
ModemImageVer : 1.0.20
BootloaderVer : 20160830_cisco
ModemAgentVer : 1.02
SerialNumber : FOC20522TRZ
PID : IXM-LPWA-900-16-K9
UTCTime : 22:51:15.493 UTC Mon Feb 27 2017
IPv4Address : 192.168.4.2
IPv6Address : none
FPGAVersion : 58
TimeZone : UTC
LocalTime : Mon Feb 27 22:51:15 UTC 2017
ACT2 Authentication : PASS
ModemVersionID : V01
ProtocolVersion : 2
ChipID : LSB = 0x2876fd04 MSB = 0x00f1400e
LoRaSerialNumber : FOC20522TUV
LoRaCalc :
<NA,NA,NA,56,38,111,102,94,85,77,69,59,50,40,31,22-NA,NA,NA,55,37,110,101,93,84,76,68,58,49,39,30,21>
CalTempCelsius : 34
CalTempCodeAD9361 : 91
RSSIOffset : -204.00,-204.00
-202.00,-202.00
AESKey : 1E5E364646EC3C3927F234FA8E200B3C
```

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

```
IR829# show virtual-lpwa 3 modem log ?
  list  Modem log list
  name  Modem log name

IR829# show virtual-lpwa 3 modem log list
Name : Virtual-LPWA 3
==========================================
dmesg           Modem kernel activity log
mdmagent        Modem agent log
messages        Modem system activity log
ipsec           Modem IPSec status log
gps             Modem GPS status log
certs           Modem Certificates log

IR829# show virtual-lpwa 3 modem log name certs
Name : Virtual-LPWA 3
==========================================
Certificate
  Serial Number: 303e7714000000000078
  Certificate Usage: Digital Signature, Key Encipherment
  Issuer: DC=com, DC=example, DC=LASSI, CN=LASSI-ROOT-CA
  Subject: C=CN, ST=Nanning, L=Nanning, O=Cisco, OU=iot, CN=cisco-iot
  CRL Distribution Points:
ldap:///CN=LASSI-ROOT-CA,CN=win-jg39jcs57o7,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=LASSI,

      DC=example,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint
  Validity Date:
    Not Before: Mar 29 17:35:17 2017 GMT
    Not After : Mar 29 17:45:17 2019 GMT
CA Certificate
  Serial Number: 4371ebdb781925be4b638ed1c5ca523c
  Certificate Usage: Digital Signature, Certificate Sign, CRL Sign
  Issuer: DC=com, DC=example, DC=LASSI, CN=LASSI-ROOT-CA
  Subject: DC=com, DC=example, DC=LASSI, CN=LASSI-ROOT-CA
  Validity Date:
    Not Before: Dec  2 21:34:38 2016 GMT
    Not After : Dec  2 21:44:38 2021 GMT

IR829#show virtual-lpwa 10 modem log name dmesg
Name: Virtual-LPWA 10
==========================================
2016-06-03T07:21:23+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T07:32:26+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T07:43:29+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T07:54:32+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:05:35+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:16:38+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:27:41+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:38:44+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T08:49:47+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
2016-06-03T09:00:50+08:00 lorawan kernel: ttyS1: 1 input overrun(s)
```

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

```
IR829#show virtual-lpwa 10 modem statistics
Name: Virtual-LPWA 10
Load Average: 0.00 0.04 0.05
Memory Usage: 0.22
Flash Usage: sys:0.03 app:0.04
```

```
Temperature: 44.5 C
```

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

```
IR829#show virtual-lpwa 10 modem status
Name: Virtual-LPWA 10
Status: Running
Uptime: 13:40:37.500000
Door: DoorClose
Upgrade Status: Ready
```

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

```
IR829#show virtual-lpwa 1 packet-forwarder info
Name : Virtual-LPWA 1
PublicKeyStatus : Installed
FirmwareStatus : Installed
PacketFwdVersion : 1.8.15
LRRID : 68ba477e
PartnerID : 0001
```

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

```
IR829#show virtual-lpwa 10 packet-forwarder status
Name: Virtual-LPWA 10
Status: Running
```

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

```
IR829#show virtual-lpwa 10 packet-forwarder log list
Name: Virtual-LPWA 10
==========================================
lrr.ini      lrr.ini information
config       Get the detail config
radio        Radio status
trace        LRR Trace log
```

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

```
IR829#show virtual-lpwa 10 packet-forwarder log name trace
Name: Virtual-LPWA 10
==========================================
05:51:35.464  (6196) [../xlap.c:726] TCP Disconnected on RTU(0x7e7b0,lrc7.thingpark.com,2404)
 fd=7 conn=1 'connection closed (eot)'
05:51:35.464  (6196) [../main.c:2299] LAP LRC DISC (2648)
05:51:35.465  (6196) [../xlap.c:553] Lap reset partial on RTU(0x7e7b0,lrc7.thingpark.com,2404)
 outq=0 ackq=3
05:51:37.405  (6196) [../xlap.c:1492] keep DNS resolution 'lrc7.thingpark.com' =>
'51.255.52.229'
05:51:37.405  (6196) [../xlap.c:1614] connect in progress on
RTU(0x7e7b0,lrc7.thingpark.com,2404) fd=7
05:51:37.405  (6196) [../xlap.c:784] CB_LapRequest(0x7e7b0,lrc7.thingpark.com,2404) fd=7
conn=0 events=0 connect progress
05:51:37.756  (6196) [../xlap.c:1139] connect accepted on RTU(0x7e7b0,lrc7.thingpark.com,2404)
```

```
 fd=7
05:51:37.756  (6196) [../xlap.c:1397] (0x7e7b0,lrc7.thingpark.com,2404) from st='SSP_INIT'to
 st='SSP_STOPPED'(1000->2000)
05:51:37.756  (6196) [../main.c:2294] LAP LRC CNX
05:51:37.756  (6196) [../main.c:2075] LAP LRC TCP KEEPALIVE HIGH lrc=-1 fd=7 alive=1 idle=5
 intvl=5 cnt=20
```

Monitoring LED Status

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

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

```
IR829#show virtual-lpwa 1 modem led
Name : Virtual-LPWA 1
LED1  : GREEN ON, Solid
LED2  : OFF !Future use
```

Checking Connectivity

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

```
IR829#show ip nat translation
Pro Inside global Inside local Outside local Outside global
icmp 192.168.0.2:3348 10.16.16.3:3348 217.69.25.85:3348 217.69.25.85:3348
tcp 192.168.0.2:49901 10.16.16.3:49901 217.69.25.85:2404 217.69.25.85:2404
IR829#
```

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

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

Debugging the LoRaWAN Gateway

On the IR800 series, beginning in privileged EXEC mode, use these commands to debug the Cisco LoRaWAN Gateway.

Command	Purpose
debug vlpwa all	Enables all vlpwa debug messages.
undebug vlpwa all	Disables all vlpwa debug messages.

Command	Purpose
debug vlpwa [**decode** | **detail** | **errors** | **memory** | **raw** | **registry** | **session** | **timers** | **trace**]	Enables the following vlpwa debug messages: • **decode**—Decoded packet information. • **detail**—Detailed trace information. • **errors**—Errors. • **memory**—Memory information. • **raw**—Raw packet information. • **registry**—Registry information. • **session**—Session information. • **timers**—Timers information. • **trace**—Trace information.

CHAPTER 6

Alarms

This chapter provides instructions for configuring the alarms on the IR809. The IR829 does not have an alarm port.

Finding Feature Information

Your software release may not support all the features documented in this chapter. For the latest feature information and caveats, see the release notes for your platform and software release.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to:

http://www.cisco.com/go/cfn.

An account on Cisco.com is not required.

Information About Alarms

If the conditions present on the IR809 do not match the set parameters, the IR809 software triggers an alarm or a system message. By default, the IR809 software sends the system messages to a system message logging facility, or a syslog facility. You can also configure the IR809 to send Simple Network Management Protocol (SNMP) traps to an SNMP server.

Alarm Port

The Cisco IR800 has alarm ports as shown in Cisco IR809 Front Panel. Additional details and instructions about connecting the alarm ports are found in the IR809 Hardware Configuration Guide and the Getting Started and Product Document of Compliance for the Cisco IR809 Integrated Services Router.

Alarm Conditions

There are two conditions that generate an alarm:

- If the alarm is connected to a door switch or an enclosure and detects a door opening.
  - This is an external alarm and requires wiring. See the IR809 Hardware Installation Guide.
- When the internal temperature is too high.
  - This is an internal alarm, no wiring required.

Note Prior to IOS 15.6(1)T, the default thresholds were set too low: minor alarm if exceeding 60°C, or major alarm if exceeding 75°C or too low of a cold temperature threshold, less than -25°C. After IOS 15.6(1)T, the default values were changed to 84C (Minor) and 93C (Major) .

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

SNMP Traps

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

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

Syslog Messages

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

Configuration Commands

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

To configure and show alarms on the IR809, use the Command Line Interface (CLI).

Command	Purpose
configure terminal	Enters global configuration mode.
alarm contact *contact-number* **description** *string*	(Optional) Configures a description for the alarm contact number. • The *contact-number* value is from 1 to 4. • The description string is up to 80 alphanumeric characters in length and is included in any generated system messages.

Command	Purpose
alarm contact {*contact-number* | **all**} {**severity critical** | **major** | **minor** | **none**} | **trigger closed** | **open**}}	Configures the trigger and severity for an alarm contact number or for all contact numbers. • Enter a contact number (1 to 4) or specify that you are configuring **all** alarms. • For **severity**, enter **critical, major**, **minor** or **none**. If you do not configure a severity, the default is **minor**. • For **trigger**, enter **open** or **closed**. If you do not configure a trigger, the alarm is triggered when the circuit is **closed**.
end	Returns to privileged EXEC mode.
show env alarm-contact	Shows the configured alarm contacts.
copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuration Examples

Configure an alarm.

```
IR809#conf term
Enter configuration commands, one per line.  End with CNTL/Z.

IR809(config)#alarm-contact 1 description
Your Descriptive Text Here

IR809(config)#alarm-contact 1 severity critical

IR809(config)#alarm-contact 1 trigger closed

IR809#
```

To show the alarm status:

```
IR809#show environment alarm-contact ! No Alarm Present
ALARM CONTACT
   Status:      Not Asserted
   Description: Test Input Alarm
   Severity:    Critical
   Trigger:     Closed
```

Example of an alarm being generated:

```
IR809# !
*Nov 27 14:54:52.573: %IR800_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_ASSERT: External alarm
 asserted, Severity: Critical
```

To show the alarm status during an event:

```
IR809#show environment alarm-contact
ALARM CONTACT
   Status:      Asserted
   Description: Test Input Alarm
   Severity:    Critical
   Trigger:     Closed
```

Example of an alarm being cleared:

```
IR809# !
*Nov 27 14:55:02.573: %IR800_ALARM_CONTACT-0-EXTERNAL_ALARM_CONTACT_CLEAR: External alarm
cleared
IR809#
```

Note With IOS version 15.6(1)T, the **show platform led** command does not provide the ALM led status.

Enabling SNMP Traps

Procedure

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

MIBs

To locate and download MIBs using Cisco IOS software, use the Cisco MIB Locator found at the following URL and choose a platform under the Cisco Access Products menu: https://mibs.cloudapps.cisco.com/ITDIT/MIBS/servlet/index

CHAPTER 7

Guest Operating System (Guest OS) Installation and Configuration

This chapter details Guest Operating System (Guest OS) installation for the Cisco IR800.

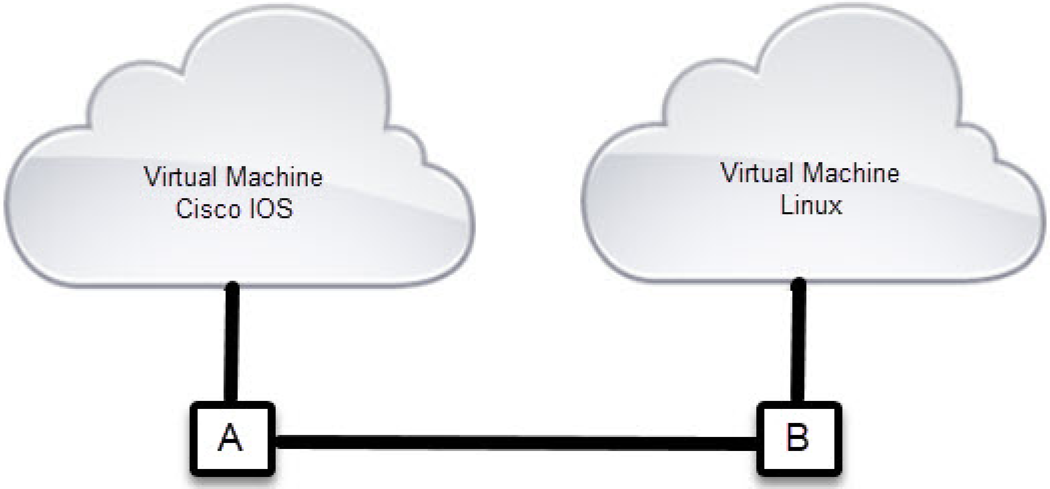
Guest Operating System Overview

The IR800 supports a Hypervisor architecture to support user-specified operating systems within an independent Virtual Machine (VM).

When you install the IR800 IOS software bundle (image) on the router, the image automatically installs the supported Guest OS (Cisco IOS and Linux OS) instance(s). You can use the Linux Guest OS running on a VM on the IR800 to run applications.

The following example shows connectivity of Guest OS and Cisco IOS. A virtual interface managed by Cisco IOS provides network connectivity to Guest OS. Cisco IOS forwards traffic from Guest OS through regular IP forwarding mechanisms.

Figure 13: Connectivity Between Cisco IOS and Guest OS



In this example, A is the interface being used on the router and B is the interface on the Linux OS.

For the Cisco IR809, A is Gigabit Ethernet 2 and B is Eth 0.

For the Cisco IR829, A is Gigabit Ethernet 5 and B is Eth 0

Additionally, the Virtual Machine Linux has a virtual console, and two virtual serial ports.

Prerequisites

Router must be running Cisco IOS 15.6(2)T or higher.

Note The IOXVM image delivered in the IOS bundle may not be the most recent. Check Cisco.com for the latest version.

Guidelines and Limitations

Note Per CDET CSCvh65331, running excessive traffic from an external host to the Guest OS on the IR800 can cause a system hang. Removing the traffic will recover the console access. Apply qos policies to rate-limit traffic to ensure IOS CPU <65%.

- The bundled Guest OS delivered with the latest IOS version, and is based on Yocto Linux Project Reference Distro, with basic services enabled:
  - IPv4/IPv6
  - DHCP
  - NTP
  - AAA (Radius)
  - Python
  - Basic debugging tools (tcpdump, top, etc)
  - bash
- Serial relay for Guest OS control of the Serial Interface
  - Async 0 and Async 1 respectively reserve line 1/5 and 1/6 to relay serial data to the corresponding Guest OS /dev/ttyS1 and /dev/ttyS2

Note Prior to 15.6(3)M, Serial Interface parameters needed to be set through IOS. 15.6(3)M allows setting the parameters directly from the Guest OS, through standard Linux commands.

- You must configure Cisco IOS to provide Guest OS connectivity.

Note There is an IOXVM image more recent than IOS bundle, (IOXVM 1.0.4) available on Cisco.com

Default Settings

The bundled Linux Guest OS:

- Uses DHCP to acquire the IPv4 address.
- Does not have a default root password.
- Uses IPv6 stateless auto-configuration to get an IPv6 address.

Note Without an IPv6 address set on both GXX and ETH0, the Guest OS will never get displayed as registered under show iox host list detail. GXX is defined as GI5 on the IR829 and GI2 on the IR809.

Installation and Upgrade

By default, IR800s ship with a software bundle that includes the latest versions of all of the required images such as Cisco IOS, Guest OS, and Hypervisor.

Note Before performing a bundle installation, shutdown the Guest OS. Performing a bundle installation on a device with an active Guest OS may result in it not functioning upon reboot.

Use the following procedure to upgrade your router to the latest software bundle. It can take several minutes for the router to upgrade and install all of the images (Hypervisor, Cisco IOS, and Guest OS).

DETAILED STEPS

Procedure

Step 1 Copy the bundle image to the IR800 IOS flash partition using scp or sftp.

Example bundle name: **ir800-universalk9-bundle.SPA.**<*VERSION*>

Step 2 Enter the following commands at the IR800 prompt:

Command	Purpose
bundle install flash: <*bundle name*>**.CG**	Installs the specified bundle.
copy running-config startup-config	Saves the current running configuration.
reload	Reloads the router.

Improvements in IOS and Guest-OS Clock Time Synchronization

In Cisco IOS releases prior to 15.8(3)M, the Guest-OS clock would synchronize with the IOS clock every 30 seconds. Now with IOS 15.8(3)M and beyond, the synchronize time is 1 second. No user configuration is required to initiate Guest-OS clock synchronization or to modify the clock settings.

IOS can be configured to synchronize to an external NTP server and the Guest-OS will sync with IOS. Additionally, the Guest-OS hardware clock time (hwclock) will be in sync with the Guest-OS (IOx) system time.

The following example shows the Guest-OS system clock and Guest-OS hwclock outputs taken at the same time:

IOS clock time:

```
IR800#show clock
08:11:18.498 UTC Mon May 7 2018
```

Guest-OS(IOX) system time and hardware time

```
IR800-GOS-1:~# date
Mon May  7 08:11:18 UTC 2018
IR800-GOS-1:~# hwclock
Mon May 7 08:11:18 2018  0.000000 seconds
```

Configuring Cisco IOS

This section describes how to configure the Cisco IOS VM to provide network connectivity to the Guest OS VM.

Guest OS connects to the network through a virtual Network Interface Card (VNIC) provided by the Hypervisor. Network attributes such as IP address, Default gateway, DNS server (as shown in the Configuring DHCP Pool, on page 118 section) on the interface are statically configured or configured for DHCP to dynamically obtain IP addresses. Guest OS network connectivity is only through Cisco IOS, using the virtual network interface provided by the Hypervisor. Network attributes such as IP address, can be configured statistically or dynamically, and are obtained from Cisco IOS using DHCP requests. The bundled Linux Guest OS is configured to use DHCP.

This section outlines the task to configure a Cisco IOS DHCP pool to provision the Linux Guest OS with an IP address, and an external Ethernet interface in Cisco IOS to allow the Guest OS network connectivity.

This section includes the following topics:

Configuring the IR800 Ethernet Interface

You must enable one of the external Ethernet interfaces on the IR800 to provide network connectivity.

Note The QoS Input Service Policy can only be configured on the WAN interface, not on the SVI interface.

Note The IR809 uses Gigabit Ethernet 2, and the IR829 uses Gigabit Ethernet 5.

IPv6 Gigabit Ethernet

On Guest OS, IPv6 is enabled by default. The following example configuration uses IPv6 on Guest OS, where Guest OS is automatically assigned an IPv6 address on the Cisco IOS interface GigabitEthernet 5.

Command	Purpose
ipv6 unicast-routing	Enables unicast routing.

Command	Purpose
ipv6 cef	Enables cef.
interface GigabitEthernet 5	Set the internal virtual interface that connects to the Linux Guest OS.
ipv6 address autoconfig	Sets the IPv6 address.
ipv6 enable	Enables IPv6.

Enabling IPv4 Gigabit Ethernet

Note Configuring an IPv4 address on a Gigabit port is not a required part of configuring the Guest OS. However, IOS interfaces must be set to enable external devices to communicate with the Guest-OS through IOS.

To enable an external Gigabit Ethernet IPv4 interface on the IR800 to provide network connectivity, enter the following commands:

Command	Purpose
config terminal	Enters global configuration mode.
interface gig 0	Configures an IPv4 address on Gigabit Ethernet interface 0, and enters interface configuration mode.
ip address 10.1.2.1 255.255.255.0	Sets the IP address and subnet mask for Gigabit Ethernet interface 0.
no shutdown	Enables the Gigabit Ethernet interface.

Configuring DHCP Pool

To configure a local DHCP pool, enter the following commands, one per line:

Note The subnet used for the local DHCP pool must be reachable externally. If you cannot allocate the whole subnet to Guest OS, use a NAT-based configuration. See Configuring Network Address Translation (NAT), on page 123.

Command	Purpose
config terminal	Enters global configuration mode.
ip dhcp pool gospool	Names the local DHCP pool.
network 10.1.2.0 255.255.255.0	Sets the network address.
default-router 10.1.2.1	Sets the router address.

Command	Purpose
domain-name utility.com	Sets the subnet address.
dns-server 10.1.1.1	Sets the DNS server address.
lease 5	Sets the duration of the IP address lease to five days.

Configuring Guest OS GigabitEthernet on Cisco IOS

The Guest OS Ethernet port (eth0) connects to a GigabitEthernet interface on Cisco IOS. The IR829 uses GigabitEthernet 5, and the IR809 uses GigabitEthernet 2.

To configure the GigabitEthernet interface with the default gateway address of the DHCP pool, enter the following commands:

Note IPv6 must always be enabled on the GigabitEthernet interface.

Note The IR809 uses Gigabit Ethernet 2, and the IR829 uses Gigabit Ethernet 5.

Command	Purpose
interface GigabitEthernet 5	Sets the internal virtual interface that connects to the Linux Guest OS.
ipv6 enable	Enables IPv6.
ipv6 address autoconfig	Sets the IPv6 address.
ipv4 address 10.1.2.1 255.255.255.0	Sets the IPv4 address.
no shutdown	Enables the Ethernet interface, changing its state from administratively down to administratively up.

Configuring Guest OS

This section describes Guest OS Configuration.

Starting Guest OS

The Guest OS starts after installation.

Command	Purpose
show iox host list detail	Displays OS: RUNNING if Guest OS is already running.

Command	Purpose
guest-os 1 start	Starts Guest OS.

During start up, Guest OS sends a DHCP request and is assigned an IP address from the local DHCP pool and an IPv6 address through IPv6 stateless auto-configuration. Guest OS is then configured with a hostname and sync time from IOS.

Note It can take a few minutes for the Guest OS to start.

Guest OS persistent logging through reload

Log files related to the Guest OS file system are stored on the /var/log directory of IOx. This is a volatile location because they may be lost when the IOS or IOx receives a reload command. for this reason, the caf.log, daemon.log, tpmc.log and syslog files from /var/log are now moved to a persistent storage location under /software/downloads (i.e. /dev/sdb filesystem) and the data in it will be restored upon multiple reloads. On reinstallation, the files under /software/downloads will be removed.

The command is persistent across IOS reloads unless a new GOS image is loaded or a bundle install to the new GOS image.

Additional CLIs are available for persistent logging:

- To enable persistent logging from IOS use following command:

  IR800# **iox host exec enable_persistent_logging <*GOS*>**

- To enable persistent logging from IOS use following command:

  IR800# **iox host exec disable_persistent_logging <*GOS*>**

- •To enable persistent logging from Guest-OS use following command:

  IR800-GOS:/etc/scripts# ./enable_persistent_logging

- •To disable persistent logging from Guest-OS use following command:

  IR800-GOS:/etc/scripts# ./disable_persistent_logging

Guest OS file system corruption detection and recovery

The Guest OS running on the IR800 series have had a higher likelihood for file system corruptions after an abrupt power failure. Upon Guest OS start or restart, a mandatory FSCK is performed on the rootfs and the datafs in order to attempt file system recovery.

This feature can be enabled or disabled using the config command **iox recovery-enable <*timeout*>**, where timeout specifies the TPMS timer timeout value in minutes. If unspecified, the default value is 5 and maximum is 15. If no registration request is received from TPMC before the timer expires, the Guest OS will be reinstalled. By default, the feature is disabled so that the customers who do not use Guest OS will not run into a situation where the Guest OS is reinstalled because networking is not configured correctly for Guest OS. The command is persistent across IOS reloads.

IOXVM Graceful Shutdown

On the IR800 router, the Guest OS will now perform a graceful shutdown before a reload of the device. Previously, the GOS would not go through the shutdown command, which sometimes would result in unexpected behavior.

Logrotate of IR8x9 Guest-OS logs

The logrotate feature has been uniformly implemented across all logs in the Guest-OS /var/log path. If persistent-logging is enabled, the specific logs will be saved on /software/downloads and logrotate is implemented on those as well. By default, log-rotate takes effect every day at 7:30am.

IOx Radius authentication

This feature allows for enabling the AAA login to IOx applications. There are different options:

- If your device shows no aaa new-model in the configuration, it will use local authentication.
- If your device shows aaa new-model in the configuration, there are two different methods of authentication.
  - If your device shows no iox aaa authentication in the configuration, it will use the default authentication list, for example: "aaa authentication login default..."
  - If your device shows iox aaa authentication WORD in the configuration, it will use the newly created list/group you specify.
  - To create a login authentication group/list, use aaa authentication login WORD. Then specify the name to use for IOX authentication using iox aaa authentication WORD For example

There is a condition in authentication that may case some confusion. The following provides more details:

Scenario: When a user enables a separate AAA Radius server to authenticate and authorize Guest-OS, instead of using local login.

Observation: In such a scenario, when a privilege 15 user logs into the Guest-OS console port 2070 from within IOS, the first login request is for the IOS username/password . The second login prompt is for the AAA Radius credential specific to Guest-OS.

Note Users will need to configure the aaa iox username in IOS.

```
IR800# show run | inc aaa
aaa new-model
aaa authentication login default local
aaa authentication login ioxList group radius local <-implies 1st preference radius, 2nd
preference: local login
aaa session-id common
iox aaa authentication ioxList <-to apply the newly created list above
```

IOXVM Storage Partition Enhancement

This enhancement to the IR800 series is to provide more flexibility to provide a customizable disk partitioning. With a smaller partition for system files, the user can put larger applications in the remaining partition.

A new CLI is introduced for this purpose:

```
IR829# guest-os 1 ?
disk-repartition Guest OS disk repartition
image Guest OS bootable image
restart Restart Guest OS
start Start Guest OS
stop Stop Guest OS
```

```
IR829# guest-os 1 disk-repartition ?
<30-90> Percentage Guest OS system partition takes
```

The user can input a number between 30 and 90 which would be rounded up to multiples of 5.

For example, typing in 30 means the system partition would take 30% of total space.

IOS communicates with VDS, which will actually perform disk repartition for GOS. After the action is completed by VDS, VDS will send a notification message back to IOS to indicate the status of operation.

After the disk repartitioning, the user will need to reinstall the GOS.

```
IR829# guest-os 1 disk-repartition 1
WARNING - Running this command will delete all application data in IOx. This operation
cannot be undone. Continue? [no]: yes
Guest-OS disk repartitioning with option 1............................... Done!
```

After the repartition is successful, you should see the following syslog message:

```
%IR800_GOS_DISK_REP-6-SUCCESS_GOS_OPERATION: Successfully performed DISK REPARTITION operation
 for GOS.
```

After the disk is repartitioned, the GOS needs to be reinstalled by one of two methods:

```
IR800# bundle install flash:ir800-universalk9-bundle.SSA.156-3.M1 exclude HV-IOS
-or
IR800# guest-os install flash:ir800-ref-gos.img.1.40.gz
```

Finally, manually restart the GOS.

```
IR800# guest-os 1 start
```

If you have an IR809 or IR829 that was originally configured with an IOS version before 15.6(3)M1, then the GOS was partitioned in a different manner than later releases. For example:

- If the router was initially booted up (first time power up) with an image **older than** 15.6(3)M1b, then the GOS is partitioned the old way with: disk1 (1530 MB) and the rest is disk2 (800 MB)
- If the router was initially booted up (first time power up) with an image **at 15.6(3)M1b or newer**, then the GOS is initially partitioned with profile 1: disk 1 (500MB) and the rest is disk2 (1800 MB)

In either case, once the router is running 15.6(3)M1b or newer, you can use the following CLI to repartition it with different options:

```
IR800# guest-os 1 disk-repartition ?
1  disk1: 500MB vs disk2: 1800MB
2  disk1: 700MB vs disk2: 1600MB
3  disk1: 900MB vs disk2: 1400MB
4  disk1: 1100MB vs disk2: 1200MB
5  disk1: 1300MB vs disk2: 1000MB
6  disk1: 1500MB vs disk2: 800MB
7  disk1: 1700MB vs disk2: 600MB
```

(Note: Actual storage available for apps will be less than the value chosen for disk2 for all profiles.)

Configuring Network Address Translation (NAT)

The following example configuration uses NAT for Guest OS network connectivity, where:

- 10.1.1.0 is the externally reachable subnet.
- 10.1.1.131 is the external IP address made available for Guest OS access.
- 192.168.1.0 is the private subnet created for Guest OS to Cisco IOS connectivity. This is not directly reachable outside the IR800.
- The IP address acquired by Guest OS through IOS local DHCP pool is 192.168.1.2. This address can be obtained using **show iox host list details** command from IOS.

Note This example shows outgoing communications. For incoming communications, proper port mapping will be required.

```
ip dhcp pool gospool
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
 domain-name utility.com
 dns-server 10.1.1.1
 lease 5
interface gig 5
 ip nat inside
 ip address 192.168.1.1 255.255.255.0
 ipv6 enable
 no shutdown

interface gig 0
 ip nat outside
 ip address 10.1.1.5 255.255.255.0
 no shutdown
ip nat inside source static 192.168.1.2 10.1.1.131
! End of configuration

IR800#sh ip nat trans
Pro Inside global Inside local  Outside local  Outside global
tcp 10.1.1.131:22 192.168.1.2:22  10.1.1.3:53649 10.1.1.3:53649
tcp 10.1.1.131:60100 192.168.1.2:60100 10.1.1.3:22   10.1.1.3:22
--- 10.1.1.131  192.168.1.2   ---      ---
```

For more information about NAT, please see the Configuring Network Address Translation: Getting Started Guide.

http://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/13772-12.html

IR800 Guest-OS USB Access from IOS

IR800 IOS releases don’t support an external USB storage directly accessible from IOS. However, USB as external storage is provided as an option during IOx application deployment from Local Manager or Fog Director.

P

New for IOS 15.6(1)T

Guest OS enhancements include:

- Cisco distribution is based on Yocto Project 1.8 Reference Distro, with basic services enabled:
    - IPv4/IPv6
    - DHCP
    - NTP
    - AAA (Radius)
    - Python 2.7
    - Basic debugging tools (tcpdump, top, etc)
    - bash
- Serial relay for Guest OS control of the Serial Interface
    - Async 0 and Async 1 respectively reserve line 1/5 and 1/6 to relay serial data to the corresponding Guest OS /dev/ttyS1 and /dev/ttyS2

New for IOS 15.6(3)M

Guest OS enhancements include:

USB Support

Previous to 15.6(3)M, the USB devices, which are connected to external USB port could be emulated on the Guest OS through OHCI mode only. With this feature Hypervisor will be enhanced to support EHCI emulation to Guest OS.

Serial Device Configuration

Previously, the Guest OS could not configure the physical serial port on the device. The serial port configuration (e.g. baud rate change) of the serial port needed to be done in IOS.

With 15.6(3)M, hypervisor and IOS are enhanced so that if the Guest OS changes the virtual serial port configuration, it notifies IOS, and IOS applies the configuration to the physical serial port.

Command line changes consist of the following:

- A new option is appended to allow the baudrate, databits, stopbits and parity propagation from Guest OS. If "propagation" is present, the control parameters will be passed from Guest OS to IOS physical port. Otherwise it functions as before.
- The serial port control parameters included in the propagation are: baudrate, databits, stopbits and parity.

```
relay line <linex> <liney> [propagation]
```

Serial Relay Configuration

```
IR800#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#inter asyn 0
IR800(config-if)# encap relay-line
IR800(config-if)# end
IR800(config)# line 1
IR800(config-line)# transport input all
IR800(config-line)#
IR800(config)# relay line 1 1/5 propagation
IR800# show line 1/5
Guest OS output for /dev/tty
```

GOS is installed through the IOX bundle install process and can be started/stopped and upgraded from IOS CLI

Verification for digitally-signed GOS image distributed via Cisco DevNet must be installed using the guest-os image install command only.

Memory Allocation Optimization

Improvements have been made in the memory allocation optimization between VDS, IOS and GOS on the IR800. Previously, the 2GB RAM was allocated as follows:

- VDS: 512MB
- IOS: 512MB
- Guest OS: 725MB
- Remainder: used by hypervisor (e.g. device share memory)

Now with optimization, the VDS memory was reduced to give at least 1GB to the Guest OS.

New for IOS 15.7(3)M

Guest OS enhancements include:

- IOx Radius authentication

  This feature allows for enabling the AAA login to IOx applications

- IOx IPv6 Networking Option

  IOx interfaces on IOS now support IPv6 addressing. See the IOx documentation for further information.

  https://developer.cisco.com/docs/iox/
- Guest OS persistent logging through reload

  Log files related to the Guest OS file system are stored on the /var/log directory of IOx. This is a volatile location because they may be lost when the IOS or IOx receives a reload command. for this reason, the caf.log, daemon.log, tpmc.log and syslog files from /var/log are now moved to a persistent storage location under /software/downloads (i.e. /dev/sdb filesystem) and the data in it will be restored upon multiple reloads. On reinstallation, the files under /software/downloads will be removed.

- Guest OS file system corruption detection and recovery

The Guest OS running on the IR800 series have had a higher likelihood for file system corruptions after an abrupt power failure. Now, upon Guest OS start or restart, a mandatory FSCK is performed on the rootfs and the datafs in order to attempt file system recovery.

- IOS APIs to Enable Native IOx Applications

Note The IOx Host Device Management service package needs to be installed for this feature to work.

A new configuration command, **hdm-enable**, has been added in this release to enable the Host Device Management service.

```
ir829-01(config)#iox ?
  aaa               IOX AAA options
  client            Configure iox client
  hdm-enable        Enable IOX Host Device Management(HDM) service
  hypervisor        Configure hypervisor policy
  recovery-enable   Set Guest OS image recovery
```

For more information on IOx, please visit:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html

Troubleshooting

To determine common causes of configuration failure, enter the following commands:

Command	Purpose
show ip arp	Verifies that Cisco IOS learned Guest OS ARP mapping.The following is example output:

`Protocol Address Age (min) Hardware Addr Type Interface`
`Internet 10.1.1.1 - 0022.bdef.c562 ARPA GigabitEthernet0`
`Internet 10.1.2.1 - 0022.bdef.c569 ARPA GigabitEthernet2`
`Internet 10.1.2.2 112 0022.bdef.c56d ARPA GigabitEthernet2`
`IR800#`	

show ipv6 neighbor	Verifies that Cisco IOS learned Guest OS IPv6 neighbor address.The following is example output:

`IPv6 Address    Age Link-layer Addr State Interface`
`FE80::1FF:FE90:8B05    0 0200.0190.8b05  REACH Gi2`	

show platform guest-os	Guest-OS started

`Guest OS status:`
`Installation: Cisco-GOS,version-1.28`
`State: RUNNING`
`IR800#`	

Command	Purpose
show iox host list detail	Guest-OS started, normal operation

```
IOX Server is running. Process ID: 319
Count of hosts registered: 1
Host registered:
===============
    IOX Server Address: FE80::76A2:E6FF:FEFD:6A6C; Port: 22222
    Link Local Address of Host: FE80::1FF:FE90:8B05
    IPV4 Address of Host:       10.15.15.2
    IPV6 Address of Host:       fe80::1ff:fe90:8b05
    Client Version:             0.1
    Session ID:                 1
    OS Nodename:                IR809-GOS-1
    Host Hardware Vendor:       Cisco Systems, Inc.
    Host Hardware Version:      1.0
    Host Card Type:             not implemented
    Host OS Version:            1.28
    OS status:                  RUNNING
    Interface Hardware Vendor:  None
    Interface Hardware Version: None
    Interface Card Type:        None
    Applications Registered:
    =======================
 Count of applications registered by this host: 0
IR800#
```

show iox host list detail	Guest-OS started but no IPv6 address set-up on the GI2 interface

```
IOX Server is running. Process ID: 319
Count of hosts registered: 0
    IOX Server Address: 0.0.0.0; Port: 22222
IR800#
```

Checking Connectivity

Use standard Linux tools (for example, ping and traceroute) to check Guest OS connectivity.

Related Documentation

Note While some of these references do not apply directly to the Cisco IR800 series of Industrial Routers, they may serve as a source of addition information.

For information on supporting systems referenced in this guide, refer to the following documentation on Cisco.com:

DevNet documentation on IOx. Provides an overview as well as details on the IR800 series by scrolling down the left hand side:

https://developer.cisco.com/site/devnet/support/

Cisco Fog Director Reference Guide:

http://www.cisco.com/c/en/us/support/cloud-systems-management/fog-director/products-technical-reference-list.html

IOx Reference Guide:

http://www.cisco.com/c/en/us/support/cloud-systems-management/iox/products-technical-reference-list.html

Release Notes:

http://www.cisco.com/c/en/us/support/cloud-systems-management/iox/products-release-notes-list.html

Other Sources:

Cisco IOS IP Application Services Command Reference

IPv6 configuration manual

CHAPTER 8

WAN Monitoring

This chapter describes the WAN Monitoring software, WANMon, as implemented in Cisco IOS deployments. WANMon monitors the backhaul and initiates recovery actions on link failure.

Information About WANMon

WANMon is a flexible solution to address the WAN link recovery requirements for the following products and interfaces:

- Physical networks: 4G LTE
- Virtual links: Non-crypto map based IPSec tunnels (either legacy or FlexVPN); that is, any IPSec tunnel you configure as an interface.

You enable WANMon to monitor your WAN links and initiate link recovery actions on receipt of link failure triggers.

Built-in Recovery Actions

The following are the three levels of built-in recovery processes specific to the link type:

Link Type	**Recovery Actions**		
	Level 0 (Immediate)	**Level 1 (Active)**	**Level 2 (Last-Resort)**
4G LTE	Clear interface, and then shut/no-shut	Module reload	System reload
Ethernet	Clear interface, and then shut/no-shut	No action taken	System reload

Link Type	Recovery Actions		
	Level 0 (Immediate)	**Level 1 (Active)**	**Level 2 (Last-Resort)**
Tunnel	Shut/no-shut	No action taken	System reload

Each level has two time-based thresholds based on which built-in recovery actions are taken. The following are the default settings for each level:

- *threshold* is the wait time in minutes after receipt of a link failure trigger to initiate the recovery action as set in the specified level.
- *mintime* is the frequency to perform the recovery action if the link remains down.

The built-in values are:

Level	threshold	mintime	Description
Level 0	10 min	10 min	Triggers Level 0 actions 10 minutes after the link went down. Repeat no more than every 10 minutes.
Level 1	60 min	60 min	Triggers Level 1 actions 10 minutes after the link went down. Repeat no more than every 60 minutes.
Level 2	480 min	60 min	Triggers Level 2 actions 480 minutes after the link went down. Repeat no more than every 60 minutes.

Note If threshold values are specified as 0, no recovery actions are taken for that level. You can use this to avoid system reload (the built-in Level 2 recovery action) on receipt of a link failure trigger where other WAN links may be operational.

Prerequisites

Ensure that the WANMon module is available. The WANMon module is included in the IOS image as the *tm_wanmon.tcl* policy file.

Guidelines and Limitations

- WANMon automatically performs IP address checking (no user configuration) as required for the link type:
    - For cellular interfaces, WANMon performs IP address checking only for external dialer configurations, not for dial-on-demand configurations.
    - For 4G LTE interfaces, WANMon always performs IP address checking.
    - For all other interfaces, WANMon never performs IP address checking.

- WANMon indirectly triggers user-specified actions by generating an application event that link resetter applets monitor.
- If your network is live, ensure that you understand the potential impact of any command.

Configuring WANMon

You can enable WANMon on the router and assign WAMMon support to specific interfaces. Optionally, you can override the built-in recovery actions, define custom recovery links, and define an event manager environment policy to set the track object value and disable IP address checking. WANMon is disabled by default.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	`event manager policy tm_wanmon.tcl authorization bypass`	Enables the WANMon link recovery module. Use **authorization bypass** to avoid authorization for CLIs invoked by this policy.
Step 2	**event manager environment wanmon_if_list**<*instance*> **{***interface name* **{ipsla**<*instance*>**}}**	Configures WANMon for the interfaces in your WAN, and indicates that this is an interface configuration command. **Note** Any environment variable with the prefix wanmon_if_list constitutes an interface configuration. Multiple interfaces are allowed by specifying an instance. Be sure to specify the full interface name (for example, *cellular3/1*). You can set the IP SLA icmp-echo trigger, if desired. Multiple IP SLA triggers are allowed by specifing an instance. **Note** WANMon only looks at the status of the SLA ID. Even though *icmp-echo* is most common, if needed any other type of SLA probe (for example, *udp-echo*) can be used instead.
Step 3	**event manager environment wanmon_if_list***x* **{***interface name* **{recovery** *Level0* {*Level1* } *Level2***}}**	(Optional) Overrides the built-in thresholds.
Step 4	**publish-event sub-system 798 type 2000 arg1** <*interface name*> **arg2** <*level* >	(Optional) Configures custom recovery actions using link resetter applets.

	Command or Action	Purpose
		<*interface* > is the full interface name (for example, cellular3/1). <*level* > is 0, 1, or 2 to match the desired link recovery action.
Step 5	**{stub** <*track-stub-id* >**}**	(Optional) Allows an event manager environment policy to set the track object value. WANMon can set a track-stub-object value to reflect the link state so that an external applet can track the stub object.
Step 6	**event manager environment wanmon_if_list***x* **{**<*interface name* > {**checkip** <*instance* >}**}**	(Optional) Disables IP address checking.

What to do next

EXAMPLES

```
event manager policy tm_wanmon.tcl authorization bypass
```

The following examples are Event Manager commands to configure cellular and Ethernet interfaces:

```
event manager environment wanmon_if_list1 {cellular3/1 {ipsla 1}}
event manager environment wanmon_if_list2 {eth2/2 {ipsla 2}}
```

This example sets custom recovery thresholds:

```
event manager environment wanmon_if_list {cellular3/1 {recovery 20 {90 75} 600}
```

where:

- The Level 0 threshold is set to 20 minutes after the link failure trigger. Level 0 recovery actions are performed for the cellular interface. Repeats indefinitely, no more than every 10 minutes (default).
- Level 1 threshold is set to 90 minutes. Level 1 recovery actions are performed for the cellular interface. Repeats no more frequently than every 75 minutes.
- The Level 2 threshold is set to 600 minutes (10 hours).

The following sets the track-stub-object value to 21:

```
conf t
track 21 stub-object
event manager environment wanmon_if_list {cellular3/1 {ipsla 1} {stub 21}
```

Verifying WANMon Configuration

Use the following steps to verify your WANMon configuraion.

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**show event manager policy registered**	Displays the WAN monitoring policy.
Step 2	**show event manager environment**	Displays the interface environment variables set during interface configuration.

What to do next

EXAMPLE

```
show event manager policy registered
1    script    system  multiple            Off   Thu Jan 16 18:44:29 2014  tm_wanmon.tcl
show event manager environment
1 wanmon_if_list                {cell3/1 {ipsla 1}}
```

Configuration Examples

The following examples are provided:

WANMon Cellular Interface Configuration Example

```
track 1 ip sla 1
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now
event manager environment wanmon_if_list {cellular3/1 {ipsla 1}}
event manager policy tm_wanmon.tcl authorization bypass
```

Multiple WAN Link Monitoring Example

```
track 1 ip sla 1
track 21 stub-object
ip sla 1
 icmp-echo 172.27.166.250
 timeout 6000
 frequency 300
ip sla schedule 1 life forever start-time now
track 2 ip sla 2
track 22 stub-object
ip sla 2
 icmp-echo 10.27.16.25
 timeout 6000
 frequency 300
ip sla schedule 2 life forever start-time now
event manager environment wanmon_if_list1 {cellular3/1 {ipsla 1} {stub 21}}
event manager policy tm_wanmon.tcl authorization bypass
```

Related Documentation

Configuring WAN Backhaul Redundancy

CHAPTER 9

Ignition Power Management

This chapter provides a description and instructions for configuration of the Ignition Power Management feature of the IR829 router. It also keeps the IR829 up and running while the vehicle is stopped. Therefore, users do not have to wait for routers to reload each time the vehicle is stopped. Ignition Power Management prevents the router from draining the charge of the battery on automotive applications.

When the engine is running, it generates energy and recharges the battery. When the ignition is turned off, the IR829 can remain operational for a pre-determined period of time. This time period is programmable between 60 to 7200 seconds (2 hours) using the IOS ignition off-timer command.

Features of Ignition Power Management

The system software (IOS) tries to prevent the discharge of the battery with the following:

- Turning the router off if the vehicle has the ignition off for a period of time (programmable).
- Turning the router off if the battery voltage drops to a certain level (programmable).
- Attempting to protect the router by turning the router off if the battery voltage rises above a certain level (fixed amount of time).

The system software (IOS) logs the following events to the system log:

- When the user turns on or off the ignition management feature with CLI
- When the ignition is turned on or off
- When the ignition-off timer expires and the system goes off
- When the user enables or disables the feature through the CLI
- Tentatively logs the under-voltage and over-voltage events

For additional information on connecting to a vehicle, see the Plugs and Pinouts section of the Hardware Installation Guide.

Command Line Interface (CLI)

The Ignition Power Management feature of the IR800 series uses a command line interface.

Configuration CLI

The following commands are used to configure the feature.

Enable ignition power management:

```
IR800#configure terminal
IR800(config)#ignition enable
```

Disable ignition power management:

```
IR800#configure terminal
IR800(config)#no ignition enable
```

Ignition off timer value. After the ignition is turned off the router will stay operational for this amount of time, then it shuts down if the ignition is still off:

```
ignition off-timer <value>
```

Under-voltage threshold. If the input voltage drops to levels below this threshold, it will cause the router to shut down.

```
ignition undervoltage threshold <value>
```

Show the status of the feature:

```
IR800#show ignition
```

Configuring 12 Volt and 24 Volt Systems

Starting with release 15.8(3)M, the Ignition Undervoltage Threshold will display in in double decimal. There is a new cli that can be used **ignition undervoltage threshold** <*Volt*> <*mV if any*>.

Important please note the following requirements.

If using a 12 volt system, it is required to set Undervoltage to 11V at a minimum.

If using a 24 volt system, it is required to set Undervoltage to 22V at a minimum.

The following example sets the Undervoltage to 11.200V for 12V input system:

```
IR800#configure terminal
IR800(config)#ignition enable
IR800(config)#ignition undervoltage threshold 11 200
IR800(config)#end
IR800#write memory
```

The following command is used to show the status of the feature:

```
IR800#show ignition
Status:
  Ignition management: Enabled
  Input voltage:       12.0 V
  Ignition status:     Power on
  Shutdown timer:      0.0 s to off [will begin power down at ~100 sec
Thresholds:
  Undervoltage:        11.200 V
  Overvoltage:         32.0 V
  Undervoltage timer:  120.0 s
  Overvoltage timer:   1.0 s
  Ignition-Off timer:  900.0 s
```

The following example sets the Undervoltage to 22.200V for 24V input system:

```
IR800#configure terminal
IR800(config)#ignition enable
IR800(config)#ignition undervoltage threshold 22 200
IR800(config)#end
IR800#write memory
```

The following command is used to show the status of the feature:

```
IR800#show ignition
Status:
  Ignition management: Enabled
  Input voltage:       24.0 V
  Ignition status:     Power on
  Shutdown timer:      0.0 s to off [will begin power down at ~100 sec
Thresholds:
  Undervoltage:        22.200 V
  Overvoltage:         32.0 V
  Undervoltage timer:  120.0 s
  Overvoltage timer:   1.0 s
  Ignition-Off timer:  900.0 s
```

Troubleshooting CLI

A set of CLIs are available for debugging purposes.

Note To turn the debug off, prepend a **no** prefix to the CLI command.

The commands are:

Enable debugging error conditions in the ignition management:

debug ignition errors

Enable debugging operating events in the ignition management:

debug ignition events

Enable debugging state transitions in the ignition management software:

```
IR800#debug ignition states

IR800#
*Mar 11 18:59:20.001: %IGNITION-5-IGN_DEBUG_SET: Ignition Management debugging states is
turned on
*Mar 11 18:59:37.217: %IGNITION: Ignition mgmt FSM: IGNITION_MGMT_STATE_IGN_OFF
```

```
*Mar 11 18:59:39.679: %IGNITION-5-IGN_TURNED_ON_OFF: The ignition is turned OFF
*Mar 11 18:59:47.065: %IGNITION: Ignition mgmt FSM: IGNITION_MGMT_STATE_PWR_ON
*Mar 11 18:59:49.527: %IGNITION-5-IGN_TURNED_ON_OFF: The ignition is turned ON
```

Enable all debugging conditions at once:

```
IR800#debug ignition all
IR800#conf t
*Mar 11 19:01:06.737: %IGNITION-5-IGN_DEBUG_SET: Ignition Management debugging all is turned
 on
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#igni
IR800(config)#ignition tim
IR800(config)#ignition of
IR800(config)#ignition off-timer 800
IR800(config)#
*Mar 11 19:01:20.357: %IGNITION: handling off-time CLI
*Mar 11 19:01:23.115: %IGNITION: event set off timerdo show ignition
Status:
  Ignition management: Enabled
  Input voltage:       12.2 V
  Ignition status:     Power on
  Shutdown timer:      0.0 s to off
Thresholds:
  Undervoltage:        11.0 V
  Overvoltage:         32.0 V
  Undervoltage timer:  60.0 s
  Overvoltage timer:   0.5 s
  Ignition-Off timer:  800.0 s
```

Turn off debugging:

```
IR800(config)#no ignition off-timer ?
  <cr>
```

Note All debugging commands are cleared through a reboot of the device.

Another troubleshooting command is **show ignition register**. This displays existing register information:

```
IR800#show ignition register
*Nov 13 20:59:32.525: %SYS-5-CONFIG_I: Configured from console by consolereg
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:59:35.081 UTC Mon Nov 13 2017
MCU Registers Dump:
===================
IR800_MCU_DEV_ID = 0x2F
IR800_MCU_IGNITION_STATE = 0x1
IR800_MCU_IGN_VOLTAGE_HI = 0x1
IR800_MCU_IGN_VOLTAGE_LO = 0x1B
IR800_MCU_IGN_CURRENT_TIMER_HI = 0x0
IR800_MCU_IGN_CURRENT_TIMER_LO = 0x0
IR800_MCU_IGN_HI_VOLTAGE_THRESHOLD_HI = 0x3
IR800_MCU_IGN_HI_VOLTAGE_THRESHOLD_LO = 0x7
IR800_MCU_IGN_LOW_VOLTAGE_THRESHOLD_HI = 0x0
IR800_MCU_IGN_LOW_VOLTAGE_THRESHOLD_LO = 0xFA
IR800_MCU_IGN_SENSE_OFF_TIMER_HI = 0x0
IR800_MCU_IGN_SENSE_OFF_TIMER_LO = 0xF0
IR800_MCU_IGN_HI_VOLTAGE_TIMER_HI = 0x0
```

```
IR800_MCU_IGN_HI_VOLTAGE_TIMER_LO = 0x1
IR800_MCU_IGN_LOW_VOLTAGE_TIMER_HI = 0x0
IR800_MCU_IGN_LOW_VOLTAGE_TIMER_LO = 0x78
IR800_MCU_IGN_SYS_FLAGS_2 = 0xF
IR800_MCU_IGN_SYS_FLAGS_1 = 0x8
IR800_MCU_IGN_ENABLE = 0x5A
```

Ignition Under-Voltage Characteristics

Under-voltage threshold: If the input voltage drops to levels below this threshold, it will cause the router to shut down.

```
ignition undervoltage threshold <value>
```

When the input voltage drops below the under-voltage threshold value, the IR829 initiates a shutdown process and will shutdown within 120 seconds. As part of the shutdown process, the IR829 initiates the under-voltage timer to count down from 120 seconds to 0 seconds.

If the input voltage is below the the under-voltage threshold for 20 seconds or more, the IR829 initiates a graceful shutdown. However, if there is a momentary flap of the input voltage for 2 to 10 seconds (for example, the router input voltage drops below the under-voltage threshold of 2 seconds and recovers back), the under-voltage timer is reset and the shutdown process is canceled.

For the router to cancel the shutdown process due to the recovery of the input voltage, the input voltage has be above the under-voltage threshold by 0.8V. This hysteresis is implemented to prevent the router from toggling between shutdown and recovery when the input voltage is very close to the under-voltage threshold.

Command Examples

The following examples illustrate the CLI commands and the associated output expected.

Out of box configuration with no ignition management configured.

```
IR800#show ignition

Status:
  Ignition management: Disabled
  Input voltage:       11.8 V
  Ignition status:     Power on
  Shutdown timer:      0.0 s to off [will begin power down at ~100 sec]
Thresholds:
  Undervoltage:        11.0 V
  Overvoltage:         32.0 V
  Undervoltage timer:  60.0 s
  Overvoltage timer:   0.5 s
  Ignition-Off timer:  900.0 s
```

Configure the device for ignition off timer of 60, and ignition under-voltage threshold of 11.

1. Turn vehicle ignition switch off.
2. **ignition off-timer 60**
3. **ignition undervoltage threshold 11**
4. **ignition enable**

```
IR800#show ignition

Status:
  Ignition management: Enabled
  Input voltage:       11.8 V
  Ignition status:     Power on
  Shut down timer:     53.0 s to off
Thresholds:
  Undervoltage:        11.0 V
  Overvoltage:         32.0 V
  Undervoltage timer:  60.0 s
  Overvoltage timer:   0.5 s
  Ignition-Off timer:  60.0 s
```

Default Values

The following default settings apply to Ignition Power Management:

Setting	Default Value	User Modifiable?
Ignition Power Management Feature	Disabled	Yes
Ignition off timer	720 seconds	Yes
Under-Voltage threshold	9 Volts (up to IOS15.7(3)M) 11 Volts (IOS15.7(3)M1 and beyond)	Yes
Under-Voltage timer	60 seconds (up to IOS15.7(3)M) 120 seconds (IOS15.7(3)M1 and beyond)	No
Over-Voltage threshold Defines the max input voltage that IR829 can handle.	32 Volts	No
Over-Voltage timer Defines the duration of the input voltage above the over-voltage threshold.	1.0 seconds	No

Note If the device is upgraded from an IOS version below 15.7(3)M to 15.7(3)M1 or above, the threshold will not automatically change. You must manually configure "ignition under-voltage" to 11V for a 12 Volt system, or 22V for a 24 Volt system.

CHAPTER 10

Licensing and Security

This chapter provides details on the security licensing for the IR800 series.

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

- S800IUK9-15503M – Cisco IR800 Series UNIVERSAL
- S800INPEK9-15503M – Cisco IR800 Series UNIVERSAL – NO PAYLOAD ENCRYPTION

The Software License PIDs are shown in the following table.

Table 5: Software License PIDs

Software PID	Name	Description
SL-IR800-IPB-K9	Cisco 800 Series Industrial Routers IP Base License	Routing (BGP, OSPF, RIP, EIGRP, ISIS,), PBR, IGMP/MLD, Multicast, QoS, AAA, Raw Sockets, Manageability
SL-IR800-SEC-K9	Cisco 800 Series Industrial Routers Security License	SSL, VPN, IPSec, DMVPN, FlexVPN, IOS Firewall
SL-IR800-SNPE-K9	Cisco 800 Series Industrial Routers No Payload Encryption License	
SL-IR800-DATA-K9	Cisco 800 Series Industrial Routers Data License	L2TPv3, IP SLA, BFD, MPLS (subset)
SWAP1530-81-A1-K9	Cisco 1530 Series Unified & Autonomous 8.1 SW	IR829 AP803 WI-FI

Licensing

Licenses are installed at manufacturing. If the securityk9 technology-package is not installed, the crypto related functions will not work. See additional information under Hardware Crypto Support, on page 142

To enable the RightToUse license, perform the following:

1. Accept the EULA.
2. Enable the technology-package.
3. Reload the IR800.

Licensing CLI

```
IR800# show version
License Info:
License UDI:
-------------------------------------------------
Device#   PID                   SN
-------------------------------------------------
*1        IR829GW-LTE-GA-EK9    FGL194520VZ
Suite License Information for Module:'ir800’
--------------------------------------------------------------------------------
Suite                 Suite Current         Type           Suite Next reboot
--------------------------------------------------------------------------------
Technology Package License Information for Module:'ir800’
------------------------------------------------------------------------
Technology    Technology-package                  Technology-package
              Current              Type           Next reboot
------------------------------------------------------------------------
ipbase        ipbasek9             Permanent      ipbasek9
security      securityk9           Permanent      securityk9
data          datak9               Permanent      datak9

IR800# conf term
license udi pid IR829GW-LTE-GA-EK9 sn FGL190726G8
license accept end user agreement
license boot module ir800 technology-package securityk9
license boot module ir800 technology-package datak9

IR829#show license feature
Feature name             Enforcement  Evaluation  Subscription   Enabled  RightToUse
ipbasek9                 no           no          no             yes      no
securityk9               yes          yes         no             yes      yes
datak9                   yes          yes         no             yes      yes
```

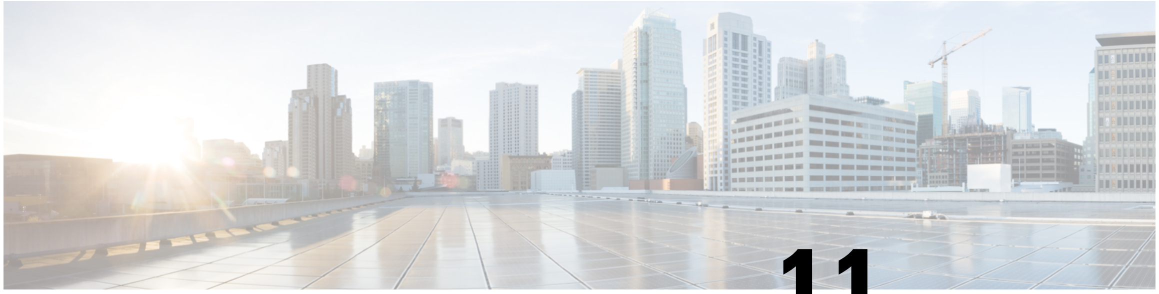
Hardware Crypto Support

The initial IOS software release, 15.5(3)M, provided only software based crypto support. With the introduction of IOS software release 15.5(3)M, hardware based crypto support was added. A security license must be installed to enable hardware based crypto support.

To see which version of crypto support is being used:

```
IR800#show crypto engine configuration

        crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
                  Location:  onboard 0
              Product Name:  Onboard-VPN
                HW Version:  1.0
               Compression:  No
```

```
                  DES:  Yes
                3 DES:  Yes
              AES CBC:  Yes (128,192,256)
             AES CNTR:  No
Maximum buffer length:  4096
     Maximum DH index:  0000
     Maximum SA index:  0000
   Maximum Flow index:  0256
 Maximum RSA key size:  0000
   crypto lib version:  22.0.0
crypto engine in slot:  0
             platform:  VPN hardware accelerator
   crypto lib version:  22.0.0
```



CHAPTER 11

mSATA SSD as Additional Storage

This section contains the following topics:

mSATA Overview

Previously, IR829 IOx/Guest-OS legacy systems on which end users can host applications, came with a disk storage of 4GB to store user data. Functionality has been added to the IR829 product line with new SKUs allowing for an mSATA SSD to add 50 GB or 100 GB of available storage.

The pluggable mSATA cards are NOT hot-swappable, the device must be powered down to install or remove it. The cards are installed in the mSATA slot (formerly known as Limited Modularity slot). Additional details are available in the Cisco IR829 Industrial Integrated Services Router Hardware Installation Guide.https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/hardware/install/guide/829hwinst.html

Note The mSATA SSD is accessible only from IOx, not IOS. For IOx CLI operation, see the command set available in the following section of the Software Configuration Guide:https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/configuration/guide/b_IR800config/b_guestos.html

Note As with any IR800 platform, for IOx, use the Fog Director or Local Manager to install applications and access the new mSATA disk storage provided on IR829M PIDs.

IR829M SKUs

The IR829M SKUs provide the following capabilities:

- Integrated Storage and Compute for IOx Edge application
- 100GB / 50GB industrial grade mSATA SSD integrated storage for IR829
- Integrated PoE to power up to four IP devices such as IP cameras
- Single & Dual LTE WAN redundancy with high reliability
- Dual Band WiFi connectivity
- Advanced routing based on signal strength, cellular technology, etc.
- Ignition Power Management to reduce downtime
- GPS for location-based services Accelerometer and Gyroscope for vehicle/driver safety
- Integrated storage has Industrial, Automotive, Railway, Marine and Military certifications

The IR829 SKUs are available in the following product IDs:

- IR829M-2LTE-EA-*K9 (Dual LTE)
    - Dual LTE IR829 with mSATA SSD connector and POE
    - US, Canada and Europe
- IR829M-LTE-EA-*K9 (Single LTE)
    - Single LTE IR829 with mSATA SSD connector and POE US, Canada and Europe

Using the mSATA SSD

Functionality-wise, there are no configuration and troubleshooting differences to the end-user in IOS or IOx, with or without mSATA. The system simply recognizes the additional storage. There are some CLI commands that will show information that pertains to the mSATA storage. Examples are show inventory, and show platform msata.

```
IR829#show inventory
NAME: "IR829M-2LTE-EA-EK9", DESCR: "IR829M-2LTE-EA-EK9 chassis"
PID: IR829M-2LTE-EA-EK9, VID: V01 , SN: FGL214591HB
NAME: "IR800-IL-POE", DESCR: "POE module"
PID: IR800-IL-POE      , VID: V01 , SN: FOC21452WHT
NAME: "mSATA module", DESCR: "mSATA module 100G"
PID: IR-SSD-mSATA-100G , VID: V00, SN:
NAME: "Modem in slot 0 on Cellular1/0", DESCR: "Sierra Wireless MC7455 4G-EA"
PID: MC7455            , VID: 1.0, SN: 352009080067148
NAME: "1000BASE-T SFP", DESCR: "1000BASE-T SFP"
PID: GLC-TE            , VID: G3., SN: AVC193822W4
NAME: "Modem in slot 1 on Cellular0/0", DESCR: "Sierra Wireless MC7455 4G-EA"
PID: MC7455            , VID: 1.0, SN: 352009080067155
```

In the above example, note that the IR829 PID changed to IR829M if the mSATA is available. The mSATA PID states if it is a 50GB or 100GB module. The same information is displayed using the show diag command as well.

```
IR829#show platform msata
SSD Lifetime:
  Lifetime Remaining: 99% -> 99% of the net disk read/write lifetime is remaining
```

```
Memory:
  Size: 99G.            -> Total disk size in Gigabytes
  Used: 93G.            -> Used disk space, inclusive of IOx CAF, Iox application, data,
etc.
  Available: 6.1G.      -> Remaining disk space in Gigabytes
  Usage: 94%.           -> Usage in percentage, same as Guest-OS 'df -h' command output
display
```

In the above example, note that the output shows SSD lifetime remaining, disk storage size, usability and availability in Gigabytes.

There are also entries shown in the syslog when 15%, 10%, and 5% of the lifetime limit remain:

*Jan 30 19:03:00.257: %IOX-4-IOX_SSD_LIFETIME_WARN: SSD Lifetime remaining in module:15

*Jan 30 19:02:30.157: %IOX-2-IOX_SSD_LIFETIME_CRITICAL: SSD Lifetime remaining in module:5

Displaying the Wear Leveling Data for the mSATA SSD

Feature applies to the IR829M

IOx Local Manager/ Fog Director can now display the wear leveling data for the mSATA SSD on the IR829M products.

In the IOx Local Manager, it is observed by selecting **System** > **Storage**.

From the IOS command line, you can monitor the lifetime using the **show platform msata** command.

The following example shows a 50G mSATA controller.

```
Router#show platform msata
SSD Lifetime:
Lifetime Remaining: 99%
Memory:
Size: 50G.
Used: 49G
Available: 932M
Usage: 99%
```

After a router reload, it will take a few minutes (approximately 5) before this data will be populated again.

When the SSD lifetime reduces to 15%, 10% and 5% of the lifetime limit, errors start getting reported in syslog.

For example:

```
*Jan 30 19:03:00.257: %IOX-4-IOX_SSD_LIFETIME_WARN: SSD Lifetime remaining in module:15
*Jan 30 19:02:30.157: %IOX-2-IOX_SSD_LIFETIME_CRITICAL: SSD Lifetime remaining in module:5
```

IR829M: MIB support for mSATA Wear Ratio and Usage

mSATA functionality was added to the IR829 product line to add extra storage in the15.8.3M release. The PID IR829M has mSATA support available in the device inventory detail. The following table shows the IR829M SKU with the OID:

Table 6: mSATA OIDs

SKU	OID
IR829M-2LTE-EA-BK9	1.3.6.1.4.1.9.1.2610
IR829M-2LTE-EA-AK9	1.3.6.1.4.1.9.1.2610
IR829M-2LTE-EA-EK9	1.3.6.1.4.1.9.1.2610
IR829M-LTE-EA-AK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-EA-BK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-EA-EK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-LA-ZK9	1.3.6.1.4.1.9.1.2609

As part of this enhancement, SNMP support has been added for the following mSATA parameters on the IR829M:

- lifetime remaining (wear leveling)
- memory usage for the mSATA SSD

As part of this enhancement, further SNMP support has been added. There is a new OID name cevMsataWlIR829 in the existing MIB CISCO-ENTITY-VENDORTYPE-OID-MIB.my under the cevModuleCommonCards functional group.

For example:

cevMsataWlIR829 OBJECT IDENTIFIER ::= { cevModuleCommonCards 689 } -- mSATA wear ratio and usage for IR829.

The entity OID value is iso.3.6.1.4.1.9.12.3.1.9.2.689

The **show platform msata** command gives information about this MIB.

Example: Actual OID and output of SNMP get/walk on OID

<OID> = STRING: "Lifetime Remaining: 99%, Usage: 30%"

Feature Details

The following conditions must be met before performing SNMP requests on the IR829M:

- An active mSATA module must be in the IR829M router.
- Verify this using the **show platform msata** CLI.

Feature Assumptions

- This feature is supported on the IR829M only.

- After a router reload it will take approximately 5 minutes before mSATA data will be populated again. Only SNMP get is allowed on OID cevMsataWlIR829 and is marked as read-only. Setting its value will not be allowed.
- Configurations to enable SNMP on IR800 are necessary for fetching MIB value.

IR829M OIDs

There are some new SNMP OIDs created for the new IR829M SKUs

Table 7: SNMP OIDs

SKU	OID
IR829M-2LTE-EA-BK9	1.3.6.1.4.1.9.1.2610
IR829M-2LTE-EA-AK9	1.3.6.1.4.1.9.1.2610
IR829M-2LTE-EA-EK9	1.3.6.1.4.1.9.1.2610
IR829M-LTE-EA-AK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-EA-BK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-EA-EK9	1.3.6.1.4.1.9.1.2673
IR829M-LTE-LA-ZK9	1.3.6.1.4.1.9.1.2609

Related documentation:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html

https://developer.cisco.com/docs/iox/

CHAPTER 12

Client Information Signaling Protocol (CISP)

This section contains the following topics:.

Client Information Signaling Protocol (CISP)

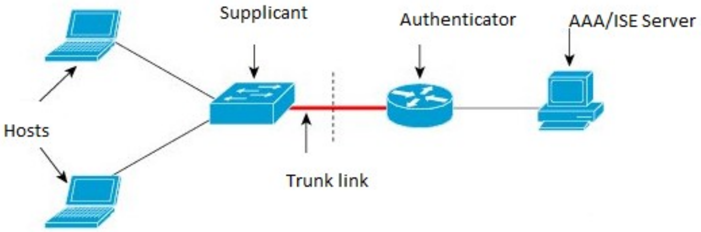
Feature is new for release 15.8(3)M1 and applies to the IR829 only

CISP is a generic protocol used by Network Edge Authentication Topology (NEAT) scenario in order to propagate client MAC addresses and VLAN information between supplicant and authenticator. CISP was already available in Cisco IOS, but is new to the IR829 platform. Complete details on this feature are available here:

https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/116681-config-neat-cise-00.html

Figure 14: Cisp in NEAT, on page 151 illustrates how the CISP feature works in NEAT in a simple scenario.

Figure 14: Cisp in NEAT



CISP Commands

The following commands have been added to the IR829:

- cisp enable
- show cisp *[client]/[interface]/[registrations]/[summary]*
- show authentication *[interface] / [method] / [registrations]/ [sessions] / [statistic]*

- debug cisp *[all]/[errors]/[events]/[packets]/[sync]*

Details on the commands follow:

cisp enable

Used to enable the CISP protocol on Authenticator as well as on Supplicants. In config mode CISP enable cli globally enable the CISP protocol on L2 interface.

```
IR800(config)# cisp enable
```

show cisp commands

- In exec mode, **show cisp client** displays all the information for authorized host mac address and VLAN details.

```
IR800#show cisp clients
Authenticator Client Table:
---------------------------
 MAC Address VLAN Interface
 --------------------------------
 001b.0d55.21c1 200 Fa0/6
 001b.0d55.21c0 1 Fa0/6
```

- In exec mode, **show cisp registrations** displays all the details of Interface(s) with CISP registered user(s).

```
IR800#show cisp registrations
Interface(s) with CISP registered user(s):
------------------------------------------
 Fa0/6
 Auth Mgr (Authenticator
```

- In exec mode, **show cisp interface** <> displays information whether the device is supplicant or authenticator, version details, and peer mode.

```
IR800# show cisp interface gigabitEthernet 1
CISP Status for interface Gi1
----------------------------
  Version:   (not negotiated)
  Mode:        Authenticator
  Peer Mode:
  Auth State:  Idle
```

CISP Prerequisites

- 802.1x Authentication is already supported on IR829.
- No support for CISP has been added to the IR809 platform, or for L3 ports on the IR829.
- Before CISP is enabled, the 802.1x authentication must be completed as both supplicant and authenticator

  .

Flow Diagrams

Trigger of CISP Packets

- On Successful authentication response from authenticator, it will start registration with Authenticator CISP.
- Once End host is authorized or unauthorized, it will update (Add / Delete) to the authenticator CISP.
- If Access links or trunk uplink goes up or down, it will clear off the local CISP Client. Table and the Authenticator CISP will clear its Client Table.
- If there is New MAC is learned or aged out, CISP will update on both sides.
- If there is no response to CISP request frames, it will retransmit the CISP frames.
- Authentication Switch ACKs CISP frame after completing desired action.

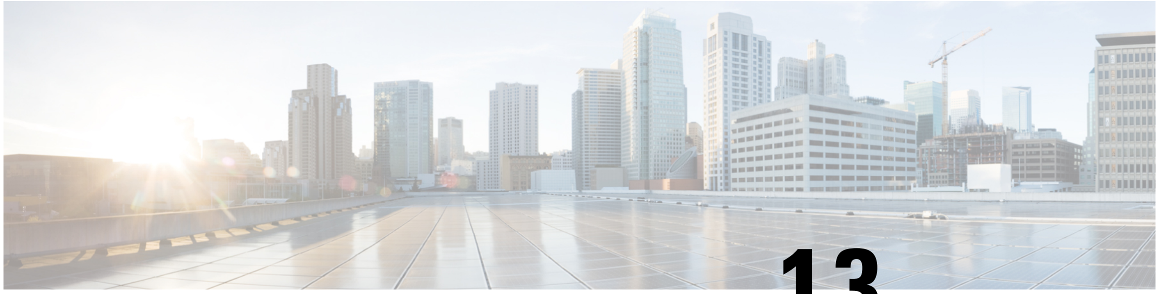
Host Disconnect/Power down/Logoff

- NEAT (Supplicant and Authenticator) utilizes the CISP protocol that securely transports authenticated hosts MAC addresses from a downstream Supplicant device to an upstream Authenticator device. CISP must be enabled on both ends.
- On a successful authentication response from the authenticator, it will start registration with Authenticator CISP. Once the authenticator authenticates the supplicant's registration packet transfer between the supplicant and the authenticator. The following are examples of the CISP packet transfer after enable the debug cisp all:

```
Oct 15 13:51:36.707: CISP-RXPAK (Fa0/6): Code: REQUEST ID:0x22 Length: 0x001C  Type:
REGISTRATION
 Oct 15 13:51:36.707: CISP-TXPAK (Fa0/6): Code: RESPONSE ID:0x22 Length:0x001C   Type:
REGISTRATION
```

Once the End host is authorized or unauthorized, it will update (Add / Delete) to the authenticator CISP. The following shows an example:

```
Oct 15 13:51:36.724: CISP-RXPAK (Fa0/6): Code: REQUEST ID:0x23 Length:0x003A  Type: ADD_CLIENT
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c1 (vlan: 200)
 to authenticator list
```



CHAPTER 13

Dot1x Supplicant Support on the L2 interface

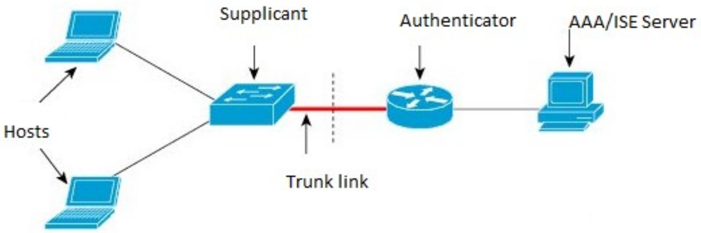
This section contains the following topics:.

Dot1x Supplicant Support on the L2 interface

Feature is new for release 15.8(3)M1 and applies to the IR829 only

IEEE 802.1X authentication enables the access point to gain access to a secured wired network. You can enable the access point as an 802.1X supplicant (client) on the wired network. A user name and password that are encrypted using the MD5 (IR8x9 platform supports only md5 method) algorithm can be configured to allow the access point to authenticate using 802.1X. Figure 15: Supplicant Topology, on page 155 illustrates the Supplicant Topology.

Figure 15: Supplicant Topology

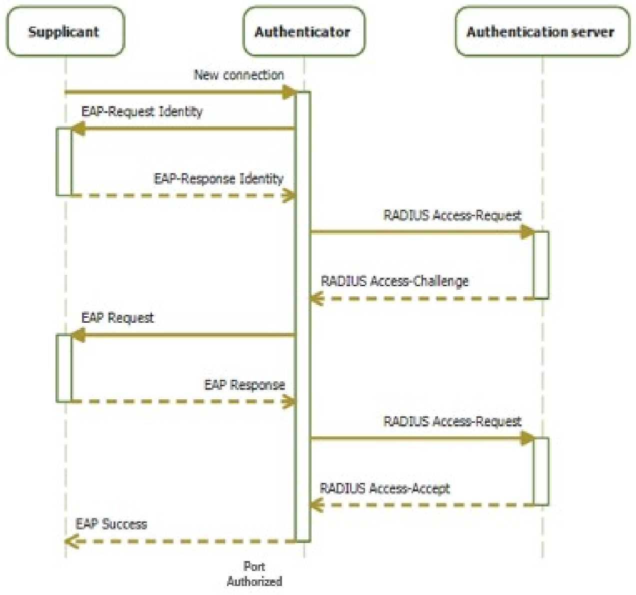


Supplicant CLI Commands

```
#IR800-supplicant(config-eap-profile)?
       Eap profile configuration commands:
       description  Provide a description for the EAP profile
       exit         Exit EAP profiles configuration submode
       method       Add an allowed  method
       no           Negate a command or set its defaults
#IR800-supplicant(config-eap-profile)method ?
      md5  EAP-MD5 method allowed
```

Refer to Figure 16: Workflow, on page 156 for the workflow.

Figure 16: Workflow



Workflow details

- On networks that use IEEE 802.1X port-based network access control, a supplicant cannot gain access to the network until the 802.1X authenticator grants access. If your network uses 802.1X, you must configure 802.1X authentication information on the WAP device, so that it can supply it to the authenticator.
- Supplicant starts with EAPOL start request to the Authenticator
- In Supplicant Request Authenticator send EAP request to supplicant
- Supplicant sends the EAP response (W/MD5 Credentials) to Authenticator
- Authenticator sends the relay request to AAA via radius to Authenticate the supplicants
- If the supplicant entry is already defined there, Radius sends accept to the Authenticator and the Supplicant port gets authorized by the authenticator
- Now the supplicant works as Authenticator for the host connected to it. The same flow happens when the host connects to the Supplicant.

Sample Configuration to Support DOT1x Supplicant on the IR829

Note More details can be found here:

https://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/116681-config-neat-cise-00.html#anc14

```
! Enable supplicant switch to authenticate devices connected
   dot1x system-auth-control

! Forces the switch to send only multicast EAPOL packets when it receives either
  unicast or multicast packets, which allows NEAT to work on the supplicant
  switch in all host modes.
   dot1x supplicant force-multicast

! configure EAP mode used by supplicant switch to authenticate itself to authenticator
switch eap profile EAP_PRO
    method md5

! Configure credentials use by supplicant switch during that authentication.
dot1x credentials CRED_PRO
 username bsnsswitch
 password 0 C1sco123
```

The connection of the supplicant to the authenticator is already configured to be a trunk port (in contrast to access port configuration on the authenticator). At this stage, this is expected; configuration will dynamically change when the ISE returns the correct attribute.

```
interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
dot1x pae supplicant
dot1x credentials CRED_PRO
dot1x supplicant eap profile EAP_PRO
```

Note For support of Dot1x in IR829 dot1x code is added in IR829 for L2 interface.

```
IR800-supplicant# show dot1x interface gigabitEthernet 1 details
Dot1x Info for GigabitEthernet1
-----------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = CRED_PRO
EAP profile               = EAP_PRO
Dot1x Supplicant Client List
-------------------------------
Authenticator             = 80e0.1d66.2ce1
        Supp SM State        = AUTHENTICATED
        Supp Bend SM State   = IDLE
Port Status               = AUTHORIZED
```

Note Dot1x supplicant on L3 interfaces is not supported.

CHAPTER 14

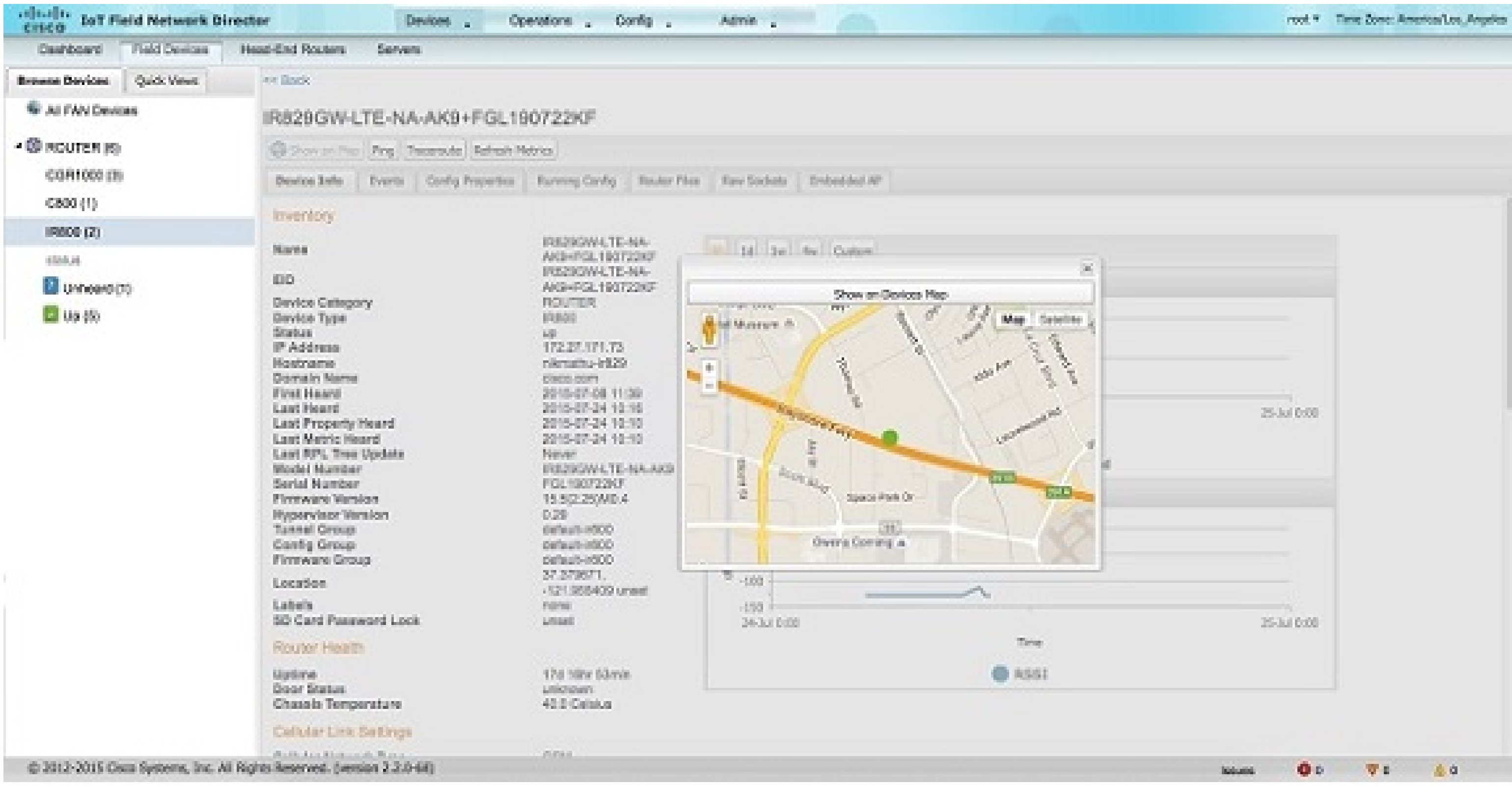
Network Management Solutions

This chapter provides details and links to the various methods of managing the IR800 series.

Network Management Solutions (NMS) that are available for the IR800 series consist of the following:

Cisco IoT Field Network Director (formerly referred to as CG-NMS)

The IR800s are supported with IOT Field Network Director which offers a single platform to manage a complete FAN solution, Raw Socket sessions management, and monitoring.



IR829GW-LTE-NA-AK9+FGL190722KF

Inventory

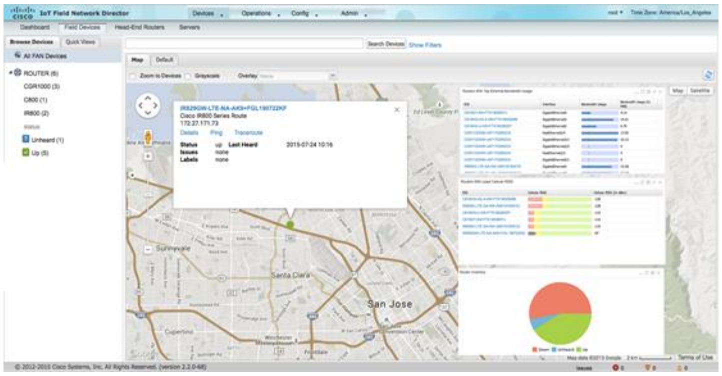
Name IR829GW-LTE-NA-AK9+FGL190722KF
EID IR829GW-LTE-NA-AK9+FGL190722KF
Device Category ROUTER
Device Type IR800
Status up
IP Address 172.27.171.73
Hostname nkmathu-ir829
Domain Name cisco.com
First Heard 2015-07-08 11:39
Last Heard 2015-07-24 10:16
Last Property Heard 2015-07-24 10:10
Last Metric Heard 2015-07-24 10:10
Last RPL Tree Update Never
Model Number IR829GW-LTE-NA-AK9
Serial Number FGL190722KF
Firmware Version 15.5(2.25)MD.4
Hypervisor Version 0.28
Tunnel Group default-ir800
Config Group default-ir800
Firmware Group default-ir800
Location 37.379671, -121.958409 unset
Labels none
SD Card Password Lock unset

Router Health

Uptime 17d 16hr 53min
Door Status unknown
Chassis Temperature 40.0 Celsius

Cellular Link Settings

© 2012-2015 Cisco Systems, Inc. All Rights Reserved. (version 2.2.0-68)



Some of the key features are:

- Geographic Information System (GIS) map -based, visualization, monitoring, troubleshooting, and alarm notifications
- Group-based configuration management for FAN routers (CGR1000, IR8x9, 819H, IR5x9 and CG-Mesh endpoints
- Rule-engine infrastructure for customizable threshold -based alarm processing and event generation
- Secure network infrastructure (inventory, rollback configuration, work order) of IR809 and IR829
- Zero Touch Provisioning - Automatically provision IR800 and head-end routers with configuration
- Collect metrics and events from FAN Routers, Head-end routers, and CG-mesh endpoints, and store them in a database. Cellular metrics and statistics for cost optimization

- Network status monitoring and diagnosis for issues. Location tracking (historical and geo-fence)
- Update firmware on groups of IR809 and IR829. IR829 AP803 (Autonomous mode only)
- North-bound integration API for transparent integration with utility head-end and operational systems, for example Outage Reporting System
- Raw Socket management and monitoring

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

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

IR809 and IR829: PNP Image Upgrade from FND

When a Cisco IR8x9 is powered on for the first time, the PnP agent process running on the IOS wakes up in the absence of the startup config and attempts to discover the address of the PnP server. The PnP agent uses methods like DHCP and DNS to acquire the desired IP address of the PnP server. Upon successfully acquiring the IP address, the PnP agent initiates a long lived, bidirectional layer 3 connection with the server, and waits for a message from the server. The PnP server application sends messages to the agent requesting for information and services to be performed on the device. The PnP server application sends the required configurations and optionally IOS image to the device.

The Cisco Plug and Play Connect cloud service works with your Smart Account and the Cisco Network Plug and Play solution to provide automatic plug and play server discovery when other methods such as DHCP or DNS are not available.

For more information go to the Plug and Play Connect webpage.

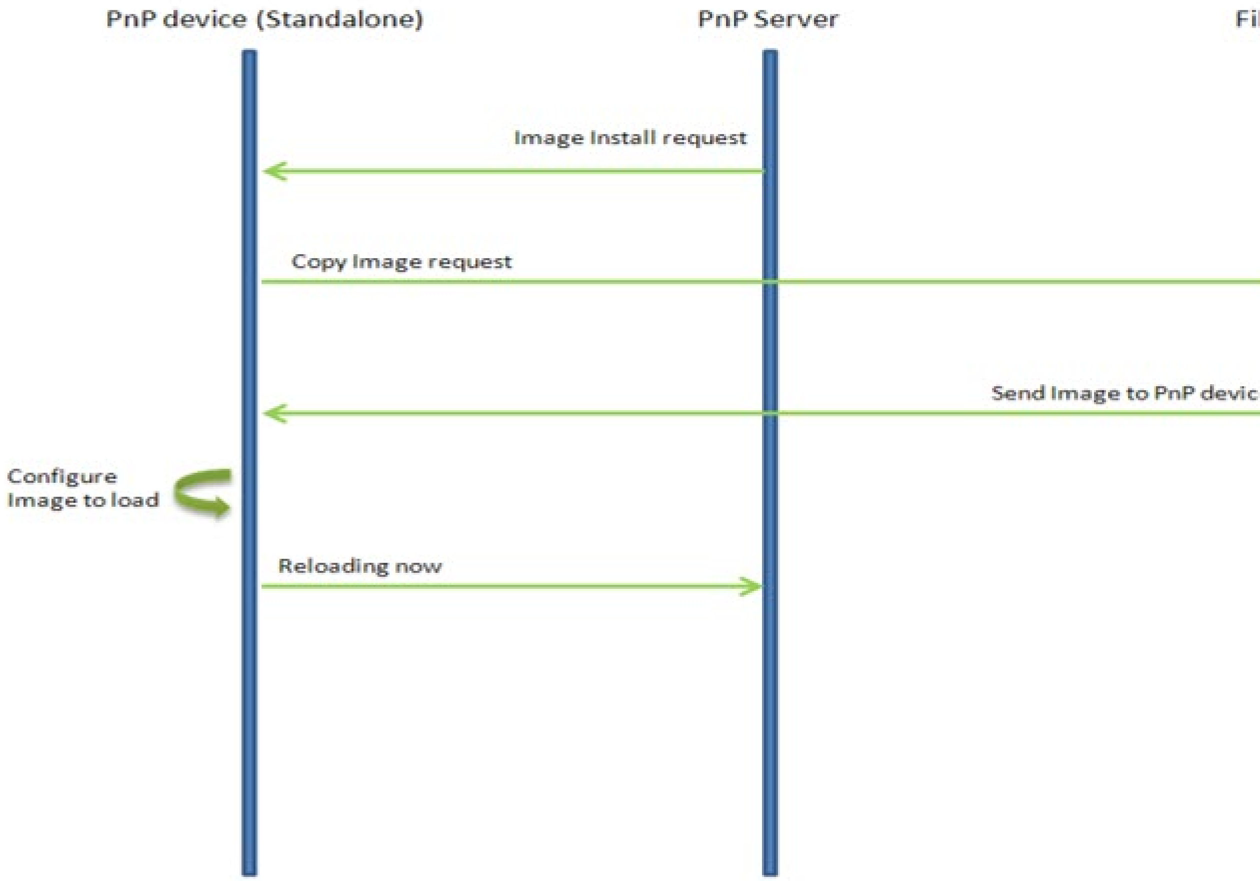
Image Installation

Image Installation service enables a PnP-enabled device to perform an image upgrade upon receiving a request from the PnP Server. The following operations are performed in sequence to successfully load the device with the new image:

1. PnP Server (FND) initiates the upgrade.
2. PnP Device will check the version of the image to be upgraded, and determine if it is a later version than the one the device is booted up with.
3. PnP Device will make a request for copying the image.
4. PnP Device will get the image and its details from PNP agent.
5. Configure the device to load the new image on next reload.
6. Reload the device.

The following graphic illustrates the message flow for a standalone device

Figure 17: PnP Message Flow



The PnP Agent on the device receives a request from the PnP Server, parses the XML payload, and identifies the request as an Image Upgrade request. It then creates an Image Install process, which identifies the request as a Standalone Image Install request.

Based on the fields populated, PnP Image Install will perform the following operations:

- Copy the image from the file server to a local disk. All the information about the file server, Image location, and destination is populated.
- Once the Image is copied, it needs to be configured to load next time the device reloads. For this operation, the 'boot system' CLI is configured in the startup-config.
- The device now sends a message to the PnP Server that it is undergoing a reload.

Feature Assumptions

- This feature is support on the IR809 and IR829 starting from Field Network Director version 4.2.
- Updated PID exists in the PnP Server for new platforms. For end-to-end PnP solution to work, the PnP-server needs to be updated for the specific PID of each new platform.
- The feature supports image upgrade for only bundle image on the IR8x9 platform.
- Upgrade starts upon a request from PnP Server Application.
- No new PnP CLIs will be added as part of this enhancement.

Cisco Configuration Professional Express

Cisco Configuration Professional Express is an embedded, device-management tool that enables bootstrap configuration and provisioning of a IR800 Series Router.

CCP Express provides you two options to bring up a brand new router. You can use the Quick Setup Wizard to perform the basic configuration tasks and Advanced Setup option for detailed configuration options. For a brand new router, Quick setup wizard is the preferred option.

Caution: If you log into an IR800 Series device as a one-time user with the cisco/cisco username and password, you must create another user through the UI or command line. Otherwise, the one-time user session is deleted, and your configurations are not saved. For more information, refer to the Cisco Configuration Professional Express Quick Start Guide at:https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/cisco_configuration_professional_express/v3_5/guides/quickstart/CiscoCPExpress-IR-3-5-qsg.html

For Cisco CP Express to be fully functional, you will need Cisco IOS Software Release 15.6.(3)M2. Cisco CP Express is supported on these browsers:

- Mozilla Firefox 25 or later
- Google Chrome 30 or later
- Microsoft Internet Explorer 11 or later
- Safari 9.1
- Microsoft Edge Version 38

For additional information about Cisco CP Express, see the Cisco Configuration Professional Express Administration Guide:https://www.cisco.com/c/en/us/td/docs/routers/access/800/829/software/cisco_configuration_professional_express/v3_5/guides/adminguide/CCP-admin-guide.html

Cisco Kinetic

Cisco Kinetic is a new class of software platform – an IoT data fabric – designed to address the challenges of a distributed environment.

Cisco Kinetic is a system of software running on distributed nodes of edge, data center and cloud.

This system of software will:

- Get gateways up and running and configured
- Extract data securely and transform it into a usable format for your applications
- Set policies about which data goes where
- Execute those policies or rules – based on business logic you (the customer) have been able to set on different layers
- Provide visualization tools and dashboards with intuitive UI
- Securely move data to the right applications at the right time, based on your policies and rules

There is wealth of information available for Cisco Kinetic at:https://salesconnect.cisco.com/c/r/salesconnect/index.html#/program/PAGE-10238

Cisco Prime Infrastructure

Cisco Prime Infrastructure provides a single platform to manage an infrastructure with a broad range of static Cisco devices. It is available on the IR829 with Cisco Prime Infrastructure release 2.2 and Device Pack 7.

For detailed information on the Cisco Prime Infrastructure, refer to the following:

https://www.cisco.com/c/en/us/products/cloud-systems-management/prime-infrastructure/index.html

Note Only Inventory and Configuration Archive are supported for the IR829.

Davra RuBAN

Single platform for telematics and network management. See the following for more information:

- Cisco Connected Fleet
- Quickstart guide to setting up the RuBAN Bus

Cisco IoT Fog Director

The Cisco IoT Fog Director brings together the IOx Application Management Module, the ability to Understand your IOx resources, and IOx Application Rollout.

About Cisco IOx

Cisco IOx is an application enablement platform that provides uniform and consistent hosting capabilities for various types of applications, or applications, across various Cisco platforms. This platform brings together Cisco IOS, the industry-leading networking operating system, and Linux, the leading open source platform. Linux-based applications can run on Cisco devices in the Cisco IOx framework, so using this platform, you can bring custom applications and interfaces to the network.

With Cisco IOx, developers can create a wide variety of IoT applications, such as data aggregation system and control systems.

About Cisco Fog Director

Cisco Fog Director allows administrators to manage, administer, monitor, and troubleshoot Cisco IOx applications and devices. It provides a web-based user interface from which you can perform activities that include the following:

- Install and uninstall applications

- Start and stop applications
- Upgrade applications
- View the status of applications
- Backup and restore applications data
- Monitor applications and devices and collect statistics
- Create and obtain debug logs for troubleshooting

Detailed information about the Cisco Fog Director is found at the home page:

http://www.cisco.com/c/en/us/support/cloud-systems-management/fog-director/tsd-products-support-series-home.html

OID and Inventory

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

IR829

```
IR829#show inventory oid
NAME: "IR829GW-LTE-GA-EK9", DESCR: "IR829GW-LTE-GA-EK9 chassis, Hw Serial#: FGL194520VZ,
Hw Revision: 2.0"
PID: IR829GW-LTE-GA-EK9, VID: V01 , SN: FGL194520VZ
OID: 1.3.6.1.4.1.9.12.3.1.3.1582
NAME: "Modem 0 on Cellular0", DESCR: "Sierra Wireless MC7304 4G-GA"
PID: MC7304, VID: 1.0, SN: 352761060426997
OID: 1.3.6.1.4.1.9.12.3.1.9.15.88
```

IR809

```
IR809#show inventory oid
NAME: "IR809G-LTE-GA-K9", DESCR: "IR809G-LTE-GA-K9 chassis, Hw Serial#: JMX1915X00Q, Hw
Revision: 1.0"
PID: IR809G-LTE-GA-K9  , VID: V00, SN: JMX1915X00Q
OID: 1.3.6.1.4.1.9.12.3.1.3.1581
NAME: "Modem 0 on Cellular0", DESCR: "Sierra Wireless MC7304 4G-GA"
PID: MC7304, VID: 1.0, SN: 352761060206340
OID: 1.3.6.1.4.1.9.12.3.1.9.15.88
```