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.

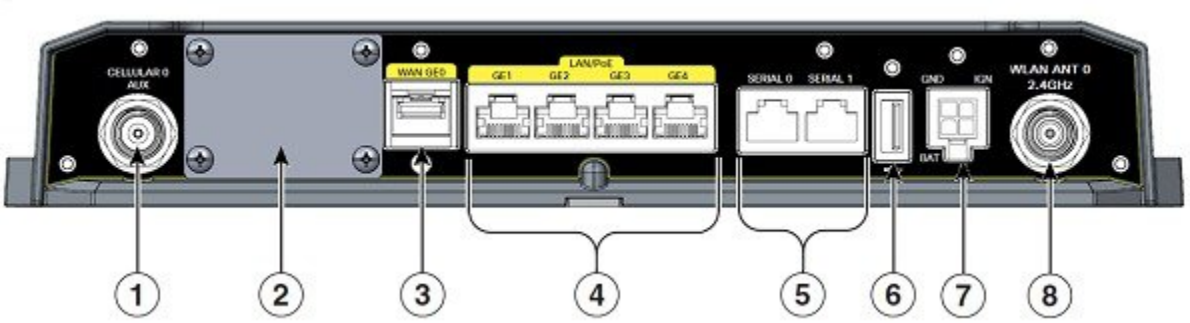
IR829 Product Overview

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.

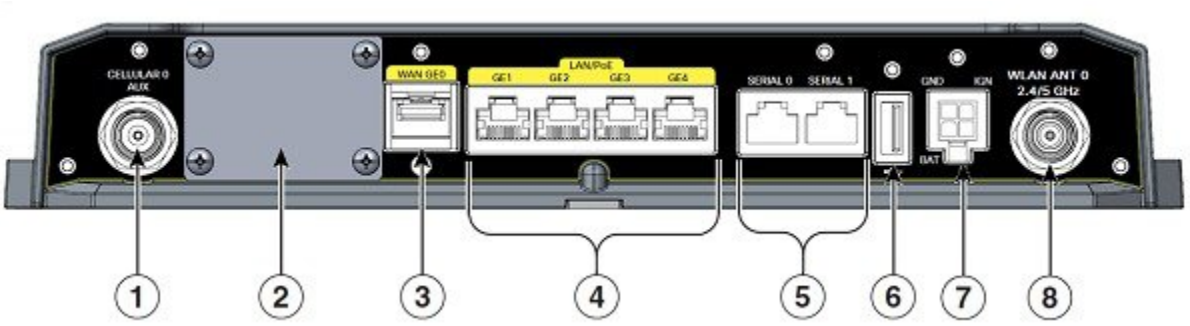
Figure 2: Cisco IR829 Front Panel Single Modem



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.

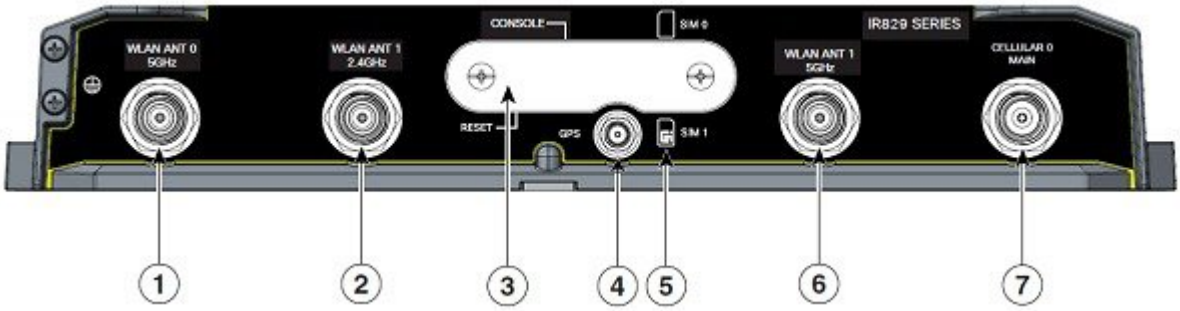
Figure 3: Cisco IR829 Front Panel Duel Modem



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.

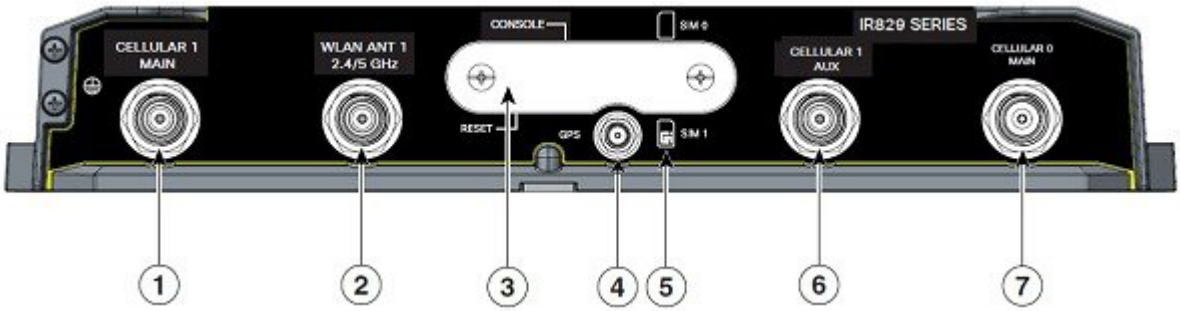
Figure 4: Cisco IR829 Back Panel Single Modem



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

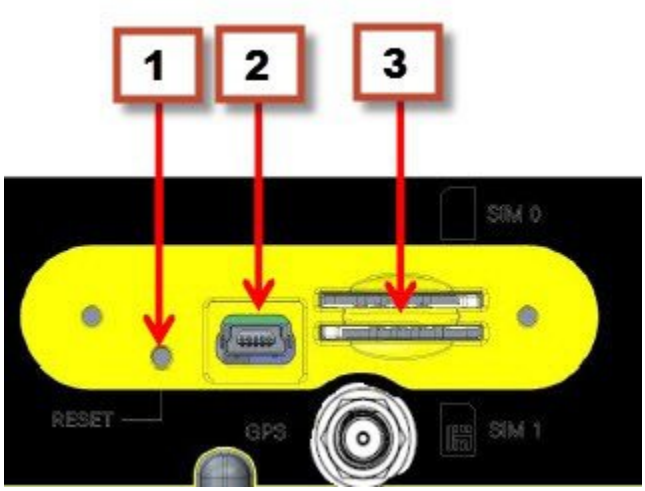


Figure 7: Cisco IR829 Top Cover, on page 6 shows the top of the Cisco IR829.

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

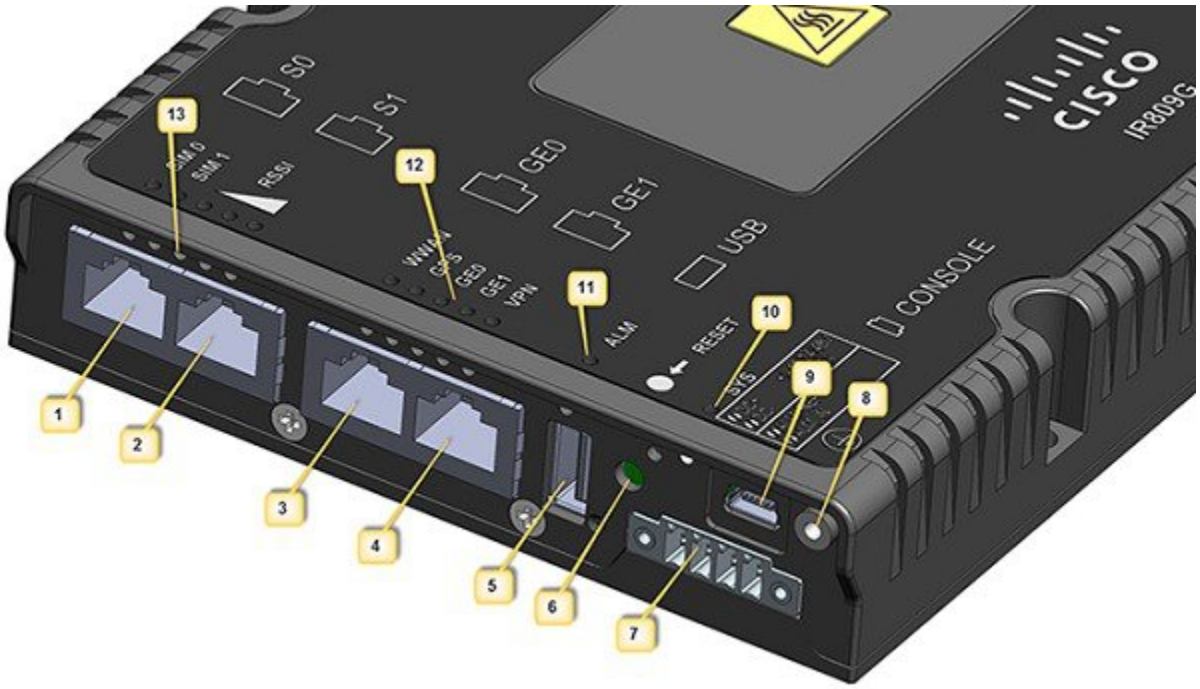
IR809 Product Overview

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



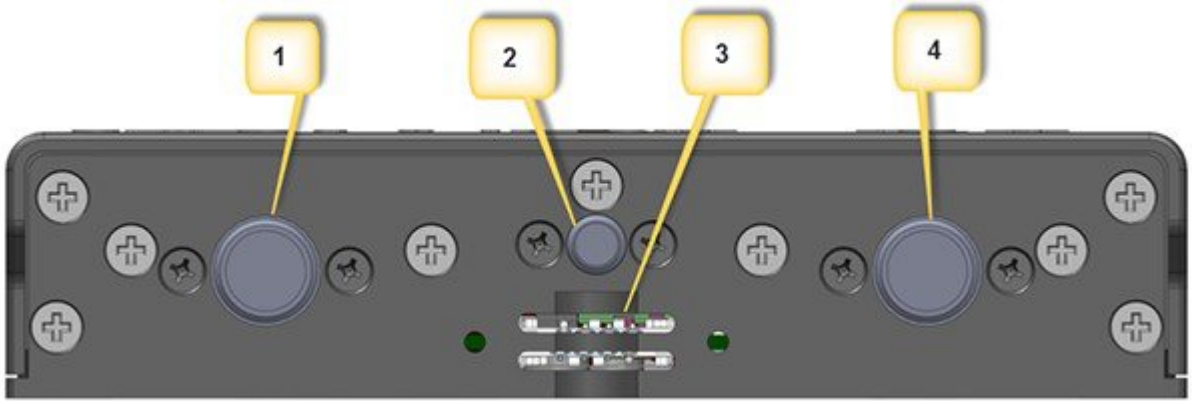
1	S0 RS232 DCE/RS485 Combo Port	8	Grounding Point

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.

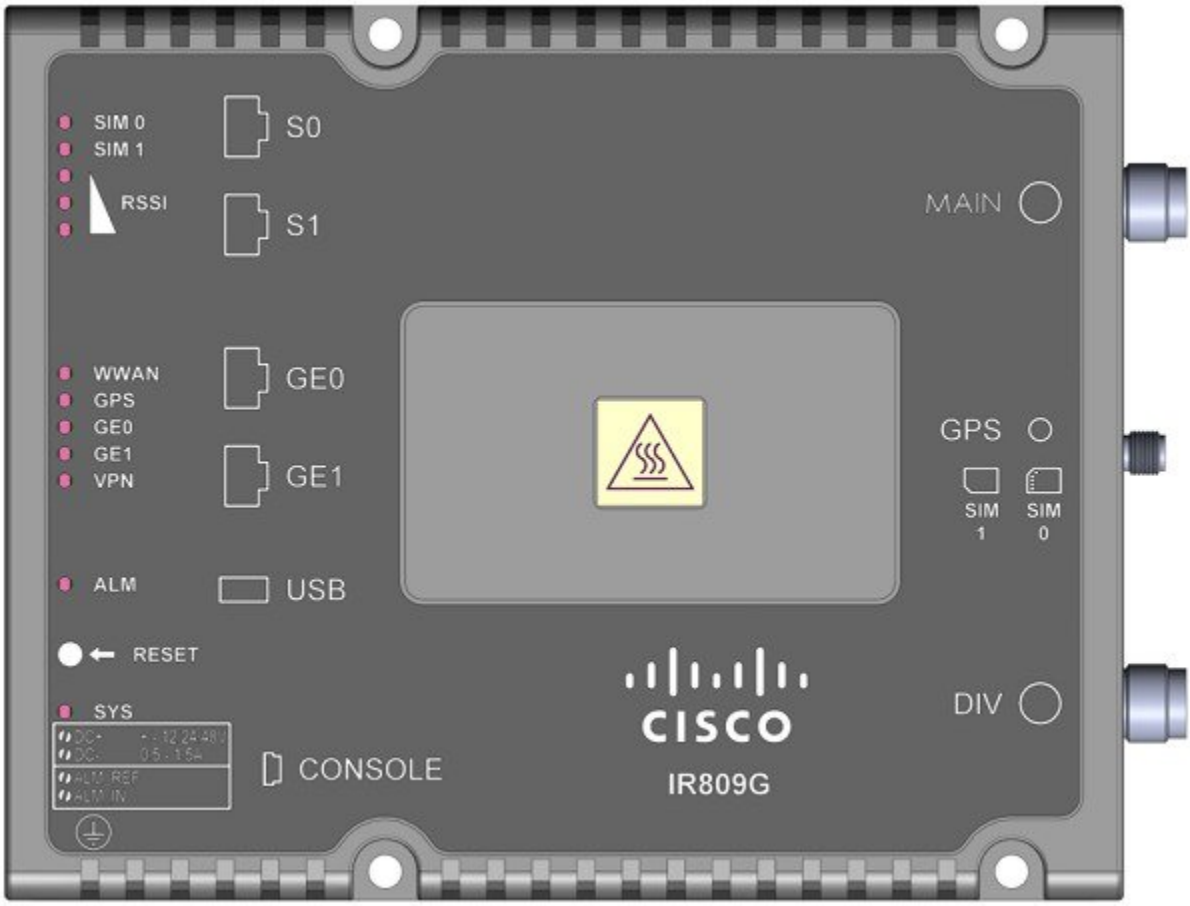
Figure 11: Cisco IR809 Back Panel



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 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