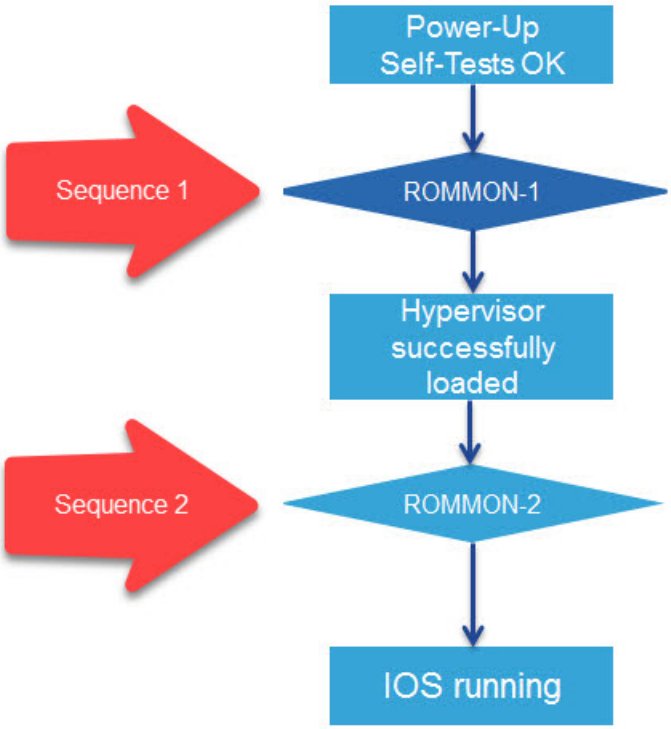
Initial Configuration

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 10 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