Cisco IOS Release 15.8(3)M1 - Release Notes for Cisco IR800 Industrial Integrated Services Routers and Cisco CGR1000 Series Connected Grid Routers

The following release notes support the Cisco IOS 15.8(3)M1 release. These release notes are updated to describe new features, limitations, troubleshooting, recommended configurations, caveats, and provide information on how to obtain support and documentation.

Contents

This publication consists of the following sections:

Image Information and Supported Platforms

Note: You must have a Cisco.com account to download the software.

Cisco IOS Release 15.8(3)M1 includes the following Cisco IOS images:

IR8x9

- System Bundled Image: ir800-universalk9-bundle.SPA.158-3.M1

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.158-3.M1
  - Guest Operating System: ir800-ref-gos.img.1.7.7.1.gz
  - Hypervisor: ir800-hv.srp.SPA.3.0.71
  - FPGA: 2.7.0
  - BIOS: 22
  - MCU Application: 33

IR807

- IOS Image: ir800l-universalk9-mz.SPA.158-3.M1

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.158-3.M1
  - IOS Version: cgr1000-universalk9-mz.SPA.158-3.M1
  - Guest Operating System: cgr1000-ref-gos.img.1.7.7.1.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.36
  - FPGA: 2.9.0
  - BIOS: 15

Software Downloads

IR800 Series

The latest image files for the IR800 product family can be found here:

https://software.cisco.com/download/navigator.html?mdfid=286287045&flowid=75322

Click on the 807, 809 or 829 link to take you to the specific software you are looking for.

IR807

The IR807 link shows the following entries:

- ir800l-universalk9-mz.SPA.<*version*>.bin
- ir800l-universalk9_npe-mz.SPA.<*version*>.bin

IR809

The IR809 link shows the following entries:

- IOS Software
  - ir800-universalk9-bundle.<*version*>.bin
  - ir800-universalk9_npe-bundle.<*version*>.bin
- IOx Cartridges
  - Yocto 1.7.2 Base Rootfs (ir800_yocto-1.7.2.tar)
  - Python 2.7.3 Language Runtime (ir800_yocto-1.7.2_python-2.7.3.tar)
  - Azul Java 1.7 EJRE (ir800_yocto-1.7.2_zre1.7.0_65.7.6.0.7.tar)
  - Azul Java 1.8 Compact Profile 3 (ir800_yocto-1.7.2_zre1.8.0_65.8.10.0.1.tar)

IR829

The IR829 link shows the following entries:

Software on Chassis

- IOS Software
  - ir800-universalk9-bundle.<*version*>.bin
  - ir800-universalk9_npe-bundle.<*version*>.bin
- IOx Cartridges
  - Yocto 1.7.2 Base Rootfs (ir800_yocto-1.7.2.tar)
  - Python 2.7.3 Language Runtime (ir800_yocto-1.7.2_python-2.7.3.tar)
  - Azul Java 1.7 EJRE (ir800_yocto-1.7.2_zre1.7.0_65.7.6.0.7.tar)
  - Azul Java 1.8 Compact Profile 3 (ir800_yocto-1.7.2_zre1.8.0_65.8.10.0.1.tar)

AP803 Access Point Module

- Autonomous AP IOS Software
  - WIRELESS LAN (ap1g3-k9w7-tar.153-3.JH1.tar)
- Lightweight AP IOS Software
  - WIRELESS LAN (ap1g3-k9w8-tar.153-3.JH1.tar)
  - WIRELESS LAN LWAPP RECOVERY (ap1g3-rcvk9w8-tar.153-3.JH1.tar)

Note: On the IR8x9 devices, the ir800-universalk9-bundle.SPA.158-3.M bundle can be copied via Trivial File Transfer Protocol (TFTP) or SCP to the IR800, and then installed using the `bundle install flash:<image name>` command. The ir800-universalk9-bundle.SPA.158-3.M.bin file can NOT be directly booted using the `boot system flash:/image_name.` Detailed instructions are found in the Cisco IR800 Integrated Services Router Software Configuration Guide.

Note: On the IR8x9 devices, the cipher **dhe-aes-256-cbc-sha** (which is used with the commands **ip http client secure-ciphersuite** and **ip http secure-ciphersuite**) is no longer available in IOS 15.6(3)M and later as part of the weak cipher removal process. This cipher was flagged as a security vulnerability.

CGR1K Series

The latest image file for the CGR 1000 Series Cisco IOS image is:

https://software.cisco.com/download/navigator.html?mdfid=284165761&flowid=75122

For details on the CGR1000 installation, please see:

http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/ios/release/notes/OL-31148-05.html#pgfId-9

Warning about Installing the Image

Note: The bundle can be copied via Trivial File Transfer Protocol (TFTP) or SCP to the device, and then installed using the `bundle install flash:<image name>` command. The bin file can NOT be directly booted using the `boot system flash:/image_name.`

Major Enhancements

This section provides details on new features and functionality available in this release. Each new feature is proceeded by the platform which it applies to.

IR800 Series: GPS NMEA Multiple Stream

Feature applies to the IR807, 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 support
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.

IR8x9 and CGR1K: Display digital signature and software authenticity-related information for a specific image file from image header.

Feature applies to the IR809, IR829, CGR1120, and CGR1240

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 IR8x9 and CGR1000 platform.

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
```

IR829: Client Information Signaling Protocol (CISP)

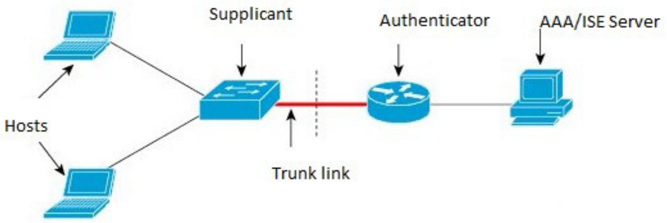
Feature applies to the IR829

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 1 illustrates how the CISP feature works in NEAT in a simple scenario.

Figure 1 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:

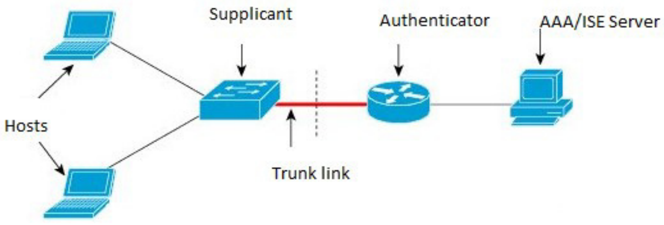
```
Oct 15 13:51:36.724: CISP-RXPAK (Fa0/6): Code: REQUEST ID:0x23 Length:0x003A  Type: ADD_CLIENT
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c1 (vlan: 200)
 to authenticator list
```

IR829: Dot1x Supplicant Support on the L2 interface

Feature applies to the IR829

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 2 illustrates the Supplicant Topology.

Figure 2 Supplicant Topology



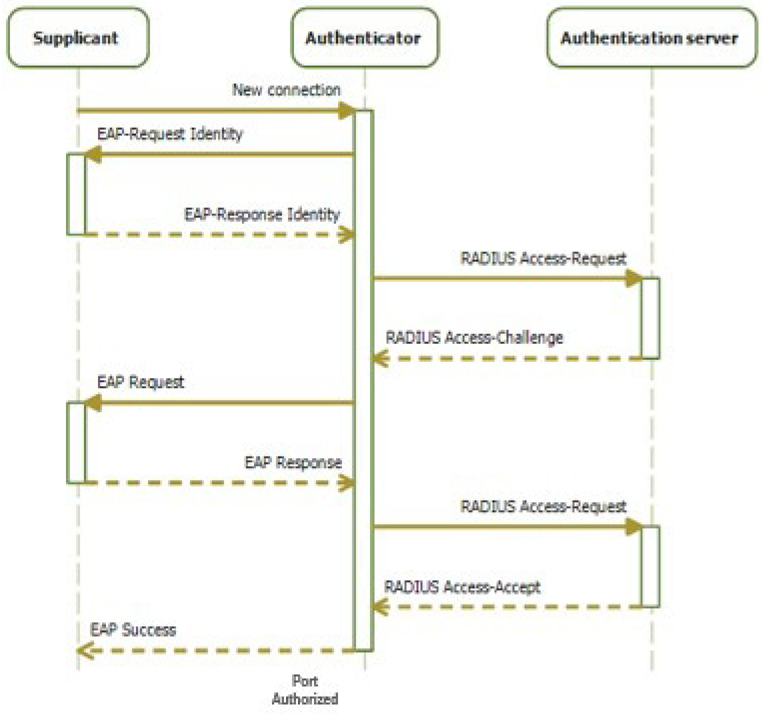
Supplicant CLI Commands

```
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 3 for the workflow.

Figure 3 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. Same flow happens when 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.

IR829: LLDP (Link Layer Discovery Protocol) Support for 3rd party PoE devices

Feature applies to the IR829

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 shows inline 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.

Related Documentation

The following documentation is available:

- Cisco IOS 15.8M cross-platform release notes:

  https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/15-8m/release/notes/15-8-3-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

- All of the Cisco CGR 1000 Series Connected Grid Routers documentation can be found here:

  http://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/tsd-products-support-series-home.html

- IoT Field Network Director

  https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/products-installation-and-configuration-guides-list.html

- Cisco IOx Documentation is found here:

  https://www.cisco.com/c/en/us/support/cloud-systems-management/iox/tsd-products-support-series-home.html

- Cisco IOx Developer information is found here:

  https://developer.cisco.com/docs/iox/

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Cisco IOS Release 15.8(3)M1

The following sections list caveats for Cisco IOS Release 15.8(3)M1:

Open Caveats

- **CSCvm60441**

  iox sched-policy 100 does not work

  Symptoms: iox sched-policy setting 100 might shut down VDS and reload router.

  Workaround: On a router reload with this configuration, the device mostly recovers. This is a troubleshooting only cli, not to be used often in deployments.

- **CSCvn36295**

  The command show cel 0 firmware does not show the correct output

  Symptoms:

```
Router#show cel 0 firmware
 Idx Carrier      FwVersion    PriVersion   Status
 1   ATT          07.12.09.00               Inactive
 2   07.12.09.00  000          .00          Active
 3   000                                    Inactive

Firmware Activation mode : AUTO
Div-PNP#
Div-PNP#

/ # echo -e 'at!image?\r\n' > /dev/ttyUSB2
/ # at!image?
TYPE SLOT STATUS LRU FAILURES UNIQUE_ID   BUILD_ID
FW   1    EMPTY  0   0 0
FW   2    GOOD   2   0 0      001.020_000 07.12.09.00_SPRINT
FW   3    EMPTY  0   0 0
Max FW images: 3
Active FW image is at slot 2

TYPE SLOT STATUS LRU FAILURES UNIQUE_ID   BUILD_ID
PRI  FF   GOOD   0   0 0      001.028_000 07.12.09.00_ATT
PRI  FF   GOOD   0   0 0      001.033_000 07.12.09.00_GENERIC
PRI  FF   GOOD   0   0 0      001.020_000 07.12.09.00_SPRINT
Max PRI images: 50


OK
exit
```

Issue seen on IR829 with the MC7455 modem as well.

```
Router#show cel 0/0 firmware
 Idx Carrier      FwVersion    PriVersion   Status
 1   ATT          02.30.01.01                Active
 2   02.30.01.01  000                        Inactive

Firmware Activation mode : MANUAL
Router#

======= IR829 Observation ====

==== IR829 ====
Issue also observed on IR829-2LTE with MC7455
Platform: IR829
Modem: MC7455MOBILE
IOS Ver: 15.8(3)M1
IR829-27455-VZW#sh cell 0/0 firm
Idx Carrier      FwVersion    PriVersion   Status
1   ATT          02.20.03.00                Inactive
2   02.24.05.06  000          .00          Inactive
3   000                       ZON          Inactive
4                052_000                   Inactive
5                                          Active
======
```

Workaround: There is no workaround.

- **CSCvm32638**

  Low power modem reset reason does not work

  Symptoms: 'power_save_mode' scenario is not working as expected in 4G_LTE.

  Workaround: NA, functionally the modem is fine, just the reset reason display has issue. Will be corrected in the next release.

Resolved Caveats

The following caveats are fixed with this release:

- **CSCvm09552- IR8x9**

  On the IR800 series, occasionally the GPS status would get stuck in " GPS location cannot be acquired" and not able to recover by itself until an IOS reboot.

- **CSCvm07801 - all IoT Routers**

On the IR800 series, SMS triggers a Cellular modem crash.

Symptoms: Upon receiving certain format SMS messages, modem crashes immediately.

Issue was reported on an IR829GW-LTE-VZ-AK9 with the MC7350 modem running IOS version 15.8-3M. FW version:SWI9X15C_05.05.58.01. However, this issue applies to both the MC73xx and MC74xx modems on all platforms.

- **CSCvm12409 - all IoT Routers**

  Modem crash action set to wrong value on modem side.

  Symptoms: The value was always set to 0 on the modem side.

- **CSCvm19614 - all IoT Routers**

  The **show cellular modem crash-action** command displays the opposite of what is configured under the controller.

  Symptoms: When " lte modem crash-action boot-and-hold" is configured under controller, the **show cellular modem crash-action** command displays " reset" and vice-versa.

- **CSCvk50787- IR8x9 and CGR1K**

  Controller doesn't show cellular modem USB-Net Driver version.

  Symptoms: The 'Driver Version' under the 'show controller cellular <interface>' command shows '<unknown>'.

- **CSCvk32829 - IR807**

  Re-enable MPDN for the IR807 WP7601 sku and revert GobiUSBNet drivers to 2.50.

  Symptoms: MPDN is not supported on the IR807 with the WP7601 modem running the 15.8(3)M release.

  Workaround: Re-enable MPDN for the IR807 with the WP7601 modem and revert GobiUSBNet drivers to 2.50.

- **CSCvm68386**

  Ignition undervoltage millivolts is not persistent on reload

  Symptoms: Ignition undervoltage threshold setting in millivolts is not persistent on reload. Volt value is intact, only the decimal value is not persistent.

  Workaround: EEM to reconfigure millivolt threshold on device bootup:

  ```
  conf t
  event manager applet ignition_uv_config
  event syslog pattern "Process IR800 Test top-level routine exited"
  action 1.0 cli command "conf t"
  action 1.1 cli command "ignition undervoltage threshold 11 999"
  ```

- **CSCvm46645 - IR8x9**

  [IOX-SS] Change monitrc to allow for infinite tries to restart secure storage

  Symptoms: IOx came up in recovery mode because secure storage service didn’t come up.

  Secure storage service log shows it failed to come up due to network connectivity to IOS. However, ping command went through fine when entered manually from Guest OS console.

  Conditions: This is timing related, triggered by the missing IOS configurations needed for Guest OS networking connectivity at device power up. Secure storage service tried to connect to the server on IOS side and gave up after 5 retries.

Workaround: Restart guest OS VM after the IOS configuration change by " guest-os 1 restart" . Or, save the configuration, and reload the router.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.