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

IR8x9

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

  This bundle contains the following components:

  - IOS: ir800-universalk9-mz.SPA.158-3.M
  - Guest Operating System: ir800-ref-gos.img.1.7.3.1.gz
  - Hypervisor: ir800-hv.srp.SPA.3.0.59
  - FPGA: 2.7.0

  - BIOS: 21
  - MCU Application: 33

IR807

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

CGR1K

- System Bundled image: cgr1000-universalk9-bundle.SPA.158-3.M
  - IOS Version: cgr1000-universalk9-mz.SPA.158-3.M
  - Guest Operating System: cgr1000-ref-gos.img.1.7.3.1.gz
  - Hypervisor: cgr1000-hv.srp.SPA.3.0.29
  - 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 he 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

Note: The cgr1000-universalk9-mz.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 cgr1000-universalk9-mz.SPA.158-3.M.bin file can NOT be directly booted using the `boot system flash:/image_name`. Detailed instructions are found in the CGR1000 documentation.

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-998856

Known Limitations

This release has the following limitations or deviations for expected behavior:

Core Dump Limitation:

On both the CGR1000 and IR8x9 platforms, the core dump fails to write into the local flash. The IOS is running as a virtual machine and then hypervisor is running underneath. The local flash is provided by the hypervisor as a virtual disk. When a crash occurs, this virtual disk is no longer available therefore copying to flash will fail. The workaround is to use an ftp server to copy the core dump to.

Platform Resource Limitation:

On both the CGR1000 and IR8x9 platforms, if the IOx interface communicating with IOx applications hosted on the Guest-OS of IR8x9 or CGR1000, it is important to note the platforms are limited in CPU resources. The recommended configuration would be to rate-limit the guest-os interface if sending traffic throughput beyond best performance (best non-drop rate: 70Mbps and IOS CPU: 65%).

Bundle Install Only for Software Upgrade Limitation:

On both the CGR1000 and IR8x9 platforms, Cisco mandates using the bundle install option only for software upgrade/downgrade. Manually downgrading a device from 15.8(3)M to previous releases from rommon mode will have consequences such as files or filesystems being wiped out.

Cellular Interfaces

These release Notes cover multiple products. The cellular interfaces mentioned will vary depending on which model of the device you are using. Table 1 should be used as a reference for cellular interface numbering and applied to examples used withing these release notes.

Table 1 Cellular Interface Details

Router	Controller	SIM	Modem Slot	PDN Interface
IR829	0	0|1	0	Cellular 0
IR829	0	0|1	0	Cellular 1
IR829 (dual modem)	0	0	0	Cellular 0/0
IR829 (dual modem)	0	0	0	Cellular 0/1
IR829 (dual modem)	1	1	1	Cellular 1/0
IR829 (dual modem)	1	1	1	Cellular 1/1
IR809	0	0|1	0	Cellular 0
IR809	0	0|1	0	Cellular 1
IR807	0	0	0	Cellular 0
CGR1120	0	0|1	3/1	Cellular 3/1
CGR1120 (dual modem)	0	0	3/1	Cellular 3/1
CGR1120 (dual modem)	1	1	4/1	Cellular 4/1
CGR1240	0	0|1	3/1	Cellular 3/1
CGR1240(dual modem)	0	0	3/1	Cellular 3/1
CGR1240(dual modem)	1	1	6/1	Cellular 6/1

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.

IR807: AutoSim and Firmware Based Switching running the WP7504 Modem

Feature applies to the IR807

The AutoSim feature will identify the SIM card of the Carrier inserted and correspondingly load the correct modem firmware. The advantages of the AutoSim feature are:

- Ease of Ordering Carrier Specific SKUs
- Quicker failover times in dual-sim deployments

Auto-SIM is supported in Sierra wireless WP7504 modem on the IR807. The WP7502 and WP7601 modems do not support this feature. A CLI is available in the cellular controller to enable/disable Auto-SIM. The modem in Auto-SIM mode selects the right carrier firmware after a SIM slot switch and an automatic modem reset. During bootup, if the Auto-SIM configuration on the modem doesn't match to the IOS configuration, the corresponding Auto-SIM or manual mode is pushed to the modem.

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

```
controller cellular 0
[no] lte firmware auto-sim
```

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

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

Enable/Disable Auto-SIM:

```
(config)#controller cellular 0
(config)# [no] lte firmware auto-sim   default is auto-sim enabled
```

Manual mode:

```
controller cellular 0
no lte firmware auto-sim
```

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

```
show cellular 0 firmware
```

For additional information, see the following guide:

Cisco 4G LTE and Cisco 4G LTE-Advanced Network Interface Module Software Configuration Guide

IR807: MTU Selection for WP76xx modems

Feature applies only to the IR807

This new feature allows the user to configure the mtu setting under the controller, up to a value of 2000, for the WP76xx modems. This requires setting the mtu on the corresponding cellular interface to match the same value as the controller.

Refer to Table 1 for details on cellular interface numbering on your particular device.

The following example shows the controller configuration commands:

```
router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router#(config-controller)#lte modem mtu ?
  <64-2000>  Mtu value
```

IR829: Plug and Play (PnP) Support on the LAN Interfaces

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
```

IR829: Auto-Negotiation Support for Gigabit-Ethernet 0

Feature applies to 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.

IR829: Ignition Undervoltage Threshold in Double Decimal

Feature applies to the IR829

With this new feature, you can now configure voltage in decimals instead of whole numbers and set the undervoltage threshold values up to the millivolt range. There is a new cli that can be used **ignition undervoltage threshold <Volt> <mV if any>**. An example of the command usage follows:

Show current ignition status

```
IR800#show ignition
Status:
  Ignition management: Disabled
  Input voltage:       0.0 V
  Ignition status:     Power on
  Shutdown timer:      0.0 s to off [will begin power down at ~100 sec]
Thresholds:
  Undervoltage:        9.000 V
  Overvoltage:         32.0 V
  Undervoltage timer:  120.0 s
  Overvoltage timer:   1.0 s
  Ignition-Off timer:  900.0 s
```

Set the undervoltage threshold

```
IR800(config)#ignition undervoltage threshold ?
  <9-24>  Threshold to shut the system off; value in volts

IR800(config)#ignition undervoltage threshold 10 ?
  <0-999>  Enter millivolt (mV), if any

IR800(config)#ignition undervoltage threshold 10 989

IR800#show ignition
Status:
  Ignition management: Disabled
  Input voltage:       12.2 V
  Ignition status:     Power on
  Shutdown timer:      0.0 s to off [will begin power down at ~100 sec]
Thresholds:
  Undervoltage:        10.989 V
  Overvoltage:         32.0 V
  Undervoltage timer:  120.0 s
  Overvoltage timer:   1.0 s
```

```
        Ignition-Off timer:  900.0 s
```

Additional command examples

To set 9.5V; Voltage=9, mV=500

```
IR800(config)# ignition undervoltage threshold 9 500
```

To set 10.95V; Voltage =10, mV=950

```
IR800(config)# ignition undervoltage threshold 10 950
```

To set 10.005; Voltage=10, mV=5

```
IR800(config)# ignition undervoltage threshold 10 5
```

IR8x9: Auto-recovery of Corrupt Filesystems

Feature applies to the IR809 and IR829

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 this release (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

Note: 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.

IR8x9: Radio Frequency Band Select

Feature applies to the IR8x9 series

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

Refer to Table 1 for details on cellular interface numbering on your particular device.

The following examples show the controller configuration commands:

```
router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
router(config)#controller cell <interface number>
router(config-controller)#lte modem ?
  band-select       Modem band select
  dm-log            Modem DM logging configuration
  fota-poll-timer   Set poll timer for AVMS to do Firmware upgrade over the air
  link-recovery     Cellular Link Recovery
  mtu               Modem mtu
  nas-log           Modem NAS logging configuration

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

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

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

```
  slot  primary SIM slot

router(config-controller)#lte modem band-select band- indices "2 4 5" slot ?
  <0-1>  Slot number

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

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

The following examples show the controller show commands:

```
router#show cellular <interface number> radio ?
  band     Show Radio band settings
  history  Show Radio history in graph format
  |        Output modifiers
  <cr>     <cr>

router#show cellular <interface number> radio band

LTE bands supported by modem:
- Bands 2 4 5 12.
LTE band Preference settings for the active sim(slot 0):
- Bands 2 4 5 12.

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

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

IR807 and IR8x9: Low Power Mode

Feature applies to IR807 and IR8x9

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

Refer to Table 1 for details on cellular interface numbering on your particular device.

The following examples show the controller show commands:

```
router# show cellular <interface number> radio
Radio power mode = OFF, Reason = User Request
Channel Number = 0
Current Band = Unknown
Current RSSI = -128 dBm
Current ECIO = -2 dBm
Radio Access Technology(RAT) Preference = AUTO
Radio Access Technology(RAT) Selected = AUTO


router# show cellular <interface number> radio details
 Radio turned off under cellular controller configuration.
router#
```

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

IR8x9 and IR807: Enhancement to Modem Crash Action

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

Generate 4G Modem Crash Dump

-or

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

A new CLI has been added to simplify the configuration to put the modem in a diagnostic mode upon a crash. The CLI is **lte modem crash-action**. The device can be set to either reset, or to boot and hold.

The following examples show the new functionality of the configuration CLI:

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

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

The following examples show the new functionality of the exec CLI:

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

This CLI will set the flag on the modem, to either 1 - reset or 0 - boot and hold respectively. This is the same as AT command **at!eroption=?**.

The following examples show the new functionality of the exec CLI:

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

Note: This feature is only used while debugging modem crash dump and should be used **ONLY** as advised by Cisco TAC. **Please do not enable this feature before consulting with Cisco TAC**.

IR829M: Displaying the Wear Leveling Data for the mSATA SSD

Feature applies to the IR829M

IOx Local Manager/ Fog Director can now display the wear leveling data for the mSATA SSD on the IR829M products.

In the IOx Local Manager, it is observed by selecting **System > Storage**.

From the IOS command line, you can monitor the lifetime using the **show platform msata** command.

The following example shows a 50G mSATA controller.

```
Router#show platform msata
SSD Lifetime:
Lifetime Remaining: 99%
Memory:
Size: 50G.
Used: 49G
Available: 932M
Usage: 99%
```

After a router reload, it will take a few minutes (approximately 5) before this data will be populated again.

When the SSD lifetime reduces to 15%, 10% and 5% of the lifetime limit, errors start getting reported in syslog.

For example:

```
*Jan 30 19:03:00.257: %IOX-4-IOX_SSD_LIFETIME_WARN: SSD Lifetime remaining in module:15
*Jan 30 19:02:30.157: %IOX-2-IOX_SSD_LIFETIME_CRITICAL: SSD Lifetime remaining in module:5
```

IR8x9 and CGR1K: Improvements in IOS and Guest-OS Clock Time Synchronization

Feature applies to IR8x9 and CGR1000

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

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

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

IOS clock time:

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

Guest-OS(IOX) system time and hardware time

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

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

CGR1K: 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 filesystem may be partially or completely inaccessible at this point.

Starting with this release (15.8(3)M), on the CGR1K 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:cgr1000-universalk9-mz.SPA.158-3.M
Installing bundle image:
/cgr1000-universalk9-mz.SPA.158-3.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'.

This backup partition is taken from the Guest-OS data partition.

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 CGR1K, 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
- 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

Note: 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, they must increase their Guest-OS free disk space manually.

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 small file is not persistent on soft reload of the router.

Alternatively, the user can also backup using:

```
CGR1K#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.

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)M

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

Open Caveats

- **CSCvk34848**

  On the CGR1K, setting config reg value to 0x100 shows false boot message in rommon2

  Symptoms: When config reg value is set to 0x100, rommon2 attempts to boot an invalid image which causes the BOT_IOS_SEQUENCE to be exhausted. For example:

```
IOFPGA @ 0xd0000000 version=0x30020900, datecode=0xd091e17 CPLD version 0x14
Reset reason (1.0):   CLI initiated reload

CGR Loader Stage 2 Version: 1.9.17


Config Register configured to stop at rommon
Autoboot string cgr1000-hv.srp.SPA.3.0.26

Booting image: cgr1000-hv.srp.SPA.3.0.26....
Autoboot failed with error=1
Last boot attempt failed, now retry 2 of 4

Booting image: cgr1000-hv.srp.SPA.3.0.26....
Autoboot failed with error=1
Last boot attempt failed, now retry 3 of 4

Booting image: cgr1000-hv.srp.SPA.3.0.26....
Autoboot failed with error=1
Last boot attempt failed, now retry 4 of 4
```

```
Booting image: cgr1000-hv.srp.SPA.3.0.26....
Autoboot failed with error=1


rommon-2>
```

Workaround: There is no workaround, will be corrected in a future release.

- **CSCvk11001**

  On the IR829, WANMon level 1 recovery doesn't power-cycle the cellular modem

  Symptoms: When cell 0/0 goes down and WANMon kicks in, the level 0 and level 2 recovery actions work, but level 1 recovery action that requires interface reload doesn't power-cycle the associated modem.

  Workaround: There is no workaround.

- **CSCvk18541**

  On the IR800, fs_recovered.ios needs to be persistent across a soft reload.

  Workaround: To be fixed in a future release.

- **CSCvj95761**

  On the CGR1K, the device may keep repeating a 4-way handshake after decreasing the mesh-key lifetime.

  Symptoms: If the Mesh-Security mesh-key lifetime is set to a high value, and keys are generated, then the Mesh-Security mesh-key lifetime is set to a lower value. The CGR router will authenticate an endpoint and do the 4-way handshake. After this is complete the CGR will keep repeating the 4-way handshake and never get to the group key messages. For example, if the expiration of the first key is 126 days, and the other keys are 180 days (original setting). If the mesh-key lifetime is then changed to 60 days, when the CGR would finish the 4-way key exchange, it would set a Temporal Key Lifetime of 120 days (2 times the current Mesh Key Lifetime). Since the 120 day lifetime is less than the first group key life time, the CGR would log the following:

  ```
  PDT: (Meshsec Process)meshsec-ses(Vi0): 0007814300D59FF4(024300D59FF4)[S_PTK_AVAIL   ]:PTK is going
  to expire soon.
  ```

  The problem exists because each mesh-key is generated with the lifetime set to current mesh-key lifetime setting at the time it is created. If the mesh-key lifetime is later changed, the previously generated mesh-keys (not yet expired) will still have the original mesh-key lifetime.

  Workaround: Users must manually expire the existing mesh-keys and regenerate new mesh-keys if the mesh-key lifetime is changed.

- **CSCvi66566**

  CGR1K: Observed on the CGR1000 CGM-SRV Compute Module.

  Workaround: Change the MTU size CGR-SRV module interfaces to match the endpoint device limitation.

- **CSCvi59098**

  show run does not reflect show line stats when line configs pushed through stty from Guest-OS

  Symptoms: Functionally there is no impact. the show line CLI reflects the correct data. The show run | i line' CLI alone reflects the same information for both line1 and line2, only when pushed from Guest-OS.

  Workaround: N/A, no functional impact.

- **CSCvi59013**

  Serial relay line propagation not working from guest-os after making config edits in IOS

Workaround: Configuration can either be pushed from the Guest-OS or IOS. If using both interchangeably, you need to execute 'no relay line propagation' or ' relay line propagation' each time.

Resolved Caveats

The following caveats are fixed with this release:

- **CSCvf36269**

  Cisco IOS and IOS XE Software Plug-and-Play PKI API Certificate Validation Vulnerability.

  Symptoms: When there is a boot failure, for example a bootable image is not found, autoboot sequence failure should go all the way to 20. On occasion, the retries will only attempt 16 or 17 times.

  Conditions: Device configured with the Cisco Plug and Play feature enabled and, with the PKI API feature enabled.

  Special Note: Be aware that going forward, Plug and Play made subject name alternative as a mandatory field.

- **CSCvi61559**

  Autoboot sequence sometimes stops at 16, instead of 20.

  Symptoms: When there is a boot failure, for example a bootable image is not found, autoboot sequence failure should go all the way to 20. On occasion, the retries will only attempt 16 or 17 times.

- **CSCvi51666**

  IOx clock must be in sync with the IOS NTP clock.

  Resolved State: Sync time is improved from 30 seconds sync to 1second sync time from this release going forward.

- **CSCvh04377**

  NTPd is not available in the CGR1000 GOS images.

  Network Time Protocol is not available in the CGR1000 GOS images (with CAF support) because the GOS time sync is now obtained through IOS via TPMC heartbeats

- **CSCvg91530**

  When changing the ignition timer with ignition already enabled, a graceful shutdown does not happen at ~100s.

- **CSCvi24557**

  Incorrect display for the Network field under the CLI **show cell *<your interface>* network**

  Symptoms: The 'show cellular <slot> all | network' command shows incorrect 'Network' field. CLI output may show all digits instead of known Network Id such as 'AT&T' or 'Verizon Wireless'. See below as an example:

```
IR829#sh cellular 1/0 network
Current System Time = Fri Mar 2 0:47:54 2018
Current Service Status = Normal
Current Service = Packet switched
Current Roaming Status = Home
Network Selection Mode = Automatic
Network = 054 154
Mobile Country Code (MCC) = 310
Mobile Network Code (MNC) = 410
...
```

Conditions: The modem is attached to a live network. Modem operation is not known to be affected by this issue. Issue is only incorrect display of the cellular Network Id.

Workaround: None in the 15.7(3)M1 release. Upgrade to IOS release 15.8 where the issue is fixed.

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.