Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco IOS Release 15.4(2)CG

First Published: January 21, 2014

Last Updated: July 16, 2014

Part Number: OL-31148-10

These release notes contain the latest information about using Cisco IOS software with the Cisco 1000 Series Connected Grid Routers (CGR 1000 or routers) for Release 15.4(1)CG and Release 15.4(2)CG, including this new information:

- Overview of new features added in this release. (See About the Cisco 1000 Series Connected Grid Routers, page 2.)
- Open caveats in this release. (See Caveats, page 16.)

Note

- You can migrate CGR 1000 Series routers installed with CG-OS Release CG3 (and later) to Cisco IOS 15.4(2)CG. For details, please contact your Cisco representative.
- Release Cisco IOS 15.4(**1**)CG **does not** support migration from Cisco CG-OS to Cisco IOS.

Tell Us What You Think

Send your feedback about this document directly to the Cisco Connected Energy Documentation Team.

Connected Energy Documentation Feedback Form

Cisco Systems, Inc.
www.cisco.com

Contents

These release notes include the following sections:

- About the Cisco 1000 Series Connected Grid Routers, page 2
- New Features, page 7
- System Requirements, page 9
- Installation Notes, page 10
- Important Notes, page 11
- Limitations and Restrictions, page 12
- Caveats, page 16
- Obtaining Documentation and Submitting a Service Request, page 22

About the Cisco 1000 Series Connected Grid Routers

Cisco 1000 Series Connected Grid Routers are multi-service communications platforms designed for use in field area networks. The portfolio consists of two models – both ruggedized to varying degrees for outdoor and indoor deployments. Both models are modular and support a wide-range of communications interfaces such as 2G/3G cellular, Ethernet, WiFi, WiMAX, and IEEE 802.15.4g/e.

Features and Capabilities

- Rugged industrial design and compliance with IEC-61850-3 and IEEE 1613 for utility substation environments
- Feature-rich software capabilities, including dual-stack (IPv4 & IPv6) support and traffic priority using IP QoS
- Comprehensive security capabilities based on open standards
- Highly resilient design that optimizes communications network uptime and availability
- Network and device management tools for easy deployment, upgrades, and remote monitoring

Command-Line Interface

The Cisco IOS software supports a command-line interface to configure and monitor the system.

Network Management

Table 1 provides an overview of the embedded management features available in this Cisco IOS release for the CGR 1000s. For feature overview and configuration details, see the software guides at www.cisco.com/go/cgr1000-docs (except as noted in the table).

Table 2 provides an overview of the software features supported on the CGR 1000 in this Cisco IOS release.

Table 3 provides an overview of the hardware features supported on the CGR 1000 in this Cisco IOS release.

Table 1 Embedded Management Features Available with this Cisco IOS Software

Feature	Description
Web Services Management Agent (WMSA)	WSMA defines a mechanism through which you can manage a network device, retrieve configuration data information, and upload and manipulate new configuration data. WSMA uses XML-based data encoding that is transported by the Simple Object Access Protocol (SOAP) for the configuration data and protocol messages.
Embedded Event Manager (EEM)	Cisco IOS EEM is a distributed and customized approach to event detection and recovery offered directly in a Cisco IOS Software device. It offers the ability to monitor events and take informational, corrective, or any desired EEM action when the monitored events occur or when a threshold is reached.
Simple Network Management Protocol (SNMP)	An application-layer protocol that provides a message format for communication between SNMP managers and agents. This software supports SNMPv1, SNMPv2c and SNMPv3.
Remote Monitoring (RMON)	RMON is a standard monitoring specification that enables various network monitors and console systems to exchange network-monitoring data. RMON requires SNMP to be configured on the server that contains the RMON MIB. Feature is not supported on Ethernet.
System message logging (syslog)	Syslog allows you to configure the destination device of the system messages and to filter system messages by severity level. System messages can be logged to terminal sessions, a log file, and to syslog servers on remote systems.

Table 2 Software Feature Support on Cisco CGR 1000 Series with Cisco IOS

Feature	Description	Related Documentation
Layer 2 and 3 switching	Includes configuration details for Fast Ethernet (Layer 2) and Gigabit Ethernet (Layer 3) interfaces and supported features.	For feature overview and configuration details, see the *Layer 2/3 Switching Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs
Layer 2 Tunnel Protocol Version 3 (L2TPv3)	Provides a method for delivering Layer 2 tunnel protocol services over an IP network.	For feature overview and configuration details, see the *Layer 2 Tunnel Protocol Version 3 Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs
FlexVPN	A flexible and scalable VPN solution that implements IPsec and IKEv2. Site-to-Site and Hub-and-Spoke implementations are supported.	For feature overview and configuration details, see the *FlexVPN Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs
VPN Routing and Forwarding (VRF)-Lite	Allows a service provider to support two or more VPNs with overlapping IP addresses using one interface. Details provided for IPv4 and IPv6.	For feature over*view and configuration details, see the VPN Routing and Forwarding (VRF)-Lite Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs
Multi-protocol Border Gateway Protocol (MP-BGP)	Supports distribution of both IPv4 and IPv6 addresses in parallel.	For feature overview and configuration details, see the *Multi-Protocol Border Gateway Protocol Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs.
Quality of Service (QoS)	Allows you to classify the network traffic, prioritize the traffic flow, and help avoid traffic congestion in your network.	For feature overview and configuration details, see the *Quality of Service Solutions Configuration Guide Library, Cisco IOS Release 15M&T* at http://www.cisco.com/en/US/docs/ios-xml/ios/qos/config_library/15-mt/qos-15-mt-library.html
WAN Link Recovery Policy (3G, WiMAX, Ethernet)	Allows you to define a recovery policy specific to supported physical links (3G GSM/CDMA, WiMAX, Ethernet connected to a satellite modem) and virtual links (IPsec tunnel interfaces)	For feature overview and configuration details, see the *WAN Link Recovery Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs.

Table 2 Software Feature Support on Cisco CGR 1000 Series with Cisco IOS (continued)

Feature	Description	Related Documentation
SNMP	Summary of supported CGR 1000 MIBs and SNMP notifications and configuration details. Software supports SNMPv1, SNMPv2c and SNMPv3.	For feature overview and configuration details, see the *SNMP Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs.
Raw Socket Transport	Method of transporting serial data through an IP network. Feature can be used to transport Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). Feature supports TCP of UDP as the transport protocol.	For feature overview and configuration details, see the *Raw Socket Transport Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs.
Protocol Translation	Allows operation of the CGR 1000 within a SCADA system by providing IEC 60870-5-101 to IEC 60870-5-104 protocol translation and DNP3 to DNP3/IP protocol translation.	For feature overview and configuration details, see the *Protocol Translation Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs

Table 3 provides an overview of the hardware features and interfaces supported on Cisco CGR 1000 Series routers with Cisco IOS.

Table 3 Hardware Feature Support on Cisco CGR 1000 Series Routers with Cisco IOS

Feature	Description	Related Documentation
Hardware features	Highlight of features: • Hardware Crypto • SD card locking • Small Form-Factor Pluggable (SFP) Modules • GPS • Real-time clock • Battery backup (CGR 1240 only)	For feature overview and configuration details for the hardware features as well as mounting and installation details for the router, see the *Cisco 1240 Connected Grid Router Hardware Installation Guide* or the *Cisco 1120 Connected Grid Router Hardware Installation Guide* at www.cisco.com/go/cgr1000-docs.
Ethernet interface	Integrated Ethernet switch module with Layer 2 Fast Ethernet ports (four on CGR 1240, six on CGR 1120) and two Gigabit Ethernet ports (Layer 2 or Layer 3).	Hardware details are addressed in the *Cisco 1240 Connected Grid Router Hardware Installation Guide* or the *Cisco 1120 Connected Grid Router Hardware Installation Guide* at www.cisco.com/go/cgr1000-docs. Feature-specific software configuration is addressed in the *Layer 2/3 Switching Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)* at www.cisco.com/go/cgr1000-docs.
WiFi interface	Integrated, short-range IEEE 802.11 b/g WiFi access point to support a wireless console connection to the CGR 1000 Series routers. Supports connection for up to five WiFi clients.	Hardware details are addressed in the *Cisco 1240 Connected Grid Router Hardware Installation Guide* or the *Cisco 1120 Connected Grid Router Hardware Installation Guide* at www.cisco.com/go/cgr1000-docs. For configuration details, see the *Cisco 1000 Series Connected Grid Routers WiFi Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.

Table 3 Hardware Feature Support on Cisco CGR 1000 Series Routers with Cisco IOS

Feature	Description	Related Documentation
Cellular interfaces (CDMA and GSM)	Wireless modules with a mini-card cellular modem (PCI-e mini-card form factor) • EVDO Rev A/0/1xRTT (CDMA version) • HSPA+/UMTS/GSM/GPRS/ EDGE (GSM version)	For feature overview and configuration details, see the: • *Cisco Connected Grid Cellular 3G CDMA Module for CGR 1000 Series Installation and Configuration Guide (Cisco IOS)* • *Cisco Connected Grid Cellular 3G GSM Module for CGR 1000 Series Installation and Configuration Guide (Cisco IOS)* at www.cisco.com/go/cgr1000-docs.
WiMAX interface	IEEE 802.16e module for providing a WAN uplink over the wireless 1.4 GHz, 1.8 GHz, 2.3 GHz and 3.65 GHz bands in Distribution Automation and AMI concentrator deployments	For feature overview and configuration details, see the *Cisco Connected Grid WiMAX Module for CGR 1000 Series Installation and Configuration Guide* at www.cisco.com/go/cgr1000-docs.

New Features

Table 4 lists new features in Release 15.4(2)CG.

Table 4 New Features in Release 15.4(2)CG

Feature	Description	First Support	Related Documentation
Dual backhaul	CGR 1000 supports dual backhauls for 3G, WiMAX, and Ethernet interfaces.	15.4(2)CG	Varied documentation given application. Please contact your Cisco representative or partner.
Power over Ethernet (PoE) on CGR 1240	CGR 1240 supports POE on Fast Ethernet port, ETH 2/5. See Documentation Updates.	15.4(2)CG	*Cisco 1240 Connected Grid Router Hardware Installation Guide*
Guest OS	CGR 1000s supports a hypervisor architecture that supports installation of multiple operating systems (Cisco IOS, Linux OS) within independent virtual machines. Specific functions include: • Serial Relay—Allows ports configured with serial relay to pass traffic directly to a Guest OS on a CGR. • Network Address Translation (NAT)	15.4(2)CG	*Guest Operating System (Guest OS) Installation and Configuration Guide for Cisco 1000 Series Connected Grid Routers* *Configuring Network Address Translation: Getting Started*

Table 4 New Features in Release 15.4(2)CG (continued)

Feature	Description	First Support	Related Documentation
CG-mesh/WPAN module support in Cisco IOS	The CG-Mesh/WPAN module provides IPv6-based, IEEE 802.15.4e/g-compliant, and highly secure wireless connectivity for the CGR 1000 to enable Field Area Network (FAN) applications. This release includes the following new CG-Mesh/WPAN features: • Support in Cisco IOS. • Capability to install the WPAN module in any slot of the CGR 1240 and CGR 1120. • Dual-PHY—A CGR 1000 can now have two WPANs, one master and one slave, using the IPv6 prefix of the master WPAN for all nodes under the two WPANs.	15.4(2)CG	*Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)*
Dynamic Port Security	Dynamic Port Security allows you to define the maximum number of devices allowed on a switch port.		See Documentation Updates for configuration command.
Per Port Storm Control	Storm control prevents traffic on a LAN from being disrupted by a broadcast, multi-cast, or unicast storm on a switch port. A LAN storm occurs when packets flood the LAN, creating excessive traffic and degrading network performance.		See the "Configuring Storm Control" section in the "Configuring Port-Based Traffic Control" chapter in the Catalyst 2950 and Catalyst 2955 Software Configuration Guide, 12.1(22)EA7 noted below: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2950/software/release/12-1_22ea/SCG/scg/swtrafc.html
MAC Authentication Bypass (MAB)	MAB uses the MAC address of a device to determine what kind of network access to provide.	15.4(2)CG	*MAC Authentication Bypass Deployment Guide* **Note** We do not support Web Authentication, Guest VLAN or Authentication Failure VLAN referenced in the Deployment Guide.

Table 4 New Features in Release 15.4(2)CG (continued)

Feature	Description	First Support	Related Documentation
SCADA T104/T101 translation enhancements	The following enhancements are added for T104/T101 translation: • Exception handling (interlock feature)—The CGR1000 can restart T104/T101 communication in the event of a connection failure. • Clock pass-through scheme —The CGR 1000 can pass its clock setting at regular intervals to the downstream T101 RTU. Clock synchronization is denied on T104 side. • Non-volatile event storage/recovery—The CGR 1000 saves a copy of a T101 change event to non-volatile memory until the T104 side confirms delivery.	15.4(2)CG	*Protocol Translation Software Configuration Guide for Cisco 1000 Series Connected Grid Routers (Cisco IOS)*
No slot limitations for 3G, WiMAX, and WPAN modules	Previously, 3G, WPAN, and WiMAX modules could not be installed in all CGR 1240 and CGR 1120 slots.	15.4(2)CG	Cisco 1000 Series Hardware Installation Guides and Module Guides www.cisco.com/go/cgr1000-docs

System Requirements

Table 5 lists the software versions associated with this release for Cisco products deployed in a Field Area Network solution.

Table 5 Minimum Software Requirements

Component	Minimum Software Version
Cisco Connected Grid Device Manager (CG-DM) for CGR 1000 Series Routers (Cisco IOS)	CG-DM 4.0
Cisco Connected Grid Network Management System (CG-NMS)	CG-NMS 2.0

Installation Notes

This section addresses the following topics:

- Determining the Software Version, page 10
- Upgrading to a New Software Release, page 10
- Erasing the Configuration File, page 11

Determining the Software Version

To identify the software version operating on the Cisco IOS router, enter the following command.

Command	Purpose
show version	Displays the software version installed on the router.

Upgrading to a New Software Release

The software image is a bundle image and includes the following components: Cisco IOS image, Guest OS, Hypervisor, and a Virtual Device Server. When you initiate installation of the software, all of the components automatically install on virtual machines with the router.

To install a new version of software, you copy the bundle image over to flash and issue the bundle install command to upgrade the software.

```
router# bundle install flash:cgr1000-universalk9-bundle.SSA.154-0.99.05.CG
```

You will then see an output similar to the one below:

```
Installing bundle image:
/cgr1000-universalk9-bundle.SSA.154-0.99.05.CG.....................................
................................................................................
................................................................................
................................................................................
........................................

updating Hypervisor image...
Sending file modes: C0444 22931642 cgr1000-hv.srp.SPA.0.30


updating IOS image...
Sending file modes: C0644 73830734 cgr1000-universalk9-mz.SSA.V154_0_99_05_CG
Done!
```

After the software installation bundle finishes and displays Done! on the screen, enter the following commands to save the configuration and complete the installation process on the router:

```
router# copy running-config startup-config
router# reload
```

Erasing the Configuration File

When you enter the **write erase {/all nvram: } /no-squeeze-reserve-space** *file-system:* | *file-system:* | **startup-config** command, it erases a specified item or initiates an action to save memory on the Cisco 1000 Series router. See specifics in the table below.

Command	Purpose
write erase {/all nvram: } /no-squeeze-reserve-space *file-system:* | *file-system:* | **startup-config**	**/all–**Erases all files in the specified file system. **nvram**–Erases all files in the NVRAM. *file-system:*–File system name, followed by a colon. For example, flash: or nvram:. **Note** This argument may not be used if the device memory contains logging persistent files. **/no-squeeze-reserve-space**–Disables the squeeze operation to conserve memory and makes the erase command compatible with older file systems. **startup-config**–Erases the contents of the configuration memory.

Important Notes

Guidelines and Limitations

Refer to the "Guidelines and Limitations" section of each chapter within the Cisco IOS software configuration guides for the Cisco 1000 Series Connected Grid Routers and the highlighted Notes, Warnings, and Cautions throughout all Cisco 1000 Series router documentation.

BBU Hardware Versions within a CGR 1240 Must Match

When you replace a BBU in the CGR 1240, we highly recommend:

- Replacing all the BBUs.
- Verifying all the replacement BBUs are the same hardware version.

When a CGR 1240 operates with different BBU versions, it may result in misbehavior in the BBU functionality. This condition is seen in CGR 1240s installed with either Cisco IOS or Cisco CG-OS software.

Disable Battery Backup Unit (BBU) During Transport or Servicing

To prevent the battery backup unit (BBU) from discharging during transport or servicing of the Cisco CGR 1240 Router, disable the BBU automatic discharge feature using the system software to reduce the discharge rate. If a pair of orange harness cables is present, ensure it is disconnected to reduce discharge rate. For details on this procedure, please see the Installing Battery Backup chapter within the Cisco 1240 Connected Grid Router Hardware Installation Guide.

BBUs are not supported on the Cisco CGR 1120 Router.

Different Index Values for SNMP and CLI on Connected Grid 3G Cellular Modules

When you use SNMP and CLI to manage the profile table for the 3G Cellular modules (GSM and CDMA), be aware that the SNMP index starts at one (1) and the CLI index starts at zero (0).

- 3G CDMA modules have profile numbers that start at 0 (read only, not configurable)
- 3G GSM modules have profile numbers that start at 1

(CSCuh99162)

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with the router. These are known limitations that will not be fixed, and there is not always a workaround for these issues. Some features might not work as documented, and some features might be affected by recent changes to the CGR 1000 router hardware or software.

Hardware Limitations

Port Limitations

Table 6 lists the limitations in this release for hardware features that are described in detail in the *Cisco Connected Grid Router Hardware Installation Guide* for the Cisco CGR 1120 or CGR 1240.

Table 6 Hardware Limitations

Feature	Label	Limitation Description
Alarm port	ALARM	Currently not supported. Supports an external alarm system for monitoring system errors and events.
IRIG-B timing port	IRIG_B	Currently not supported. Provides timing output to a connected device.
USB ports (2)	0 1	Currently not supported.

Software Limitations

- **CSCuh18075**

  Symptom: On the CGR, "%Please shutdown the interface before removing it" displays when you configure the dialer as a default interface.

  Conditions: Dialer is already in a shutdown state, and the console displays "%Please shutdown the interface before removing it". Dialer is configured as a default interface.

  Workaround: Remove Dialer Pool and then the **default interface dialer 1** command executes with no errors.

Minimal Support for SNMP write on ciscoWan3gMib for Security Reasons

The read-write operation only permits the following OIDS in CISCO-WAN-3G-MIB.

```
c3gRssiOnsetNotifThreshold
c3gRssiAbateNotifThreshold
c3gEcIoOnsetNotifThreshold
c3gEcIoAbateNotifThreshold
c3gModemTemperOnsetNotifThreshold
c3gModemTemperAbateNotifThreshold
c3gModemReset
c3gModemUpNotifEnabled
c3gModemDownNotifEnabled
c3gServiceChangedNotifEnabled
c3gNetworkChangedNotifEnabled
c3gConnectionStatusChangedNotifFlag
c3gRssiOnsetNotifEnabled
c3gRssiAbateNotifEnabled
c3gEcIoOnsetNotifEnabled
c3gEcIoAbateNotifEnabled
c3gModemTemperOnsetNotifEnabled
c3gModemTemperAbateNotifEnabled
```

Note See related **ciscoWan3gMib** caveats in this section **CSCuh85612, CSCuh88771, CSCuh88904, CSCuh88968, CSCui00861, CSCui01208, CSCui01347, CSCui03505**

- **CSCuh85612**

  Symptom: A write on c3gGsmRoamingPreference results in commit failed."

  SNMP write on most of ciscoWan3gMib is not supported for security reasons.

  Conditions:

  When you issue **snmp set** on c3gGsmRoamingPreference, you get the error message “Commit failed.”

  Workaround: There is no workaround. Limitation is by design for security reasons.

- **CSCuh88771**

  Symptom: c3gMsisdn shows an empty string in an SNMP walk.

  Conditions: SNMPget on c3gMsisdn.

  Workaround: There is no workaround. This issue is carrier dependent. When this issue is seen in the field, check with your service provider to see whether MsIsdn is populated by the service provider. For example, at&t does provide the MsIsdn value and T-mobile does not.

- **CSCuh88904**

  Symptom: When a SNMP set is issued to create a row in the PDP profile table, commitFailed was seen.

```
snmpset -v 3 -u sgbublr -l authPriv -a MD5 -A cisco1234 -x AES128 -X cisco1234
172.27.168.114 c3gGsmPdpProfileRowStatus.22.2 i 4
Error in packet.
Reason: commitFailed
Failed object: CISCO-WAN-3G-MIB::c3gGsmPdpProfileRowStatus.22.2
```

  Conditions: SNMP set operations are not allowed on c3gGsmPdpProfileTable for security reasons.

  Workaround: Use the CLI to create a new profile for profile 3 as shown in the example below:

```
cgr1000# cellular 3/1 gsm profile create 3 PRO3
Profile 3 will be created with the following values:
PDP type = IPv4
APN = PRO3
Are you sure? [confirm]
Profile 3 written to modem
```

- **CSCuh88968**

  Symptom: ciscoWan3Gmib does not support a **write** function for the c3gGsmChv1 object.

  Conditions: When a user issues a **set c3gGsmChv1** command, the set fails. By design, the write function (disabled by default) does not work on most of the ciscoWan3gMib for security reasons.

  Workaround: Enter the command **cellular** *slot/port* **gsm sim change-pin** *Old-PIN New-PIN* to set Card Holder Verification 1 (CHV1). Example below:

```
CGR1K# cellular 5/1 gsm sim  change-pin  0000 1111
```

- **CSCui00861**

  Symptom: A write on c3gCdmaSecurityTable results in commit failed.

```
Error: Commit failed
Error index: 1
1: c3gCdmaPinSecurityStatus.23 (INTEGER) unknown(1)
***** SNMP SET-RESPONSE END *****
```

  Conditions: User uses snmp create a row in the security table as the MIB has access to create a row. This results is failure as write is not supported in IOS for this MIB.

  Workaround: There is no workaround for this issue. SNMP write on most of ciscoWan3gMib is not supported for security reasons.

  Either objects are pre-set or can be set through CLI. SNMP set is not supported.

- **CSCui01208**

  Symptom: The OID c3gHdrDdtmPreference is not writable even though it is a read-write object. SNMP write on c3gHdrDdtmPreference is not supported for security reasons.

  Conditions: The requested set on c3gHdrDdtmPreference always results in Commit Failed errors.

  Workaround: Enter the **[no] cdma ddtm** command to set the c3gHdrDdtmPreference for a cellular preference as enabled or disabled. For example:

  To enable cdma ddtm for cellular 3/1:

```
CGR1000#config terminal
CGR1000(config)#controller cellular 3/1
CGR1000(config-controller)# cdma ddtm
```

- **CSCui01347**

  Symptom: MIB OID c3gCdmaRoamingPreference does not have corresponding CLI. The write operation of c3gCdmaRoamingPreference results in "Commit failed" errors. The write of c3gCdmaRoamingPreference is not supported due to security reasons.

  Conditions: User wants to identify the Roaming Preference through CLI. its not shown. It is available only via mib get.

  The write of c3gCdmaRoamingPreference results in "Commit failed" errors.

  Workaround: Use c3gCdmaRoamingPreference get to retrieve the Roaming Preference value.

- **CSCui03505**

  Symptom: Issue snmpset on any of c3gMdn,c3gCurrentNid, c3gCurrentSid,c3gSipUsername or c3gSipPassword MIB objects. The following occurs:

  ```
  Error: Commit failed
  Error index: 1
  1: c3gSipUsername.23 (DisplayString) 0000005308@vzw3g.com
  [30.30.30.30.30.30.35.33.30.38.40.76.7A.77.33.67.2E.63.6F.6D (hex)]
  ```

  Conditions: SNMP write on most of the ciscoWan3gMib is not supported for security reasons.

  Workaround: There is no workaround.

- **CSCuj72458**

  Symptom: Cannot SSH into the CGR with SSHv2 protocol.

  Conditions: SSH process is operating in its default configuration. That is, it is neither configured with **ip ssh version** *X* nor is it configured with **ip ssh version 2**.

  In addition, the SSH process is not configured with **ip ssh rsa keypair-name** *XXXX* to specify a SSH host key.

  Subsequently, SSH process uses the SUDI RSA key as SSH host key.

  Workaround:

  User should manually create a new SSH host key by following these steps:

  1) To generate a new key, enter command **crypto key generate rsa modulus 2048 label** *XXXX* in configuration (config) command mode.

  2) To specify the use of key *XXXX* as SSH host key, enter command **ip ssh rsa keypair-name** *XXXX* in config command mode.

  3) To specify the use of the SSHv2 protocol, enter command **ip ssh version 2** in config command mode.

- **CSCul82192**

  Symptom: When using Airspan base station with CGR1000 dot16 modules, the latency may increase if the dot16 uplink throughput is very low (around 200 Kbps or less).

  Conditions: If the uplink throughput is very low (around 200 Kbps or less), the latency may increase (especially with the Best Effort service-class). This is because Airspan base stations expect a certain minimum rate of traffic before processing the traffic.

  Workaround: Configure a QoS scheduling method like rTPS on the base station to minimize the increase in the uplink latency at very low traffic rates.

- **CSCum84292**

  Symptom: You cannot download the software image bundle for this release when operating with SSHv1.

Conditions: By default, the GOS image that comes with the software bundle image only supports SSHv2. You must enable SSHv2 in Cisco IOS in order to download any TPMC package or application to the GOS.

Workaround: Enable SSH2 in Cisco IOS.

Caveats

This section addresses the open caveats in this release and provides information on how to use the Bug Toolkit to find further details on those caveats. This section includes the following topics:

- Open Caveats, page 16
- Accessing Bug Search Tool, page 20

Open Caveats

- **CSCuh79081**

  Symptom: The message, modem is not present, is seen when the modem is plugged in.

  Conditions: Module is stressed with power UP/DOWN, dual SIM failovers, and modem power cycles and resets along with traffic.

  Workaround: There is no workaround for this issue. Reboot the CGR.

- **CSCui66025**

  Symptom: Modem crash memdump from the modem is not retrieved.

  Conditions: Even when the modem crash tool is enabled, the memdump is not retrieved.

  Workaround: There is no workaround for this issue.

- **CSCuj43190**

  Symptom: The AT Command response from the modem is very slow when bidirectional traffic is sent across the cellular interface.

  Conditions: Bidirectional traffic is sent across the cellular interface.

  Workaround: Stop all traffic and reload the CGR to access the AT commands.

- **CSCuj51188**

  Symptom: The following tracebacks are seen when GSM/CDMA modem crashes:

  %SYS-3-BAD_RESET: Questionable reset of process 314 on tty3/1

  -Process= "TTY Daemon", ipl= 0, pid= 333

  -Traceback= 1845341z 1733927z 1734FA8z 22D2AA0z

  Conditions: Occurs when CDMA/GSM modem crashes.

  Workaround: Perform module reload by entering the command: **hw-module reload** ***slot-number.***

- **CSCul15013**

  Symptom: Fully empty battery displays high charge values.

  Conditions: Occurs at high and low temperature conditions, when a battery is completely drained.

  Workaround: There is no workaround for this issue.

- **CSCul57458**

  Symptom: After booting, a cellular interface might not automatically be placed in an admin non-shut state when its 3G module is administratively powered up from a powered-down state.

  Conditions: When the 3G module is powered down, its cellular interface will also be put in admin shut state. When the 3G module is powered up again, its 3G interface will be automatically put back in admin no-shut state.

  However, if the 3G module is powered-down and the CGR is rebooted, the 3G interface may not be put in admin no-shut state when the 3G module is powered up again. Users may see this error "cellular_error_log: DS instance init issue". When such an error occurs, the cellular interface will not be automatically put in admin no-shut state when the 3G module is powered up.

  Workaround: Try to manually bring up the cellular interface by using the **no shutdown** command

- **CSCul63882**

  Symptom: Cellular 3G interface is shown in shutdown state even after the module is powered on.

  Conditions: CGR (with a 3G module installed) was powered off and reloaded to ensure that the cellular interface was not in an admin down state. After the CGR boots up and the 3G module is powered on, the module remained in an admin down state.

  Workaround: Shutdown and **no shutdown** commands need to be performed on the cellular interface after the CGR boots up.

- **CSCul63973**

  Symptom: The dot16 interface may be set to admin shut in startup-config under some race conditions.

  Conditions: Under some race condition (e.g. a copy run start operation is happening during a module power-cycle due to recovery or wan-mon), the dot16 interface configuration may be set to administrative shutdown. If the CGR is reloaded, this interface may stay in admin shut state

  Workaround: Issue **no shutdown** in the interface configuration mode if the interface stays in the admin shut state after a reload.

- **CSCul67773**

  Symptom: c3gModemTemperAbateNotif trap generates only after the c3gModemTemperOnsetNotif trap has already been generated once.

  Conditions: c3gModemTemperAbateNotif is working like recovery trap rather than a discrete trap.

  Workaround: There is no workaround.

- **CSCum11557**

  Symptom: After an uninstall of Guest OS followed by an install of the same Guest OS package, the install may timeout.

  Conditions: After an uninstall of Guest OS followed by an install of the same Guest OS package, the install may timeout.

  Workaround: Do not perform an installation of the same Guest OS package after you do an uninstall. Instead, download the Guest OS package again before attempting another install on the Guest OS.

- **CSCum56437**

  Symptom: The dot16 interface may still be shown in up state even though its module is powered down in battery power mode.

Conditions: If the dot16 module is powered down because it is configured to be automatically powered down when the system runs on battery power, its interface may still be shown in up state.

Workaround: Manually power up and then power down the dot16 module (instead of having its power-down triggered by battery power mode).

- **CSCum84292**

  Symptom: IOx Client package or GoS applications cannot be downloaded to GoS if SSHv1 is enabled.

  Conditions: By default, the GOS image that comes with the bundled image only supports SSHv2, so SSHv2 must be enabled in IOS in order to download any IOx client package or application to the GOS.

  Workaround: Enable SSHv2.

- **CSCun11696**

  Symptom: The system reset-reason may show “Thermal Trip” after a power outage.

  Conditions: When a CGR is power-cycled due a power loss event, the system reset-reason may show a false “Thermal Trip” reset instead of “Power-on”. This is because the unstable voltage on the mainboard may trigger a false “Thermal Trip” reset-reason.

  Workaround: After the CGR comes back up, issue **show environment temperature** to check the sensor temperature. If they show normal values, the Thermal Trip reset-reason can be ignored and no further action needs to be taken.

- **CSCun77609**

  Symptom: The line protocol on the dot16 interface may not go down after restoring the interface to default configuration.

  Conditions: Configure the necessary settings for the dot16 interface to come online. Restore the interface to default settings. The dot16 interface line protocol may stay up.

  Workaround: Perform a shutdown on the interface.

- **CSCuo01279**

  Symptom: Malloclite memory leak occurs every 15-20 minutes.

  Conditions: This issue is reproducible, but not consistently. An example is shown below:

```
Chunk Elements:

AllocPC  Address  Size  Parent   Name
 396D354 11EBC210   100 12F462CC (MallocLite)
 396D354 13EFD8C4    48 13036424 (MallocLite)
 396D354 13EFE484    48 13036424 (MallocLite)
 396D354 13EFE504    48 13036424 (MallocLite)
```

  Workaround: There is no workaround. Router reboot does not help.

- **CSCuo52773**

  Symptom: Incorrect timer expiration events might be sent to the WPAN CG-mesh module leading to tracebacks.

  Conditions: Incorrect timer expiration events might be sent to the WPAN CG-mesh module leading to tracebacks.

```
Sample Tracebacks:
*Feb 6 09:10:55.219 PDT: %SCHED-3-STUCKMTMR: Sleep with expired managed timer BD02F90,
time 0x38BFFE (00:00:00 ago). -Process= "cgna main", ipl= 6, pid= 338
```

```
-Traceback= 194224Az 32B2623z 32B2B40z 32B1B63z F57485z F57039z F58AA0z F83664z
1889AECz 1888C8Bz 188764Cz FD16DCz FD0D7Fz FD0875z FD2A25z FCFA15z
*Feb 6 10:10:58.991 PDT: %SCHED-3-STUCKMTMR: Sleep with expired managed timer BD02F90,
time 0x6FBD68 (00:00:00 ago). -Process= "cgna main", ipl= 6, pid= 338
```

Workaround: There is no workaround.

- **CSCuo74199**

  Symptom: Connected Grid Endpoints (CGEs) associated with the slave WPAN do not join RPL of the master WPAN in some instances.

  Conditions: If a CGR has multiple WPAN/CG-mesh modules with at least one Dual-PHY master-slave pair, then certain following conditions or events on the router might lead to the master-slave relationship not working as expected.

  The events after which the Dual-PHY Master-Slave might not work are:

  - After a reload of master slot WPAN
  - After a reload of slave slot WPAN
  - After a reload of CGR
  - After an image upgrade of CGR and subsequent mandatory reload

  The CG endpoints under the Slave WPAN link-neighbor table may not join the RPL tree under the Master WPAN.

  Workaround: To retain or reestablish DualPHY, after any of the above conditions occur, the CGR requires the following two actions:

  1. First, reload the slave module(s) by entering:

     ```
     Router(config)# hw poweroff <slave-slot>
     Wait for WPAN down message plus 90 secs, and then enter:
     Router(config)# no hw poweroff <slave-slot>
     ```

  2. Reload the master WPAN module by entering:

     ```
     Router(config)# hw poweroff <master-slot>
     (Wait for WPAN down message plus 90 secs, then enter)
     Router(config)# no hw poweroff <master-slot>
     ```

  3. Check status of the CGR, by entering (for each CGE associated with the slave module):

     ```
     show wpan <slave-slot>/1 link-neighbor table
     show wpan <master-slot>/1 rpl table

     When you see the CGEs join the RPL tree, the master-slave relationship is active.
     ```

- **CSCuo94079**

  Symptom: Invalid encrypted WiFi password may result in dot11 interface remaining down.

  A WiFi SSID is configured and applied to the radio dot11 2/1 interface, but the interface remains down while displaying the following error on console:

  ```
  *May 21 15:52:42.186 PST: %CGR1K_DOT11-3-RADIO_RESET: DOT11 radio hard reset
  *May 21 15:53:55.004 PST: %CGR1K_DOT11-3-RADIO_RESET: DOT11 radio hard reset
  *May 21 15:55:07.842 PST: %CGR1K_DOT11-3-RADIO_RESET: DOT11 radio hard reset
  ```

  Conditions: SSID is configured with an invalid encrypted password - likely due to shorter than eight characters in length or invalid characters.

Workaround: To ensure the encrypted password used is valid:

1. Configure the dot11 SSID with a valid clear, non-encrypted password.
2. Capture the 'encrypted 7' password string (created from a valid clear password in step above) as shown in the CGR config.
3. Use that valid 'encrypted 7' type password in configs.

Accessing Bug Search Tool

You can use the Bug Search Tool to find information about caveats for this release, including a description of the problems and available workarounds. The Bug Search Tool lists both open and resolved caveats.

To access Bug Search Tool, you need the following items:

- Internet connection
- Web browser
- Cisco.com user ID and password

To access the Bug Search Tool, enter the following URL:

https://tools.cisco.com/bugsearch/search

To access the Bug Search Tool to search on a specific caveat, enter the following URL:

https://tools.cisco.com/bugsearch/search/<BUGID>

Accessing Error Message Decoder

You can look up explanations for console error message strings found in system logs at the following location:

http://www.cisco.com/en/US/partner/support/tsd_most_requested_tools.html

Documentation Updates

Please note this pending addition to the *Cisco 1240 Connected Grid Router Installation Guide*.

- PoE Support on Port ETH 2/5
- Port Security

PoE Support on Port ETH 2/5

In release 15.4(2)CG and later, CGR 1240 supports PoE on Port ETH 2/5 when the following minimum hardware and firmware revisions exist:

Hardware and Firmware Requirements

- Hardware version of 0x23xxxxxx (P2) or greater.

  To determine the hardware version, enter:

```
cgr1000(config)#: service internal
cgr1000# test cgr1000 reg fpga r32 0x00
Offset [0x0] = 0x23020900
```

- Firmware version of 11.3b or greater.

  To determine the firmware version, enter:

```
cgr1000(config)#: boot diags <---Look under menu [b][z]
cgr1000# test cgr1000 reg fpga r32 0x00:
  Device      Current Version       New Version
-----------------------------------------------------
  Golden FPGA           02.09.00     02.07.00
  Upgrade FPGA          02.09.00      02.07.00
  Golden BIOS           Build #7     Build # 12 - Wed 06/27/2012
  Upgrade BIOS          Build #10    Build # 12 - Wed 06/27/2012
  Power Sequencer 1 0001-00          0001-00
  Power Sequencer 2 0001-00          0001-00
  PoE PSOC        11.3b        11.3b
```

New Commands Supported

Configuration Commands

The default command, **power inline auto** automatically powers the port when the router detects and classifies the powered device.

```
CGR1000(config-if)# power inline ?
  auto   Automatically detect and power inline devices (Default)
  never  Never apply inline power

CGR1000(config-if)# power inline auto ?
  <cr>

CGR1000(config-if)# power inline never ?
  <cr>
```

Show Commands

```
CGR1000#show power inline ?
  FastEthernet     FastEthernet IEEE 802.3
  GigabitEthernet  GigabitEthernet IEEE 802.3z
  actual           Show current power status
  configured       Show configured power status
  |                Output modifiers
  <cr>

CGR1000#show power inline
PowerSupply   SlotNum.   Maximum   Allocated       Status
-----------   --------   -------   ---------       ------
EXT-PS           0        15.400     0.000          PS GOOD
Interface     Config    Device   Powered       PowerAllocated
---------   ------   ------   -------    --------------
Fa2/5       auto     Unknown  Off             0.000 Watts

CGR1000#show power inline FastEthernet 2/5
PowerSupply   SlotNum.   Maximum   Allocated       Status
```

```
-----------   --------   -------   ---------        ------
EXT-PS            0        15.400     0.000           PS GOOD
Interface     Config     Device     Powered      PowerAllocated
---------   ------     ------    -------      --------------
Fa2/5       auto       Unknown    Off          0.000 Watts

    CGR1000# show power inline actual
Interface            Power
-------------------- -----
Fa2/5                no

CGR1000#show power inline configured
Interface            Config
-------------------- ------
Fa2/5                auto
```

Port Security

In release 15.4(2)CG and later, CGR 1000 supports Static and Dynamic Port Security.

Use the following command to configure either static or dynamic port security on a router port.

Command	Purpose
`Router(config)#` **mac-address-table secure** [*<mac-address>*| **maximum** *maximum addresses*] **fastethernet** *interface-id* [**vlan** *<vlan id>*]	To enable static port security, enter the <mac-address> To enable dynamic port security, enter the keyword maximum.

Related Documentation

Find Cisco 1000 Series Connected Grid Routers product documentation at:

www.cisco.com/go/cgr1000-docs.

Find Connected Grid Modules for Cisco 1000 Series Connected Grid Routers documentation at:

www.cisco.com/go/cg-modules

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the What's New in Cisco Product Documentation as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the Related Documentation section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

No combinations are authorized or intended under this document.

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.

© 2014 Cisco Systems, Inc. All rights reserved.