Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco IOS Release 15.4(1)CG

First Published: January 21, 2014

Last Updated: February 6, 2014

Part Number: OL-31148-03

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, 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 11.)

Note CGR 1000 Series routers installed with CG-OS **cannot** be upgraded to Cisco IOS Release 15.4(1)CG.

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

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.

Note The WPAN module is not supported in Cisco IOS Release 15.4(1)CG.

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 3provides 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 ov*erview 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 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 with Cisco IOS (continued)

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.

Installation Notes

This section addresses the following topics:

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!
```

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.

Battery Backup Unit

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. 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

Table 4 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 4 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)		Currently not supported.

Software Limitations

- **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.

- **CSCul08158**

  Symptom: WIFI interface may show an all zero MAC address.

Conditions: After Cisco IOS comes Online, the WIFI device might not be detected properly in some rare conditions. When such a condition occurs, the dot11 interface may show an all-zero MAC address and the dot11 interface will not work at all.

Workaround: Reload the CGR.

- **CSCug30240, CSCul87513**

  Symptom: 3G and WiMAX modules must be inserted into specific slots on the CGR 1240 and 1120.

  Conditions:

  For CGR1240:

  - The 3G module is not recognized when installed in slots 4 or 6.
  - The WiMAX module is not recognized when installed in slots 3 or 5.

  For CGR1120:

  - The 3G module is not recognized when installed in slot 4.
  - The WiMAX module is not recognized when installed in slot 3.

  Workaround:

  - Install the 3G module in slot 3 of the CGR 1240 and CGR 1120.
  - Install the WiMAX module in slot 4 or 6 of the CGR 1240 and slot 4 of the CGR 1120.

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, and includes the following topics:

- Open Caveats, page 11
- Accessing Bug Search Tool, page 26

Open Caveats

- **CSCuf54058**

  Symptom: CGR 1000 does not support an image check on an IOS image file because the file is not in czip format.

  Conditions: After entering the **verify flash0:***imagename* command on a CGR 1000, nothing displays. This behavior differs from other Cisco IOS devices.

  Workaround: There is no workaround.

- **CSCuh04444**

  Symptom: The configuration register setting of 0x102 i that displays in **show version** or **show hardware**) on CGR does not work in the same way as other Cisco IOS platforms.

  Conditions: A configuration register setting of 0x102 indicates that the boot system command is enabled. However, it also implies that if an IOS image is not specifically set for the boot system command, ROMMON will attempt to load the first valid IOS image on the flash: partition.

  However, for AMI security reasons CGR only boots the exact image being set in the boot system config, not any image on the flash: partition if the configured image is missing. This behavior is by design.

Workaround: There is no workaround.

- **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 in shutdown state.

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

- **CSCuh42117**

  Symptom: The cellular connection (GSM/CDMA) is not established when the RSSI or operating bands is varied with IMIX traffic sent across cellular interface.

  Conditions: IMIX traffic is sent across cellular interface (GSM/CDMA) along with varying RSSI or varying operating bands.

  Workaround: There is no workaround for this issue.

- **CSCuh64535**

  Symptom: When modem reset and module off and on was performed, the following message was seen "cellular_dip_ip_address_negotiated: failed to find profile ID for". With an IPSec tunnel configuration, the tunnel does not come up.

  Conditions: Modem reset and module power off and on was performed.

  Workaround: When WAN link recovery was configured, the link was recovered.

- **CSCuh65379**

  Symptom: Entering the **show memory debug incremental debug leaks lowmem** command causes the console display to freeze. You are unable to enter any more commands and nothing else displays to the console.

  Conditions: Console connected to a CGR 1240.

  Workaround: There is no workaround.

- **CSCuh71719**

  Symptom: The global configuration command, **snmp-server enable traps c3g**, command only enables one Cellular 3G trap, ModemReset.

  Conditions: Enabling 3G traps for the 3G modules (GSM and CDMA) requires entry of multiple commands.

  Workaround: Enable the desired individual traps by following the two steps below:

  1) Enter the global config command: **snmp-server enable traps c3g**

  2) Enter either the **gsm event** or **cdma event** command to define the desired traps.

  The example below shows the event options for the cellular 3g GSM module.

```
CGR1000(config-controller)#gsm event ?
  connection-status  connection status
  ecio               ecio
  modem-state        modem state
  network            enable trap for network
  rssi               rssi
  service            enable trap for service
  temperature        modem temperature
```

- **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.

- **CSCuh85612**

  Symptom: c3gGsmRoamingPreference has read-write access' however, it is not writable.

```
Error: Commit failed
Error index: 1
1: c3gGsmRoamingPreference.23 (INTEGER) home(2)
***** SNMP SET-RESPONSE END *****
```

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

  Workaround: The CISCO-WAN-3G-MIB currently supports the following OIDs:

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

- **CSCuh88771**

  Symptom: When you attach CGR to a Basic Service Set (BSS) network (or simulator), the c3gMsisdn value is empty during an SNMP walk. For example: CISCO-WAN-3G-MIB::c3gMsisdn.22 = STRING:.

  Conditions: Occurs when a CGR initiates an SNMPget on c3gMsisdn within a BBS network or on a simulator and the Service Provider blocks access to MSISDN from SNMP. Issue does not occur within a live line network.

  Workaround: Check with your 3G Service Provider to see if they block access to MSISDN from SNMP.

- **CSCuh88904**

  Symptom: When a SNMP set is issued to create a row in the PDP profile table, commitFailed is 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 CLI to create new profile by entering the following commands:

```
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.

  Workaround: By design, the **write** function (disabled by default) does not work on most of the ciscoWan3gMib for security reasons. The software does not allow SNMP set on Card Holder Verification 1 (CHV1).

- **CSCui00861**

  Symptom: A write on this table 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: 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.

  The only objects supported for writing are listed below.

  The read-write operation is permitted only on 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
```

- **CSCui01406**

  Symptom: Issue snmp set on c3gCdmaHybridModePreference. It will result is "Commit Failed".

  Conditions: This object has a preset value that cannot be modified in CLI. SNMP set is not supported on most of ciscoWan3GMib due to security reasons.

  Workaround: There is no workaround. Behavior performs as designed.

- **CSCui03505**

Symptom: Issue snmpset on any of c3gMdn,c3gCurrentNid, c3gCurrentSid,c3gSipUsername and c3gSipPassword MIB objects.

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: The requested set function is not supported for the requested MIB objects.

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

The read-write operation is permitted only on 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
```

- **CSCui10734**

  Symptom: When using a reverse telnet session from Cisco IOS to Guest OS, after a disconnect from GOS and after reconnection, the user will not be prompted for user name and password.

  Conditions: When using a reverse telnet session from Cisco IOS to Guest OS, a user is able to reconnect after a disconnect without re-authentication.

  Workaround: There is no workaround. Conditions are by design because the user already has full control of Cisco IOS given reverse Telnet setup (Cisco IOS to GOS).

- **CSCui12895**

  Symptom: GuestOs echos configuration change syslog message when configuring a host.

  Conditions: Whenever a host is changing configuration, the syslog message "Configured from console by vty0 (10.10.10.101)" displays.

  Workaround: There is no workaround.

- **CSCui31056**

  Symptom: When running stress tests with **shutdown** and **no shutdown** on the cellular interface along with bidirectional traffic, the data flow stops and does not recover. Even if traffic is stopped, the pings fail to go through.

  Conditions: Occurred during stress tests with **shutdown** and **no shutdown** on the cellular interface along with bidirectional traffic.

  Workaround: Modem power cycle recovers the data flows.

- **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.

- **CSCuj05806**

  Symptom: There is no command to show the dot16 service flow information in the Cisco IOS software for CGR.

  Conditions: In the CG-OS software for the CGR, a command to show the dot16 service flow information exists.

  Workaround: There is no workaround.

- **CSCuj15534**

  Symptom: The SIM status in indicating as "Removed" when the SIM is present. The following message is seen: “SIM read failed for slot 1". The modem is put into LPM mode when temperature changes from -40C to 76.0C.

  Conditions: Seen when temperature changes from -40C to 76C

  Workaround: Increase temperature of the SIM beyond the low temperature recovery range.

- **CSCuj15788**

  Symptom: Unexpected problem might arise with Guest OS (GOS) when operations are not executed in a proper order.

  Conditions: Currently, supported GoS operations can be executed in any random order. This might present unexpected problems.

  Workaround: Since the GoS virtual machine (VM) is always running by default, precede any change in the GOS image (such as installing and uninstalling) with a GoS VM stop. After successful execution of the GoS VM stop, proceed with the desired GoS operation.

- **CSCuj27089**

  Symptom: Inconsistencies in cellular 3G CDMA/GSM commands.

  Conditions: The parameter, Modem Status, displays in the hardware section of 3G GSM module but not for the CDMA. IMSI is reported as MSID in the **show cellular 3/1 all** output for CDMA in Cisco IOS. However IMSI is reported as IMSI in **show cellular 3/1 all** output for CG-OS. In DDR and Dialer configuration mode, **show interfaces** and **show interfaces cellular x/x** should include Tx and Rx for the cellular interface and 3G IPaddress.

  Workaround: There is no workaround.

- **CSCuj31593**

  Symptom: Sweep ping over a 3G GSM cellular interface with Base Station is less than 100%.

  Conditions: Sweep ping via 3G GSM cellular interface using a base station over an entire sweep range has varying success rate. The success rate lies between 95% to 99% in most cases; however it is never 100 percent.

  Workaround: There is no workaround.

- **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: There is no workaround.

- **CSCuj54687**

  Symptom: Cellular connection is not established when network disconnects are issued along with bidirectional traffic over cellular interface.

  Conditions: Seen when network disconnects are issued and bidirectional traffic was being sent across the cellular connection.

  Workaround: Perform a modem power cycle.

- **CSCuj60827**

  Symptom: With FlexVPN enabled, users may see memory leaks in the **show memory debug leak** chunk output

```
Address    Size   Alloc_pc  PID  Alloc-Proc       Name
135C810C       84  1732115  0    *Init*          AAA SG All Server Handles
13901D34       84  1732115  0    *Init*          AAA SG All Server Handles
```

  Conditions: This issue also exists in other IOS platforms that are running the IOS 15.4 branch. Users can safely ignore these memory leaks since they do not affect the functionalities.

  Workaround: There is no workaround.

- **CSCuj60930**

  Symptom: When a 3G (CDMA) module is installed within the CGR, these warning messages may be shown in console during the CGR bootup.

```
This command has no effect on this line; use modem AT commands instead
This command has no effect on this line; use modem AT commands instead
```

  Conditions: The cause of these warnings is the existence of "rxspeed 3100000" and " txspeed 1800000" in the default settings of the 3G (CDMA) interface as seen below:

```
line 3/1
 script dialer cdma
 no exec
 rxspeed 3100000  <==
 txspeed 1800000
```

  Workaround: There is no workaround.

- **CSCuj65368**

  Symptom: The Guest OS console does not connect.

  Workaround: Configure line 1/4 on the CGR as follows:

```
router# Configure terminal
router(config)# line 1/4
router(config)# transport input all
```

- **CSCuj67150**

  Symptom: When type-6 AES encryption is enabled on the router, the digest secret for L2TPv3 control channel authentication is not currently encrypted to type-6 format. Only the type-7 encryption for the digest secret takes effect.

  Conditions: Type-6 AES encryption is not supported in this software release.

  Workaround: There is no workaround.

- **CSCuj74047**

  Symptom: TOS/DSCP based classification does not work.

  Conditions: Packets are marked with TOS/DSCP byte in the IP header and are encrypted using hardware crypto. The command, **qos pre-classify**, is not configured in either the crypto map definition or the tunnel interface.

  Workaround: Enable **qos pre-classify**. For a crypto-map based configuration, add the command to the crypto-map definition. For a virtual tunnel interface (VTI) based configuration, add the command to the tunnel interface.

- **CSCuj74925**

  Symptom: Cellular interface and tunnel goes down when this traceback and message appears and does not recover.

  Conditions: While running stress test on GSM modem with bidirectional traffic of 2Mbps UL +2 Mbps DL, the following error message displayed and the cellular interface and tunnel went down and never recovered.

  Workaround: Perform a **shutdown** and **no shutdown** on the dialer to recover.

- **CSCuj84666**

  Symptom: Sometimes when chassis temperature increases from negative to positive temperatures, chassis temperature is stuck at 0 degrees C.

  In some instances, the following syslog appears "%CGR1K_ENV-2-TEMPERATURE_OK: CGR Module 1 temperature 1C normal" and within 5 to 10 minutes the syslog appears with the correct temperature statistics.

  Conditions: Temperature variations below and above 0 degrees C.

  Workaround: There is no workaround.

- **CSCuj86456**

  Symptom: Bidirectional data traffic stops flowing after sometime with FlexVPN and software crypto over CDMA in operation.

  Conditions: With FlexVPN and software crypto over CDMA and bidirectional traffic of 5Mbps is sent, the uplink or downlink data traffic keeps going to 0 and eventually settles at 0. Even with the change in the crypto throttle to 5000 pps , the same behavior is seen.

  Workaround: Stop traffic and the cellular connection reconnects.

- **CSCuj95972**

  Symptom: Unable to retrieve certificate on WiMAX interface.

  Conditions: WiMAX security will not return the CA certificate if the trustpoint is not associated with a certificate chain.

  Workaround: There is no workaround.WiMAX Security is not supported.

- **CSCul09238**

  Symptom: Memory leak for USB Startup occurred when stress testing SIM failovers on the 3G GSM module.

  Conditions: Memory leak observed.

  Workaround: Continuous DUAL SIM failover performed.

- **CSCul09277**

  Symptom: The following error message - %CELL_MSG-1-MGMT_ERROR: [Cellular5/1] Error response (0x1032) received from modem (err1:) was seen when 3G CDMA module was powered up and down continuously.

  Conditions: 3G CDMA module was powered up and down continuously.

  Workaround: There is no workaround for this issue.

- **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.

- **CSCul16090**

  Symptom: Low flash space messages may randomly show up even if there is plenty of free flash space.

  Conditions: These messages "%CGR1K_ENV-4-LOW_FLASH_SPACE: Flash usage is greater than 90 percent" may be generated even though the actual flash usage is much less than 90%.

  Workaround: Users can ignore the low flash space message.

- **CSCul17891**

  Symptom: If a CGR reloads (by a user or power outage) while a flash operation (read/write) is happening, it can corrupt the flash: partition. Sometimes a single fsck operation will help clear the corruption, sometimes it may not.

  Conditions: If there are corrupted sectors or data on flash: (e.g. due to power loss or reloads during read/write operations), running fsck will attempt to fix the corrupted sectors and move the corrupted data to one or more ORPHAN directories on the flash: partition. However, if there are a lot of corrupted data in ORPHAN directories, dir or other fs commands may fail to calculate correctly the available free space on the flash: properly, since they fail to calculate the amount of space being taken by the corrupted files that fsck moves to the ORPHAN directories.

  Workaround: Manually deleting all the corrupted files in ORPHAN directories and issuing another fsck attempt will help clear out the issue.

- **CSCul24428**

  Symptom: Changing from software to hardware crypto (**crypto engine onboard 0**) on the router might not take effect when a tunnel is in use.

  Conditions: Entering the **show crypto engine config** command indicates that the hardware crypto change is in effect; however, the data is still running with software crypto.

  Workaround: Tear down the tunnel completely and switch from software crypto to hardware crypto and then reconfigure the tunnel. The command for enabling hardware crypto on the router is **crypto engine onboard 0**.

- **CSCul24920**

  Symptom: When you configure software crypto on the CGR, default packets might not forward during periods of heavy congestion.

  Conditions: Software crypto was active on the CGR.

  Workaround: Enable **qos pre-classify** on the CGR. For crypto-map based configurations, add the **qos pre-classify** command to the crypto-map definition. For a virtual tunnel interface (VTI) based configuration, add the **qos pre-classify** command to the tunnel interface.

- **CSCul26286**

  Symptom: CGR reboots with uplink undirectional traffic of 64 bytes (2 Mbps), which is sent across the FlexVPN config ((hardware crypto) over a 3G cellular interface.

  Conditions: Occurs when uplink unidirectional traffic of 64 bytes (2 Mbps) is sent across a FlexVPN configuration ((hardware crypto) over the 3G cellular interface.

  Workaround: There is no workaround.

- **CSCul27834**

  Symptom: The **hw-module poweroff** <*3-6*> command displays an incorrect slot range of <3-6> for the CGR 1120.

  Conditions: The CGR 1120 only supports slots 3 and 4.

  Workaround: For a CGR 1120, only assign a value of 3 or 4 in the **hw-module poweroff** <*3-6*> command.

- **CSCul28166**

  Symptom: New 802.11 (dot11) settings may not take effect when applying to the dot11 interface.

  Conditions: If a new setting (like SSID broadcast or others) is applied on the dot11 interface that is in an administrative no shutdown state, the setting will not take effect.

  Workaround: The dot11 interface needs to be shutdown before applying any new setting by entering the **shutdown** command. Once the setting is applied, enter the **no shutdown** command on the interface.

- **CSCul35551**

  Symptom: Entering the following request resulted in an error:

  ```
  snmpset -v 2c -c private 11.1.1.83 ciscoEntityExtMIBObjects.5.1.0 i 1
  Error in packet.
  Reason: notWritable (that object does not support modification)
  Failed object: CISCO-ENTITY-EXT-MIB::ciscoEntityExtMIBObjects.5.1.0
  ```

  Conditions: User wants to enable door open close traps via SNMP.

  Workaround: Enable the trap via CLI by entering the following: **snmp-server enable traps entity-ext**.

- **CSCul39340**

  Symptom: Dot11 wpa/wpa2/wpa-mixed key is always automatically encrypted to type-7 format even when type-7 password encryption is not enabled.

  Conditions: A password or secret should only be encrypted to type-7 when type-7 encryption is enabled. For the dot11 wpa/wpa2/wpa-mixed pre-shared key, it is always encrypted to type-7 even if the type-7 encryption is still disabled.

  Workaround: We recommend enabling type-6 password encryption in order for the dot11 wpa/wpa2/wpa-mixed pre-shared key to be encrypted to the much stronger AES encryption.

- **CSCul39369**

  Symptom: Deletion of a dot11 (802.11) SSID may randomly fail.

  Conditions: When a dot11 SSID is not associated with the dot11 interface, deleting it may fail with the message: ssid deletion failed.

  Workaround: You may need to reboot the CGR and try to delete the dot11 SSID again.

- **CSCul39687**

  Symptom: Dot11 association may show no client being associated despite the presence of actual client associations.

  Conditions: When showing the dot11 association for a certain client using its specific MAC address, the output may indicate that there is no associated client.

  Workaround: There is no workaround.

- **CSCul43851**

  Symptom: The error %ARP-4-NULL_SRC_MAC: NULL MAC address from 192.10.0.36 on D66/1 may display.

  Conditions: If the dot16 interface is configured with a static IP address, the error: %ARP-4-NULL_SRC_MAC: NULL MAC address from 192.10.0.36 on D66/1 may be shown during booting and power-up of the dot16 module. No such error is shown if the interface is configured with DHCP addressing.

  Workaround: You can safely ignore such error messages.

- **CSCul47760**

  Symptom: Authentication user password is not encrypted to type-6 format.

  Conditions: When type-6 encryption is enabled, configuring authentication user password does not automatically convert it to type-6 format.

  Workaround: There is no workaround.

- **CSCul47773**

  Symptom: The following messages may display on the console after the router reload.

  ```
  *Nov 18 11:32:37.443: %SYS-5-RELOAD: Reload requested by console. Reload Reason:
  Reload Command.
  *Nov 18 11:33:12.481: %PRST_VBL-3-GENERAL: Persistent general error: Is API usable -
  No, going down
  ```

  Conditions: Router reloaded.

  Workaround: There is no workaround. The message does not impact the functionality of the router.

- **CSCul48623**

  Symptom: Enable password is not encrypted to type-6 format.

  Conditions: When type-6 encryption is enabled, configuring the enable password will not automatically convert it to type-6 format.

  Workaround: There is no workaround.

- **CSCul53780**

  Symptom: When removing the Dot16 module, you may encounter a message showing:

  ```
  *Nov 20 20:23:49.849: %CGR1K_SYS-5-MODULE_REMOVED: Module removed from slot 6.

  *Nov 20 20:23:49.849: %CGR1K_DOT16-3-NO_DEL_MODULES: No Dot16 Modules to remove
  ```

Conditions: Dot 16 module was removed.

Workaround: The second message is cosmetic. It does not impact the functionality of the router.

- **CSCul54568**

  Symptom: UDEVd might fail to process the device creation events during Guest OS (GOS) booting, and users may see many of the following errors:

```
udevadm settle - timeout of 120 seconds reached, the event queue contains:
  /sys/devices/virtual/tty/ptyy9 (1676)
  /sys/devices/virtual/tty/ptyya (1677)
  /sys/devices/virtual/tty/ptyyb (1678)
 ....
```

  Conditions: When there is high CPU utilization caused by flash read/write operation and traffic in IOS, the udevadm settle mechanism may time out when waiting for udevd to process the device creation events during GOS booting.

  Workaround: Restart GOS from Cisco IOS.

- **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

- **CSCul60516**

  Symptom: Entering the command **default interface cellular** *x/y* crashes the CGR immediately several times in succession, but it does not occur consistently every time.

  Conditions: The following configuration existed when the problem occurred:

  - default interface cell3/1
  - Interface Cellular3/1 was set to default configuration

  At this point, the router crashed and displayed the following:

```
Unexpected exception to CPU: vector D, PC = 0x1989D0D
-Traceback= 1989D0D 1989ABF
```

  The problem occurs once when there is no traffic at the time. The problem also occurs once right after the router reloads.

  Workaround: There is no workaround.

- **CSCul61117**

  Symptom: 802.11 (dot 11) association output might show the access point (AP) as a client.

  Conditions: Occurs when you configure the 802.11 interface in client/non-root mode.

  Workaround: You can safely ignore the dot11 association output when the dot11 interface is configured in client mode.

- **CSCul61137**

Symptom: Rate Set and MCS set are always empty in the dot11 controller output.

Conditions: The dot11 controller output fails to show the Rate Set and MCS set.

Workaround: There is no workaround.

- **CSCul61146**

  Symptom: The RF PHY noise level on a dot 11 interface always displays as:

  ```
  Phy Noise: not measured yet
  ```

  Conditions: The symptom is seen in both access point and client mode configurations.

  Workaround: There is no workaround.

- **CSCul62616**

  Symptom: When you configure FlexVPN between a CGR and a Catalyst 3900 with 14 Mb/s unidirectional traffic from the CGR to the 3900, the router reloads after a while and indicates system watchdog as the reload reason.

  Conditions: CGR was operating with hardware crypto. This problem is not seen when using software crypto.

  Workaround: Use software crypto (**no crypto engine onboard 0**) on the CGR rather than hardware crypto when sending 14Mb/s unidirectional traffic between the CGR and Catalyst 3900.

- **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: There is no workaround.

- **CSCul63973**

  Symptom: Race condition may put 3G module/dot 16 in an admin shutdown state at startup.

  Conditions: A power-cycle was performed on the 3G module and after reload the module remained in admin shutdown state.

  Workaround: There is no workaround. Reload the 3G module to see if the admin shutdown state disappears.

- **CSCul65333**

  Symptom: When you configure a read-write community string on the CGR and perform an snmp set on **ciscoMemoryPoolLowMemoryNotifEnable**, you will see the following error:

  ```
  ciscoMemoryPoolLowMemoryNotifEnable is read-write access MIB variable and should be
  allowed to set.
  ```

  Conditions: User was setting **ciscoMemoryPoolLowMemoryNotifEnable** in SNMP.

  Workaround: Use the CLI to set the SNMP variable by entering the following command at the global config mode: **snmp-server enable traps mempool.**

- **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.

- **CSCul69845**

  Symptom: Dot16 interface MTU may not be properly applied after entering the **shutdown** and **no shutdown** commands.

  Conditions: After changing the MTU setting for the dot16 interface from the default 1500 bytes, the new MTU may not take effect after entering the interface **shutdown** and **no shutdown** commands.

  Workaround: There is no workaround.

- **CSCul73703**

  Symptom: Applying a default interface on asynchronous interface 1/1 throws an error message.

  Conditions: Configured a default interface on an asynchronous interface.

  Workaround: Error has no affect on functionality.

- **CSCul79309**

  Symptom: Dot11/Dot16 interfaces may be down and flash (read/write) may become inaccessible.

  Conditions: If relatively heavy traffic (around 4 Mb/s per direction) is sent between Dot11 interface (as client) and Ethernet interface, or between Dot11 (as AP) and Dot16 interfaces, the VDS may become stuck in a lockup state. This will cause Dot11 and Dot16 interfaces to be down and flash service to be inaccessible.

  Workaround: Reload the CGR1000 router to clear up the VDS lockup condition.

- **CSCul89155**

  Symptom: When the WiFi interface is configured as UP but remains not connected and in DOWN mode with error messages such as: "%CGR1K_DOT11-3-SSID_ERROR: no ssid configured -1", the router eventually crashes.

  Conditions: Entered **no shut** command on the dot11 radio interface but with the absence of valid SSID configuration, the interface remains in a DOWN state as expected, but error messages keep popping up in system log.

  Workaround: There is no workaround.

- **CSCul93594**

  Symptom: CGR crashed due to subcmd **default escape-character BREAK** under Line configuration.

  Conditions: Configuring a random line with escape-character and attempting to set it back to default value using **default** command crashes the router:

```
line 1/1/1 1/1
   escape-character BREAK
   default escape-character BREAK

+++ 22:09:06 SGBU-CGR3-1120 receive +++
Traceback= 18411C9 1840EC7 17D1C04 17D14E8 17CF68E

CPU Register Context:
EAX = 0x00000000  ECX  = 0x00000000  EDX = 0x1E000000  EBX  = 0x00000000
ESP = 0x0EEBF0F0  EBP  = 0x0EEBF0F4  ESI = 0x10E5CCA0  EDI  = 0x00000028
EIP = 0x018411C9  PS   = 0x00010246  CS  = 0x00000008  SS   = 0x00000010
DS  = 0x00000010  ES   = 0x00000010  FS  = 0x00000010  GS   = 0x00000010

Writing crashinfo to flash:crashinfo_20131208-220903-PST
```

  Workaround: Use the **no** form of the command, and set the value back to the desired value.

- **CSCum06290**

  Symptom: During the Image bootup the INIT_FAILED message below might display:

```
*Jan  2 00:00:00.823: %LICENSE-6-EULA_ACCEPT_ALL: The Right to Use End User License
Agreement is accepted
*Jan  2 00:00:16.159: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
cgr1000 Next reboot level = ipbasek9 and License = No valid license found
*Jan  2 00:00:16.317: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name =
cgr1000 Next reboot level = securityk9 and License = securityk9
*Dec 13 08:35:39.251: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State changed to:
Initialized
*Dec 13 08:35:39.253: %VPN_HW-6-INFO_LOC: Crypto engine: onboard 0  State changed to:
Enabled
*Dec 13 08:35:40.397: %PA-3-PA_INIT_FAILED: Performance Agent failed to initialize
(Missing Data and APPX License)
*Dec 13 08:35:40.827: API: In http config params settings
*Dec 13 08:35:40.827: API: setting server life timer
*Dec 13 08:35:40.827: API: setting server idle timer
*Dec 13 08:35:40.827:  API: setting client idle timer
*Dec 13 08:35:43.323: %ACT2-5-STARTED: ACT2 process started.
```

  Conditions: Booted up a router and image and INIT_FAILED message displayed.

  Workaround: There is no workaround. The issue does not affect the performance of the router.

- **CSCum09188**

  Symptom: When CGR1240 is on battery power and the battery has drained, the router will attempt to reload itself rather than gracefully shutdown as expected.

  Conditions: CGR 1240 does not have an AC power supply. The router will not complete the reload until AC power is provided.

  Workaround: Plug in the router into an AC power supply, and the router will boot and come up properly.

- **CSCum10989**

  Symptom: Bundle install fails when performing install during a period of high CPU utilization.

  Conditions: When the router is under high CPU utilization, bundle install will fail.

  Workaround: Lower CPU utilization before trying bundle install.

- **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.

- **CSCum13646**

  Symptom: CLI command **username WORD callback-line 1/1/1** causes router to crash.

  Conditions: CLI command **username WORD callback-line 1/1/1** causes router to crash.

  Workaround: There is no workaround.

- **CSCum49899**

  Symptom: Customer performs an SNMP walk on the IF-MIB and the ifIndex of Async1/1 and Async1/2 interfaces are not listed. However, entering the command **show snmp mib ifmib ifindex** lists the ifIindex.

  This is a discrepancy and interface traps for Async Interfaces do not get generated.

  Conditions: IF-MIB was used to manage Async interfaces.

  Workaround: There is no workaround.

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

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

For information on supporting systems referenced in this release note, see the following documentation on Cisco.com:

Cisco 2000 Series Connected Grid Routers

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.