Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco CG-OS Release CG2(1)

Last updated: January 09, 2013
Part Number: OL-27580-02

These release notes contain the latest information about using CG-OS software with the Cisco 1000 Series Connected Grid Routers, including this new information:

- Overview of new features added in this release. See New Features in Cisco CG-OS Release CG2(1), page 2.
- Cisco CG-OS Release CG2(1) resolves open caveats in previous releases. To see details about the open and resolved caveats, see Caveats, page 15.

Tell Us What You Think

> Send your feedback about this document directly to the Connected Energy Documentation Team.
>
> Connected Energy Documentation Feedback Form

Contents

This release note includes the following sections

New Features in Cisco CG-OS Release CG2(1)

Table 1 lists the new features added in this release.

Table 1   New Features in Cisco CG-OS Release CG2(1)

Feature	Description	Related Documentation
Support for the Cisco 1120 Connected Grid Router (CGR 1120)	The CGR 1120 is a ruggedized communication platform, designed for use inside substations or utility cabinets. This platform is built to meet the communication infrastructure needs of electric, gas, and water utilities. Applications for the CGR 1120 include Advanced Metering Infrastructure (AMI), Distribution Automation (DA), integration of Distributed Energy Resources (DER), and remote workforce automation.	For more information about the CGR 1120, see the *Cisco 1120 Connected Grid Router Hardware Installation Guide* at www.cisco.com/go/cgr1000-docs.
IEC 60870-5-101 to IEC 60870-5-104 Protocol Translation	IEC 60870-5-101 to IEC 60870-5-104 protocol translation enables Cisco 1000 Series Connected Grid Routers to provide end-to-end secure communication between Control Centers (CC) and remote terminal units (RTUs) within a Supervisory Control and Data Acquisition (SCADA) System. **Note** The Protocol Translation feature requires a software license (LIC-CGR1K-SW-PT) to operate. To obtain this license, contact your Cisco representative or reseller.	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Embedded Event Manager (EEM)	EEM provides a framework for monitoring the router for events that require recovery or troubleshooting, then taking action when these events occur, according to user-defined policies.	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.

Table 1 **New Features in Cisco CG-OS Release CG2(1) (continued)**

Feature	Description	Related Documentation
Cisco Control-Plane Policing (CoPP)	CoPP increases security on the router by protecting the system from unnecessary traffic or Denial of Service (DoS) attacks and giving priority to important control-plane and management traffic. You can configure CoPP policies that protect the router CPU from DoS attacks through restricting synchronization (sync) packets, finish (FIN) packets and IP fragments.	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Support for WPA and WPA/WPA2 mixed mode operation on the WiFi interface	WPA/WPA2 mixed mode operation permits the coexistence of WPA and WPA2 clients on a common SSID. In WPA/WPA2 mixed mode, clients can connect to the SSID with WPA/TKIP and WPA2/AES-CCMP. This is useful if you want to use AES-CCMP, but also need to support older clients that can only use WPA/TKIP.	For an overview of WiFi support on the router and configuration details, see the *Cisco 1000 Series Connected Grid Routers WiFi Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
SNMP support	Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network. Cisco CG-OS supports SNMPv2c and SNMPv3.	For information about configuring SNMP, as well as supported MIBs, on Cisco 1000 Series Connected Grid Routers, see the *Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Support for PPP over the serial interfaces	PPP support over CGR 1000 serial interfaces allows IP network access for downstream devices (such as a Low Voltage Concentrator). Either one or both of the serial ports can be provisioned to run the PPP protocol.	See the *Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
RS232 and RS485 support	CGR 1000 serial ports can be configured as RS232 and RS485 (DCE only) to allow connection to Remote Terminal Units (RTUs).	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.

About the Cisco 1000 Series Connected Grid Routers

Cisco 1000 Series Connected Grid Routers (Cisco CG-OS 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, and WiFi.

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 prioritization 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 CG-OS software supports a command-line interface to configure and monitor the system.

Network Management

The Cisco Connected Grid Device Manager (Device Manager) is a Windows-based application that field technicians can use to manage the Cisco CG-OS Router remotely. The Device Manager connects to the Cisco CG-OS Router by using a secure Ethernet or WiFi link.

Table 2 provides an overview of the software features supported on Cisco CG-OS Routers.

Table 2   Software Feature Support on Cisco CG-OS Routers

Feature	Support	Related Documentation
Layer 3 features	• IPv4 unicast forwarding • IPv6 unicast forwarding • IP services (DNS, DHCP)	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Routing	• Open Shortest Path First version 2 (OSPFv2) and OSPFv3 routing • Static routing	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Quality of Service (QoS)	• Classification • Marking • Priority queuing to manage traffic flow	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.

Table 2   Software Feature Support on Cisco CG-OS Routers (continued)

Feature	Support	Related Documentation
System management	• SNMP • Network Time Protocol (NTP) • System Message Logging • Embedded Event Manager (EEM) • Backhaul Manager	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Security	• Authentication, Authorization, and Accounting (AAA) using RADIUS and TACACS+ • SSHv2 and Telnet secure access • IPSec static virtual tunnel interface • IKEv2 • Role-based access control (RBAC) for user accounts • IP access control lists (ACLs) to filter traffic	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Diagnostics and troubleshooting	• Remote wireless access to the Cisco CG-OS Router from a laptop client for diagnostic and troubleshooting by field personnel	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers WiFi Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Supervisory Control and Data Acquisition (SCADA) connectivity	• Ability to provide IP connectivity within a SCADA system	For feature overview and configuration details, see the *Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide* at www.cisco.com/go/cgr1000-docs.

Table 3 provides an overview of the hardware features and interfaces supported on Cisco CG-OS Routers.

Table 3   Hardware Feature Support on Cisco CG-OS Routers

Feature	Description	Related Documentation
Hardware features	• 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 Cisco CG-OS 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 four Fast Ethernet ports and two Gigabit Ethernet ports.	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 *Cisco 1000 Series Connected Grid Software Configuration Guide Set* at www.cisco.com/go/cgr1000-docs.
WiFi interface	Integrated, short-range WiFi access point to support a wireless console connection to the router.	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 CG-OS Routers (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 Module for CGR 1000 Series Installation and Configuration Guide* at www.cisco.com/go/cgr1000-docs.
Small Form-Factor Pluggable (SFP) Modules	The following SFP modules are supported on the Cisco CG-OS routers: • GLC-SX-MM-RGD • GLC-LX-SM-RGD • GLC-FE-100LX-RGD • GLC-FE-100FX-RGD • GLC-ZX-SM-RGD Other SFP modules, including those made by third-party manufacturers, are not supported.	For installation instructions, 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.

System Requirements

Table 4 lists the hardware and software versions associated with this release for Cisco products deployed in a Field Area Network solution.

Table 4   *Minimum Hardware and Software Requirements*

Component	Minimum Software Requirement
Cisco Connected Grid Field Device Manager	CGD Manager release 1.0.12.105 or later (CGR 1240) CGD Manager release v1.1.0.129 or later (CGR 1120)
Cisco ASR 1002 Aggregation Services Router (Cisco ASR) serving as a head-end router	Cisco IOS-XE 15.1(3)5
Cisco 3945 Integrated Services Router (Cisco ISR) serving as a Registration Authority	Cisco IOS 15.1(2)T2.1

Installation Notes

This section addresses the following topics:

Determining the Software Version

To identify the software version operating on the Cisco CG-OS router, enter the following command.

Command	Purpose
show version	Displays the software version installed on the Cisco CG-OS router.

Upgrading to a New Software Release

You can upgrade the software on the Cisco CG-OS router by employing the **install all** command. Listed below are the two possible approaches when downloading images using the **install all** command. You must select one of the following approaches:

- Download the images (kickstart and system image) from a remote server into the volatile memory of the Cisco CG-OS router by employing the **install all** command to specify the path to the remote server and the protocol. After the download, the software installation begins *automatically*.

- Download the images (kickstart and system image) from a local server directly into the bootflash of the Cisco CG-OS router, and then *manually* enter the **install all** command to initiate the software upgrade.

The following table provides detailed command syntax for the **install all** command.

Command	Purpose
install all [kickstart {bootflash: ❘ **ftp:[**//*server*][/*path*] ❘ **scp:[**//[*username*@]*server*][/*path*] ❘ **sftp:[**//[*username*@]*server*][/*path*] ❘ **tftp:[**//*server*[:*port*]][/*path*] ❘ **volatile:}** *kickstart-filename*] [**system {bootflash:** ❘ **ftp:[**//*server*][/*path*] ❘ **scp:[**//[*username*@]*server*][/*path*] ❘ **sftp:[**//[*username*@]*server*][/*path*] ❘ **tftp:[**//*server*[:*port*]][/*path*] ❘ **volatile:}** *system-filename*] [**non-interactive**]	Specifies the software images being downloaded (kickstart and system images), the method used to download the images such as FTP, SCP, TFTP (remote server downloads only), and the destination of the images (bootflash or volatile) on the Cisco CG-OS router. • Define **bootflash:** as the destination in the **install all** command when the download is from a local server. • Define **volatile:** as the destination in the **install all** command when you are downloading the software from a remote server (such as Cisco.com or a remote server in your own network). **kickstart bootflash:** *kickstart-file-name*–Identifies the file as a kickstart image and the file name of that image. Format of the kickstart filename is as follows: cg-os_kick.bin. File name is case sensitive. **system bootflash:** *system-filename*–Specifies internal flash memory as the destination of the software images. Format of the bootflash filename is as follows: cg-os_sys.bin. File name is case sensitive. **ftp:** Specifies File Transfer Protocol (FTP) as the transfer method for the software images (kickstart and system). **scp:**–Specifies Secure Copy Protocol (SCP) as the transfer method for the software images (kickstart and system). **sftp:**–Specifies Secure Shell FTP (SFTP) as the transfer method for the software images (kickstart and system). **tftp:**–Specifies Trivial FTP (TFTP) as the transfer method for the software images (kickstart and system). *username*@–Specifies the username on the server. Username is case-sensitive. //*path*–Defines the path to the server on which the software images reside. //*server*–Defines the IPv4 address or name of the server on which the software images reside. **[non-interactive]**–Eliminates the need for interaction or responses from an administrator during the process. Process proceeds to completion without requesting approval by the user.

EXAMPLES

This example shows how to download the software images from a remote FTP server onto the Cisco CG-OS router bootflash. After download, the software installation starts automatically on the Cisco CG-OS router.

```
cgr1000# install all kickstart ftp://10.10.1.1/cg-os_kick.bin
system ftp://10.10.1.1/cg-os_sys.bin
```

This example shows how to download the software images from a remote SCP server onto the Cisco CG-OS router bootflash. After download, the software installation starts automatically on the Cisco CG-OS router.

```
cgr1000# install all kickstart scp://adminuser@10.10.1.1/cg-os_kick.bin
system scp://adminuser@10.10.1.1/cg-os_sys.bin
```

This example shows how to copy the image from a remote SCP server onto the Cisco CG-OS router bootflash and then *manually* upgrade the software by using the **install all** command.

```
cgr1000# copy scp://adminuser@10.10.1.1/cg-os_kick.bin bootflash:
cgr1000# install all kickstart bootflash:cg-os_kick.bin system bootflash:cg-os_sys.bin
```

This example shows how to copy the image from a remote SCP server onto the Cisco CG-OS router bootflash without requiring any action or entry by the administrator. All actions proceed automatically.

```
cgr1000# copy scp://adminuser@10.10.1.1/cg-os_kick.bin bootflash:
cgr1000# install all kickstart bootflash:cg-os_kick.bin system bootflash:cg-os_sys.bin
non-interactive
```

Note An output similar to the one below displays during the install. The same output displays for local and remote installations.

```
Verifying image bootflash:///cgr1000-uk9-kickstart.5.2.1.CG2.0.195.SPA.bin for boot
variable "kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:///cgr1000-uk9.5.2.1.CG2.0.195.SPA.bin for boot variable
"system".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Extracting "system" version from image bootflash:///cgr1000-uk9.5.2.1.CG2.0.195.SPA.bin.
[####################] 100% -- SUCCESS

Extracting "kickstart" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG2.0.195.SPA.bin.
[####################] 100% -- SUCCESS

Extracting "bios" version from image bootflash:///cgr1000-uk9.5.2.1.CG2.0.195.SPA.bin.
[####################] 100% -- SUCCESS

Extracting "loader" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG2.0.195.SPA.bin.
[####################] 100% -- SUCCESS

Performing module support checks.
2012 Jan 3 00:12:23 Router %$ VDC-1 %$
[####################] 100% -- SUCCESS
```

```
        Notifying services about system upgrade.
        [####################] 100% -- SUCCESS

        Compatibility check is done:
        Module  bootable         Impact  Install-type  Reason
        ------  --------  --------------  ------------  ------
            1      yes   non-disruptive         none

        Images will be upgraded according to following table:
        Module    Image              Running-Version(pri:alt)      New-Version  Upg-Required
        ------  --------  ------------------------------------  --------------  ------------
            1    system                        5.2(1)CG1(3c)    5.2(1)CG2(1)          yes
            1  kickstart                       5.2(1)CG1(3c)    5.2(1)CG2(1)          yes
            1     bios                                     :                           no
            1    loader                               1.2(2)          1.2(2)          no
            1     fpga                                  2_4_0           2_6_0          yes
            1    gsm fw                          T1_0_3_2BT      T1_0_3_2BT           no

        Do you want to continue with the installation (y/n)?  [n] y

        Install is in progress, please wait.

        Performing runtime checks.
        [####################] 100% -- SUCCESS

        Setting boot variables.
        [####################] 100% -- SUCCESS

        Performing configuration copy.
        [####################] 100% -- SUCCESS

        Module 1: Refreshing compact flash and upgrading bios/loader/bootrom/fpga/modem firmware.
        Warning: please do not remove or power off the module at this time.
        [####################] 100% -- SUCCESS

        Install has been successful.

        cgr1000#
```

✎

Note   The Cisco CG-OS router reboots after a successful installation.

Erasing the Configuration File

When you enter the **write erase [boot | debug | secrets]** command, it erases all of the persistent memory of the Cisco CG-OS Router *except* for items noted in the table below.

Command	Purpose
**write erase [boot	debug	secrets]**	**boot–**Erases the configuration file (with the exception of the certificates, the private keys, the password encryption master key, and the cellular interface profile) from the persistent memory of the router. (CSCto56948)
	debug–Erases only the debug configuration file from the persistent memory of the router.
	secrets–Erases the certificates, private keys and the password encryption master key from persistent memory on the router.

Important Notes

Battery Backup Unit

To prevent the battery backup unit (BBU) from discharging during transport or servicing of the Cisco CG-OS 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 CG-OS 1120 router.

Guidelines and Limitations

Refer to the "Guidelines and Limitations" section of each chapter within the Cisco 1000 Series Connected Grid Routers Software Configuration Guides and the highlighted Notes, Warnings, and Cautions throughout all Cisco CG-OS Router documentation.

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 CG-OS router hardware or software.

Hardware Limitations

Table 5 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 CGR 1120 or CGR 1240.

Table 5   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

- **CSCto16391**

   Symptom: Creating a username (not password) within the local database on the router that already exists on the external AAA server, generates an inaccurate error message such as "`Please first delete that account using "no" option`".

   Conditions: CG-OS software allows use of the same username in both the local router database and an external server.

   Workaround: Create the username on the local authentication store of the router first; and, then replicate it on the external AAA server. The AAA server will not complain.

- **CSCtw44740**

   Symptom: In some cases, over the air service provisioning (OTASP) might not be successful or might time out.

   Workaround: Re-attempt OTASP activation.

- **CSCtw87711**

   Symptom: The term "switch" is used in the CGR 1000 command-line interface (CLI). The CGR is a router.

   Conditions: The term is used in various places in the CLI.

   Workaround: There is no workaround for this issue.

- **CSCty61792**

   Symptom: The CGR 1000 fails certificate authentication.

   Conditions: This issue can occur when authenticating the router using Simple Certificate Enrollment Protocol (SCEP). If the enrollment profile refers to a Cisco IOS registration agent (RA), and the RA refers to a sub-certificate authority (SubCA) instead of a certificate authority (CA), the authentication fails.

   Workaround: Use one of the following workarounds: Authenticate to the SubCA over a terminal connection, or authenticate to the SubCA but do not use a Cisco IOS RA.

- **CSCua61556**

    Symptom: The syslog message for backup battery units does not take into account BBUs in inhibit discharge mode.

    Conditions: This issue occurs when the router has three BBUs: two of the BBUs are in uninhibit discharge mode, and one is in inhibit discharge mode. The syslog message reporting the status of the BBUs shows the capacity of the BBUs in uninhibit discharge mode, but the capacity value does not take into account the capacity of the BBU in inhibit discharge mode.

    Workaround: There is no workaround for this issue.

- **CSCua93975**

    Symptom: The BIOS on routers running Cisco CG-OS Release 5.2(1)CG1(3c) or earlier cannot be upgraded to a new version.

    Conditions: Software releases earlier than Cisco CG-OS Release CG2(1) do not support BIOS upgrade. When you run the **install all** command, the upgrade table shows nothing in the `Running-Version` or `New-Version` columns for the BIOS, and the `Upg-Required` column for the BIOS always shows `no`.

    Workaround: Support for BIOS upgrade was added in Cisco CG-OS Release CG2(1). After you upgrade the router to Cisco CG-OS Release CG2(1), you will be able to upgrade the BIOS.

- **CSCua94010**

    Symptom: The router BIOS cannot be downgraded to an earlier version.

    Conditions: This issue occurs when you attempt to downgrade the router software from Cisco CG-OS Release CG2(1) to an earlier version. When you enter the **install all** command, the upgrade table shows nothing in the `New-Version` column for the BIOS, and the `Upg-Required` column for the BIOS shows `no`.

    Workaround: There is no workaround for this issue. Software releases earlier than Cisco CG-OS Release CG2(1) do not support BIOS downgrade.

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

- **CSCto92724**

    Symptom: The **show ip adjacency statistics** command displays inaccurate statistics. All packet and byte counts are displayed as 0. Entering the **clear ip adjacency statistics** command does not resolve this issue.

    Conditions: This issue can occur when the system is passing data.

    Workaround: There is no workaround for this issue.

- **CSCtr21995**

  Symptom: The **tacacs-server host test** command does not display related messages.

  Conditions: This issue occurs when using any of the command keywords: {**idle-time** *minutes* | **password** *password* [**idle-time** *minutes*] | **username** *name* [**password** *password* [**idle-time** *minutes*]]}

  Workaround: Enter the **test aaa** configuration mode command to display related messages. See the *Cisco 1000 Series Connected Grid Router Security Software Configuration Guide* for more information about this command: www.cisco.com/go/cgr1000-docs

- **CSCtr82241**

  Symptom: The command **aaa authentication login error-enable** fails to return any error message when the external AAA server is unreachable, other than `Access denied. Using keyboard-interactive authentication.` if the user enters valid credentials that exist on the external AAA server.

  Conditions: The AAA command **aaa authentication login error-enable** is configured and the external AAA server is unreachable or the AAA daemons are down.

  Workaround: Define authentication locally on the router.

- **CSCts11031**

  Symptom: DHCP debug commands are not supported for DHCPv4 devices. These debug commands include the following: **debug dhcp all**, **debug dhcp errors**, **debug dhcp mts-errors**, **debug dhcp mts-events**, **debug dhcp pkt-events**, **debug dhcp pss-errors**, and **debug dhcp pss-events**.

  Conditions: This issue occurs under all conditions.

  Workaround: Use the **show logging log** command to gather general information for DHCP4 devices.

- **CSCtt27515**

  Symptom: When the CGR 1000 ports Ethernet 2/1 and Ethernet 2/4 are connected to a SmartBit test device, the router displays the following message, and then the ping times out:

  ```
  switch %$ VDC-1 %$ %ARP-2-DUP_SCRIP: rap [3453] Source address of packet received from
  0000.0000.1010 on Ethernet2/1 is duplicate of local, 10.100.10.1
  ```

  Conditions: This issue occurs when traffic is sent over the affected ports.

  Workaround: Use MAC addresses instead of IP addresses for the destination and source address configuration.

- **CSCtu41227**

  Symptom: The CGR 1000 Router Ethernet interfaces stop detecting Ethernet traffic when both IPv4 and IPv6 is sent over the interface.

  Conditions: This issue occurs when a huge amount of IPv6 and IPv4 packets are sent to a router Ethernet interface that is configured with both an IPv4 address and an IPv6 address.

  Workaround: There is no workaround for this issue.

- **CSCtv24634**

  Symptom: Certain fields in the **show cellular** command output are not populated with data.

  Conditions: Always.

  Workaround: There is no workaround for this issue.

- **CSCtw50574**

    Symptom: You cannot use the **ip address interface** configuration command to configure a static IP address on a router interface that has DHCP enabled.

    Conditions: This issue occurs on interfaces with DHCP enabled.

    Workaround: Use the **no ip address dhcp interface configuration** command to disable DHCP on the interface, then configure a static IP address on the interface.

- **CSCtw59629**

    Symptom: The CGR 1000 displays NTP syslog errors when there is no NTP configuration on the router.

    Conditions: This issue can occur when an NTP configuration exists on the router, and is then removed, and the router is reloaded.

    Workaround: There is no workaround for this issue.

- **CSCtw66798**

    Symptom: The **show environment power** command does not display data from the CGR 1000 AC power supply. Instead the command display includes the following error:

    ```
    Failed to read data from power supply unit!
    ```

    Conditions: This issue occurs when the BBU provides power for the router.

    Workaround: There is no workaround for this issue.

- **CSCtw79047**

    Symptom: The IP ARP table that displays when you enter the **show ip arp** command show the state INCOMPLETE in the MAC address column.

    Conditions: This issue can occur when the Ethernet cable is removed from an Ethernet port that is actively transferring data.

    Workaround: Stop the traffic flow and rediscover ARP.

- **CSCtw85126**

    Symptom: The **show version** command does not display EPLD versions for modules installed in the CGR 1000.

    Conditions: This issue occurs under all conditions.

    Workaround: There is no workaround for this issue.

- **CSCtx04502**

    Symptom: Entering the **show clock** command in boot mode on the CGR 1000 displays the following error message:

    ```
    /isanboot/bin/vshboot: symbol lookup error: /isanboot/lib/libsyscli_boot.so: undefined
    symbol: mts_bind
    ```

    Conditions: This issue occurs in boot mode.

    Workaround: There is no workaround for this issue.

- **CSCtx18250**

    Symptom: A learned OSPF route is given preference over the same static route configured in the CGR 1000.

    Conditions: This issue occurs when the same router is both a learned OSPF route and a configured route.

Workaround: To resolve this issue, remove the learned OSPF route from the router configuration. To prevent this issue from occurring, do not use OSPF on an interface for which you want to use static routes.

- **CSCtx35868**

  Symptom: The CGR 1000 displays the following syslog error:

  ```
  2012 Jan 13 15:48:44 far_1_1 Jan 13 15:48:44 %KERN-3-SYSTEM_MSG: [134526.000040]
   NETDEV WATCHDOG: usb0 (sierra_net): transmit timed out - kernel
  ```

  Conditions: This issue can occur when constant bidirectional traffic is sent over the CG 3G module interface over an IPSEC GRE tunnel for long durations.

  Workaround: Reload the CGR 1000.

- **CSCtx75113**

  Symptom: In some cases, the PPP engine might stop working when a 3G cellular module is trying to establish a connection to a CDMA network.

  Conditions: Poor signal strength or deactivated modem.

  Workaround: The cellular link is normally able to reconnect. Reload the module.

- **CSCtx84604**

  Symptom: The cellular module does not return a CGDM netconf error when the module is not available. Instead, it returns netconf data containing an error message, Modem is not available - WAITING!

  Conditions: When the cellular module is not ready or is unavailable.

  Workaround: There is no workaround for this issue.

- **CSCtx86753**

  Symptom: During boot up, the system indicates through the console that it is sending the following callhome registration message:

  ```
  System is coming up ... Please wait ...
  2012 Feb  7 21:41:49  %$ VDC-1 %$ %CALLHOME-2-EVENT: REGISTRATION_NOTIFICATION
  System is coming up ... Please wait ...
  ```

  Conditions: The issue exists occurs before boot up is completed.

  Workaround: The router will retry the registration; the console message can be ignored.

- **CSCtx90382**

  Symptom: A static route to a subnet cannot be removed from the CGR 1000 with the **no ip static-route** command until after the router is rebooted.

  Conditions: This issue occurs when the **ip static-route** command is used to configure a static route to a subnet.

  Workaround: To prevent this issue, avoid configuring static routes to subnets. To resolve this issue remove the static router after rebooting the router.

- **CSCtx98806**

  Symptom: The output of the **show module** command indicates that a module is fully functional when it might still be going through initialization.

  Conditions: The output of the **show module** command displays Ok in the Status column while the module is still being initialized, and might not yet be fully functional.

Workaround: There is no workaround for this issue. After the **show module** command displays status Ok for the module, you might need to wait up to 1 minute before the module is fully functional and able to pass traffic.

- **CSCty01486**

    Symptom: When sent through Connected Grid Device Manager (CGDM), the **dir** *file* command does not return a missing file error message if the *file* does not exist.

    Conditions: This issue occurs when the **dir** *file* command is sent through CGDM. If the **dir** *file* command does not contain the full path of *file,* and *file* does not exist, then CGDM returns a listing of the files in bootflash, rather than a message indicating that *file* does not exist.

    Workaround: There is no workaround for this issue.

- **CSCty01882**

    Symptom: A tunnel interface is configured with **no keepalive** by default.

    Conditions: This issue occurs on all tunnel interfaces.

    Workaround: Use the **keepalive** interface configuration command to enable keepalive on the tunnel interface.

- **CSCty02486**

    Symptom: When the CGR is experiencing a SYN flood attack, the message message buffer overflowed appears on the console.

    Conditions: This issue occurs when the CGR is under a SYN flood attack. You might see the message message buffer overflowed as you enter commands on the router console.

    Workaround: You can safely ignore the message buffer overflowed messages.

- **CSCty05226**

    Symptom: Many error messages flood the console and syslog, and the CPU utilization might reach 100%, which negatively impacts traffic and other router functions. This could be due to Fuzzing UDPSIC attacks. These are a type of Denial of Service (DoS) attack that attempts to send random bad data or all kinds of malformed packets (UDP-based in this case) to a target device to see if that causes problems on the target device when copying the bad data.

    Conditions: Without proper access control lists (ACLs) in place when SNMP is in use, the CGR 1000 Router could become the target of UDPSIC attacks.

    Workaround: Configure ACLs on the CGR 1000 Router to protect against Fuzzing UDPSIC attacks by allowing only specific traffic to and from specific IP addresses and specific server listening ports. For more information about configuring ACLs, see the "Configuring IP ACL" chapter of the Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide.

- **CSCty14312**

    Symptom: The CGR 1000 does not respond with an echo reply to link-local echo requests.

    Conditions: This issue occurs when the router receives a link-local request for the first time. The router does send an echo reply to subsequent link-local echo requests.

    Workaround: There is no workaround for this issue.

- **CSCty20444**

    Symptom: When you disable the command, **feature scada-gw**, by entering **no feature scada-gw** the command options for the **scada-gw** command remain in the global configuration mode.

Conditions: Disabling the **feature scada-gw** should disable all options associated with that command and they should not appear as configurable options in the global configuration command mode.

Workaround: There is no workaround for this issue.

- **CSCty24151**

  Symptom: The **install all** command returns a message `Invalid bootvar specified in the input`.

  Conditions: This issue occurs when you enter the **install all** command and specify one of the following URIs with the **bootflash** parameter: `bootflash://module-1/`, `bootflash://sup-1/`, `bootflash://sup-active/`, or `bootflash://sup-local/`.

  Workaround: When issuing the **install all** command, do not use these bootflash URIs: `bootflash://module-1/`, `bootflash://sup-1/`, `bootflash://sup-active/`, `bootflash://sup-local/`.

- **CSCty26855**

  Symptom: AAA commands and config-commands accounting misreports a failed certificate enrollment as successful.

  Conditions: With the following commands configured for AAA:

  ```
  aaa authentication login default group tactical
  aaa authorization config-commands default group tactical local
  aaa authorization commands default group tactical local
  aaa accounting default group tactical
  ```

  Workaround: There is no workaround for this issue.

- **CSCty44261**

  Symptom: The serial number is not displayed for the Ethernet module when the router is booting.

  Conditions: When the router is booting, hardware authentication messages for the Ethernet module do not display the module serial number, while a serial number displays for the other modules.

  Workaround: There is no workaround for this issue.

- **CSCty47211**

  Symptom: Message `Busy bit is not cleared` appears in the syslog.

  Conditions: The syslog contains the messages: `Error: busy bit is not cleared - kernel`

  Workaround: These messages can be safely ignored.

- **CSCty53142**

  Symptom: Parse error messages appear when executing a rollback operation following a checkpoint operation.

  Conditions: This issue occurs if you try to roll back a checkpoint configuration on a CGR after a **write erase** and **reload** operation. The system might display parse error messages.

  Workaround: There is no workaround for this issue.

- **CSCty86005**

  Symptom: When attempting to register a CGR with CG-NMS, the following error appears in the CG-NMS logs:`javax.net.ssl.SSLException: Received fatal alert: unknown_ca`

  Conditions: This error occurs due to one of the following conditions:

  – There are multiple Trustpoints configured on the CGR and the certificates for each Trustpoint is multi-layered, meaning that there is a hierarchy in the certificate chain (sub-ca --> root-ca).

— The two Trustpoints are pointing to the same CA and the CA is in a hierarchy of CAs.

Workaround: Delete one of the multi-layered certificates from one of the unused Trustpoints, and the CGR should be able to register with CG-NMS successfully.

- **CSCty95779**

  Symptom: When configuring an Ethernet interface with default configuration by using the **default interface ethernet** *slot/port* command, no logging event CLIs are being configured by default.

  Conditions: Currently, the software displays logging event information, in error, when you enter the **show running-config** command for the interface (as shown below):

  ```
  show running-config int e2/8
  interface Ethernet2/1
  interface Ethernet2/2
    no logging event port link-status
    no logging event port trunk-status
   ...
  interface Ethernet2/8
    logging event port link-status
    logging event port trunk-status
    no shutdown
  ```

  (partial display)

  Workaround: There is no workaround for this issue.

- **CSCty98998**

  Symptom: The input rate on the serial interface of the CGR 1120 always displays as zero (0) in the serial interface statistics summary even though the received input packet count shows an increase.

  Conditions: Connecting to the serial port on a CGR 1120 via Hyperteminal.

  Workaround: This is no workaround for this issue.

- **CSCty99047**

  Symptom: Entering the **shutdown** command on the serial port of the CGR 1120 resets the input packet count to zero.

  Conditions: Input packet count had a value greater that zero prior to entering the **shutdown** command.

  Workaround: There is no workaround for this issue.

- **CSCtz24578**

  Symptom: The CPU temperature sensor on the router might not report accurate information.

  Conditions: This issue occurs when the router reads the CPU temperature.

  Workaround: There is no workaround for this issue.

- **CSCtz32469**

  Symptom: Unable to log into the router immediately after a reload.

  Conditions: This issue occurs when you try to log into the router from the command prompt right after you have reloaded the router configuration; the login attempt will be unsuccessful.

  Workaround: Wait approximately two minutes after reloading the router before trying to log into it.

- **CSCtz47793**

  Symptom: On rare occasions, the CGR sends the registration request before the CGDM is initialized.

Conditions: The CGR sends a registration request to CG-NMS before the CGR CGDM Jetty server has bound to the port and is listening for requests, and if CG-NMS responds quickly to the registration request, the connection CG-NMS tries to establish to the CGR CGDM service is rejected. This shows up in the CG-NMS log as `java.net.ConnectException`.

Workaround: There is no workaround for this issue.

- **CSCtz54022**

    Symptom: This error message appears on the router console:

    ```
    %DEVICE_TEST-2-RTC_FAIL: Module 1 has failed test RealTimeClock 20 times ondevice
    RealTimeClock due to error The rtc open clock failed
    ```

    Conditions: This error message displays when the router is left running idle for a long time.

    Workaround: There is no workaround for this issue.

- **CSCtz84766**

    Symptom: In some cases, entering the **show scada-gw internal database** command on the CGR 1120 to query data on remote terminal units (RTUs) can cause the scada-engine to stop working on the system.

    Conditions: Protocol Translation is active on the CGR 1120 with greater than 500 RTU data points queried by the router.

    Workaround: Do not query more than 500 RTUs when employing the **show scada-gw internal database** command.

- **CSCua07862**

    Symptom: A Backup Battery Initializing message is shown when no BBU installed.

    Conditions: This issue occurs when the router is starting up; the output of the **show env power** command displays the message `Backup Battery Initializing` even when there is no backup battery installed.

    Workaround: There is no workaround for this issue.

- **CSCua07936**

    Symptom: The **install all** command fails during image verification.

    Conditions: This issue occurs infrequently. Upgrading the router by entering the **install all** command failed. Messages indicating `Signature verification failed` and `Image verification failed` display.

    Workaround: Try running the **install all** command again.

- **CSCua12473**

    Symptom: The `Current band` information from the **show cellular** command output does not match the band information from the modem.

    Conditions: This is seen for the GSM EDGE bands (1800, 1900, 850 and 900).

    Workaround: There is no workaround for this issue.

- **CSCua19031**

    Symptom: When the router executes the **install all** CLI command, the AAA accounting logs show user accounts "admin" and "root" as the users who executed the command instead of the real user.

    Conditions: This happens when AAA commands accounting is enabled (via TACACS+) on the router.

    Workaround: There is no workaround for this issue.

- **CSCua19068**

  Symptom: When you disable **snmp-server enable traps link** *command-options* and execute the **install all** command, these commands are re-enabled instead of remaining disabled.

  Conditions: This happens whenever you use the **install all** command after disabling **snmp-server enable traps link** *command-options*.

  Workaround: There is no workaround for this issue.

- **CSCua27018**

  Symptom: The **show interface ethernet** command displayed the incorrect media type as SFP when SFP was inserted.

  Conditions: When RJ-45 connectors were replaced with SFP connectors in the Ethernet ports, the output of the **show interface ethernet** command still indicated that the media-type installed was RJ-45.

  Workaround: There is no workaround for this issue.

- **CSCua33398**

  Symptom: The vsh process might crash when making repeated configuration changes and issuing **copy running-config startup-config** commands.

  Conditions: When making repeated configuration changes and issuing **copy running-config startup-config** commands after every configuration change, the vsh process might crash.

  Workaround: The vsh process automatically restarts itself after crashing. The CLI interface remains operational.

- **CSCua37913**

  Symptom: Repeatedly reloading the 3G cellular module, and entering the **shut** and **no shut** commands caused the router to reload unexpectedly.

  Conditions: This issue occurs when the module is reloaded multiple times and the commands **shut** and **no shut** are entered several times for the cellular interface on the module.

  Workaround: There is no workaround for this issue.

- **CSCua39529**

  Symptom: Removing a RADIUS server with the **no radius-server host** command returns a message indicating the server could not be removed from the configuration, although the RADIUS server actually is removed from the configuration.

  Conditions: This issue occurs when type 6 password encryption is enabled.

  Workaround: None necessary, although you should enter the **show running-config** command to make sure that the RADIUS server was removed from the configuration.

- **CSCua39905**

  Symptom: `Service not responding` messages appear during NMS-triggered golden config rollback.

  Conditions: When the NMS is rolling back the router's configuration to the golden config file, `Service not responding` messages might appear.

  Workaround: You can safely ignore these error messages.

- **CSCua42108**

  Symptom: The NG3 3G connection was lost due to a defect in tracking.

  Workaround: There is no workaround for this issue.

- **CSCua55580**

  Symptom: In some circumstances, entering the **show env power** command on the CGR 1240 yields the following error:

  ```
  Failed to write IOH I2C rc=-1, errno=1(Operation not permitted)
  Power Supply Summary:
  ---------------------
  Read PSU: Unable to write command
  Failed to read data from power supply unit!
  ```

  Conditions: This occurs when you enter the **show env power** command shortly after the follow activities have occurred on the CGR 1240:

  System is powered on, the BBU has initialized, and the syslog message (MOD_DETECT) displays indicating that some modules have been detected.

  Workaround: Do not enter the **show env power** command until the router completes the startup process. This requires approximately 30 seconds.

- **CSCua61061**

  Symptom: BBU status messages show 2% charge remaining, but BBU Battery Status is shown as Fully Discharged.

  Conditions: When the router is being powered by a BBU, the output of the **show env power** command shows that the BBU has 2% charge remaining (BBU Absolute State Of Charge), but the BBU Battery Status is Fully Discharged.

  Workaround: There is no workaround for this issue.

- **CSCua61556**

  Symptom: The syslog message for BBUs does not take into account BBUs that are in the inhibit discharge mode.

  Conditions: This issue occurs when the router has three BBUs: two of the BBUs are in the uninhibit discharge mode, and one is in the inhibit discharge mode. The syslog message reporting the status of the BBUs shows the capacity of the BBUs in the uninhibit discharge mode, but the system does not take into account the capacity of the BBU in the inhibit discharge mode.

  Workaround: There is no workaround for this issue.

- **CSCua68702**

  Symptom: In some cases, when you disconnect a RTU from the SCADA system, the connections to the Control Centers might remain connected. Initiating a General Interrogation of the RTU might also indicate that all RTUs are in good shape.

  Conditions: It is expected that the RTU would disconnect from the Control Centers.

  Workaround: Reset the SCADA gateway to show the correct states of the RTU.

- **CSCua68924**

  Symptom: The configured number of SSH login-attempts does not match the actual allowed number of SSH login-attempts.

  Conditions: This issue occurs when you set the number of attempts an SSH user can make to enter their username and password to 3 (this is also the default). When a user subsequently tries to log in using SSH, the system only allows two tries to enter the correct username and password.

  Workaround: There is no workaround for this issue.

- **CSCua77881**

    Symptom: When configuring four strict-priority egress queues on an interface, packets in the higher priority queue (Queue 1) experience lower latency than those in the lower priority queues (Queues 2, 3, and 4), as expected. However, the packet loss, which is supposed to be less in the higher priority queues, is the same for packets in Queues 2, 3, and 4, with Queue 4 being the lowest priority queue.

    Conditions: When the packets are marked at ingress and assigned to different priority queues at egress.

    Workaround: Premark the input traffic and use ingress priority queuing.

- **CSCua87345**

    Symptom: The **snmpset** command for **ceExtSysBootImageList** and **ceExtKickstartImageList** fails sometimes due to timeout.

    Conditions: Image validation takes more than five seconds by bootvar (a process that runs in the background), which is the expected behavior. This can cause the **snmpset** command to fail due to timeout. Because the image size is very big (more than 100 MB), additional optimization to reduce the image validation time is not possible.

    Workaround: There are two ways to work around this issue:

    - Use the **-t 3** option when using the **snmpset** command.

        For example, instead of using this command:

        ```
        snmpset -v2c -cprivate 172.27.161.88 ceExtSysBootImageList.22 s
        "bootflash:/cgr1000-uk9.5.2.1.CG2.0.179.SSA.gbin"
        ```

        Use this command:

        ```
        snmpset -v2c -t 3 -cprivate -t 3 172.27.161.88 ceExtSysBootImageList.22 s
        "bootflash:/cgr1000-uk9.5.2.1.CG2.0.179.SSA.gbin"
        ```

    - When executing multiple **snmpset** commands, allow for a time gap between these commands.

- **CSCua94746**

    Symptom: When a receiver sends the join message, `no (S,G)` is created in the mroute table on the router.

    Conditions: The router adds the `no (S,G)` entry to the mroute table when the user configures Source Specific Multicast (SSM) on the router, and a receiver sends the join (G) request to the router.

    Workaround: There is no workaround for this issue.

- **CSCua94766**

    Symptom: The output of the **show system reset-reason** command displays `Unknown`.

    Conditions: This issue occurs when you run the **install all** command. Reset reason 88 displays before the system reload, but after the reload completes, entering the **show system reset-reason** command displays `Unknown` for the reset reason.

    Workaround: There is no workaround for this issue.

- **CSCua96673**

    Symptom: When you enter the **install all** command to upgrade the router, the image table listing the system images to be upgraded shows the version number of the current running BIOS image as blank.

    Conditions: This issue occurs when the BIOS image has become corrupted.

    Workaround: There is no workaround for this issue.

- **CSCub03864**

  Symptom: Entering the **system no watchdog kgdb** command does not power-cycle the router.

  Conditions: This issue occurs when you enter the **system no watchdog kgdb** command. The router displays the message `System watchdog kgdb has been disabled` and does not power cycle the router.

  Workaround: There is no workaround for this issue.

Resolved Caveats

- **CSCto95431**

  Symptom: The Cisco Secure ACS Max Sessions feature, which determines the maximum number of simultaneous connections to the CGR 1000 router per user or per group, fails to prompt valid users to log in when configured for 1 or 2 maximum sessions.

  Conditions: The issue occurs when the maximum number of simultaneous sessions is set to 1 or 2. When the maximum simultaneous sessions is set to 3 or more, this feature works as expected and the router supports up 64 simultaneous sessions.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtu65146**

  Symptom: When the Netstack process on the CGR 1000 router ends for any reason, cellular interface modules cannot reconnect to and ping the router.

  Conditions: This issue occurs when the router has a cellular module installed, and the Netstack process ends for any reasons.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtw70336**

  Symptom: The QoS policy does not effectively prioritize high priority traffic, and the router might drop high-priority traffic.

  Conditions: The issue occurs on all interface types when there is congestion on the interface, and different queues are classified at ingress and prioritized to different levels

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtw87364**

  Symptom: The output for the show **ip interface brief** command is incorrect for the link state and the admin state. These value for these fields should be either UP or DOWN, however the output displays the following message:

  `link-state TRUE or FALSE admin-state TRUE or FALSE`

  Conditions: This issue occurs after entering the **show ip interface brief** command.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtw87639**

  Symptom: The CGR 1000 software incorrectly displays the software name as "Cisco Nexus Operating System (NX-OS) Software" and displays the software version number as 5.2(1).

  Conditions: This issue occurs in various instances in the router command-line interface.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx22265**

  Symptom: The CGR 1000 free memory decreases, which can be verified by viewing the output of the show system resources command.

  Conditions: This issue might occur when the router has been operating for 10 days or longer.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx30607**

  Symptom: The CGR 1000 sends a COLD_BOOT Call Home notification (indicating possible power outage on the router) when it should send a WARM_BOOT notification.

  Conditions: This issue occurs when the Call Home feature is configured on the router, and the system software is restarted with the command-line interface (CLI) or with the CG Device Manager software.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx31096**

  Symptom: The CGR 1000 console session hangs and then the following error message displays:

  ```
  Process did not respond within the expected time frame, please try again.
  ```

  Conditions: This issue occurs when you enter the **show logging persistent** command during a router console session.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx52882**

  Symptom: Enabling DHCP on an interface removes any IP address configured on the interface.

  Conditions: This issue occurs when you enable DHCP on an interface that is already enabled for DHCP.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx58117**

  Symptom: The IP routing table displayed with the **show ip route** command shows all IPv4 routes in a pending state.

  Conditions: This issue occurs in all conditions for IPv4 routes only (not for IPv6 routes).

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx60322**

  Symptom: The **class-map** configuration command does support the **match-all** command option for access list and packet length matching combined.

  Conditions: This issue occurs when using the **class-map match-all** option with access-list and packet length matching combined.

  Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCtx95796**

  Symptom: The CGR 1000 displays the private key password in clear text in the accounting logs and on external AAA (TACACS+) servers.

  Conditions: This issue occurs when manually importing a PKCS #12 formatted certificate that has already been copied to the CGR bootflash with the command **crypto ca import** *Trustpoint-name* **pkcs12 bootflash:***PKCS-#12-certificate-filename private-key-password*.

The private key password displays when AAA (TACACS+) config-commands and command authorization, and accounting are enabled.

Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCty07645**

    Symptom: The CGR 1000 command-line interface (CLI) displays the maximum supported value for the **air-sync server port** command to be 99999. The actual supported maximum value is 65535.

    Conditions: This issue occurs in all conditions.

    Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

- **CSCty81424**

    Symptom: The CGR 1240 router does not support SFP model GLC-FE-100FX-RGD.

    Conditions: This issue occurs under all conditions.

    Workaround: This issue is resolved in Cisco CG-OS Release CG2(1).

Accessing Bug Toolkit

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

To access Bug Toolkit, you need the following items:

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

To use the Bug Toolkit, follow these steps:

Step 1 To access the Bug Toolkit, go to the following link:

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

Step 2 Log in with your Cisco.com user ID and password.

Step 3 To look for information about a specific problem, enter the bug ID number in the **Search for bug ID** field and click **Go**.

Step 4 To look for information when you do not know the bug ID number, do the following:

a. From the Select Product Category menu, choose **Routers**.

b. From the Select Products menu, choose **Cisco 1000 Series Connected Grid Routers**.

c. From the Software Version menu, choose the version number.

d. Under Advanced Options, choose either **Use default settings** or **Use custom settings**.

   – When you select **Use default settings**, the system searches for severity 1, 2, and 3 bugs, open and fixed bugs, and only those bugs containing bug details.

   – When you select **Use custom settings**, you can specify the severity and status parameters or search for keywords within the bug headline and description.

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 ASR 1000 Series Aggregation Services Routers Configuration Guide

Cisco 3945 Series Integrated Services Router

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.