



Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco CG-OS Release CG3

Last updated: June 2013
Part Number: OL-27811-07

These release notes contain the latest information about using CG-OS software with the Cisco 1000 Series Connected Grid Routers (Cisco CG-OS routers) for CG3, including this new information:

- Overview of new features added in this release. (See [New Features in Cisco CG-OS Release CG3, page 2.](#))
- Open and resolved caveats in releases CG3(1), CG3(2), and CG3(3). (See [Caveats, page 20.](#))
- Release Note structure. (See [Documentation Updates, page 38.](#))

Tell Us What You Think



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

[Connected Energy Documentation Feedback Form](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

These release notes include the following sections:

- [New Features in Cisco CG-OS Release CG3, page 2](#)
- [About the Cisco 1000 Series Connected Grid Routers, page 6](#)
- [System Requirements, page 10](#)
- [Installation Notes, page 10](#)
- [Important Notes, page 16](#)
- [Caveats, page 20](#)
- [Documentation Updates, page 38](#)
- [Related Documentation, page 39](#)
- [Obtaining Documentation and Submitting a Service Request, page 39](#)

New Features in Cisco CG-OS Release CG3

[Table 1](#) lists the new features added in the Release CG3 software base.

Table 1 **New Features in Cisco CG-OS Release CG3**

Feature	Description	First CG3 Release that Feature was Supported	Related Documentation
<p>IEEE 802.15.4g/e WPAN module, to support IETF 6LoWPAN and RPL protocols</p> <p>6LoWPAN: RFC 6282</p> <p>RPL: RFCs 6206, 6650, 6651, 6553, 6554, and 6719</p>	<p>The WPAN module provides the CGR 1000 Series routers an IEEE 802.15.4g/e wireless interface for communicating with IEEE 802.15.4g/e Connected Grid Endpoints (CGEs) such as smart meters for a given transmission range by using mesh networking technology.</p> <p>CGEs with embedded firmware support open standards-based IPv6 communication using IETF 6LoWPAN and RPL protocols. Additional functionality includes a frequency-hopping radio link, network discovery, link-layer network access control, network-layer auto configuration, IPv6 routing and forwarding, firmware upgrade, and power outage notifications.</p>	CG3(1)	<p>For feature overview and configuration details, see the <i>Cisco Connected Grid WPAN Module for CGR1000 Series Installation and RFLAN Configuration Guide</i> at www.cisco.com/go/cgr1000-docs.</p>
Compromised Node Eviction (for Mesh Security)	<p>Compromised node eviction occurs when the condition of a trusted node on the network changes such that it loses its group temporal key (GTK). The GTK is necessary to gain access to the network which is granted by the AAA server. When an AAA server recognizes that a node does not have a GTK, it evicts the node from the network.</p>	CG3(1)	<p>For feature overview and configuration details, see the <i>Cisco Connected Grid WPAN Module for CGR1000 Series Installation and RFLAN Configuration Guide</i> at www.cisco.com/go/cgr1000-docs.</p>
WiMAX module	<p>The IEEE 802.16e WiMAX module for Cisco CG-OS router provides a WAN interface for communication over WiMAX wireless (1.8 or 2.3GHz) infrastructure in multi-services FAN (Field Area Networks) deployments.</p>	CG3(1)	<p>For feature overview and configuration details, see the <i>Cisco Connected Grid WiMAX Module for CGR 1000 Series Installation and Configuration Guide</i> at www.cisco.com/go/cgr1000-docs.</p>
EAP-Tunneled Transport Layer Security (EAP-TTLS) on WiMAX	<p>The WiMAX module supports EAP-TTLS, as defined in RFC 5281. EAP-TTLS allows a client to be authenticated by a server using a secure tunneled connection after the server has been securely authenticated to the client using its CA certificate.</p>	CG3(1)	<p>For feature overview and configuration details, see the <i>Cisco Connected Grid WiMAX Module for CGR 1000 Series Installation and Configuration Guide</i> at www.cisco.com/go/cgr1000-docs.</p>

Table 1 ***New Features in Cisco CG-OS Release CG3 (continued)***

Feature	Description	First CG3 Release that Feature was Supported	Related Documentation
Raw Socket Transport	<p>Raw Socket Transport is a method for transporting serial data through an IP network. The feature can be used to transport Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs) to a utility management system over an IP network.</p> <p>Raw Socket Transport supports point-to-point and point-to-multipoint connections.</p>	CG3(1)	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
Incremental software image upgrade	<p>Starting in this release, the CG-OS software image files (kickstart and system image) are now available in two formats:</p> <ul style="list-style-type: none"> • Full software image (large file) • Incremental software image (smaller patch file) <p>The incremental image file contains only the differences between the previous software image and the new software image.</p> <p>Using the CLI, you can combine the incremental image file from the new release with the full image file from the previous release to get the equivalent of the full image file for the new release.</p> <p>The combined software image file can be used to upgrade the software on the Cisco CG-OS router with the install all command.</p>	CG3(1)	See Generating Software Images Using Incremental Image Files , page 14.

Table 1 **New Features in Cisco CG-OS Release CG3 (continued)**

Feature	Description	First CG3 Release that Feature was Supported	Related Documentation
Control-plane Policing (part of QoS)	Control-plane policing (CoPP or CPP) is used to prevent the Cisco CG-OS router CPU from Denial of Service (DoS) attacks. CoPP increases security on the router by protecting the system from unnecessary or DoS traffic and giving priority to important control-plane and management traffic. To protect the control plane against DoS attacks and to restrict specific flows, there should be a flexible way to police different classes of traffic destined to the CPU.	CG3(1)	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
BBU firmware upgrade	The BBU firmware is upgraded from version 2082 to version 8272 to provide updates for BBU longevity (CSCud72898). The firmware is upgraded as part of the CG3(2) installation using the install all command. To check the BBU firmware version, use the show env power command.	CG3(1)	See Upgrading to a New Software Release , page 11. For BBU details, see the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> at www.cisco.com/go/cgr1000-docs .
3G Module Reload Enhancement	An internal 3G module reload procedure automatically initiates when it detects more than 10 data call failures. This enhancement prevents a modem from losing the ability to process calls. (CSCuf00246) Note For pre-CG3(3) releases, you must enable the backhaul manager feature on the CGR 1240 to detect and recover from this issue without user intervention.	CG3(3)	See “Configuring Backhaul Manager” in the <i>Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs

Table 1 **New Features in Cisco CG-OS Release CG3 (continued)**

Feature	Description	First CG3 Release that Feature was Supported	Related Documentation
AAA_SERVER_UNAVAILABLE Alerts Enhancement	Added enhancements to the software to limit generation of an AAA_SERVER_UNAVAILABLE alert to no more than one alert every 10 minutes. (CSCuf41398)	CG3(3)	None.
Scheduler Enhancement	Added enhancements to the software to handle situations when runaway jobs occur for jobs configured using the scheduler job name <i>job-name</i> command. Additionally, a warning message displays when you schedule a job beyond your configured repeat interval. (CSCuf04644)	CG3(3)	None.

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, WiFi, WiMAX, and IEEE 802.15.4g/e.

Features and Capabilities

- Rugged industrial design and compliance with IEC-61850-3 and IEEE 1613 for utility substation environments
- Feature-rich software capabilities, including dual-stack (IPv4 & IPv6) support and traffic 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. 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	<ul style="list-style-type: none"> IPv4 unicast forwarding IPv6 unicast forwarding IP services (DNS, DHCP) IP tunnels IPv6 Multicast Listener Discovery (MLD) (partial support) 	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
Routing	<ul style="list-style-type: none"> Open Shortest Path First version 2 (OSPFv2) and OSPFv3 routing Static routing IPv6 Routing protocol for Low Power and Lossy Network (RPL) Route re-distribution between RPL and OSPFv3 Object tracking 	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
Quality of Service (QoS)	<ul style="list-style-type: none"> Classification Marking Priority queuing to manage traffic flow 	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers QoS Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
System management	<ul style="list-style-type: none"> SNMP Network Time Protocol (NTP) System Message Logging Embedded Event Manager (EEM) Backhaul Manager Power outage notification 	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .

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

Feature	Support	Related Documentation
Security	<ul style="list-style-type: none"> • 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 <i>Cisco 1000 Series Connected Grid Routers Security Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
Diagnostics and troubleshooting	<ul style="list-style-type: none"> • 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 <i>Cisco 1000 Series Connected Grid Routers WiFi Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
Supervisory Control and Data Acquisition (SCADA) connectivity	<ul style="list-style-type: none"> • Ability to provide IP connectivity within a SCADA system 	For feature overview and configuration details, see the <i>Cisco 1000 Series Connected Grid Routers SCADA Software Configuration Guide</i> 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	<ul style="list-style-type: none"> • 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 <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> or the <i>Cisco 1120 Connected Grid Router Hardware Installation Guide</i> at www.cisco.com/go/cgr1000-docs .
Ethernet interface	<p>Integrated Ethernet switch module with Fast Ethernet ports (four on CGR 1240, six on CGR 1120) and two Gigabit Ethernet ports</p> <p>The Ethernet ports are currently Layer 3 only</p>	<p>Hardware details are addressed in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> or the <i>Cisco 1120 Connected Grid Router Hardware Installation Guide</i> at www.cisco.com/go/cgr1000-docs.</p> <p>Feature-specific software configuration is addressed in the <i>Cisco 1000 Series Connected Grid Software Configuration Guide Set</i> at www.cisco.com/go/cgr1000-docs.</p>
WiFi interface	Integrated, short-range IEEE 802.11 b/g WiFi access point to support a wireless console connection to the CG-OS router	<p>Hardware details are addressed in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> or the <i>Cisco 1120 Connected Grid Router Hardware Installation Guide</i> at www.cisco.com/go/cgr1000-docs.</p> <p>For configuration details, see the <i>Cisco 1000 Series Connected Grid Routers WiFi Software Configuration Guide</i> at www.cisco.com/go/cgr1000-docs.</p>
Cellular interfaces (CDMA and GSM)	<p>Wireless modules with a mini-card cellular modem (PCI-e mini-card form factor)</p> <ul style="list-style-type: none"> • EVDO Rev A/0/1xRTT (CDMA version) • HSPA+/UMTS/GSM/GPRS/EDGE (GSM version) 	For feature overview and configuration details, see the <i>Cisco Connected Grid Cellular 3G Module for CGR 1000 Series Installation and Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
WiMAX interface	IEEE 802.16e module for providing a WAN uplink over the wireless 1.8 GHz or 2.3 GHz bands in Distribution Automation and AMI concentrator deployments	For feature overview and configuration details, see the <i>Cisco Connected Grid WiMAX Module for CGR 1000 Series Installation and Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .

Table 3 **Hardware Feature Support on Cisco CG-OS Routers (continued)**

Feature	Description	Related Documentation
WPAN interface	IEEE 802.15.4g/e module to support IETF 6LoWPAN and RPL protocols for Connected Grid Endpoints (CGE)	For feature overview and configuration details, see the <i>Cisco Connected Grid WPAN Module for CGR1000 Series Installation and RFLAN Configuration Guide</i> at www.cisco.com/go/cgr1000-docs .
Small Form-Factor Pluggable (SFP) Modules	<p>The following SFP modules are supported on the Cisco CG-OS routers:</p> <ul style="list-style-type: none"> • GLC-SX-MM-RGD • GLC-LX-SM-RGD • GLC-FE-100LX-RGD • GLC-FE-100FX-RGD • GLC-ZX-SM-RGD <p>Other SFP modules, including those made by third-party manufacturers, are not supported</p>	For installation instructions, see the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> or the <i>Cisco 1120 Connected Grid Router Hardware Installation Guide</i> 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 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)S
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, page 11](#)
- [Upgrading to a New Software Release, page 11](#)
- [Erasing the Configuration File, page 15](#)

Determining the Software Version

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

Command	Purpose
<code>show version</code>	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 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.



Note

The kickstart and system images are each available in two formats: as full images, and as incremental software images. An incremental image file contains only the differences between the previous software image and the new software image. You can combine the incremental image from the new release with the full image file from the previous release to get the equivalent of the full image file for the new release.

The combined software image file can then be used to upgrade the software on the Cisco CG-OS router using the **install all** command. See [Generating Software Images Using Incremental Image Files](#), page 14.

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

Command	Purpose
<pre>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]</pre>	<p>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.</p> <ul style="list-style-type: none"> 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). <p>kickstart bootflash: <i>kickstart-file-name</i>—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.</p> <p>system bootflash: <i>system-filename</i>—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.</p> <p>ftp: Specifies File Transfer Protocol (FTP) as the transfer method for the software images (kickstart and system).</p> <p>scp:—Specifies Secure Copy Protocol (SCP) as the transfer method for the software images (kickstart and system).</p> <p>sftp:—Specifies Secure Shell FTP (SFTP) as the transfer method for the software images (kickstart and system).</p> <p>tftp:—Specifies Trivial FTP (TFTP) as the transfer method for the software images (kickstart and system).</p> <p><i>username@</i>—Specifies the username on the server. Username is case-sensitive.</p> <p><i>//path</i>—Defines the path to the server on which the software images reside.</p> <p><i>//server</i>—Defines the IPv4 address or name of the server on which the software images reside.</p> <p>[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.</p>

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.CG3.0.195.SPA.bin for boot
variable "kickstart".
-- SUCCESS

Verifying image bootflash:///cgr1000-uk9.5.2.1.CG3.0.195.SPA.bin for boot variable
"system".
-- SUCCESS

Verifying image type.
-- SUCCESS

Extracting "system" version from image bootflash:///cgr1000-uk9.5.2.1.CG3.0.195.SPA.bin.
-- SUCCESS

Extracting "kickstart" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG3.0.195.SPA.bin.
-- SUCCESS

Extracting "bios" version from image bootflash:///cgr1000-uk9.5.2.1.CG3.0.195.SPA.bin.
-- SUCCESS

Extracting "loader" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG3.0.195.SPA.bin.
-- SUCCESS

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

```

Notifying services about system upgrade.
-- 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)CG3(1)	yes
1	kickstart	5.2(1)CG1(3c)	5.2(1)CG3(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.
-- SUCCESS

```

```

Setting boot variables.
-- SUCCESS

```

```

Performing configuration copy.
-- 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.
-- SUCCESS

```

```

Install has been successful.

```

```

cgr1000#

```


Note

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

Generating Software Images Using Incremental Image Files

The kickstart and system images are both available as incremental image files. Incremental image files contain only the differences between the previous software image and the new software image. An incremental software image can be combined with the previous software image to get the equivalent of the full version of the new software image, which can then be installed with the **install all** command, as described in the previous section.

For example, an incremental image file for CG3(1) contains only the differences between CG3(1) and the previous software release, CG2(1). You can combine the CG3(1) incremental image file with the CG2(1) software image to get the equivalent of the full version of the CG3(1) software image. There are separate incremental image files for the kickstart and system images.

To generate software images using incremental patch files, you use the **image-patch** command in privileged EXEC mode. The following table provides detailed command syntax for the **image-patch** command.

Command	Purpose
image-patch seed-image <i>seed_img</i> patch-file <i>diff_img</i> target-path <i>target_url</i>	<p>Combines a specified seed image file with a specified incremental patch file, and copies the combined file to a specified target URL.</p> <ul style="list-style-type: none"> Define seed-image as the name of the image you are upgrading from. There should be a copy of this image on the CGR bootflash. Define patch-file as the name of the incremental patch file for image you are upgrading to. Define target-path as the location for the combined seed and patch file. The original seed and incremental patch files are left as-is.

EXAMPLE

This example shows how to combine the CG2(1) seed image file `cgr1000-uk9.5.2.1.CG2.0.59.SPA.bin` with the CG3(1) incremental patch file `cgr1000-uk9.5.2.1.CG3.0.16-CG2.0.59.SPA.bin` and place the combined file into bootflash:

```
cgr1000# image-patch seed-image cgr1000-uk9.5.2.1.CG2.0.59.SPA.bin patch-file
cgr1000-uk9.5.2.1.CG3.0.16-CG2.0.59.SPA.bin target-path bootflash:
```



Note

An output similar to the one below displays during the image patching process.

```
Image patching is in progress, please wait.

Patching image.
[#####] 100%
Target image URL: /bootflash//cgr1000-uk9.5.2.1.CG3.0.16.SPA.bin.
-- SUCCESS
```

The resulting file in bootflash is equivalent to the full `cgr1000-uk9.5.2.1.CG3.0.16.SPA.bin` image file. Run the **image-patch** command for both the kickstart and system images. After you have generated both images, run the **install all** command to upgrade the router to the new software version. See [Upgrading to a New Software Release](#), page 11.

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]	<p>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)</p> <p>debug—Erases only the debug configuration file from the persistent memory of the router.</p> <p>secrets—Erases the certificates, private keys and the password encryption master key from persistent memory on the router.</p>

Important Notes

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.

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.

DHCP Client IP Route Setup Changes

In Cisco CG-OS Release CG3(1), the software reports all IP routes set up by the DHCP client directly to the IP routing table. To review the information added by the DHCP client, enter the **show ip route detail** command. If an IP route entry of `ip route 0.0.0.0 0.0.0.0 x.x.x.x 254` or `ip route 0.0.0.0 0.0.0.0 x.x.x.x` appears when you are operating with CG3(1) software, you must remove the entry by entering the **no ip route** command. This IP route process differs from that of Cisco CG-OS Release CG2(1) and earlier releases. In those earlier software releases, you entered the **show running-config** command to review the IP route entry.

- In Cisco CG-OS Release CG2(1), the default route had a route preference of 254 when DHCP was enabled on the router.
- In Cisco CG-OS Release CG1(1), the default route had a route preference of 1 when DHCP was enabled on the router.

Manual Start for NTP Service

To start the Network Time Protocol (NTP) service on the router, you must now enter the **feature ntp** command. In previous releases, the NTP service was started by default when the router was booted, and it could not be disabled.

After the NTP service is enabled, you can disable it with the **no feature ntp** command. Note that when the NTP service is disabled, the NTP-related statements in the router configuration are disabled.


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 Cisco 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.

- **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.

- **CSCtx77959**

Symptom: The CGR 1000 reports hardware and environmental power data about a single power supply only, even though it has both AC and DC power supplies.

Conditions: This issue occurs because CGR actually has hardware for just the AC power supply. The DC power supply input is to the AC power supply, and the DC power supply is managed by the AC power supply hardware. Consequently, the CGR 1000 reports information about the AC power supply hardware only.

Workaround: There is no workaround for this issue.

- **CSCtx82513**

Symptom: For configured security changes to take effect on the WiMAX interface, you must remove the EAP-TLS or EAP-TTLs configuration then add it again.

Conditions: When changing existing security settings on the WiMAX interface (for example, changing the server or device trustpoint).

Workaround: Disable and then enable the corresponding auth-method again by using the following commands:

Disable the auth-method: **no pkm auth-method**

Re-enable the auth-method: **pkm auth-method eap-tls or pkm auth-method eap-ttls**

- **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.

- **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: None.

- **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.

- **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: None.

- **CSCua32723**

Symptom: A cell power module (cell PM) restart causes the 3G module to reload.

Conditions: When a 3G-related process was killed.

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.

- **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: None.

- **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) or later 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.

- **CSCub49104**

Symptom: Output from **show mesh-security session all** does not show all current mesh security sessions.

Conditions: This issue occurs in the output of the **show mesh-security session all** command.

Workaround: To find out the mesh-key status of a meter, use the **show mesh-security session mac <mac-address>** command.

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 20](#)
- [Resolved Caveats, page 29](#)
- [Accessing Bug Toolkit, page 38](#)

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.

- **CSCtu25387**

Symptom: AAA authorization fails for a CGDM client (CG-NMS and CGDM) if an "admin" user account does not exist in the external TACACS+ user database. This user also has to have the correct privileges equivalent to a network-admin role.

Conditions: With an AAA TACACS+ server host configured, along with the following AAA policies configured on the CGR:

aaa authentication login default group <TACACS+_server_group>

aaa authorization commands default group <TACACS+_server_group>

aaa authorization config-commands default group <TACACS+_server_group>

Workaround: Create an "admin" user account within the external AAA TACACS+ user database and assign it privileges equivalent to a network-admin role.

- **CSCtu41227**

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

Conditions: This issue occurs when both IPv6 and IPv4 Ethernet 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.

- **CSCtw56773**

Symptom: The state of the interface is listed as `none` in the reason field, `state_rsn_desc`, of the **show interface e2/x** command output when it should show `Line protocol is up`. It also states that `Link not connected` when it should say `Line protocol is down`.

Conditions: Issue is present when line protocol is up and when line protocol is down.

Workaround: None

- **CSCtw79027**

Symptom: When two or more IMIX data streams that are configured with different priorities are sent in both directions over the 3G interface, the data stream set to default priority is given a higher priority than data streams configured with a higher priority.

Conditions: This issue occurs when no QoS priorities are applied on either the egress or ingress, and there is data congestion on the interface.

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.

- **CSCtx43958**

Symptom: The Call Home feature does not send a Call Home notification if the CGR 1000 is booted up and operating without a battery backup unit (BBU) installed.

Conditions: This issue occurs when the Call Home feature is enabled on the router and there is no BBU installed in the router.

Workaround: There is no workaround for this issue.

- **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.

- **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.

- **CSCtx96418**

Symptom: Duplicate Address Detection (DAD) indicates that a duplicate IPv6 address being used on a CGR 1000 Ethernet interface is valid. DAD should indicate the address as invalid because the address is already in use by an interface on another network device.

Conditions: This issue occurs after performing the following steps on the CGR 1000 interface that is using the duplicate address: 1) Use DAD to verify the IP address. 2) Change the MAC address.

Workaround: Configure the affected interface with another, unique IPv6 address.

- **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.

- **CSCty20444**

Symptom: When you disable the **feature scada-gw** command by entering **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: None.

- **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: None.

- **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: None.

- **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: There are multiple trustpoints configured on the CGR and the certificates for each trustpoint are 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 interface as a default Ethernet interface by using the **default interface Ethernet <slot/port>** command, it should remove the previous configuration of the interface. Therefore, when you enter a command to check the running configuration (for example: **show running-config int e2/8**) it should not show any configuration or logging event details for the interface. The modified Ethernet interface should only show minimal information as shown below:

```
!Time: Thu Jul 26 08:36:47 2012
version 5.2(1)CG2(1)
```

```
interface Ethernet2/8
```

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: None.

- **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 than zero prior to entering the **shutdown** command.

Workaround: There is no workaround for this issue.

- **CSCtz08283**

Symptom: If the 3G module was inserted into a different slot and was configured (for example, with a static route), the configuration details are seen in the running configuration when you issue the show run command. However, if you tried to remove the route, you could not because the module was in a different slot now.

Conditions: 3G Module was moved to a different slot.

Workaround: Move the 3G module back to the original slot and remove the route.

- **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: 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 and greater than 500 RTU data points are queried by the CGR 1120.

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

- **CSCtz89502**

Symptom: When pinging a multicast address to get echo responses with the correct latency numbers, only the first response has the correct latency number. Subsequent responses do not show up until the next echo request is sent and their latency values (for the replies of previous request) show incorrectly calculated figures.

Conditions: When ping6 is done to a multicast address through a WPAN interface.

Workaround: None

- **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.

- **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.

- **CSCua39841**

Symptom: A bad Address Resolution Protocol (ARP) message appears at random times.

Conditions: Issue is present after establishing connection on a WiMAX module after a reboot.

Workaround: There is no workaround for this issue.

- **CSCua40129**

Symptom: The output of the **show interface transceiver** command indicates that a transceiver is not installed when one actually is installed in the module.

Conditions: This issue occurs when non-supported SFPs are installed in the module.

Workaround: Only use supported SFPs. See [Table 3 on page 9](#) for a list of supported SFPs

- **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.

- **CSCua79320**

Symptom: The logging message `AAA_SERVER_UNAVAILABLE` appears when device authentication failed due to wrong certificate.

Conditions: The Device presented the wrong certificate for authentication to the AAA server.

Workaround: None

- **CSCua87345**

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

Conditions: Image Validation takes more than 5 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.

- **CSCua92049**

Symptom: IGMP when configured does not work on the CGR. The IGMP process does not work.

Conditions: Clients send IGMP join messages to the CGR.

Workaround: There is no workaround.

- **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.

- **CSCua97316**

Symptom: Rollback to a previous checkpoint configuration failed.

Conditions: This issue occurs when you configure AAA commands, save a checkpoint, modify the AAA configuration, and save another checkpoint. Attempting to roll back to the first checkpoint fails, and the output of the **show rollback log verify** command indicates that the verification patch contains AAA commands.

Workaround: Remove the AAA commands from the running-config.

- **CSCub08942**

Symptom: The rollback function did not roll back the **logging logfile** configuration statement.

Conditions: This issue occurs when the **logging logfile** statement exists in the running config. If you save a checkpoint, then configure a new **logging logfile** statement, when you roll back to the previous checkpoint, the **logging logfile** statement from the checkpoint is not applied.

Workaround: There is no workaround for this issue.

- **CSCub21940**

Symptom: If **feature scp-server** is enabled, only the admin user can log into the CGR. With **feature sftp-server** enabled (which uses the SSHd mechanism), only the admin user account can be used to log into the CGR. When using a valid set of credentials that exist in the AAA server, no other user can be used. This means that the admin user account has to be replicated in the external AAA database which may violate some company's security policy since it is a known username and some AAA servers treat this account differently than others. The normal SSH process allows valid AAA user credentials.

Conditions: The command **feature scp-server** is enabled

Workaround: To allow non-admin accounts with network-admin user role to access the CGR, enable **feature sftp-server**.

- **CSCub24790**

Symptom: Inconsistent service LED results in output of **show cellular x/x led**. Service LED is listed as `slow blink` although no service is available.

Conditions: When the Sprint Module is plugged into the CGR 1120 slot and no service is available.

Workaround: None

- **CSCub43740**

Symptom: This error message displays in the console: `ERROR: Ethernet2/2: Requested speed is not supported by transceiver`

Conditions: If you enter these commands, you get the error message.

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# int e2/2
Router(config-if)# speed 100
ERROR: Ethernet2/2: Requested speed is not supported by transceiver
Router(config-if)# duplex full
ERROR: Ethernet2/2: Incompatible Speed and Duplex settings on interface
```

Workaround: None.

- **CSCub60426**

Symptom: When upgrading the RFLAN module 3.7 firmware, the command **install all** fails.

Conditions: Issue occurs if the `CommModuleStatisticsReadPeriod` rate is changed to more than 50 seconds.

Workaround: Change the `CommModuleStatisticsReadPeriod` to default value of 30 seconds.

- **CSCub66408**

Symptom: The CGR 1000 console receives an SNMP critical log message: `netsnmp_tcp_send: TRACE - send returned error.`

Conditions: No crash or unusual behavior was observed during the execution of SNMP reads and writes when malformed packets were sent to the router.

Workaround: It is safe to ignore the messages.

- **CSCub68564**

Symptom: When using the Connected Grid Device Manager (CGDM), the command and its options `show logging last <1-9999>` fails to display properly.

Conditions: None

Workaround: There is no workaround for this issue.

- **CSCub72376**

Symptom: A CGR 1000 connected to a Verizon 3G modem intermittently loses the 3G connection.

Conditions: This issue occurs randomly.

Workaround: Reload the 3G module or reboot the router. Disabling then re-enabling the interface does not resolve the issue. Additionally, configure Backhaul Manager on the CGR 1000 to monitor backhauls and to provide corrective action when a backhaul such as a 3G connection is down.

- **CSCub82645**

Symptom: The following messages are shown in the syslog messages:

```
Failed to error in getting kernel ifindex for usb0
```

Conditions: These error messages appear when the 3G module is reloaded.

Workaround: There is no workaround for this issue.

- **CSCub99905**

Symptom: When the DHCP configuration is removed from the CGR, it sends a DHCPRelease packet, but the packet is dropped by some DHCP relay agents, and the DHCP server keeps the IP address leased until the lease time expires.

Conditions: This issue occurs when the DHCP client on the CGR is connected to a non-ISC DHCP relay agent.

Workaround: There is no workaround for this issue.

- **CSCuc02555**

Symptom: Error reading image seed file during downgrading.

Conditions: This issue occurs when downgrading from CG3-b73 to CG2(1) image. Extracting the CDMA firmware might be the cause of the downgrade operation to fail.

Workaround: There is no workaround for this issue.

- **CSCuc18128**

Symptom: The CGR failed to install CG-OS software version 3.0.67 from the CG-NMS and returned code 0x40B30029 (Operation failed. Fabric is already locked).

Conditions: This issue was seen while upgrading the image on the CGR from the CG-NMS.

Workaround: Reload the router or perform an **install all** from the CGR console.

Resolved Caveats

- [Caveats Resolved in Cisco CG-OS Release CG3\(3\), page 29](#)
- [Caveats Resolved in Cisco CG-OS Release CG3\(2\), page 30](#)
- [Caveats Resolved in Cisco CG-OS Release CG3\(1\), page 33](#)

Caveats Resolved in Cisco CG-OS Release CG3(3)

- **CSCub72376**

Symptom: A CGR1240 operating with a 3G Module (CDMA) lost its 3G connection intermittently.

Conditions: Connection failed to reconnect when the connection was disconnected from the carrier network.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(3).

For earlier releases, use the following workaround:

Enable the backhaul manager feature on the CGR 1240 to detect and recover from this issue without user intervention. (See “Configuring Backhaul Manager” in the *Cisco 1000 Series Connected Grid Routers System Management Software Configuration Guide* at www.cisco.com/go/cgr1000-docs)

Alternatively, reload the 3G module, or reload the router. Using the **shutdown** and **no shutdown** command on the interface does not resolve this issue.

- **CSCud89777**

Symptom: When you enabled TACACS+ on a CGR, the router sent two authorization requests, rather than one as expected, to the external AAA/TACACS+ server.

Conditions: TACACS+ was enabled on a CGR after entering the following commands:

aaa authorization commands default group <TACACS+ _server_group> local

aaa authorization config-commands default group <TACACS+ _server_group> local

Workaround: This issue is resolved in Cisco CG-OS Release CG3(3).

- **CSCud98129**

Symptom: When a NTP server was identified with a name rather than an IP address, the CGR had problems resolving the name, after bootstrap completed.

Conditions: NTP server was assigned a name rather than IP address.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(3).

- **CSCue44618**

Symptom: The TACACS+ server groups were not using the configured source interface to access TACACS+ servers.

Conditions: Global source interface was configured for TACACS+ server groups to use when accessing TACACS servers.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(3).

- **CSCue62156**

Symptom: When CG-NMS pushed a DHCP configuration for an CGR Ethernet interface in a certain sequence, the DHCP client might fail to receive the DHCP IPv4 address.

Conditions: Occurred when CG-NMS was used to configure DHCP on an CGR Ethernet interface.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(3).

For earlier releases, enter the following commands as a workaround:

```
configure terminal
interface interface
no ip address
ip address dhcp
end
```

- **CSCue76682**

Symptom: An upgrade from CG1 (3d) or CG1(6) to Release CG3(3) using the **install all** command did not upgrade the BBU firmware from version 2082 to 8272.

Conditions: The **install all** command did not have the capability to upgrade the BBU firmware from 2082 to 8272. Changes were made to initiate a BBU firmware upgrade after a successful upgrade from CG1 to CG3; and, a reload of the router.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(3).

Caveats Resolved in Cisco CG-OS Release CG3(2)

- **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: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCty14205**

Symptom: When the IPv6 address is changed for the WPAN interface 4/1, the CGR 1000 Series router requires a reboot for changes to enable meters to join the network.

Conditions: This issue occurs when the WPAN interface configuration is changed using the **prefix** or **ip address interface** configuration commands.

Workaround: After configuring the interface, the CGR 1000 Series router must be reloaded for changes to take effect. However, if the PANID is changed, the meter will get a new IPv6 address and the CGR reload is avoided.

- **CSCtz97810**

Symptom: The WiMAX download (DL) dynamic modulation does not function as expected. The DL carrier-to-noise-plus-interference ratio (CINR) does not get updated on the base-station side. This results in the download modulation not decreasing as per CINR thresholds.

Conditions: Issue is present when the DL link is saturated as RF conditions worsen.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCuc20535**

Symptom: The CGR 1000 was unable to connect to Release 2.0 of the Device Manager.

Conditions: Command authorization was enabled on the CGR 1000.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCuc22845**

Symptom: NTP did not support resolving the hostname for the IPV6 NTP server.

Conditions: The **show ntp peers** command did not display IPV6 address for the hostname of the IPV6 NTP server.

Workaround: Use the **ntp server ipv6 address** command instead.

- **CSCuc91336**

Symptom: The dialer retry timer always reset after the 3G module was reloaded.

Conditions: This issue occurred when the 3G module was reloaded.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCuc91969**

Symptom: Memory leaks were observed with faceplate manager related commands such as show door.

Conditions: The software did not release objects associated with processing show command inquiries, which resulted in memory leaks.

Workaround: This issue is resolved in CG-OS CG3(2).

- **CSCuc94606**

Symptom: In some cases, the system clock on the CGR 1000 would change to an older system clock after a system reboot. The modified clock setting could be several days old. This affected any applications dependent on the system clock.

Conditions: A reboot of the CGR 1000 reset the system clock to a previous date.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCud12701**

Symptom: IKEv2 handshake failed given IKEv2 can only accept messages of up to 2048 bytes.

Conditions: CGR 1000 was configured with IKEv2 for authentication by using RSA signatures and certificates. IKEv2 authentication resulted in packets that were larger than 2048, which IKEv2 could not accept.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCud15097**

Symptom: In some circumstances, when you configure the CGR call home notification to report every minute, CG-NMS makes repeated queries to the CGR, which might cause memory leaks in related processes over a long period of time.

Conditions: The call home notification frequency had a setting of one minute. Settings of 15 minutes or greater are the norm.

Workaround: Software changes in CG3(2) reduce the incidence of these call home memory leaks.

- **CSCud39260**

Symptom: WPAN port manager forwarded Power Restoration Notification (PRN) Messages to the CG-NMS.

Conditions: PRN messages were generated by the mesh node (meters or any other device where a communications module (CM) is used) when power was restored. Each mesh device sent a maximum of 3 PRN messages, with a random back off of 30 seconds in between them. The CGR forwarded these messages to the CG-NMS.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

- **CSCud62889**

Symptom: Memory leaks were associated with the 802.1X authentication process on the CGR 1000.

Conditions: The meter to which the CGR 1000 was communicating had 802.1X enabled.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(2).

Caveats Resolved in Cisco CG-OS Release CG3(1)

- **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 were connected to a SmartBit test device, the router displayed the following message, and then the ping timed 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 occurred when traffic was sent over the affected ports.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtw50574**

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

Conditions: This issue occurred on interfaces with DHCP enabled.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtw59629**

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

Conditions: This issue could occur when an NTP configuration existed on the router and was then removed, and the router was reloaded.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtw66798**

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

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

Conditions: This issue occurred when the BBU provided power for the router.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtw85126**

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

Conditions: This issue occurred under all conditions.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtx04502**

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

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

Conditions: This issue occurred in boot mode.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCty05226**

Symptom: Many error messages flooded the console and syslog, and the CPU utilization might reach 100%, which negatively impacted traffic and other router functions. This could have been 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 have become the target of UDPSIC attacks.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCty47211**

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

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

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtz47793**

Symptom: On rare occasions, the CGR sent the registration request before the CGDM was initialized.

Conditions: The CGR sent a registration request to CG-NMS before the CGR CGDM Jetty server had bound to the port and was listening for requests, and if CG-NMS responded quickly to the registration request, the connection CG-NMS tried to establish to the CGR CGDM service was rejected. This showed up in the CG-NMS log as `java.net.ConnectException`.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCtz54022**

Symptom: This error message appeared 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 displayed when the router was left running idle for a long time.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua07862**

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

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

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua07936**

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

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

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua12473**

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

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

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua31437**

Symptom: The **show module** command displayed the wrong number of Ethernet ports.

Conditions: The output of the **show module** command indicated that the Ethernet module in slot 2 had 7 Ethernet ports when it actually had 6 Ethernet ports.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **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 occurred when the module was reloaded multiple times and the commands **shut** and **no shut** were entered several times for the cellular interface on the module.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua39905**

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

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

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua55580**

Symptom: In some circumstances, entering the **show env power** command on the CGR 1240 yielded 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 occurred when you entered the **show env power** command shortly after the following activities occurred on the CGR 1240:

System was powered on, the BBU had initialized, and the syslog message (`MOD_DETECT`) displayed indicating that some modules had been detected.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua61061**

Symptom: BBU status messages showed 2% charge remaining, but BBU Battery Status was shown as `Fully Discharged`.

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

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua89352**

Symptom: Rolling back the configuration to checkpoint failed.

Conditions: Occurred on a fully configured Dialer1 interface when using the **rollback running-config checkpoint <checkpoint_name>** configuration command where the checkpoint did not have Dialer1 configured. The roll back failed if the running-config contained:

```
interface Dialer1
    dialer persistent
    dialer pool 1
    dialer string cell_script
    no shutdown
```

And the checkpoint had this:

```
interface Dialer1
    no shutdown
```

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCua94766**

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

Conditions: This issue occurred when you ran the **install all** command. Reset reason 88 displayed before the system reload, but after the reload completed, entering the **show system reset-reason** command displayed `Unknown` for the reset reason.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCub03864**

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

Conditions: This issue occurred when you entered the **system no watchdog kgdb** command. The router displayed the message `System watchdog kgdb has been disabled and did not power cycle the router`.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCub09014**

Symptom: Occasionally, error messages like these about RealTimeClock failure display in the console:

```
2012 Jul 16 06:00:05 calabria-p3 %DEVICE_TEST-2-RTC_FAIL: Module 1 has failed test
RealTimeClock 20 times on device RealTimeClock due to error The rtc open clock failed
```

```
2012 Jul 16 06:00:05 calabria-p3 %MODULE-4-MOD_WARNING: Module 1 (serial: JAF1619ARQB)
reported warning due to The rtc open clock failed in device 0 (device error 0x0)
```

Workaround: You can safely ignore these errors.

- **CSCub27668**

Symptom: The default timeout setting of 5 seconds for Simple Certificate Enrollment Protocol (SCEP) was not sufficient for running the protocol over a satellite link.

Conditions: SCEP traffic was running over a satellite link.

Workaround: The default timeout setting is now set to 25 seconds for the SCEP client on the CGR. This issue is resolved in Cisco CG-OS Release 5.2(1)CG1(3d).

- **CSCub67494**

Symptom: The snmpwalk process failed with the following error:

```
"Error: OID not increasing: CISCO-IMAGE-UPGRADE-MIB::ciuImageVariableName."kickstart"
>= CISCO-IMAGE-UPGRADE-MIB::ciuImageVariableName."seed"
```

Conditions: This error occurred when snmpwalk was performed at ISO; for example:

```
snmpwalk ?v 2c ?c public x.x.x.x .iso
```

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCub70509**

Symptom: The RADIUS service on the router crashed when you attempted to re-encrypt the password.

Conditions: If you configured a RADIUS server, but did not specify a key, if you then entered the **encryption re-encrypt obfuscated** command, it caused the RADIUS service to crash.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(1).

- **CSCub70713**

Symptom: The **raw-socket tcp client** command allowed a TCP port to be configured for multiple client connections.

Conditions: When configuring the **raw-socket tcp client** command, it was possible to assign the same TCP port to multiple clients.

Workaround: This issue is resolved in Cisco CG-OS Release CG3(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.
-

Documentation Updates

Changes

Release Notes for Cisco 1000 Series Connected Grid Routers have been restructured to contain information for all maintenance releases for a given software release within one Release Note. For example, the Release Notes for CG-OS CG3 include details on releases CG3(1), CG3(2), and so on. Previously, we had separate Release Notes for these iterative releases.

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](#)

[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.

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

No combinations are authorized or intended under this document.

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

© 2012-2013 Cisco Systems, Inc. All rights reserved.

