



Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco CG-OS Release CG4

First Published: April 2013

Last Updated: January 9, 2014

Part Number: OL-29357-08

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 CG4, including this new information:

- Overview of new features added in this release. (See [New Features in Cisco CG-OS Release CG4, page 2.](#))
- Open and resolved caveats in release CG4(3), CG4(2) and CG4(1). (See [Caveats, page 21.](#))



Note

Cisco CG-OS CG4 includes the resolved caveats of Cisco CG-OS CG3.

Tell Us What You Think



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

[Connected Energy Documentation Feedback Form](#)



Cisco Systems, Inc.
www.cisco.com

Contents

These release notes include the following sections:

- [New Features in Cisco CG-OS Release CG4, page 2](#)
- [About the Cisco 1000 Series Connected Grid Routers, page 7](#)
- [System Requirements, page 11](#)
- [Installation Notes, page 12](#)
- [Important Notes, page 17](#)
- [Caveats, page 21](#)
- [Documentation Updates, page 37](#)
- [Related Documentation, page 37](#)
- [Obtaining Documentation and Submitting a Service Request, page 38](#)

New Features in Cisco CG-OS Release CG4

Table 1 lists the new features added in Release CG4.

Table 1 ***New Features in Cisco CG-OS Release CG4***

Feature	Description	First CG4 Release that Supports Feature	Related Documentation
Backhaul Manager Reload Event	CGR 1000 reports a new event, reload link-recovery , when a reload occurs due to a link outage. (CSCuj23382, CSCuj59287)	CG4(3)	For feature overview and configuration details, see the “Configuring WAN Backhaul Redundancy” chapter in the <i>Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide</i> at: www.cisco.com/go/cgr1000-docs
Dual backhaul	CGR 1000 supports dual backhuls for 3G, WiMAX, and Ethernet interfaces.	CG4(3)	Varied documentation given application. Please contact your Cisco representative or partner.
Route redistribution	Support for route redistribution of external RPL routes in CG-mesh network for application modules and MAP-T addresses in DA gateways. (CSCuj23382, CSCuj59287, CSCul03569)	CG4(3)	For feature overview and configuration details, see the <i>Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide</i> at www.cisco.com/go/cgr1000-docs

Table 1 **New Features in Cisco CG-OS Release CG4 (continued)**

Feature	Description	First CG4 Release that Supports Feature	Related Documentation
Expanded route support for DHCP clients.	Each interface supports up to 16 routes for DHCP clients. (CSCu11674)	CG4(3)	For feature overview and configuration details, see the “Configuring IP Services” chapter in the <i>Cisco 1000 Series Connected Grid Routers Unicast Routing Software Configuration Guide</i> at: www.cisco.com/go/cgr1000-docs
Secure Digital (SD) flash memory module (SD card) locking	<p>Allows locking and unlocking of the SD card through software to limit access and protect configuration information on the module.</p> <p>You can also enable password-strength check when defining the password and check whether a password is defined for the SD card module.</p> <p>(CSCug62713, CSCuh47814, CSCuh50418, CSCuh53071, CSCui65513)</p> <p>Note If you want to employ password strength on the SD card, you must enable password strength on the router, before you create the password.</p> <p>To enable password strength check on the SD module, enter:</p> <pre>router(config)#: password-strength check</pre> <p>There are two new commands:</p> <p>To create a password for the SD card, enter:</p> <ul style="list-style-type: none"> router(config)#: [no] sd password word word—64-byte case-sensitive string <p>To check if the SD card has password protection and has a pending reload, enter:</p> <ul style="list-style-type: none"> show sd-card password status 	CG4(3)	<i>Cisco 1240 and 1120 Connected Grid Router Hardware Installation Guides</i> www.cisco.com/go/cgr1000-docs
SD flash reset reason for SD flash removal	<p>When you remove an SD card from an online CGR 1000, the router automatically reloads.</p> <p>When this occurs, a reset-reason will indicate that the system reload is due to an SD card removal. (CSCui82859)</p>	CG4(3)	

Table 1 ***New Features in Cisco CG-OS Release CG4 (continued)***

Feature	Description	First CG4 Release that Supports Feature	Related Documentation
Modem Band Selection for 3G module	<p>A new command allows you to specify the preferred connection rate(s) for the 3G GSM module (CSCtn94963):</p> <p>cellular interface number/port number gsm band {auto-band all-bands exclude all-900-bands}</p> <ul style="list-style-type: none"> • auto-band (default)—scans for all available bands and connects to a 3G service, if available. • all-bands exclude-900-bands—scans for all available bands except all the 900 MHz bands. <p>To verify the setting, use the show cellular interface number/port number radio command.</p>	CG4(2)	<p>For details on the 3G module, see the <i>Cisco Connected Grid Cellular 3G Module for CGR 1000 Series Installation and Configuration Guide</i> at:</p> <p>www.cisco.com/go/cgr1000-docs</p>
Low temperature threshold alarms	<p>New call home alarms on the router provide low temperature threshold warnings; and, include the following alarms (CSCuh07528):</p> <p>TEMPERATURE_MAJOR_ALARM TEMPERATURE_MAJOR_ALARM_RECOVERY TEMPERATURE_MINOR_ALARM TEMPERATURE_MINOR_ALARM_RECOVERY TEMPERATURE_SENSOR_FAILURE TEMPERATURE_LOW_MAJOR_ALARM TEMPERATURE_LOW_MAJOR_ALARM_RECOVERY TEMPERATURE_LOW_MINOR_ALARM TEMPERATURE_LOW_MINOR_ALARM_RECOVERY</p>	CG4(2)	

Table 1 **New Features in Cisco CG-OS Release CG4 (continued)**

Feature	Description	First CG4 Release that Supports Feature	Related Documentation
3G GSM module low temperature threshold changes	<p>When operating in a router with CG4(2) software, the 3G GSM module supports the following low temperature threshold settings (CSCug55056):</p> <ul style="list-style-type: none"> The low critical temperature threshold setting is -26 degrees C (In release CG4(1) and earlier, the setting remains at -16 degrees C) The low critical temperature recovery threshold setting is -23 degrees C (In release CG4(1) and earlier, the value remains at -6 degrees C) <p>The router automatically detects lower ambient temperatures on the 3G GSM module, and automatically puts the modem in a lower power mode when the module reaches the <i>low critical temperature threshold</i>; and, restores full power mode when the ambient temperature reaches the <i>low critical temperature recovery threshold</i>.</p>	CG4(2)	<p>For details on the 3G module, see the <i>Cisco Connected Grid Cellular 3G Module for CGR 1000 Series Installation and Configuration Guide</i> at:</p> <p>www.cisco.com/go/cgr1000-docs</p>
Enhanced BBU firmware version 5213 raises threshold value for turning off charging functionality.	BBU charging functionality of new firmware, stops when cell voltage drops under 2.0V rather than 1.5V. (CSCuh07282)	CG4(2)	<p>For details on upgrading your BBU firmware, see the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> at:</p> <p>www.cisco.com/go/cgr1000-docs</p>
SD flash module removal alert	When you remove the SD flash module from a Cisco 1000 Series router, the system sends a callhome alert of severity 7 to CG-NMS. (CSCua21506, CSCug41521).	CG4(2)	<p>See “About the SD Flash Memory Module” chapter in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> and the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> at:</p> <p>www.cisco.com/go/cgr1000-docs</p>

Table 1 **New Features in Cisco CG-OS Release CG4 (continued)**

Feature	Description	First CG4 Release that Supports Feature	Related Documentation
Fully Qualified Domain Support (FQDN) on the WPAN module (version 5.2.82 and later)	Allows you to specify a host name and domain name for a mesh outage server in the interface configuration mode: (CSCue96374) outage server [hostname IPv6 address] where IPv6 address format options is: aaaa:bbbb:cccc:dddd:eeee:ffff:gggg:hhhh The CGR 1000 only supports an IPv6 address format for the mesh outage server. The router does not support the IPv4 option in the command.	CG4(2)	For feature overview and configuration details, see the <i>Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide</i> at www.cisco.com/go/cgr1000-docs
Support for 1.4 GHz and 3.65 GHz bands on the WiMAX module	The WiMAX module supported on the CGR 1000 Series routers, now supports 1.4 GHz and 3.65 GHz bands in addition to 1.8 GHz and 2.3 GHz.	CG4(1)	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
Ability to disable the console port	A new command at the global configuration mode allows you to lock the console: line console {lock no lock} <ul style="list-style-type: none">The line console lock command stops all input and output of data on the console.The line console unlock command allows you to log in to the console and print log information. (CSCud89992,CSCue68818)	CG4(1)	
Encryption of passwords and certificates on the CGR 1000 SD flash module	In release CG4(1) and later, passwords and certificates will be encrypted on the SD flash module of the CGR 1240 and CGR 1120. (CSCue02872).	CG4(1)	See “About the SD Flash Memory Module” chapter in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> and the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> at: www.cisco.com/go/cgr1000-docs

Table 1 **New Features in Cisco CG-OS Release CG4 (continued)**

Feature	Description	First CG4 Release that Supports Feature	Related Documentation
Display IDPROM information for Battery Backup Units (BBUs). Note Available on CGR 1240 only.	You can view details on the BBU IDPROM for up to three BBUs in the following commands: <ul style="list-style-type: none"> • show hardware • show inv [power] • show sprom [power] (CSCuc04854)	CG4(1)	See “Installing Battery Backup Units” chapter in the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> and the <i>Cisco 1240 Connected Grid Router Hardware Installation Guide</i> at: www.cisco.com/go/cgr1000-docs
New Syslog message for Backhaul Manager feature	Any change associated with the scheduler timer of the Backhaul Manager causes the router to generate a Syslog message. (CSCuf95967)	CG4(1)	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

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 1.4 GHz, 1.8 GHz, 2.3 GHz and 3.65 GHz bands in Distribution Automation and AMI concentrator deployments	For feature overview and configuration details, see the <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 3.1 Required to view all supported WiMAX GHz bands, including 1.4 GHz and 3.65 GHz bands introduced in CG4(1)
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 12](#)
- [Upgrading to a New Software Release, page 12](#)
- [Erasing the Configuration File, page 16](#)

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 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 15](#).

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.CG4.0.195.SPA.bin for boot
variable "kickstart".
-- SUCCESS

Verifying image bootflash:///cgr1000-uk9.5.2.1.CG4.0.195.SPA.bin for boot variable
"system".
-- SUCCESS

Verifying image type.
-- SUCCESS

Extracting "system" version from image bootflash:///cgr1000-uk9.5.2.1.CG4.0.195.SPA.bin.
-- SUCCESS

Extracting "kickstart" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG4.0.195.SPA.bin.
-- SUCCESS

Extracting "bios" version from image bootflash:///cgr1000-uk9.5.2.1.CG4.0.195.SPA.bin.
-- SUCCESS

Extracting "loader" version from image
bootflash:///cgr1000-uk9-kickstart.5.2.1.CG4.0.195.SPA.bin.
-- SUCCESS

Performing module support checks.
2013 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)CG4(1)      yes
      1  kickstart          5.2(1)CG1(3c)      5.2(1)CG4(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 12.

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 21](#)
- [Resolved Caveats, page 30](#)
- [Accessing Bug Search Tool, page 36](#)

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.

- **CSCtu34138**

Symptom: When the CGR 1000 router is configured with a Generic Router Encapsulation (GRE) tunnel for IPv6, the tunnel receiving end indicates an invalid link-layer address (LA) when it receives a Route Advertisement.

Conditions: This issue occurs when a GRE tunnel on the router sends IPv6 data.

Workaround: There is no workaround for this issue.

- **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.

- **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.

- **CSCtw80920**

Symptom: The **show interface wimax interface scan** command does not display all scanning results. Details for base stations only appear for those stations on which the network entry procedure was performed.

Conditions: When associated to a base station the **show interface wimax interface scan** command also displays periodic scanning results.

Workaround: None.

- **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.

- **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.

- **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 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.

- **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.

- **CSCua33348**

Symptom: In certain conditions, the WiMAX supplicant might automatically switch from EAP-TTLS authentication to EAP-TLS authentication after receiving a few rejects from EAP-TTLS authentication. Additionally, the authentication method (Auth method) displays incorrectly in the **show interface wimax slot/port association** command.

Conditions: The user configured an incorrect mschapv2 password for EAP-TTLS authentication.

Workaround: The RADIUS server needs to be configured to accept only EAP-TTLS in this situation. This prevents the WIMAX supplicant from attempting to fall back to EAP-TLS and pass a successful EAP-TLS authentication, should its configured EAP-TTLS authentication method fail.

- **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.

- **CSCua39807**

Symptom: WiMAX uplink traffic might stop transmitting after 500 to 600 ICMP packets when you configure the QoS automatic repeat request (ARQ) parameter on the base station.

Conditions: QoS automatic repeat request (ARQ) parameter is configured on the base station.

Workaround: You must deregister the WiMAX module from the base station; and, then re-register the module with the base station to re-establish the data path.

- **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 10](#) 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_UNAVILABLE` 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.CG4.0.179.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.CG4.0.179.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.

- **CSCub14610**

Symptom: The logging level setting for wimaxpm does not display any information after configuring the **logging level wimaxpm <1 to 7>** command.

Conditions: Entering the **show logging level | grep wimax** command displays no results.

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: There is no workaround for this issue.

- **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: There is no workaround for this issue.

- **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.

- **CSCub82645**

Symptom: The following message displays in the syslog:

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

Conditions: This error message appears when the 3G module reloads.

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.

- **CSCuf82333**

Symptom: WiMAX modules with a product identification of CGM-WIMAX-3.6GHZ do not correctly display support for the frequency range of 3.3 to 3.8 GHz within its inventory data.

```
NAME: "Slot 5", DESCR: "Connected Grid Module - IEEE 802.16e WIMAX 3.5-3.8 GHz"
PID: CGM-WIMAX-3.6GHZ , VID: V00 , SN: JAF1601ALCK
```

Instead, the module only shows support for the frequency range of 3.5 to 3.8 GHz.

Conditions: WiMAX modules with a product identification of CGM-WIMAX-3.6GHZ do not correctly display support for the frequency range of 3.3 to 3.8 GHz within its inventory data.

Workaround: None.

- **CSCuh08498**

Symptom: The BBU Average Time to Full statistic might display a five-digit value instead of the usual three-digit value.

Conditions: Router has three BBUs installed; and, BBU0 and BBU2 are fully charged. BBU1 is in a charging state of 85% or greater.

Workaround: None. Five-digit value displays only temporarily. The correct value generally displays within five minutes.

Resolved Caveats

Caveats Resolved in Cisco CG-OS Release CG4(3)

- **CSCub75502**

Symptom: Under certain conditions, the system would generate one or more syslog messages about "serial8250: too much work for irq19 - kernel".

Conditions:

%KERN-3-SYSTEM_MSG: [508.896918] serial8250: too much work for irq19 - kernel

%KERN-3-SYSTEM_MSG: [508.900154] serial8250: too much work for irq19 - kernel

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCug32806**

Symptom: Any interface could fail to stop processing traffic due to memory (MBUF) leaks.

Conditions: When a CGR 1000 communicates with the CG-NMS server via callhome, it executes many **show** commands, compresses their output and sends them to CG-NMS as part of the payload of callhome periodic inventory notifications. These payloads can be very big and might exceed the interface MTU of intermediate routers, which in this case is the tunnel interface of the head-end router (Cisco ASR). This causes the ASR to send ICMPv6 unreachable messages to the CGR.

CGR attempts to allocate memory to these messages but then fails to release such memory after processing them. This will eventually cause CGR to lose all its MBUF and render all interfaces unable to route any traffic.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

For earlier CG4 releases, use the following workaround:

On the CGR1240: Configure the GRE tunnel with an MTU of 1280 bytes, and the IPSec tunnel with an MTU of 1304 bytes.

On the ASR side: Configure the tunnel with an MTU of 1304 bytes because IOS will automatically subtract 24 bytes for the GRE tunnel.

- **CSCui02983**

Symptom: The Device Manager (CG-DM) failed to connect to a CGR with a valid work order. This failure occurred after a previous attempt to access the same CGR failed because of an invalid work order.

Conditions: Device Manager was operating in NMS mode with the user role of Tech.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCui43638**

Symptom: An FPGA upgrade failure could occur during an **install all** upgrade and cause the **install all** upgrade to fail.

Conditions: The current FPGA upgrade procedure in CG1(3d), CG3(3) and CG4(2) relies on an average timeout value plus some additional buffer time. It needs to be updated to take the WIP bit into account during FPGA sector erase operations. This will help eliminate the potential variability of the FPGA sector erase timeout.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCui94707**

Symptom: CG-NMS needed to collect the history of CGR system reset reasons.

Conditions: Format of the **show logging onboard reset-reason** command was not in XML format and CG-NMS could not interpret the data.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCuj21105**

Symptom: CGR might keep reloading due to Platform Manager crashes.

Conditions: The router was showing 0 BBU and could not roll back to the ps-start-config because the Platform Manager crashed during the rollback.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCuj78400**

Symptom: An invalid cell ID was shown in the output of **show cellular x/y network** and **show cellular x/y all**.

Conditions: An invalid cell ID was shown because the first 16 bits returned by the CnS API were not cleared as zero. The last 16 bits are the cell ID number.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCul91346**

Symptom: TTY line crashed.

Conditions: When data to send was accumulated on TCP socket, the send() would get stuck which caused the process to be killed.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

In previous releases, be sure to make sure there is no data jam, when you configure raw socket back-to-back.

- **CSCul96185**

Symptom: Netstack would stop processing interface traffic if static MTU settings were not properly applied for GRE / IPSec tunnels on both CGR1000 and the peer ASR.

Conditions: If the GRE and IPSec tunnel interfaces on the CGR were configured either with or without static MTU configurations, while the peer ASR's GRE and IPSec tunnels' MTU settings were not statically set to match those on the corresponding CGR's GRE and IPSec tunnel interfaces, MBUF leak would occur and cause Netstack to stop processing interface traffic.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

In previous releases, apply the matching static MTU configurations on both GRE and IPSec tunnels on the CGR as well as the peer ASR.

- **CSCum03905**

Symptom: Certificates were deleted from the SD card on the CGR.

Conditions: Unknown.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

In previous releases, there was no workaround.

- **CSCum19297**

Symptom: PON message was not sent to CG-NMS.

Conditions: After receiving a PON message, there was a delay in resolving the hostname. This delay caused the PON message not to be sent to CG-NMS. When the static hostname to IPv6 mapping was present, this issue was not seen.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

- **CSCum23547**

Symptom: In the Itron meter farm, many CSMP packets with source address 0 are received.

Conditions: Unknown.

Workaround: This issue is resolved in Cisco CG-OS CG4(3).

In previous releases, use **ipv6 access list** to drop CSMP packets with source address 0 under the wpan interface, as shown in the following example:

```
IPv6 access list WPAN_BLOCK_0
    statistics per-entry
    10 deny ipv6 [ipv6 address with source address 0] any [match=0]
    20 permit ipv6 any any [match=0]

interface Wpan4/1
    dot1x pae authenticator
    ipv6 traffic-filter WPAN_BLOCK_0 in
    no shutdown
    rpl dag lifetime 240
    panid 1006
    ssid soltest_50
    txpower 2
    outage server [outage server ipv6 address]
    ieee154_beacon_async 10 10 0
    ipv6 address [wpan ipv6 address with subnet mask]
    ipv6 dhcp relay client-interface
```

- **CSCum37793**

Symptom: Callhome code uses the ISO 8601 standard when reporting year. Sometimes the year reported is not the same as the calendar year.

Conditions: ISO 8601 calculates the year based on the first Monday of January rather than using the calendar year. Thus, Dec 30 2013 is considered in ISO 8601 year 2014 because it is the first Monday of January 2014.

Workaround: This issue is resolved in Cisco CG-OS CG4(3). Callhome now always displays the calendar year.

In previous versions, Callhome displays the ISO 8610 year.

Caveats Resolved in Cisco CG-OS Release CG4(2)

- **CSCtv24634**

Symptom: Certain fields in the **show cellular** command output did not populate with data.

Conditions: Always.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCty86005**

Symptom: When attempting to register a CGR with CG-NMS, the following error appeared in the CG-NMS logs:

```
javax.net.ssl.SSLException: Received fatal alert: unknown_ca
```


Conditions: This error occurred due to one of the following:

- There were multiple trustpoints configured on the CGR and the certificates for each trustpoint were multi-layered, meaning that there was a hierarchy in the certificate chain (sub-ca --> root-ca).
- The two trustpoints were pointing to the same CA; and, the CA was in a hierarchy of CAs.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCty98998**

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

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

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCtz32469**

Symptom: You were unable to log into the router immediately after a reload.

Conditions: This issue occurred when you tried to log into the router from the command prompt right after you had reloaded the router configuration; the login attempt was unsuccessful.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCue76914**

Symptom: A cellpm memory leak could occur over an extended period of time on the 3G Module.

Conditions: The 3G module was connected to a live network.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCug28208**

Symptom: When there are two or more NTP server hostnames configured on the CGR, and the hostnames are not resolved by the configured name-server, then the CGR saves the first hostname and drops all others from the running config.

Conditions: The DNS failed to resolve NTP server hostnames due to a connectivity issue or some other reason.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCug40927**

Symptom: NTP server minimum and maximum poll timers could not be changed on CGR.

Conditions: When the NTP server minimum and maximum poll timer commands were configured, the timers could not be changed by reentering the command with different timer values without removing the NTP server configuration from the CGR configuration and then reentering the NTP server configuration with the revised values.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCug87639**

Symptom: CGR might continue to reboot after an NMS-initiated upgrade if the router loses AC power and runs on BBU power during its first reload after an upgrade.

Conditions: Problem occurs when the Configuration Template for a device group includes the **backup-battery un-inhibit discharge** command; and, an CG-NMS registered CGR (FAR) loses power any time during the first reload and boot after an upgrade by NMS. The CGR will roll-back to the golden-config and fail to complete a registration to NMS. CGR continues to undergo a cycle of repeated NMS-initiated reloads every 10 minutes until AC power is restored to the router.

Workaround: Remove the **backup-battery un-inhibit discharge** command from the Configuration Template for the device group in CG-NMS.

- **CSCuh04372**

Symptom: The tacacs process could exhibit some gradual memory leaks when processing command accounting and authorization; and, login authentication.

Conditions: User privileged EXEC command and global configuration command authorizations were enabled for TACACS+; and, CG-DM was initiating commands for **callhome periodic-inventory** notifications and **callhome periodic-configuration heartbeat** notifications.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCuh04897**

Symptom: Registration of the CGR failed when either CG-NMS was creating the golden-config file or when CG-NMS sent the device config followed by the copy r s command.

Conditions: CGR was trying to register with the CG-NMS.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCuh18355**

Symptom: When the trustpoint for a CGR contained both a subordinate certificate authority (subCA) and a root CA, the Connected Grid Device Manager (CG-DM) was unable to connect to the CGR when using a work order issued by the CG-NMS.

Conditions: CG-DM was unable to connect to CGR and displayed the following error: AuthorizationManager: The host name did not match any of the valid hosts for this certificate.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCuh36230**

Symptom: A CGR software upgrade from CG1(3d) to CG4(1) caused duplicate registration requests to be sent to CG-NMS, within the same second.

Conditions: CGR was being upgraded from CG1(3d) to CG4(1).

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

- **CSCuh45413**

Symptom: When a NMS-registered FAR (CGR) was rolled back to express-config or golden-config, the WIFI wpa | wpa2 | wpa-mixed passphrase could be missing in the running-config.

Conditions: If type-6 encryption and password strength-check were enabled, and the WIFI wpa | wpa2 | wpa-mixed pre-shared key was configured in an NMS-registered FAR, then reloading or upgrading it to CG3(3) or CG4(1) could cause its WIFI pre-shared key to be missing in the running-config. It was the config rollback (to express-config or golden-config) during the reload or upgrade operations that caused this problem.

Workaround: This issue is resolved in Cisco CG-OS CG4(2).

For earlier releases, disable password strength check. You might need to modify the express-config or golden-config file by hand.

Upgrade to CG4(2).

Caveats Resolved in Cisco CG-OS Release CG4(1)

- **CSCtu25387**

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

Conditions: An AAA TACACS+ server host configured, 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: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCtx75113**

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

Conditions: Poor signal strength or deactivated modem.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCty99047**

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

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

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCtz54240**

Symptom: Syslog messages associated with the DHCP server (dhcpd) reported in error for the router. The router does not support the DHCP server function. See related caveat, CSCua74908.

Conditions: Unexpected syslog messages and errors associated with dhcpd reported.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCua39841**

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

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

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCua74908**

Symptom: Syslog messages associated with the DHCP server (dhcpd) were reported in error for the router. The router does not support the dhcp server function. See related caveat, CSCtz54240.

Conditions: A non-supported process, dhcpd, was sending syslog messages.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **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) and CG4(1).

- **CSCud94169**

Symptom: Holding down the Ctrl-C key, while booting the router, formatted the flash. Afterward, the system displayed the loader prompt and the bootflash was empty. This occurred intermittently.

Conditions: Ctrl-C was held down while booting the router.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCue06692**

Symptom: The wifipm process for the WiFi interface crashed when modifying the channel frequency and power values on the interface.

Conditions: A script was used to update the frequency and power for the WiFi interface. A manual update of the values was also performed.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCue09971**

Symptom: Restoration table on the CGR 1000 router did not clear entries as expected.

Conditions: Restoration table on the CGR 1000 router did not clear entries as expected.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

- **CSCue12562**

Symptom: Power restoration notices (PRNs) from the CGR 1000 were not forwarded to CG-NMS.

Conditions: Power restoration notices (PRNs) from the CGR 1000 were not forwarded to CG-NMS.

Workaround: This issue is resolved in Cisco CG-OS CG4(1).

Accessing Bug Search Tool

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

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

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

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

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

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

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

Accessing Error Message Decoder

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

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

Documentation Updates

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 CG4 include details on releases CG4(1), CG4(2) and CG4(3). Previously, we had separate Release Notes for each of 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.

© 2013–2014 Cisco Systems, Inc. All rights reserved.