Release Notes for CG-Mesh Release 5.7.27

First Published: 2017-12-20

Content

These release notes contain the latest information about using CG-Mesh software with IPv6 connected grid endpoints (CGEs) such as meters.

CG-Mesh is an embedded network stack for Smart Grid assets within a Neighborhood Area Network. CG-Mesh provides end-to-end IPv6 communication and implements open-standard protocols at every layer in the network stack, including but not limited to IEEE 802.15.4e/g, 6LoWPAN, IPv6, RPL, UDP, and CoAP. In Smart Grid assets such as residential electric meters, the CG-Mesh software functions within a dedicated Communications Module that connects to an Application Module through a PPP link.

Note For a detailed description of the CG-Mesh software in Release 5.7.x, refer to *Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide: www.cisco.com/go/cgr1000-docs.*

Cisco Systems, Inc.
www.cisco.com

New Features for This Release

Table 1 lists the enhancements specific to this release.

Table 1 Enhancements for CG-Mesh Release 5.7.x

Platform	Enhancement	Description	First Cisco IOS Release that Supports the Feature
CGM WPAN	Dual-Phy support	Support for RF/PLC dual phy mode.	15.7(3)M1
EV8600	Platform enabled	Enable RF-Only CG-Mesh to run on EV8600.	
EV8610	Platform enabled	Enable RF&PLC Dual-PHY CG-Mesh to run on EV8610.	

System Requirements

If you plan to run CG-Mesh 5.7.x Release, you must have the following required hardware and software components:

Platform	Minimum Cisco Software Release Required
Cisco 1000 Series Connected Grid Router	Cisco IOS Release 15.7(3)M1
WPAN module: CGM-WPAN-FSK-NA (LIC-CGR1K-WPAN-ip)	cg-mesh-bridge-ITRDPKG-5.7.27-604ab01-itron30.bin

Supported Software Features

This section covers the following software features:

- Compromised Node Eviction, page 3
- RPL, page 3
- 6LoWPAN, page 3
- Frequency Hopping, page 3
- Firmware Upgrade Procedure, page 3
- FND Configuration, page 3
- CoAP Simple Management Protocol, page 4
- Power-outage Notification, page 4
- Registration of Endpoint, page 4

Compromised Node Eviction

A compromised node is one where the device can no longer be trusted by the network and/or operators. Nodes within an IEEE 802.15.4 PAN must possess the currently valid Group Temporal Key (GTK) to send and receive link-layer messages. The GTK is shared among all devices within the PAN and is refreshed periodically or on-demand. By communicating new GTKs to only trusted devices, compromised nodes may be evicted from the network.

RPL

In its route-over architecture, CG-Mesh performs routing at the network layer using the Routing Protocol for Low-Power and Lossy Networks (RPL).

CG-Mesh requires a Cisco 1000 Series Connected Grid Router (CGR) to provide connectivity to other IPv6 networks. The CGR (Field Area Router (FAR)) must serve as a RPL Directed Acyclic Graph (DAG) root and store information reported in DAO messages to forward datagrams to individual nodes within the mesh network.

6LoWPAN

The 6LoWPAN adaptation layer adapts IPv6 to operate efficiently over low-power and lossy links such as IEEE 802.15.4. The adaptation layer sits between the IPv6 and IEEE 802.15.4 layers and provides IPv6 header compression, IPv6 datagram fragmentation, and optimized IPv6 Neighbor Discovery.

Frequency Hopping

CG-Mesh implements frequency hopping across channels with 400/800-kHz spacing in the 902 to 928 MHz ISM band. The frequency-hopping protocol used by CG-Mesh maximizes the use of the available spectrum by allowing multiple sender-receiver pairs to communicate simultaneously on different channels. The frequency hopping protocol also mitigates the negative effects of narrowband interferers.

Firmware Upgrade Procedure

The CG-Mesh Bridge firmware can be installed by CLI or from Cisco IoT Field Network Director (FND).

For more information on upgrading the firmware, see the Release Notes for Cisco 1000 Series Connected Grid Routers for Cisco IOS Release 15.7(3)M1 at: www.cisco.com/go/cgr1000-docs.

FND Configuration

CG-Mesh solution is managed and monitored by the IoT FND, which provides the necessary backend network configuration, monitoring, event notification services, network stack firmware upgrade, as well as FND outage and meter registration. IoT FND also retrieves statistics on network traffic from the interface.

For more information on using IoT FND, refer to the *Cisco IoT Field Network Director User Guide, Release 4.0.x*.

Note For a detailed description on the CG-Mesh CLI, refer to Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS).

CoAP Simple Management Protocol

CG-Mesh implements the CoAP Simple Management Protocol (CSMP) for remote configuration, monitoring, and event generation over the IPv6 network. The CSMP service is exposed over both the mesh and serial interfaces.

Power-outage Notification

CG-Mesh supports timely and efficient reporting of power outages and restorations.

In the event of a power outage, CG-Mesh enters power-outage notification mode and the node stops listening for traffic to conserve energy. CG-Mesh triggers functions to conserve energy by notifying the communication module and neighboring nodes of the outage. The outage notification is sent using the same security settings as any other UDP/IPv6 datagram transmission.

In the event of a power restoration, a CG-Mesh node sends a restoration notification using the same communication method as the outage notification. The communication modules unaffected by the power outage event deliver the restoration notification.

Registration of Endpoint

You can register and manage CG-Mesh Endpoints (CGEs) such as (meters) using the CSMP protocol.

Limitations and Restrictions

Cisco recommends that you review this section before you begin working with the module. 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.

- **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 and Resolved caveats that are relevant to CG-mesh.

This section also provides information on how to use the Bug Tool Kit to find further details on the caveats, and includes the following topics:

- Open Caveats, page 5
- Resolved Caveats, page 5
- Accessing Bug Search Tool, page 5
- Accessing Error Message Decoder, page 6

Open Caveats

This section summarizes open caveats specific to the CG-mesh.

- CSCvg13367

  Node could not display more than 13 PLC hardware link neighbors in TLV95.
- CSCvg87873

  1/1000 Duplicated Packets on PLC media when node have only one parent.
- CSCvh03696

  Node probably fails to sync with bcast schedule in master-slave mode.

Resolved Caveats

This section summarizes resolved caveats specific to the CG-mesh.

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

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

Feature History

Feature	Cisco IOS Release	Feature information
CG-mesh WPAN Module firmware 5.7.27	15.7(3)M1	CG-mesh enhancement.

Related Documentation

Consult the following resources for related information about the Connected Grid WPAN Module for technical assistance.

Hardware Overview and Installation

- Cisco CG-OS Release Notes for CGR 1000

  http://www.cisco.com/go/cgr1000-docs
- Cisco Connected Grid Module Guides
  http://www.cisco.com/go/cgmodules
- *Cisco CGR 1240 Hardware Installation Guide*

  http://www.cisco.com/go/cgr1000-docs
- *Cisco CGR 1120 Hardware Installation Guide*

  http://www.cisco.com/go/cgr1000-docs
- Cisco IR500 Series WPAN Gateway and WPAN Range Extender

  https://www.cisco.com/c/en/us/support/routers/500-series-wpan-industrial-routers/tsd-products-support-series-home.html

Supported Cisco Antennas and Accessories

Cisco CGR 1000 and 2000 Series Connected Grid Antennas Guides
http://www.cisco.com/en/US/docs/routers/connectedgrid/antennas/installing/cg_antenna_install_guide.html

Regulatory, Compliance, and Safety Information

Cisco Network Modules and Interface Cards Regulatory Compliance and Safety Information

http://www.cisco.com/en/US/docs/routers/access/interfaces/rcsi/IOHrcsi.html

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

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.