Release Notes for Cisco Resilient Mesh Release 5.6.42

First Published: 2020-11-25

Release Notes for Cisco Resilient Mesh Release 5.6.42

These release notes contain the latest information about using Cisco Resilient Mesh (CR-Mesh, formerly known as CG-Mesh) software with IPv6 Resilient Mesh Endpoints (RMEs) such as meters, and the IR529 WPAN Range Extender.

Cisco Resilient Mesh is an embedded network stack for Smart Grid assets within a Neighborhood Area Network. Cisco Resilient 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 Cisco Resilient Mesh software functions within a dedicated Communications Module that connects to an Application Module through a PPP link.

New Features for This Release

The following table lists the enhancements specific to this release.

- Firmware update enhancement for Itron30 and CGRREF2—Provides the ability to upgrade CR-mesh (Release 5.6.21) network to Wi-SUN (Release 6.3) network.
- Support EST on Itron30 platform to support re-enrollment of LDevID certificate and FND certificate.
- Support to push a channel notching configuration for deployed Itron meters.

System Requirements

If you plan to run Cisco Resilient Mesh Release 5.6.42, you must have the following required hardware and software components:

Platform	Minimum Cisco IOS Software Release Required
Cisco 1000 Series Connected Grid Router	Cisco IOS Release 15.8(3)M5
Cisco IR529	cg-mesh-node-5.6.42-5c0ea42-RELEASE-ir529.bin
WPAN module (CGM-WPAN-FSK-NA)	cg-mesh-bridge-ITRDPKG-5.6.42-5c0ea42-itron30.bin
IoT Field Network Director	Release 4.7

Supported Software Features

This section covers the supported software features.

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, Cisco Resilient Mesh performs routing at the network layer using the Routing Protocol for Low-Power and Lossy Networks (RPL).

Cisco Resilient 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

Cisco Resilient Mesh implements frequency hopping across 64 channels with 400-kHz spacing in the 902 to 928 MHz ISM band. The frequency-hopping protocol used by Cisco Resilient 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 Cisco Resilient Mesh bridge firmware can be installed by CLI or from IoT FND.

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

FND Configuration

Cisco Resilient Mesh solution is managed and monitored by the Cisco IoT Field Network Director (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 latest version of Cisco IoT Field Network Director User Guide at:

https://www.cisco.com/c/en/us/support/cloud-systems-management/iot-field-network-director/products-installation-and-configuration-guides-list.html

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

CoAP Simple Management Protocol

Cisco Resilient 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

Cisco Resilient Mesh supports timely and efficient reporting of power outages and restorations.

In the event of a power outage, Cisco Resilient Mesh enters power-outage notification mode and the node stops listening for traffic to conserve energy. Cisco Resilient 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 Cisco Resilient 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 Cisco Resilient Mesh Endpoints (RMEs) 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 Cisco Resilient Mesh. This section also provides information on how to use the Bug Tool Kit to find further details on the caveats.

Open Caveats

This section summarizes open caveats to the Cisco Resilient Mesh.

- **CSCvu87032**

  Symptom: Itron30 does not report its certificates info to FND after ldevid/CAs reenrollment or during register. so admin cannot view the Itron30's certificates information on FND GUI.

  Conditions: When Itron30 is registered to FND, it will not send its certificates info to FND. When Itron30 completes to reenroll CAs/LDevid, it will not send the updated certificates info to FND.

  Workaround: Using CSMP tool on FND to get the certificates info by TLV172.

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
Cisco Resilient Mesh firmware 5.6.42	Cisco IOS Release 15.8(3)M5	Cisco Resilient 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/cg-modules

- 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

Supported Cisco Antennas and Accessories

Cisco CGR 1000 and 2000 Series Connected Grid Antennas Guides

https://www.cisco.com/c/en/us/td/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