

Release Notes for Cisco Resilient Mesh Release 6.2

First Published: 2020-02-21

Release Notes for Cisco Resilient Mesh Release 6.2

These release notes contain the latest information about using Cisco Resilient Mesh (formerly known as CG-Mesh) with IPv6 Resilient Mesh Endpoints (RMEs) such as meters and the Cisco IR500 Series WPAN Gateway Range Extenders.

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.



Note For a detailed description of the Cisco Resilient Mesh software in Release 6.2, refer to [Cisco Connected Grid WPAN Module for CGR 1000 Series Installation](#) and [Cisco Resilient Mesh Configuration Guide](#).

New Features for This Release

The following table lists the enhancements specific to this release.



Note It's only supported that you upgrade to Cisco Resilient Mesh Release 6.2 from Release 5.6.21 or later.

Table 1: Enhancements for Cisco Resilient Mesh Release 6.2

Platform	Enhancement	Description	First Cisco IOS Release that Supports the Feature
IR510, IR530, WPAN-OFDM	Wi-SUN 1.x Adaptive Modulation	Support OFDM Option 3 (Mandatory) and Option 2 (Needed), and FSK. Peers to negotiate operating rates based on the available rate set configured on both. Cisco CGR1240 and IR510 to interop with L&G 2450*, R650 and N550IoT FND to manage the AM feature for both Cisco CGR1240/IR510 and L&G Series 5 devices.	15.9(3)M1
IR510, IR530, WPAN-OFDM	Wi-SUN 1.x Power outage and restoration	Update PON/PRN notification to use CSMP (Layer 2 to CSMP messages). Nodes are able to exchange power capability in addition to the routing metrics.	15.9(3)M1
CGEREF2/CGEREF2PLUS CGEREF3/CGERFPLCREF3	Group multicasting	Group multicasting (Streetlighting, demand & response)	15.9(3)M1
IR510, IR530, WPAN-OFDM	Mesh backward compatibility	Mesh backward compatibility: (Release 6.2, 5.6.21, and 5.2.82)	15.9(3)M1
IR510, IR530, WPAN-OFDM	Wi-SUN 1.x Customer Deployable features	Support the existing CG-Mesh features to make it field deployable: <ul style="list-style-type: none"> • Time distribution • QoS • Fast reformation • PAN Migration 	15.9(3)M1
CGEREF2	Wi-SUN 1.0 SDK that fits CGEREF2 design	Wi-SUN 1.0 feature set available in the SDK	15.9(3)M1
IR510, IR530, WPAN-OFDM	Achieve 2.4 Mbps data rate	Support OFDM Option 1 (2.4 Mbps) data rate	15.9(3)M1

Platform	Enhancement	Description	First Cisco IOS Release that Supports the Feature
IR510, IR530	CSDL Compliance - FTT Authorization Procedure	CG-Mesh implements FTT key enablement in Release 6.2 for IoT-DM CSDL compliance.	15.9(3)M1
All platforms	CG-mesh image size optimization	Optimize the mesh image size and offer more resources to the customer	15.9(3)M1
CGEREF2/CGEREF2PLUS CGEREF3/CGERFPLCREF3	Third-party Firmware Upgrade	OTA of third-party app to second MCU using FND (SDK user) – Multicast the file to third party end points.	15.9(3)M1
IR510, IR530	EST enhancement	Support auto-enrollment for a node to request a new certificate before its own certificate (Manufacturer IDevID) expires.	15.9(3)M1

System Requirements

If you plan to run Cisco Resilient Mesh Release 6.2, you must have the following required hardware and software components:

Platform	Minimum Cisco IOS/CG-OS Software Release Required
Cisco 1000 Series Connected Grid Router	Cisco IOS Release 15.9(3)M1
Cisco IR530	cg-mesh-node-6.2-6219-ir530-1bf449d.bin
Cisco IR529	cg-mesh-node-6.2-6219-ir529-1bf449d.bin
Cisco IR510	cg-mesh-dagw-6.2-6219-ir510-1bf449d.bin
Cisco IR509	cg-mesh-dagw-6.2-6219-ir509-1bf449d.bin
WPAN module (CGM-WPAN-FSK-NA)	cg-mesh-bridge-ITRDPKG-6.2-6219-iron30-1bf449d.bin
OFDM WPAN (CGM-WPAN-OFDM-FCC)	cg-mesh-bridge-6.2-6219-ir510-1bf449d.bin
IoT Field Network Director	Release 4.6
IOx	1.10

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.



Note For IR510 and IR530 endpoints, high data rates 1.2Mbps with 31 channels are also supported.

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.



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 \(Cisco IOS\)](#).



Note IR510 and IR530 will be supported only with FND Release 4.1 or greater. Refer to the [Cisco IoT Field Network Director User Guides](#) for details.

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.

- **CSCvs69721**

Symptom: IR530 will hang if downgrading from 6.2 to 6.0.19 with unsupported phy modes configured.

Conditions: This issue occurs when IR530 configured with phy mode 1 or 2 is downgraded from 6.2 to 6.0.19 (phy modes 1 and 2 are supported in 6.2 but not supported in 6.0.19).

Workaround: The workaround is (1) creating a configuration file with supported phy modes in 6.0, or (2) changing phy mode to a supported phy mode in 6.0 before downgrade.

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.

- **CSCvn79551**

Symptom: No EAP response after sending the first EAP fragment to IR529 or CGEREFx.

Conditions: 1) Set the EAP fragment size to 1024 bytes on radius server. 2) Cert file of the server is larger than 1024 bytes. 3) Trigger mesh node to do authentication. After radius server sent the first EAP fragment to mesh node, mesh node didn't reply any information, thus the authentication failed to continue.

Workaround: Modify the max EAP fragment size to 512 bytes on radius server.

- **CSCvn79799**

Symptom: Node can't get online after downgraded from 6.x to 6.0.19 when mesh mixed with 6.0 and 6.x.

Conditions: The WPAN image is not downgraded.

Workaround: Downgrade the WPAN image and all other nodes to 6.0.19 as well.

- **CSCvo80623**

Symptom: When IR509 is upgraded from 5.6 to 6.x, the MAPTStatus, ETHconfig, and NAT44StaticMap configuration will be lost.

Conditions: This issue occurs when IR509 is upgraded from 5.6 to 6.x.

Workaround: Reconfigure MAPTStatus, ETHconfig, and NAT44StaticMap.

- **CSCvs56568**

Symptom: 6.2 bridge can not work with Wi-SUN 6.1 if enable PON RPL.

Conditions: This issue occurs when WPAN image is 6.2, and RPL PON instance is set on CGR.

Workaround: Disable RPL PON instance on CGR, or upgrade all ir5xx to 6.2 image.

- **CSCvs57388**

Symptom: Wi-SUN: Node cannot register to fnd when node and wpan version mismatch.

Conditions: This issue occurs when node is in release 6.1 and CGR WPAN is in release 6.2. Same problem exists when node is in release 6.2 and WPAN is in release 6.1.

Workaround: Use the same release image on node and CGR WPAN. When upgrade from 6.1 to 6.2 using FND, upgrade the node first and then upgrade WPAN.

- **CSCvs57488**

Symptom: After image upgrade to 6.2.16 or later, IR510 EUI may be changed. Node may get a new global ipv6 address. The old EUI/address in CGR RPL table and FND will not work anymore.

Conditions: This issue occurs when upgrade image from 6.x (for example, 6.0.x or 6.1.x) to 6.2.16 or later. Some IR510 EUI may be changed, but not all of them have this issue.

Workaround: Import the new EUI to the FND and remove the old EUI. Wait for the old address timeout on the CGR RPL table.

Resolved Caveats

This section summarizes resolved caveats to the Cisco Resilient Mesh.

- **CSCvg11696**

IR510: IPv6 Ethernet address is shown as lowpan address.

- **CSCvo81976**

AM/AR prefers higher rate in high_rssi_high_loss scenario induced by noise leading to continuous loss.

- **CSCvp88638**

IR510: GPS status retrieve periodically failed after reload.

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 6.2	Cisco IOS Release 15.9(3)M1	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

- IR510 WPAN Gateway and IR530 WPAN Range Extender Hardware Installation Guide
https://www.cisco.com/c/en/us/td/docs/routers/ir510-ir530/hig/ir5X0_wpan_HIG.html
- Cisco 1000 Series Connected Grid Routers Release Notes
<https://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/products-release-notes-list.html>
- Cisco Connected Grid Module Guides
<http://www.cisco.com/go/cg-modules>
- Cisco CGR 1240 Hardware Installation Guide
<https://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/products-installation-guides-list.html>
- Cisco CGR 1120 Hardware Installation Guide
<https://www.cisco.com/c/en/us/support/routers/1000-series-connected-grid-routers/products-installation-guides-list.html>

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>

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.