



Release Notes for Cisco Resilient Mesh, Release 6.2.47

Cisco Resilient Mesh, Release 6.2.47	3
New software features	3
Resolved issues	3
Open issues	4
Known issues	4
Supported hardware and software	4
Related resources	6
Legal information	7

Cisco Resilient Mesh, Release 6.2.47

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

CR-Mesh is an embedded network stack for Smart Grid assets within a Neighborhood Area Network. CR-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 utility meters, the CR-Mesh software functions within a dedicated Communications Module that connects to an Application Module through a secure PPP link.

Table 1. Updates to Release notes

Date	Description
12/19/2025	CR-Mesh Release 6.2.47

New software features

This section provides a brief description of the new software features introduced in this release.

Table 2. New software features for CR-Mesh Release 6.2.47

Product Impact	Feature	Description
Performance	Optimize Itron CE Meter readrate	Improves Itron Collection Engine(CE) meter readrate performance, For more information refer, CSCwj01674
Ease of use	Set Wi-SUN as default stack mode	Itron meter boots by default in Wi-SUN stack mode when stack mode is not explicitly configured in boot config.bin. For more information see, CSCws36096

Resolved issues

This table lists the resolved issues in this specific software release.

Note: This software release may contain bug fixes first introduced in other releases. To see additional information, click the bug ID to access the [Cisco Bug Search Tool](#).

Table 3. Resolved issues for CR-Mesh Release 6.2.47

Bug ID	Description
CSCwj01674	Improves Itron Collection Engine(CE) meter readrate performance,
CSCws36096	Itron meter boots by default in Wi-SUN stack mode when stack mode is not

Bug ID	Description
	explicitly configured in boot config.bin.

Open issues

There are no open issues in CR-Mesh Release 6.2.47

Known issues

This table lists the limitations for this release. Click the bug ID to access the [Cisco Bug Search Tool](#) and see additional information

Table 4. Known issues for CR-Mesh

Bug ID	Description
CSCvz38077	Symptom: Fail to refresh pub key via EST when OFDM WPAN and Itron node are working in PHY mode 2. Conditions: This issue occurs when: CG-mesh stack mode with phymode 2 OFDM WPAN in Release 6.2 + Itron node in Release 5.6 or 6.2 802.1x certificate length is too long (more than 700 bytes) Workaround: Use certificate less than 700 bytes.
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.

Supported hardware and software

This section lists the hardware and software support information for CR-Mesh

Table 5. Supported hardware for CR-Mesh Release 6.2.47

Product	Supported release
Cisco 1000 Series Connected Grid Router	Cisco IOS Release 15.9(3)M4 or later
Cisco Catalyst IR8100 Heavy Duty Series Routers	Cisco IOS-XE Release 17.6.1a or later
Cisco IR530	cg-mesh-node-6.2MR-6247-RELEASE-ir530-55443e5.bin

Product	Supported release
Cisco IR510	cg-mesh-dagw-6.2MR-6247-RELEASE-ir510-55443e5.bin
WPAN FSK module	cg-mesh-bridge-ITRDPKG-6.2MR-6247-iron30-55443e5.bin
WPAN OFDM module	cg-mesh-bridge-6.2MR-6247-ir510-55443e5.bin
Cisco IoT FND	Cisco IoT FND Release 4.9.0 or later
IOx	1.6.1.3

Table 6. Supported software features for CR-Mesh

Software features	Description
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, and 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) or Cisco Catalyst IR8140 Heavy Duty Router (IR8140H) to provide connectivity to other IPv6 networks. The CGR or IR8140H (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	CR-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. For IR510 and IR530 endpoints, high data rates 1.2Mbps with 31 channels are also supported.

Software features	Description
CoAP Simple Management Protocol	CR-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. For backward compatibility on Itron RMEs 30 (meters), CSMP service is exposed via both CoAP RFC port (UDP 61628) and Draft port (UDP 61624). But communication with Cisco IoT FND will continue to be on RFC port for all the RMEs.
Power outage notification	<p>CR-Mesh supports timely and efficient reporting of power outages and restorations.</p> <p>In the event of a power outage, CR-Mesh enters power-outage notification mode and the node stops listening for traffic to conserve energy. CR-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.</p> <p>In the event of a power restoration, a CR-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.</p>
Registration of Endpoints	You can register and manage Cisco Resilient Mesh Endpoints (RMEs) such as meters using the IoT FND (which uses the CSMP protocol).

Related resources

Firmware and configuration

- Cisco IoT FND Configuration: CR-Mesh solution is managed and monitored by the Cisco IoT FND, which provides the necessary backend network configuration, monitoring, event notification services, network stack firmware upgrade, as well as FND outage, meter registration, and periodic metrics features. Cisco IoT FND also retrieves statistics on network traffic from the interface.
- For a detailed description on the Cisco Resilient Mesh IOS CLI, refer to [Cisco Connected Grid WPAN Module for CGR 1000 Series Installation and Cisco Resilient Mesh Configuration Guide \(Cisco IOS\)](#).
- For more information on the IR8140H router configuration, refer to [Cisco Catalyst IR8140 Heavy Duty Series Router Software Configuration Guide](#).
- 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
- Firmware upgrade procedure: The CR-Mesh bridge firmware can be installed by CLI or from Cisco 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, or see the *Installing the Software* chapter of [Cisco Catalyst IR8140 Heavy Duty Series Router Software Configuration Guide](#).

Hardware overview and installation

- Cisco Catalyst IR8140 Heavy Duty Router Installation Guide
<https://www.cisco.com/c/en/us/td/docs/routers/ir8140/hig/b-ir8140h-hig.html>
- 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
- Selecting and Installing Antennas on IR8140H
<https://www.cisco.com/c/en/us/td/docs/routers/ir8140/hig/b-ir8140h-hig/m-antenna-select.html>

Legal information

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)

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.

© 2025 Cisco Systems, Inc. All rights reserved.