Cisco 1000 Series Connected Grid Routers

The Cisco® 1000 Series Connected Grid Routers (CGR 1000 Series) are versatile communications platforms built to meet the communication infrastructure needs of industrial verticals such as utilities, energy, and smart cities. These routers allow utilities to integrate multiple applications, such as Advanced Metering Infrastructure (AMI), Distribution Automation (DA), integration of Distributed Energy Resources (DER), and remote workforce automation onto a single platform. The CGR 1000 Series supports outdoor wired and wireless sensor networks, enabling applications such as street lighting, smart parking, and other smart city applications.

Product Overview

The CGR 1000 Series Routers are ruggedized, modular platforms on which utilities and other industrial customers can build a highly secure, reliable, and scalable communication infrastructure. The products are certified to meet harsh environmental standards. They support a variety of communications interfaces, such as Ethernet, serial, cellular, Radio-Frequency (RF) mesh, and Power Line Communications (PLC).

The Cisco CGR 1000 Series run Cisco IOS® Software, the operating system powering millions of Cisco routers worldwide. Grid operators gain the benefits of Cisco IOS Software's wide variety of Layer 3 services such as FlexVPN. The distributed intelligence capabilities of the CGR 1000 Series allow customers to run 3rd party applications such as application protocol translation, distributed data processing and filtering, and application security on the routers directly leveraging Cisco IOx - an open, extensible environment for hosting applications at the network edge.

The Cisco CGR 1000 Series includes two platforms, shown in Figure 1: The Cisco 1120 Connected Grid Router (CGR 1120), which is designed for indoor deployments; and the Cisco 1240 Connected Grid Router (CGR 1240), which is a weatherproof router in a NEMA Type 4 enclosure for outdoor deployments.

Figure 1. Cisco 1000 Series Connected Grid Routers

Connected Grid Field Area Network Solution and CGR 1000 Series

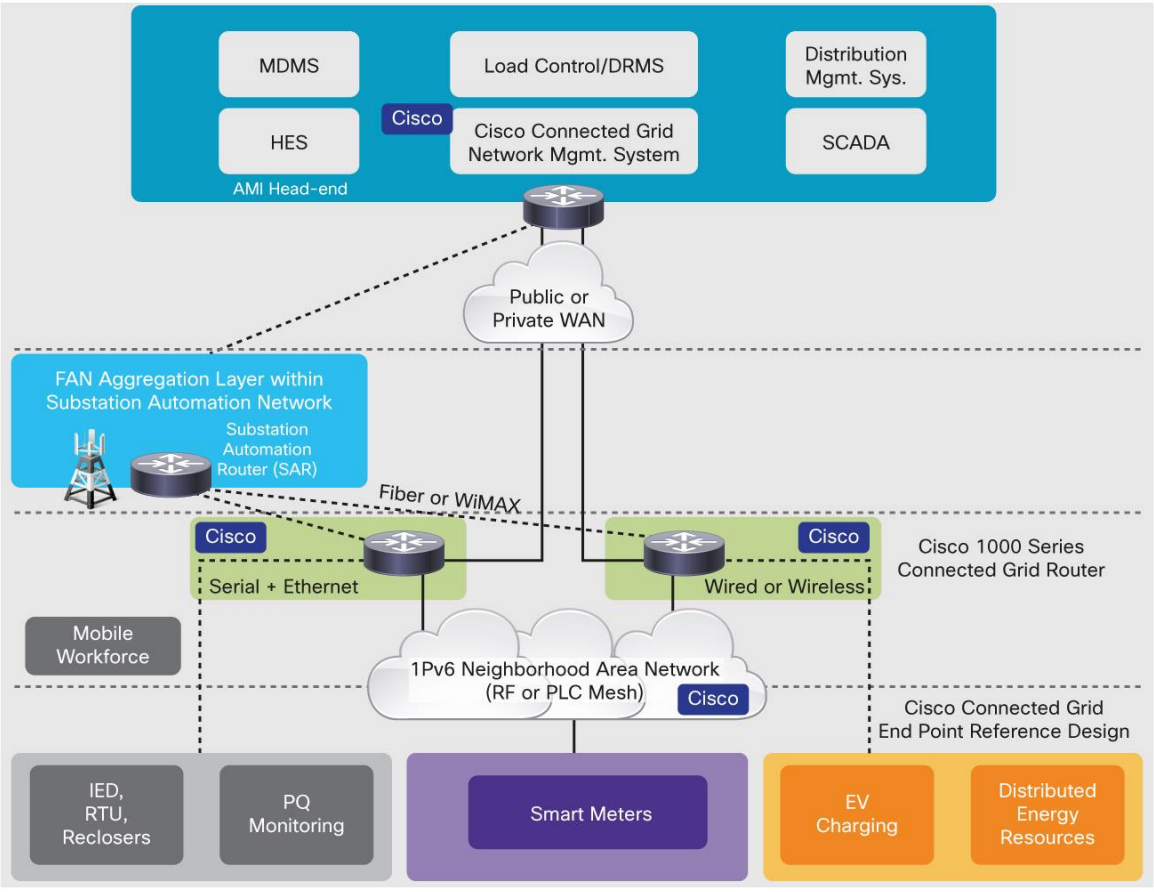
Utilities all over the world are transitioning their grids from transmission to consumption. Regulatory mandates are driving initiatives around smart metering, grid reliability, and the integration of solar and wind farms into the distribution grid. The situation imposes a unique set of challenges for utilities to build a bidirectional communications Field Area Network (FAN) that enables these diverse applications and also scales across millions of endpoints.

The Cisco Connected Grid FAN solution has been specifically developed to meet these challenges, using design principles from industry-leading Cisco GridBlocks™ architecture. Under the GridBlocks architecture, a typical communications network for the distribution grid is a two-tier architecture with a Neighborhood Area Network (NAN) and a Wide Area Network (WAN).

The NAN provides network connectivity to endpoints such as smart meters, street lights, and other environmental sensors. These endpoints form a resilient mesh network based on Radio-Frequency (RF) or Power-Line Communications (PLC) technologies. The resilient mesh network is aggregated at a CGR 1000 mounted on pole tops or in secondary distribution substations. The CGR 1000 can also aggregate locally connected devices for Distribution Automation (DA). The WAN tier provides network connectivity from the CGR 1000 to the utility's control center over a public cellular network, or WiFi network, or an Ethernet fiber network.

Figure 2 displays the solution within the network.

Figure 2. Cisco Connected Grid FAN Solution



The Connected Grid FAN solution comprises the following products: Cisco CGR 1000 Series, IoT Device Manager, IoT Field Network Director, and Resilient Mesh End Point (RME) reference design. The RME is an open standards-based IPv6 networking stack that can be embedded in a variety of smart grid endpoints, such as smart meters. Partners with sensors or actuators who want to integrate the RME RF Mesh or RF+PLC Mesh into their products need to join the Cisco Developer Network/DevNet: https://www.cisco.com/go/cdn.

Business Benefits and Architectural Features

The CGR 1000 Series Routers take full advantage of Cisco core IP networking technologies. Our hardware and software can be used to create an open platform for industrial customers to build highly secure, multiservice FANs while lowering their total cost of ownership.

Converged Multiservice Network Architecture

The CGR 1000 Series is a modular platform that supports various wired and wireless interfaces. It supports a 902-928 MHz IPv6 RF mesh that can aggregate up to 5000 endpoints such as smart meters. The router has integrated Ethernet and serial interfaces to connect to DA devices such as sensors, capacitor bank controllers, recloser controllers, and remote terminal units.

Supervisory Control And Data Acquisition (SCADA) protocol (serial-to-IP) translation features allow customers to easily integrate legacy (non-IP) devices onto an IP network. An integrated Wi-Fi port can enable remote workforce automation and secure wireless console access while an integrated Global Positioning System (GPS) enables location mapping of the router. The modular design provides an easy upgrade path to future communication interfaces without platform replacement.

The CGR 1000 Series portfolio offers platforms for both indoor and outdoor deployments. These platforms come with flexible mounting kits that allow utilities to deploy the routers on a broad array of existing assets such as distribution poles, walls, and inside pad-mounted enclosures. In addition, the CGR 1000 Series offers a wide range of external antenna choices to meet coverage, throughput, and range requirements.

Cisco IOS Software provides a set of network- and application-layer services to help enable customers run multiple applications on a converged communication network. Network segmentation and Quality of Service (QoS) features allow the logical separation of application traffic with specific constraint policies applied on each traffic flow. In addition, the CGR 1000 Series is capable of integrating and hosting customer or partner specific applications.

This allows customers to eliminate the cost, space, power, and complexity of deploying and managing disparate devices.

Security

Cisco integrates security as a fundamental building block of the FAN architecture. The CGR 1000 Series security adheres to Cisco Connected Grid security principles and widely adopted cryptography and security standards (see Table 1).

Table 1. Cisco Connected Grid Security Principles

Security Principle	CGR 1000 Features and Capabilities
Access Control	• Mutual authentication and authorization of all nodes connected to the network • IEEE 802.1x-based authentication, Role-Based Access Control (RBAC) • Certificate-based identity, strong username, and passwords
Data Integrity, Confidentiality, and Privacy	• Link-layer encryption in the NAN mesh (AES-128) • Network-layer encryption in the WAN (IPsec and FlexVPN) • Scalable key management, generation, exchange, and revocation of encryption keys
Threat Detection and Mitigation	• Network segmentation of users, devices, and applications in NAN and WAN • Access lists on field area router to filter traffic between users and devices • High-performance firewall in the control center to protect critical assets
Device and Platform Integrity	• Tamper-resistant mechanical design; security alerts generated if compromised • Hardware chip to store the router's X.509 certificate and other security credentials • Tamper-proof secure storage of router configuration and data

Open Standards

The Cisco approach has been to encourage the creation and adoption of open communication standards for the smart grid. This approach promotes the growth of an ecosystem of standards-based, interoperable devices and applications from different vendors. An interoperable ecosystem ultimately reduces utilities' risk of adopting new technologies. The Cisco Connected Grid is built on several open standards, many of them adopted from IP technologies such as IPv6. With these standards, customers are able to architect and design their network independent of the application- or physical-layer infrastructure. This functionality protects existing investments while lowering the total cost of ownership for the communications network over time.

Network Reliability and High Availability

The CGR 1000 Series Routers contain both device-level and network-level reliability to meet harsh physical environments. The CGR 1000 Series is built to meet stringent compliance standards such as IEEE 1613 and IEC 61850-3. The routers have enhanced thermal design and conduction cooling with no moving parts. This attribute allows extended temperature support. Additionally, the routers offer mechanisms for backup power to increase uptime for mission-critical applications in the event of power outages. Finally, the support for multiple WAN communication modules and the network resiliency and routing features in Cisco IOS Software allow utilities to deploy enterprise-class high availability in their communication networks for the distribution grid.

Communications Network Management

Network management applications are critical for lowering utility Operating Expenses (OpEx) while improving communications network availability. These tools simplify and automate many of the day-to-day tasks associated with managing diverse network requirements. The embedded management features available in the CGR 1000 Series, along with IoT Field Network Director and CG-DM applications, allow customers to effectively meet these requirements.

IoT Field Network Director is a modular software platform for managing smart grid multiservice communication networks and security infrastructure. It is designed to foster an ecosystem of multivendor capabilities for interoperability across not only communications networks, but also legacy and next-generation power grid equipment.

IoT Device Manager is an easy-to-use Windows application that engineers and operators use to quickly configure, test, and troubleshoot Cisco 1000 Series Connected Grid Routers. For example, field technicians can check and update device configurations, perform firmware upgrades, and collect real-time router statistics.

The Cisco FAN solution provides operators with extensive instrumentation and diagnostic information for geographic locations, wireless interfaces, battery management, and other grid-specific details. This information can be fed into the IoT Field Network Director for day-to-day operations, operator dashboards, and real-time troubleshooting. Ease-of- use features such as secure zero-touch commissioning and a graphical field tool let non-IT field technicians deploy and manage FAN communications equipment.

In addition to the utility-specific functionality, the Cisco solution provides customers with true enterprise-class Fault, Configuration, Accounting, Performance, and Security (FCAPS) functionality. Examples include a programmatic XML interface based on the Network Configuration Protocol (NETCONF) industry standard, Role-Based Access Control (RBAC), over-the-air software upgrades, and security management functionality.

Cisco 1000 Series Connected Grid Routers Specifications

Table 2 lists hardware specifications and Table 3 lists the features and protocols support for the CGR 1000 Series routers.

Table 2. Cisco CGR 1000 Series Hardware Specifications

	CGR 1240 (Pole-Mount)	CGR 1120 (Din-Rail or Wall Mount)
Physical Specifications		
Dimensions (Height x Width x Depth)	28.7 cm x 24.6 cm x 21.6 cm 11.3 in. x 9.7 in. x 8.5 in. (without antennas)	8.9 cm x 22.9 cm x 20 cm 3.5 in. x 9.0 in. x 7.8 in.
Rack Height	N/A	2 RU
Pole Mount	Yes	No
Wall Mount	Yes	Yes
Din-Rail Mount	No	Yes
Typical Weight Fully Configured	23 lbs (10.4 kg) Unit weight includes base chassis with four communication modules, AC power supply, and 8-Amp-hr battery backup unit	8 lbs (3.6 kg) Unit weight includes base chassis with two communication modules, AC/DC power supply
Operating Temperature[1]	−40°C to +70°C (-40°F to 158°F) with type test to 85°C (185°F) for 16 hours	-40°C to +60°C (-40°F to 140°F) with type test up to 85°C (185°F) for 16 hours
Typical Power Consumption or Dissipation	20-28 Watts depending on configuration (without battery charging) Additional power consumption for battery charging and external radios	16-23 Watts depending on configuration
Maximum Power Consumption or Dissipation	75 Watts	40 Watts
Communication & Compute Module		
IEEE 802.15.4g WPAN	Yes	Yes
4G LTE for Global	Yes	Yes
4G LTE for North America	Yes	Yes
3.5G AT&T HSPA+/UMTS/GSM/GPRS/EDGE	Yes	Yes
3.5G (Non-US) HSPA+/UMTS/GSM/GPRS/EDGE	Yes	Yes
CDMA EV-DO Rev A/0/1xRTT-Verizon	Yes	Yes
CDMA EV-DO Rev A/0/1xRTT-Sprint	Yes	Yes
CDMA EV-DO Rev A/0/1xRTT-Generic	Yes	Yes
Dual 4G LTE module	Yes	Yes
Compute Module	Yes	Yes

	CGR 1240 (Pole-Mount)	CGR 1120 (Din-Rail or Wall Mount)
Onboard Interfaces		
Gigabit Ethernet Combination Ports (10/100/1000 Copper, 100/1000 SFP)	2	2
SFPs Supported	GLC-SX-MM-RGD (1000BASE-SX Short wavelength, rugged) GLC-LX-SM-RGD (1000Base-LX/LH long wavelength, rugged) GLC-FE-100LX-RGD (100BASE-LX10 SFP, rugged) GLC-FE-100FX-RGD (100BASE-FX SFP, rugged) GLC-ZX-SM-RGD (1000BASE-ZX extended distance, rugged) Single Fiber Bi-directional transceivers: GLC-BX-D and GLC-BX-U	
10/100 Fast Ethernet Copper Ports	4	6
Wi-Fi (IEEE 802.11 b/g/n)	Yes (autonomous)	Yes (autonomous)
Serial (RS-232/RS-485)	2	2
GPS for Location	Yes	Yes
IRIG-B[2]	BNC connector	No
Digital Alarm Inputs[2]	2	3
Digital Alarm Outputs[2]	2	1
USB Type A host ports[2]	2	1
Console and AUX Port (RJ-45)	1	1
SD Flash Slot (Memory)	1 (2 GB)	1 (2 GB)
Power Options		
Power Supply	AC power supply: • 100-240 VAC	Integrated AC/DC power supply: • 3-phase AC power supply: 100-240 VAC • 10.6-52 VDC (nominal), 9-60 VDC (maximum)
Battery Backup Options	Integrated modular battery backup unit (BBU) and smart charging and monitoring system • CGR 1240 can be deployed with up to three BBU modules stacked and provide up to 12 Amp hours	N/A
Power Options for Third-Party Radios	The CGR 1240 provides support for powering third-party radios: • Voltage output: 12 VDC plus or minus 5 percent • Power output: 12 W (continuous)	N/A
Regulatory Compliance		
Environmental Compliance	• IEC-61850-3 • IEEE1613	• IEC-61850-3 • IEEE1613
Immunity	• EN61000-6-2 • IEC 61000-6-4 • IEC 61000-6-5 (AC, DC, I/O) • EN61000-4-2 (ESD) • EN61000-4-3 (RF) • EN61000-4-4 (EFT) • EN61000-4-5 (SURGE) • EN61000-4-6 (CRF) • EN61000-4-11 (VDI) • IEC 61000-4-12 (AC, DC, I/O) • EN 55024, CISPR 24 • EN50082-1 • IEEE 1613: High Voltage Impulse	• EN61000-6-2 • IEC6 1000-6-4 • IEC 61000-6-5 (AC, DC, I/O) • EN61000-4-2 (ESD) • EN61000-4-3 (RF) • EN61000-4-4 (EFT) • EN61000-4-5 (SURGE) • EN61000-4-6 (CRF) • EN61000-4-11 (VDI) • IEC 61000-4-12 (AC, DC, I/O) • EN 55024, CISPR 24 • EN50082-1 • IEEE 1613: High Voltage Impulse

	CGR 1240 (Pole-Mount)	CGR 1120 (Din-Rail or Wall Mount)
EMC	• 47 CFR, Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI V-3 • CNS 13438 • EN 300-386	• 47 CFR, Part 15 • ICES-003 Class A • EN55022 Class A • CISPR22 Class A • AS/NZS 3548 Class A • VCCI V-3 • CNS 13438 • EN 300-386
Safety	• USA: UL 60950-1 • Canada: CAN/CSA C22.2 No. 60950-1 • Europe: EN 60950-1 • China: GB 4943 • Australia/New Zealand: AS/NZS 60950.1 • Rest of world: IEC 60950-1 • UL certified to UL/CSA 60950-1, 2nd Ed. • CB report to IEC60950-1, 2nd Ed., covering all group differences and national deviations • Insulation effectiveness: ◦ AC Input to chassis/ground - 1500V~/2121Vdc ◦ AC Input to output/accessible connectors ◦ - 3000V~/4242Vdc	• USA: UL 60950-1 • Canada: CAN/CSA C22.2 No. 60950-1 • Europe: EN 60950-1 • China: GB 4943 • Australia/New Zealand: AS/NZS 60950.1 • Rest of world: IEC 60950-1 • CSA certified to UL/CSA 60950-1, 2nd Ed. • CB report to IEC60950-1, 2nd Ed., covering all group differences and national deviations • Insulation effectiveness: ◦ AC Input to chassis/ground - 1500V~/2121Vdc ◦ AC Input to output/accessible connectors ◦ - 3000V~/4242Vdc ◦ DC input to chassis/ground/accessible connectors - no requirement

[1] Operating temperature range is impacted by choice of communication modules and battery backup options. For a CGR1240, you must install the compute module in Slot 5, If a cellular module is installed in slot 6, the max operating temp is derated to 50C.

[2] Interfaces built into platform hardware. Software support will be available in future releases.

Table 3. Cisco IOS Features and Protocols Support

Protocols
IPv4 (RFC 791, 1812, 1918), IPv6 (RFC 2375, 2460, 2464, 2711, 3306, 3315, 3484, 3587, 3849, 4193, 4291, 4443, 4861, 4862), Static Routes, Open Shortest Path First-OSPFv2/v3 (RFC 2328, 2370, 3101, 3137, 5340), UDP (RFC 768), TCP (RFC 791), Multiprotocol Border Gateway Protocol (MP-BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), Internet Key Exchange v2 (IKEv2)
Multicast: Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast-PIM (RFC 4601), Multicast Listener Discovery Version 2- MLDv2 (RFC 3590, 3810)
Generic Routing Encapsulation (RFC 2473, 2784, 2890), PPP/CHAP
IEEE 802.15.4g/e, IEEE 1901.2, IETF 6LOWPAN (RFC 4919, 4944, 6282), IETF RPL (RFC 6550, 6551, 6553, 6554, 6206), IETF CoAP
Ethernet, Serial (RS-232/485), WiFi (IEEE 802.11b/g), WiMAX (IEEE 802.16e)
SCADA support over serial link: IEC 60870-5-101/104 protocol translation and DNP3 serial to IP protocol translation
Raw socket support on serial ports (for transport of non-IP protocols). Raw socket over L2 VPN.
Virtual Routing and Forwarding Lite (VRF-Lite), Virtual LANs (VLAN)
NTPv4 (RFC 5905), DHCP (RFC3246, 3260, 3736), DNS (RFC 1591, 3596), DHCP relay and server for IPv4 and IPv6
L2TPv3
Mapping of Address and Port Using Translation (MAP-T) Border Router (used with IR509)
Security
IEEE 802.1x
Encryption: IPSec VPN (RFC 4301-3, 4306, 4308, 4835), WPA2 for WiFi, FlexVPN
Dynamic Multipoint VPN (DMVPN)
Device identity: IEEE 802.1AR
RBAC for device configuration

L3-L4 ACLs
Authentication, Authorization: EAP TLS/EAP TTLS
RF and PLC Mesh security solution
Secure Shell v2 (SSHv2) and SNMPv3 Crypto
Control plane policing and protection
Certificate revocation list (CRL) and Online Certificate Status Protocol (OCSP)
QoS (RFC 2475)
Classification and marking: ACLs, Layer 3-IP Precedence, Differentiated Services Code Point (DSCP)
Congestion management: Policing, Priority Queuing (PQ), class-based weighted fair queuing, low latency queue, weighted round robin with four priority queues
Embedded Management
NETCONF(RFC 6241), HTTPS (RFC 2818), SSH (RFC 4251-4), Syslog (RFC 5424, 5426)
SNMP v3, v2, v1 along with MIBs for interfaces and system parameters
Embedded Event Manager (EEM) and object tracking
Secure zero-touch commissioning
Battery health monitoring (not available for CGR 1120)
Door tamper detection (not available for CGR 1120)
Network Timing Protocol (NTP)

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information on the Cisco 1000 Series Connected Grid Routers, visit https://www.cisco.com/go/cgr1000.

For more information on the Cisco Field Area Network solution, visit https://www.cisco.com/go/fan.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C78-696278-07 01/18