

Cisco Ethernet Switch Modules for Cisco 2000 Series Connected Grid Routers

The Cisco® Ethernet Switch Module (ESM) for the Cisco 2010 Connected Grid Router (CGR 2010) can reduce your total cost of ownership by integrating Gigabit Ethernet (GE) and Fast Ethernet (FE) switch ports within the Cisco 2000 Series Connected Grid Router. This integration allows you to build redundant high-availability architectures and provides an all-in-one device to deliver advanced routing and switching, valuable for space-constrained environments.

Product Overview

The Cisco Ethernet Switch Module (CGR 2010 ESM) (Figure 1) greatly expands the Cisco 2010 Connected Grid Router's capabilities by integrating industry-leading Layer 2 and Layer 3 (optional) switching with feature sets comparable to those found in the Cisco 2520 Connected Grid Switches (<http://www.cisco.com/go/cgs2500>). The new Cisco Ethernet Switch Module along with the Cisco 2010 Connected Grid Router (CGR 2010) are designed specifically for use in connected energy applications such as grid automation, distributed generation, integrated renewable energy, trackside substations, and water, oil, and gas applications. The CGR 2010 ESM uses Cisco IOS® Software, which is the operating system powering millions of Cisco switches worldwide, and provides the benefits of improved security, network resiliency and reliability, and scalability.

Figure 1. Cisco 2010 Connected Grid Router Ethernet Switch Modules (CGR 2010 ESM)



Primary CGR 2010 ESM features:

- Rugged industrial design and substation compliance: IEC-61850-3 and IEEE 1613 for utility substation environments
- Tools for easy deployment, management, and replacement
- Extensive instrumentation and remote diagnostic capabilities

- Advanced quality of service (QoS) capabilities to support mission-critical substation applications such as Supervisory Control and Data Acquisition (SCADA) and IEC 61850 Generic Object Oriented Substation Events (GOOSE) messaging
- Comprehensive network security features based on open standards

Cisco Ethernet Switch Module Types

Two types of CGR 2010 Ethernet Switch Modules are available (Table 1): 10-port ESM and 6-port ESM.

Table 1. Ethernet Switch Module Models

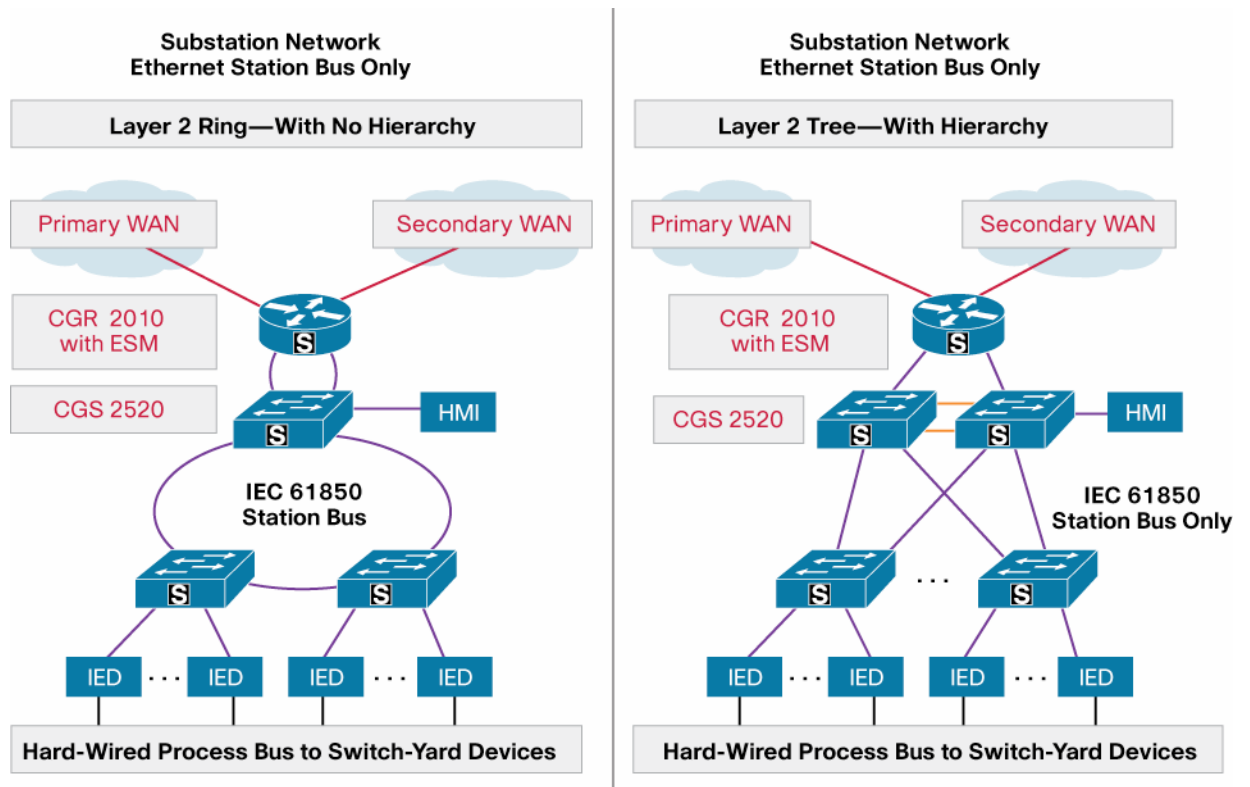
Model	Description
GRWIC-D-ES-2S-8PC	<ul style="list-style-type: none"> • 8xFE RJ45 ports (Power over Ethernet [PoE]* support on first 4 ports) • 1xGE combo port • 1xGE fiber Small Form-Factor Pluggable (SFP) port
GRWIC-D-ES-6S	<ul style="list-style-type: none"> • 4xFE fiber SFP port • 1xGE combo port • 1xGE fiber SFP port

*If two GRWIC-D-ES-2S-8PC modules are installed on the CGR 2010, there is a maximum of 61.5W PoE power available across both modules.

Networking Solutions and CGR 2010 ESM: Substation Automation Example

Substation automation promises to bring more automation and intelligence to the power grid network to address a myriad of utility concerns such as how to reduce operational expenses to ways to meet new regulatory requirements. The CGR 2010 ESM deployed together with the [Cisco 2010 Connected Grid Router \(CGR 2010\)](#) offers utilities a rugged networking solution to enable reliable and secure two-way communication for substation automation. Figure 2 depicts the place in the network where the CGS 2520 switch and CGR 2010 router with Ethernet Switch Module can be deployed.

Figure 2. Deployment Scenario: CGR 2010 ESM



Product Overview

The CGR 2010 ESM is purpose-built for harsh environments. The CGR 2010 ESM offers:

- Rugged design for T&D power substations, including compliance with IEC-61850-3 and IEEE 1613 specifications for extended environmental, shock/vibration, and surge ratings; a complete set of DC and AC power input options for the CGR 2010; and convection cooling (no fans)
- Compact double-wide (2x GRWIC slot) form factor
- Easy setup and management using the Cisco Configuration Professional graphical user interface and supporting management tools, including CiscoWorks LAN Management Solution (LMS)
- High availability, deterministic QoS behavior, and reliable security using Cisco IOS Software
- Smartport templates that implement recommended software configurations for T&D substation applications at the touch of a button
- Hardware support for IEEE1588v2, a precision timing protocol with nanosecond-level precision for precise timing applications
- Improved ring and hub-and-spoke resiliency with the support of Resilient Ethernet Protocol (REP) and Flexlink
- Transparent IT integration with the support of Layer 3 routing protocols (IP Services image optional)
- PoE support on model GRWIC-D-ES-2S-8PC

Configurations

The CGR 2010 ESM includes the following configurations:

- **GRWIC-D-ES-2S-8PC:** Rugged Ethernet switch with 8 10/100BaseTX PoE ports (a maximum of 4 standard PoE ports supported), one dual-purpose Gigabit Ethernet uplink (dual-purpose Gigabit Ethernet uplinks allow the user to activate either copper or fiber media), and one Gigabit Ethernet fiber SFP port. The Layer 2 LAN Base image is included.
- **GRWIC-D-ES-6S:** Rugged Ethernet switch with 4 Fast Ethernet (FE) SFP ports, one dual-purpose Gigabit Ethernet uplink, and one Gigabit Ethernet fiber SFP port. The Layer 2 LAN Base image is included.
- **PWR-RGD-LOW-DC:** Low DC (24/48V) power supply module available for the CGR 2010 router, which can also be used in the CGS 2520 switch.
- **PWR-RGD-AC-DC:** High AC/DC (88-300VDC/85-264VAC) power supply module available for the CGR 2010 router, which can also be used in the CGS 2520 switch.

The CGR 2010 ESM offers two different Cisco IOS Software feature images: LAN Base and IP Services. The LAN Base image offers advanced QoS, flexible VLAN handling, SCADA protocol classification support, resilient Ethernet protocol (REP) for improved convergence time in ring topologies, Flexlink for fast failover in hub-and-spoke topologies, and comprehensive security features. In addition, the IP Services image adds advanced Layer 3 features such as support for advanced IP routing protocols, Multi-VPN Routing and Forwarding Customer Edge (Multi-VRF CE/VRF-Lite), and policy-based routing (PBR).

The SFP-based uplink ports accommodate a range of industrial-grade SFP transceivers, including 1000BASE-SX, 1000BASE-LX, 1000BASE-ZX, 100BASE-FX, and 100BASE-LX10.

Primary Business Benefits

The CGR 2010 ESM is designed for network security, high availability, ease of use, and durability. Table 2 lists the business benefits of the CGR 2010 ESM.

Table 2. Primary Business Benefits of the CGR 2010 ESM

Benefits	Description
Rugged design for substation compliance	<ul style="list-style-type: none">• Compliant with IEEE 1613 and IEC-61850-3 substation standards for rugged design.• Convection cooled with no moving parts or fans for maximum reliability and reduced network outages.
Network security	<ul style="list-style-type: none">• Advanced Cisco IOS Software features such as 802.1x, Layer 2-Layer 4 access control lists (ACLs), port security, protected port/private VLAN, UNI/ENI default control traffic shutdown, and configuration file security to prevent unauthorized network access and reduce operational costs of securing the network.
High availability and redundancy	<ul style="list-style-type: none">• Advanced Cisco IOS Software features such as REP and Flexlink provide fast reconvergence in ring and hub-and-spoke topologies, minimizing network downtime and associated costs.• Field-replaceable components such as power supplies and SFPs reduce redeployment time.• Optional redundant, hot-swappable power supply provides additional redundancy.
Ease of use	<ul style="list-style-type: none">• Intuitive graphical user interface (GUI) in Cisco Configuration Professional simplifies configuration of switches and reduces training time and costs. Utility-focused enhancements have been added to further increase ease of use.• Smartport templates provide one-touch global and port-level macros to simplify switch deployments.
Investment protection	<ul style="list-style-type: none">• Two Cisco IOS Software images are available to choose from. This allows you to choose the right feature set for your networking needs.• An advanced Layer 2 switching feature set comes standard with the CGR 2010 ESM; Layer 3 feature set optional.• Ongoing development of software capabilities lead to a longer product lifecycle, lowering the total cost of ownership.

Software Optimized for Connected Energy Applications

The CGR 2010 ESM software is optimized for Connected Energy applications such as grid automation, distributed generation, integrated renewable energy, trackside substations, and water, oil, and gas applications and builds on the strength of Cisco IOS Software, which powers mission-critical networks across the world. Numerous new features make the CGR 2010 ESM the optimal Ethernet switch module for energy network operators, such as Smartport templates, which enable simple configuration for utility environments. In addition, many default behaviors of the CGR 2010 ESM are different from those of traditional Ethernet switches, making the CGR 2010 ESM easier to configure, manage, secure, and troubleshoot.

High Availability and Redundancy

High availability is a vital requirement for networks that transport mission-critical data. The CGR 2010 supports dual-redundant field-replacable power supplies and SFP modules, which increase network uptime for GRWICs such as the CGR 2010 ESM.

To further increase high availability on a networkwide level, CGR 2010 ESM offers REP and Flexlink for fast reconvergence, link-state tracking, IEEE 802.1w Rapid Spanning Tree Protocol (RSTP), per-VLAN Rapid Spanning Tree Plus (PVRST+), and the Cisco Hot Standby Router Protocol (HSRP). These capabilities help to create redundant, failsafe topologies. Strong, built-in security helps prevent the device and the network from succumbing to malicious attacks, thereby enhancing network uptime.

Security

The wide range of security features on the CGR 2010 ESM protects mission-critical traffic, prevents unauthorized access, and maintains uninterrupted operation. The CGR 2010 ESM protects operational and nonoperational data by focusing on securing connectivity, defending against network threats, and providing trust and identity features.

Protecting a network begins with securing connectivity. For example, ACLs can be used to restrict access to sensitive portions of the network. To defend against network threats such as Dynamic Host Configuration Protocol (DHCP) spoofing, DHCP snooping can be used to allow only DHCP requests (but not responses) from untrusted user-facing ports. Workforce management is a critical use case where trust and identity features such as IEEE 802.1x can be used to enable strong security policies, yet provide maximum mobility to a remote workforce.

Table 3 lists these and other primary features of the security solution.

Table 3. Primary Features for Each Area of Comprehensive Security Solution

Secure Connectivity	Threat Defense	Trust and Identity
UNI/ENI default: control traffic shut down	Configurable control plane security	ACLs
DHCP snooping and IP source guard	Storm control	IEEE 802.1x
Dynamic ARP inspection	Port security	UNI/ENI default: port down
Private VLAN	Configurable per-VLAN MAC learning	Configuration file security

Switch Management Options

The CGR 2010 ESM offers an easy-to-use graphical user interface (GUI) for configuration through the Cisco Configuration Professional tool as well as a superior command-line interface (CLI) for detailed configuration. In addition, the switches support CiscoWorks and Simple Network Management Protocol (SNMP) for networkwide

management. Network operators can integrate the CGR 2010 ESM transparently into their network operations centers and enable improved flow-through provisioning.

Network operators can also manage the CGR 2010 ESM using SNMP Versions 2 and 3. A comprehensive set of MIBs, including comprehensive temperature and voltage monitoring, is provided for network operators to collect traffic information in the CGR 2010 ESM.

Primary Features and Benefits

Table 4 lists the main features and benefits of the CGR 2010 ESM.

Table 4. Features and Benefits

Feature	Benefit
Designed for harsh connected energy applications	<ul style="list-style-type: none"> Extended temperature, vibration, shock and surge, and noise immunity ratings comply to specifications for substation environments Compact, double-wide GRWIC form factor ideal for space-constrained environments Variety of power input options covers a wide range of power requirements for T&D power substations Copper and fiber connectivity options; SFP modules provides uplink connectivity supporting 100BASE-LX10, 100BASE-FX, 1000BASE-SX, 1000BASE-LX, and 1000BASE-ZX options.
Availability and Scalability	
High-availability mechanisms	<p>Hardware</p> <ul style="list-style-type: none"> Dual field-replaceable, hot-swappable power supplies for the CGR 2010 and SFP modules increase network uptime. <p>Software</p> <ul style="list-style-type: none"> Resilient Ethernet Protocol (REP) provides fast Layer 2 reconvergence in a ring topology and offers an alternative to Spanning Tree Protocol. Flexlink provides fast link failover for hub-and-spoke topologies, including dual-homed designs. Link-state tracking accelerates network reconvergence by binding the state of downlink ports to the state of associated uplink ports. IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) provides rapid spanning-tree convergence independent of spanning-tree timers and offers the benefit of distributed processing. Per-VLAN Rapid Spanning Tree (PVRST+) allows rapid spanning-tree reconvergence on a per-VLAN spanning-tree basis, without requiring the implementation of spanning-tree instances. IEEE 802.1s Multiple Spanning Tree Protocol allows a spanning-tree instance per VLAN, enabling Layer 2 load sharing on redundant links. Cisco Hot Standby Router Protocol (HSRP) is supported to create redundant, fail-safe routing topologies. Unidirectional Link Detection Protocol (UDLD) and Aggressive UDLD allow unidirectional links caused by incorrect/failed fiber-optic connections or port faults to be detected and disabled on fiber-optic interfaces. Switch-port autorecovery (error disable) automatically attempts to reactivate a link that is disabled because of a network error. Equal-cost routing provides for load balancing and redundancy.
High-performance IP routing (optional IP Services image required)	<ul style="list-style-type: none"> Cisco Express Forwarding hardware routing architecture delivers extremely high-performance IP routing. Basic IP Unicast routing protocols (static and RIP versions 1 and 2) are supported for small-network routing applications. Advanced IP Unicast routing protocols (OSPF, EIGRP, IS-IS, and BGPv4) are supported for load balancing and constructing scalable LANs. HSRP provides dynamic load balancing and failover for routed links. Inter-VLAN IP routing provides for full Layer 3 routing between two or more VLANs. Protocol Independent Multicast (PIM) for IP Multicast routing is supported, including PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode. The IP Services image is required. Cisco recommends 128 switch virtual interfaces (SVIs). A maximum of 1005 is supported (depending on the number of routes and multicast entries). IPv6 improves the scalability of IP networks by supporting the growing number of users, applications, and services. The functionalities supported include ACLs, DHCP, routing (Unicast routing, RIP, OSPFv3, static routes), MLD snooping, stateless autoconfig, default router preference, HTTP/HTTPS.
QoS and Control	
Advanced QoS	<ul style="list-style-type: none"> Hardware-based advanced QoS functionality based on Cisco's ASIC technology enabling control-plane and data-plane QoS ACLs to help ensure proper marking on a per-packet basis. The Cisco modular QoS CLI provides a modular and highly extensible framework for deploying QoS, by standardizing

Feature	Benefit
	<p>the CLI and semantics for QoS features across all platforms that are supported by Cisco IOS Software.</p> <ul style="list-style-type: none"> • 1-rate 2-color ingress policing to enable more flexible QoS offerings. • Standard 802.1p class of service (CoS) and VLAN-based classification are provided, allowing for granular control and monitoring of GOOSE traffic (on a per VLAN basis). • Differentiated services code point (DSCP) and Layer 4 TCP/UDP port number-based classification allows granular classification/control and monitoring of TCP/IP-based SCADA protocols- DNP3 IP, IEC 60870-5-104 and so on. • Ingress marking and remarking capabilities to help ensure proper QoS treatment and to prevent DoS attacks from improperly marked traffic streams. • Shaped Round Robin (SRR) scheduling helps ensure differential prioritization of packet flows by intelligently servicing the queues. • Weighted Tail Drop (WTD) provides per QoS class congestion avoidance at the queues before a disruption occurs. • Strict priority queuing helps ensure that the highest-priority packets are serviced ahead of all other traffic. Optionally, Priority queue rate limiting provides optional protection against lower-priority queue starvation. • Configurable control plane queue assignment allows prioritization of control plane traffic. This is done by setting QoS markings globally for CPU-generated traffic so these protocol packets will receive priority in the network.
Network Security	
Comprehensive security solutions	<p>Trust and Identity</p> <ul style="list-style-type: none"> • IEEE 802.1x allows dynamic, port-based security, providing user authentication. • IEEE 802.1x with VLAN assignment allows a dynamic VLAN assignment for a specific user regardless of where the user is connected. • IEEE 802.1x and port security are provided to authenticate the port and manage network access for all MAC addresses, including those of the client. • IEEE 802.1x with an ACL assignment allows for specific identity-based security policies regardless of where the user is connected. • IEEE 802.1x with Guest VLAN allows guests without 802.1x clients to have limited network access on the guest VLAN. • Web authentication for non-802.1x clients allows non-802.1x clients to use an SSL-based browser for authentication. • MAC Auth Bypass (MAB) for voice allows third-party IP phones without an 802.1x supplicant to get authenticated using their MAC address. <p>Secure Connectivity</p> <ul style="list-style-type: none"> • Control Plane Security prevents DoS attacks on the CPU. • Cisco security VLAN ACLs (VACLs) on all VLANs prevent unauthorized data flows from being bridged within VLANs. • Cisco standard and extended IP security router ACLs (RACLs) define security policies on routed interfaces for control- and data-plane traffic. • Port-based ACLs (PACLs) for Layer 2 interfaces allow application of security policies on individual switch ports. • SSHv2, Kerberos, and SNMPv3 provide network security by encrypting administrator traffic during Telnet and SNMP sessions. SSHv2, Kerberos, and the cryptographic version of SNMPv3 require a special cryptographic software image because of U.S. export restrictions. • Private VLAN Edge provides security and isolation between switch ports, helping ensure that users cannot snoop on other users' traffic. • TACACS+ and RADIUS authentication enable centralized control of the switch and restrict unauthorized users from altering the configuration. • Multilevel security and configuration file security on console access prevents unauthorized users from altering the switch configuration. <p>Threat Defense</p> <ul style="list-style-type: none"> • Port security secures Layer 2 access or trunk ports based on MAC address. • Unknown unicast and multicast port blocking allows tight control by filtering packets that the switch has not already learned how to forward. • Bidirectional data support on the Switched Port Analyzer (SPAN) port allows the Cisco Secure Intrusion Detection System (IDS) to take action when an intruder is detected. • MAC address notification allows administrators to be notified of users added to or removed from the network. • Dynamic ARP Inspection (DAI) helps ensure user integrity by preventing malicious users from exploiting the insecure nature of the ARP protocol. • DHCP snooping allows administrators to help ensure consistent mapping of IP to MAC addresses. This can be used to prevent attacks that attempt to poison the DHCP binding database, and to rate limit the amount of DHCP traffic that enters a switch port. • IP source guard prevents a malicious user from spoofing or taking over another user's IP address by creating a binding table between the client's IP and MAC address, port, and VLAN. • Spanning-Tree Security mechanisms like Spanning tree BPDU guard and Spanning Tree Root Guard (STRG) prevents edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes. • Remote Switched Port Analyzer (RSPAN) allows for remote monitoring of the user interface.

Feature	Benefit
Manageability	
Superior manageability	<ul style="list-style-type: none"> • The Cisco IOS Software command line interface (CLI) provides a common user interface and command set with Cisco routers and switches. • CGR 2010 ESM can be configured and monitored using Cisco Configuration Professional with enhanced menus targeted to simplify utility-specific configurations. • For easier deployments, the CGR 2010 ESM switches support default global or port-level macros with Cisco recommended configurations, allowing the user to easily set up the switch in a configuration optimized for utility deployments. • The CGR 2010 ESM ships with MODBUS memory map support that can be used by human machine interface (HMI) applications to query the switch for information using the MODBUS protocol. • Switching Database Manager templates for Layer 2 and Layer 3 deployment allow administrators to easily optimize memory allocation to the desired features based on deployment-specific requirements. • VLAN trunks can be created from any port, using standards-based 802.1Q tagging. Up to 1005 VLANs per switch and up to 128 spanning-tree instances per switch are supported simultaneously. 4094 VLAN IDs are supported. • RSPAN allows administrators to remotely monitor ports in a Layer 2 switch network from any other switch in the same network. • For enhanced traffic management, monitoring, and analysis, the embedded Remote Monitoring (RMON) software agent supports four RMON groups (history, statistics, alarms, and events). • All nine RMON groups are supported through a SPAN port, permitting traffic monitoring of a single port, a group of ports, or the entire stack from a single network analyzer or RMON probe. • Domain Name System (DNS) provides IP address resolution with user-defined device names. • Trivial File Transfer Protocol (TFTP) reduces the cost of administering software upgrades by downloading from a centralized location. • Network Timing Protocol (NTP) provides an accurate and consistent time stamp to all intranet switches. • Configuration Rollback helps in error recovery by providing the capability to replace the current running configuration with any saved Cisco IOS Software configuration file. • Embedded Events Manager (EEM) offers the ability to monitor events and take user-defined action when the monitored events occur or a threshold is reached. • Dynamic Host Configuration Protocol (DHCP)-based auto configuration and image update simplifies management of large number of switches by automatically downloading specified configuration and image.
Remote monitoring and diagnostics	<ul style="list-style-type: none"> • The Cisco IOS Software CLI provides a common user interface and command set with all Cisco routers and Cisco Catalyst® desktop switches. • Cisco Service Assurance Agent (SAA) provides service-level (latency/frame loss) management throughout the network. • IEEE 802.1ag Connectivity Fault Management provides standard support for transport fault management. It allows for discovery and verification of path for Layer 2 paths, allowing utilities to monitor the safe transmission of GOOSE messages, both inside the substation and between substations. • Ethernet Local Management Interface enables utilities to communicate service configuration and status information to the switches/routers. • IEEE 802.3ah Ethernet in the first mile provides standard support for monitoring, remote failure indication, loopback, and OAM discovery on a per-Ethernet-link between the complaint switching and routing equipment. The CGS 2520 as well as CGR 2010 are IEEE 802.3ah compliant. • ITU-T Y.1731 introduces the support for fault management functions, including alarm indication signal (AIS), remote defect indication (RDI) and locked signal (LCK) to detect and signal a failure in a Layer 2 path. This allows utilities to proactively monitor the health of Layer 2 network. • Cisco IP SLA provides service-level management throughout the network. CGS 2520 supports IP SLA for both Layer 2 and Layer 3-based services allowing network operators to monitor parameters such as latency and frame loss for critical protection and control traffic (such as GOOSE). • Port and VLAN loopbacks allow utility network operators to proactively monitor the end to end network characteristics on a per port/per VLAN basis. This would be very useful to proactively determine the health of the network for critical time-sensitive traffic such as GOOSE messages. • Digital optical monitoring (DOM) support enable service providers to perform in-service transceiver monitoring and troubleshooting operations. DOM threshold functions allow the monitoring of real time optical parameters on DOM SFPs and the comparison against factory-reset values, generating alarm and warning thresholds.
Cisco Configuration Professional software	<ul style="list-style-type: none"> • Cisco Configuration Professional is a free, Windows-based easy-to-use graphical user interface application that simplifies the administration of substation network. Cisco Configuration Professional has been enhanced with utility-specific configuration and monitoring features for ease of use. • In addition to the CGR 2010 ESM, Cisco Configuration Professional (version 2.5 and higher) also supports CGR 2010 rugged routers and Cisco 2520 rugged switches, providing single management tool for both the substation switches and routers. • Using Cisco configuration professional, the CGR 2010 ESM can be remotely managed from any supported desktop or laptop. • Upgrading the Cisco IOS Software on CGR 2010 ESM is a simple matter of pointing and clicking, with one-click upgrades.

Feature	Benefit
	<ul style="list-style-type: none"> Task-based Cisco Configuration Professional user interface provides for faster and easier configuration of specific functionality such as QoS, Security. The interface also provides a quick snapshot of switch configuration through the dashboard view on the homepage. Role-based access feature uses the Cisco IOS Software CLI views feature to define restricted task-based roles for different switch administrators and users.
Cisco Express setup	<ul style="list-style-type: none"> Cisco Express Setup simplifies initial configuration of a switch through a web browser, eliminating the need for more complex terminal emulation programs and CLI knowledge. The web interface helps less-skilled personnel quickly and simply set up switches, thereby reducing the cost of deployment.
CiscoWorks support	<ul style="list-style-type: none"> CiscoWorks network-management software provides management capabilities on a per-port and per-switch basis, providing a common management interface for Cisco routers, switches, and hubs. SNMP v1, v2c, and v3 and Telnet interface support delivers comprehensive in-band management, and a CLI-based management console provides detailed out-of-band management. Cisco Discovery Protocol Versions 1 and 2 help enable a CiscoWorks network-management station for automatic switch discovery. The CiscoWorks LAN Management Solution (version 3.2 and 4.x and higher) supports the CGR 2010 ESM.

Table 5 lists the primary features in the LAN Base and IP Services images.

Table 5. Primary Features for LAN Base and IP Services Image

LAN Base		IP Services
Per port per VLAN ingress policing	Resilient Ethernet Protocol	All LAN Base features plus:
SCADA protocol classification using ACLs	Flexlink	Static routing, Inter-VLAN routing
Per GOOSE VLAN classification/statistics	Link-state tracking	Multi-VRF CE (VRF-lite)
Configurable egress queue bandwidth	UDLD	Policy-based routing
Configurable egress buffers/thresholds	xSTP: 802.1s/802.1w	RIP Versions 1 and 2
Strict priority queuing with optional policer	EtherChannel/LACP/PAgP	EIGRP, OSPF, and IS-IS
IEEE 802.1x and identity-based network services	Modbus memory map support	BGPv4
Web- and MAC-based authentication	Express Setup	IPv6 routing
Port security + Cisco enhancements	Cisco Configuration Professional	HSRP
DHCP snooping, dynamic ARP inspection, IP source guard	Utility Specific Smartport macros	Multicast routing: PIM (SM, DM)
Spanning Tree Protocol security mechanisms	DHCP Auto Config/Image upgrade	Source Specific Multicast
Storm control	Config Rollback/Replace	Source Specific Multicast mapping
Wire-speed L2-L4 ACLs	SPAN/RSPAN	Bidirectional Forwarding Detection
Private VLAN	Layer 3 IP SLA	Multicast support for VRF (mVRF-Lite)
Secure connectivity: SSH/SSL/SCP	IETF TWAMP Responder Support	VRF-aware services (ARP, ping, SNMP, HSRP, uRPF syslog, traceroute, FTP, and TFTP)
RADIUS/TACACS+	Port and VLAN Loopback	
SNMPv3 crypto	Time Domain Reflectometry (Copper ports)	
Configuration file security	Digital Optical Monitoring (DOM), Optical ports	
UNI/ENI and NNI port types (configurable on all ports)	Ethernet OAM Connectivity Fault Management (CFM): IEEE 802.1ag Ethernet in the first mile (EFM): IEEE 802.3ah Ethernet LMI (PE) -MEF Ethernet LMI (CE): MEF CFM to E-LMI Interworking CFM to EFM Interworking 802.1ag + IP SLA (Ethernet SLAs)	
Configurable per VLAN MAC learning		

LAN Base		IP Services
MAC address learning and aging notifications		
Configurable control plane security		
IEEE 802.1AR for hardware-based security on the CGR 2010		

Product Specifications

Table 6 lists product specifications for CGR 2010 ESM.

Table 6. Product Specifications

Description	Specification
Performance	<ul style="list-style-type: none"> Forwarding bandwidth: <ul style="list-style-type: none"> Cisco GRWIC-D-ES-2S-8PC: 8 Gbps Cisco GRWIC-D-ES-6S: 8 Gbps Forwarding rate: <ul style="list-style-type: none"> Cisco GRWIC-D-ES-2S-8PC: 6.5 mpps Cisco GRWIC-D-ES-6S: 6.5 mpps 256-MB DDR2 SDRAM Configurable up to 4000 MAC addresses Configurable up to 4000 unicast routes Configurable up to 1000 IGMP groups and multicast routes Configurable maximum transmission unit (MTU) of up to 9000 bytes, for bridging on Gigabit Ethernet ports, and up to 1518 bytes for bridging and routing on Fast Ethernet ports
Connectors and cabling	<p>10/100 Ports:</p> <ul style="list-style-type: none"> 10/100BASE-TX ports: RJ-45 connectors, 2-pair Category 5 unshielded twisted pair (UTP) cabling <p>100FX SFP Ports (GRWIC-D-ES-6S only):</p> <ul style="list-style-type: none"> 100BASE-FX and -LX: Duplex LC receptacle fiber connectors (multimode and single mode) 100BASE-BX: Single-fiber LC receptacle connector (single-mode fiber) 100BASE-EX and -ZX: Single mode fiber, which respectively spans up to 40 kilometers long and 80 kilometers long <p>Gigabit Ports:</p> <ul style="list-style-type: none"> 1000BASE-T SFP-based ports: RJ-45 connectors, 4-pair Category 5 UTP cabling, 10/100/1000BASE-T operation in host systems with SGMII interface 1000BASE-BX: Single-fiber LC receptacle connector (single-mode fiber) 1000BASE-EX: Single Mode Fiber with DOM support 1000BASE-SX, -LX/LH, and -ZX and CWDM and DWDM: Duplex LC receptacle fiber connectors (multimode and single-mode fiber) Cisco Catalyst 3560 SFP Interconnect Cable for establishing low-cost Gigabit Ethernet point-to-point connections
Indicators	<ul style="list-style-type: none"> Per-port status LEDs: Link integrity, port disabled, and activity indications System-status LED: System activity, system integrity, PoE (GRWIC-D-ES-2S-8PC only): PoE activity, PoE integrity, and PoE disabled
Dimensions (H x W x D)	<ul style="list-style-type: none"> Cisco GRWIC-D-ES-2S-8PC: 3.0 x 4.0 x 7.8 in. (7.62 x 10.16 x 19.8 cm) Cisco GRWIC-D-ES-6S: 3.0 x 4.0 x 7.8 in. (7.62 x 10.16 x 19.8 cm)
Module height	<ul style="list-style-type: none"> Cisco GRWIC-D-ES-2S-8PC: Double-wide GRWIC Cisco GRWIC-D-ES-6S: Double-wide GRWIC
Weight	<ul style="list-style-type: none"> Cisco GRWIC-D-ES-2S-8PC: 2.1lbs (0.95kg) Cisco GRWIC-D-ES-6S: 2lbs (0.91kg)

Power Specifications

Table 7 gives power specifications for the CGR 2010 ESM.

Table 7. Power Specifications (preliminary data and subject to change)

Description	Specification
Power consumption	<ul style="list-style-type: none">• Cisco GRWIC-D-ES-2S-8PC: 7 Watts (with no PoE devices)• Cisco GRWIC-D-ES-6S: 9 Watts

Management and Standards

Table 8 provides management and standards support information for the CGR 2010 ESM.

Table 8. Management and Standards

Description	Specification
Management	<ul style="list-style-type: none">• BRIDGE-MIB (RFC1493)• BGP4-MIB (RFC1657)• CISCO-CABLE-DIAG-MIB• CISCO-BULK-FILE-MIB• CISCO-CDP-MIB• CISCO-CONFIG-COPY-MIB• CISCO-CONF-MAN-MIB• CISCO-DATA-COLLECTION-MIB• CISCO-ENVMON-MIB• CISCO-ERR-DISABLE-MIB• CISCO-ETHERNET-ACCESS-MIB• CISCO-FLASH-MIB• CISCO-FTP-CLIENT-MIB• CISCO-HSRP-MIB• CISCO-HSRP-EXT-MIB• CISCO-IETF-DOT3-OAM-MIB• CISCO-IGMP-FILTER-MIB• CISCO-IPLSA-ETHERNET-MIB• CISCO-PAGP-MIB• CISCO-PAE-MIB• CISCO-PING-MIB• CISCO-POE-EXTENSIONS-MIB• CISCO-PRIVATE-VLAN-MIB• CISCO-PROCESS-MIB• CISCO-PORT-QOS-MIB• CISCO-PORT-SECURITY-MIB• CISCO-PORT-STORM-CONTROL-MIB• CISCO-IMAGE-MIB• CISCO-LAG-MIB• CISCO-L2L3-INTERFACE-CONFIG-MIB• CISCO-MAC-NOTIFICATION-MIB• CISCO-MEMORY-POOL-MIB• CISCO-RTTMON-MIB• CISCO-STP-EXTENSIONS-MIB• CISCO-SYSLOG-MIB• CISCO-TCP-MIB• CISCO-UDLD-MIB• CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB• CISCO-VLAN-MEMBERSHIP-MIB• ENTITY-MIB (RFC2737)• ETHERLIKE-MIB• IEEE8021-PEA-MIB• IEEE8023-LAG-MIB• IF-MIB (RFC 1573)• IGMP-MIB• IPMROUTE-MIB• OLD-CISCO-CHASSIS-MIB• OLD-CISCO-FLASH-MIB• OLD-CISCO-INTERFACES-MIB• OLD-CISCO-IP-MIB• OLD-CISCO-SYS-MIB• OLD-CISCO-TCP-MIB• OLD-CISCO-TS-MIB• OSPF-MIB (RFC 1253)• PIM-MIB• RFC1213-MIB (MIB-II)• RMON-MIB (RFC 1757)• RMON2-MIB (RFC 2021)• SNMP-FRAMEWORK-MIB (RFC2571)• SNMP-MPD-MIB (RFC 2572)• SNMP-NOTIFICATION-MIB (RFC 2573)• SNMP-TARGET-MIB (RFC 2573)• SNMPv2-MIB (RFC 1907)• SNMP-USM-MIB (SNMP-USER-BASED-SM-MIB) (RFC2574)• SNMP-VACM-MIB (SNMP-VIEW-BASED-ACM-MIB) (RFC2575)• TCP-MIB (RFC 2012)• UDP-MIB (RFC 2013)
Standards and protocols	<ul style="list-style-type: none">• IEEE 802.1s• IEEE 802.1w• IEEE 802.1x• IEEE 802.3ad• IEEE 802.3ah

Description	Specification
	<ul style="list-style-type: none"> • IEEE 802.1ag • IEEE 802.3x full duplex on 10BASE-T, 100BASE-TX, and 1000BASE-T ports • IEEE 802.1D Spanning Tree Protocol • IEEE 802.1p CoS classification • IEEE 802.1Q VLAN • IEEE 802.3 10BASE-T • IEEE 802.3u 100BASE-T • IEEE 802.3ab 1000BASE-T • IEEE 802.3z 1000BASE-X • IEEE 802.3af (on GRWIC-D-ES-2S-8PC only) • IEEE 1588v2 hardware ready • IP routing: Static, RIP versions 1 and 2, EIGRP, OSPF, BGPv4, PIM-SM, and PIM-DM (metro IP access only) • IPv6: MLD Snooping v1 and v2 • IPv6: RIP, OSPFv3, static routes Management: SNMP versions 1, 2, and 3

SFPs for Cisco CGR 2010 ESM

Table 9 describes SFP support.

Table 9. SFP Support

Description	Description	Temperature Range*
GLC-FE-100FX-RGD=	100Base-FX Multi Mode Rugged SFP	IND
GLC-FE-100LX-RGD=	100Mbps Single Mode Rugged SFP	IND
GLC-SX-MM-RGD=	1000Mbps Multi-Mode Rugged SFP (supported on gigabit SFP ports only)	IND
GLC-LX-SM-RGD=	1000Mbps Single Mode Rugged SFP (supported on gigabit SFP ports only)	IND
GLC-ZX-SM-RGD=	1000BASE-ZX Single Mode Rugged SFP (supported on gigabit SFP ports only)	IND

Temperature Range	CGS 2520 Operating Temperature Range Support
IND	-40°F to +140°F (-40°C to +60°C)

Safety and Compliance

Table 10 gives safety and compliance information for the CGR 2010 ESM.

Table 10. Safety and Compliance Specifications

Description	Specification
Environmental substation compliance	<ul style="list-style-type: none"> • IEC 61850-3 (reference certificate of approval) • IEEE1613 (reference certificate of approval)
EMC interface immunity	<ul style="list-style-type: none"> • IEC61000-4-2 [Criteria A—Class 2]* • IEC61000-4-3/ENV50204 [Criteria A] • IEC61000-4-4 [Criteria A/Criteria B] • IEC61000-4-5 [Criteria B] • IEC61000-4-6 [Criteria A] <p>*On optical interfaces</p>
Standard electromagnetic emissions certifications	<ul style="list-style-type: none"> • FCC Part 15 Class A • EN 55022B Class A (CISPR22 Class A) • EN 55024

Description	Specification
	<ul style="list-style-type: none"> • EN 300 386 • VCCI Class I • AS/NZS 3548 Class A or AS/NZS CISPR22 Class A • KCC • CE Marking
Standard safety certifications	<ul style="list-style-type: none"> • UL 60950-1 • CSA 60950-1 • EN 60950-1 • IEC 60950-1
Storage environment	<ul style="list-style-type: none"> • Temperature: -40 to +85 °C

Ordering Information

These products can be ordered by a Cisco authorized partner. Please refer to the partner locator on [cisco.com](http://www.cisco.com): <http://www.cisco.com/web/partners/index.html>. For more information about product availability, please contact your Cisco representative.

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, refer to Cisco Technical Support Services or Cisco Advanced Services at <http://www.cisco.com/go/services>.



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 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: 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)