System Release 7.17.2
ASTRO® 25
INTEGRATED VOICE AND DATA

GGM 8000 System Gateway

Feature Guide

SEPTEMBER 2020

MN004336A01-B

Copyrights

The Motorola Solutions products described in this document may include copyrighted Motorola Solutions computer programs. Laws in the United States and other countries preserve for Motorola Solutions certain exclusive rights for copyrighted computer programs. Accordingly, any copyrighted Motorola Solutions computer programs contained in the Motorola Solutions products described in this document may not be copied or reproduced in any manner without the express written permission of Motorola Solutions.

No part of this document may be reproduced, transmitted, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without the prior written permission of Motorola Solutions, Inc.

Furthermore, the purchase of Motorola Solutions products shall not be deemed to grant either directly or by implication, estoppel or otherwise, any license under the copyrights, patents or patent applications of Motorola Solutions, except for the normal non-exclusive, royalty-free license to use that arises by operation of law in the sale of a product.

Disclaimer

Please note that certain features, facilities, and capabilities described in this document may not be applicable to or licensed for use on a specific system, or may be dependent upon the characteristics of a specific mobile subscriber unit or configuration of certain parameters. Please refer to your Motorola Solutions contact for further information.

Trademarks

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners.

European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases).

As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste.

Customers or end-users in EU countries should contact their local equipment supplier representative or service centre for information about the waste collection system in their country.

Contact Us

The Solutions Support Center (SSC) is the primary contact for technical support included in your organization's service agreement with Motorola Solutions.

Service agreement customers should be sure to call the SSC in all situations listed under Customer Responsibilities in their agreement, such as:

- Before reloading software
- To confirm troubleshooting results and analysis before taking action

Your organization received support phone numbers and other contact information appropriate for your geographic region and service agreement. Use that contact information for the most efficient response. However, if needed, you can also find general support contact information on the Motorola Solutions website, by following these steps:

1. Enter motorolasolutions.com in your browser.
2. Ensure that your organization's country or region is displayed on the page. Clicking or tapping the name of the region provides a way to change it.
3. Select "Support" on the motorolasolutions.com page.

Comments

Send questions and comments regarding user documentation to documentation@motorolasolutions.com.

Provide the following information when reporting a documentation error:

- The document title and part number
- The page number or title of the section with the error
- A description of the error

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to https://learning.motorolasolutions.com to view the current course offerings and technology paths.

Document History

Version	Description	Date
MN004336A01-A	Original release of the *GGM 8000 System Gateway Feature Guide*.	November 2017
MN004336A01-B	Updated section: • Downloading a Stored Configuration File to the GGM 8000 on page 93	September 2020

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About GGM 8000 System Gateway Feature Guide

This manual provides an introduction to the GGM 8000 ASTRO® 25 Gateway. The manual contains a description of the hardware, installation and configuration procedures and where it is used in an ASTRO ® 25 system.

What Is Covered In This Manual?

This manual contains the following chapters:

- GGM 8000 Introduction and Common Procedures on page 28 provides a high-level description of the GGM 8000 gateway and contains the GGM 8000-related procedures common to all configurations.
- ASTRO 25 Master Site (L Zone Core) on page 173 provides information about the GGM 8000 gateway in an ASTRO® 25 Master Site (L Zone Core).
- ASTRO 25 Repeater Site on page 189 provides information about the GGM 8000 gateway in an ASTRO® 25 Repeater Site.
- ASTRO 25 HPD Site on page 193 provides information on the GGM 8000 gateway in an ASTRO® 25 HPD Site.
- ASTRO 25 Dispatch Console Subsystem on page 197 provides information about the GGM 8000 gateway in an ASTRO® 25 Dispatch Console subsystem.
- ASTRO 25 IP Simulcast Subsystem on page 200 provides information about the GGM 8000 gateway in an ASTRO® 25 IP Simulcast subsystem.
- ASTRO 25 K Core and Sites on page 221 provides information about the GGM 8000 gateway in an ASTRO® 25 K Core Conventional Master Site.
- ASTRO 25 Conventional Subsystem Architectures on page 234 provides information about the GGM 8000 gateway in ASTRO® 25 Conventional architectures.
- ASTRO 25 Standalone Conventional Voting System on page 248 provides information about the GGM 8000 gateway in an ASTRO® 25 Standalone Conventional Voting System.
- ASTRO 25 Customer Enterprise Network on page 255 provides information about the GGM 8000 gateway in ASTRO® 25 Customer Enterprise Network.
- ASTRO 25 Interoperability on page 260 provides information about the GGM 8000 gateway ASTRO® 25 Interoperability.
- System Gateways Disaster Recovery on page 267 provides information about the GGM 8000 gateway disaster recovery.

Helpful Background Information

Motorola Solutions offers various courses designed to assist in learning about the system. For information, go to http://www.motorolasolutions.com/training to view the current course offerings and technology paths.

Related Information

For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.

Related Information	Purpose
Standards and Guidelines for Communication Sites	Provides standards and guidelines that should be followed when setting up a Motorola Solutions communications site. Also known as R56 manual. This document may be purchased by calling the North America Parts Organization at 800-422-4210 (or the international number: 302-444-9842).
System Overview and Documentation Reference Guide	Provides an overview of the ASTRO® 25 new system features, documentation set, technical illustrations, and system-level disaster recovery that support the ASTRO® 25 radio communication system.
S6000 and S2500 Routers Feature Guide	Provides information relating to the installation, configuration, and management of the S6000 and S2500 routers used in various network locations.
Enterprise OS Software Reference Guide *Enterprise OS Software User Guide* *Motorola GGM 8000 Hardware User Guide*	Available on the Motorola Online website: http://businessonline.motorolasolutions.com To access the manual, select **Resource Center** → **Product Information** → **Manuals** → **Network Infrastructure** → **Routers and Gateways**.
GGM 8000 with IP Link Converter (IPLC) Functionality User Guide	Provides an overview of the IP Link Converter (IPLC) feature and describes how to cable, configure, and troubleshoot a GGM 8000 with IPLC functionality.
MCC 7500E Dispatch Console User Guide	Provides setup and operational details for the MCC 7500E Dispatch Console feature and describes the requirements and considerations necessary for implementing this feature in ASTRO® 25 systems.

Chapter 1

GGM 8000 Introduction and Common Procedures

This chapter provides a high-level description of the GGM 8000 gateway and contains the GGM 8000-related procedures common to all configurations.

1.1 GGM 8000 Equivalents for MNR Routers

The Motorola Solutions GGM 8000 Gateway is a modular multi-purpose network communications platform, designed to interconnect devices and networks within ASTRO® 25 public safety network systems. It replaces the MNR S6000 and MNR S2500 platforms in the network positions listed in the following table. In addition, the GGM 8000 supports the following functionality:

- A GGM 8000 equipped with an Enhanced Conventional Gateway module supports IP Link Converter (IPLC) functionality in a 3.x conventional system. A GGM 8000 with IPLC functionality allows users with fielded MCC 5500 consoles to replace circuit backhaul connectivity with IP backhaul connectivity and transition site devices (stations and comparators) used to support digital-only and mixed mode conventional channels to G-series and MLC 8000 devices. Users also have the option to retain circuit backhaul networks (T1s/E1s).
  The GGM 8000 with IPLC functionality is not covered in this manual. For configuration, functionality, cabling and installation, troubleshooting, and deployment topologies, see the *GGM 8000 with IP Link Converter (IPLC) Functionality User Guide*.
- A GGM 8000 with a connection to a WAN and with a conventional channel interface (v.24, analog, and/or IP) functions as a Site and Conventional Channel Gateway.

Table 1: GGM 8000 Equivalents for MNR S6000s and S2500s by ASTRO 25 Network Position

MNR Platform	Network Position	GGM 8000 Equivalent	Functionality
MNR S6000	Core router	Core Gateway	Zone-to-Site traffic (Intra-Zone).
	Exit router	Exit Gateway	Zone-to-Zone traffic (Inter-Zone).
	Core/Exit router	Core/Exit Gateway	GGM 8000 combines the role of the core and exit routers. Dual Function: Zone-to-Site traffic (Intra-Zone) and Zone-to-Zone traffic (Inter-Zone).
	Gateway router	GGM 8000 Gateway	GGM 8000 is used for network traffic between the various subnets within the zone core (ZC/PDG/Console traffic).
	Border router	Border Gateway	GGM 8000 serves as an interface between a peripheral network and the Motorola Radio Network Infrastructure (RNI).

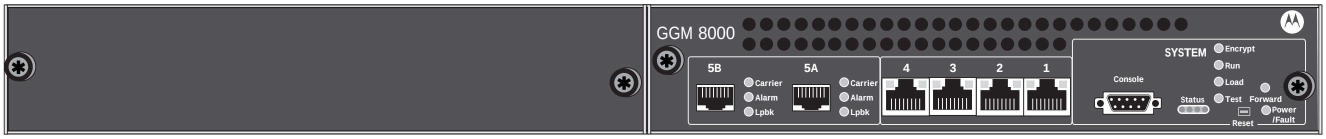
MNR Platform	Network Position	GGM 8000 Equivalent	Functionality
	IP simulcast remote site access router (T1/E1 or Ethernet links)	Remote Site Access Gateway **NOTICE:** The GGM 8000 replaces the MNR S6000 for all Ethernet configurations; all T1/E1 configurations require an MNR S6000.	GGM 8000 serves as the interface between the prime site and the remote site.
	IP simulcast prime site router (T1/E1 or Ethernet links)	Site Gateway **NOTICE:** The GGM 8000 replaces the MNR S6000 for all Ethernet configurations and links requiring one or two T1/E1s. If the link between the master site and the prime site requires three or more T1/E1s, an MNR S6000 must be used.	GGM 8000 provides a connection to a Wide Area Network (WAN) with no conventional channel interface (V.24, analog, and/or IP).
	Trunking subsystem prime site router (Ethernet links)	Site Gateway **NOTICE:** The GGM 8000 replaces the MNR S6000 for all Ethernet configurations and links.	GGM 8000 provides a connection to a Wide Area Network (WAN) with no conventional channel interface (V.24, analog, and/or IP).
	Trunking subsystem remote site access router (Ethernet links)	Remote Site Access Gateway **NOTICE:** The GGM 8000 replaces the MNR S6000 for all Ethernet configurations.	GGM 8000 serves as the interface between the prime site and the remote site.
MNR S2500	Dispatch site router	Site Gateway	GGM 8000 provides a connection to a Wide Area Network (WAN) with no conventional channel interface (V.24, analog, and/or IP).
	(Repeater) site router		
	IP simulcast remote site router (T1/E1 or Ethernet links)		
	Trunking subsystem subsite router (Ethernet links)		

MNR Platform	Network Position	GGM 8000 Equivalent	Functionality
	ISSI.1 router		
	SmartX router		
	CCGW	Conventional Channel Gateway	GGM 8000 Conventional Channel Gateway supports additional channel types (mixed mode: V.24 and IP, IP conventional, MDC 1200, and ACIM) as well as the analog conventional and digital conventional channels supported by the MNR S2500 CCGW. With an analog and V.24 interface kit, CCGW supports four analog and four V.24 ports. With a Low Density Enhanced Conventional Gateway option, CCGW supports four enhanced analog interfaces (two physical analog ports per interface) and four V.24 ports. With a High Density Enhanced Conventional Gateway option, CCGW supports eight enhanced analog interfaces and eight V.24 ports.

1.2 Physical Description

The GGM 8000 base system, shown in the following figure,supports four 10/100/1000 Ethernet ports and two T1/E1 (CSU/DSU) ports, as well as a console port and a removable power supply subsystem (on the rear of the chassis).

Figure 1: GGM 8000 Base Unit



The GGM 8000 front panel features two side-by-side slots which support externally accessible modules.

- The right-hand slot supports the base module which provides the GGM 8000’s base configuration. The base module also configures and controls the optional expansion module and the daughterboards it carries, as well as the optional Enhanced Conventional Gateway modules. For more information, see Base Module on page 32.
- The left-hand slot supports one of the following optional modules:
  - The expansion module is a carrier card that supports one analog slot and two I/O slots to accommodate the following optional daughterboards:

  + Analog/V.24 interface kit (E&M daughterboard and DSP SIMM, and two V.24 daughterboards).
  + FlexWAN daughterboard(s).

  For more information about the expansion module, see Expansion Module on page 33

- The Enhanced Conventional Gateway module, that is available in either a low density or high density configuration, provides an enhanced analog interface. The interface can be configured to provide the same functionality as the expansion module with analog/V.24 interface kit or add a superset of analog capabilities.
  For more information about the Enhanced Conventional Gateway module, see GGM 8000 Enhanced Conventional Channel Gateway Modules on page 34.

  NOTICE: The Enhanced Conventional Gateway module requires EOS version 16.4 or higher.

The base module and the expansion module or the base module and the Enhanced Conventional Gateway module are interconnected through the GGM 8000 backplane. All modules can be removed and replaced without removing the GGM 8000 from the rack.

The GGM 8000 chassis was redesigned in 2013. Figure 2: GGM 8000 Base Unit with two TORX screws on top on page 31 illustrates the new chassis design. Figure 3: GGM 8000 Base Unit without TORX screws on top on page 32 illustrates the old chassis design. As shown in Figure 2: GGM 8000 Base Unit with two TORX screws on top on page 31, the new chassis can be identified by the two TORX® screws on the top of the chassis.

Figure 2: GGM 8000 Base Unit with two TORX screws on top

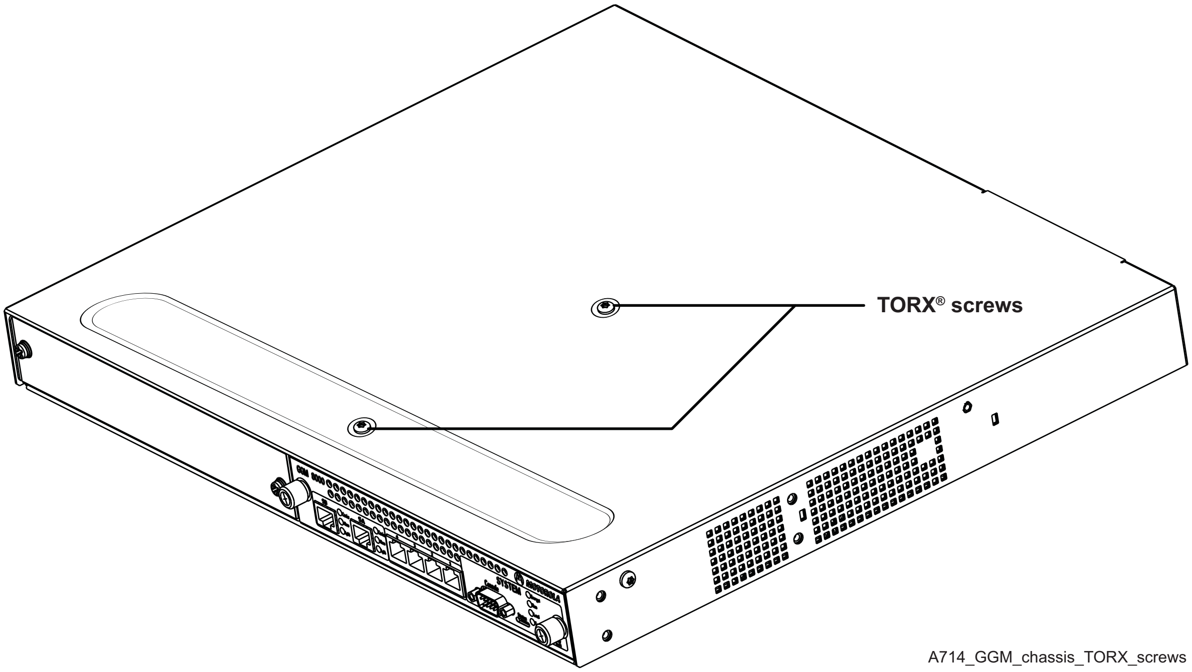
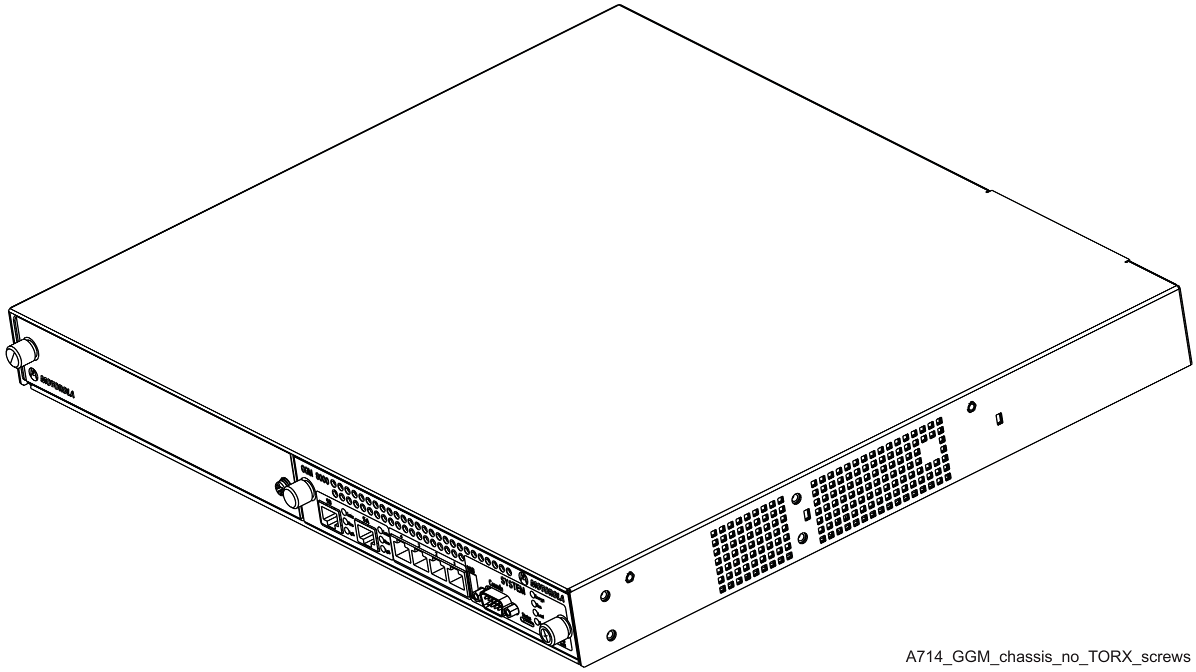


Figure 3: GGM 8000 Base Unit without TORX screws on top

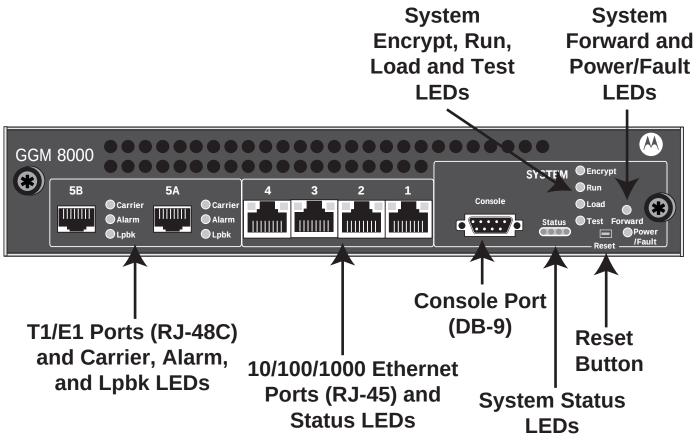


A714_GGM_chassis_no_TORX_screws

1.2.1 Base Module

The GGM 8000 base module provides the GGM 8000 base system and must be present in any GGM 8000 configuration.

Figure 4: Features of the GGM 8000 Base Module


System Encrypt, Run, Load and Test LEDs
System Forward and Power/Fault LEDs
GGM 8000
5B
5A
Carrier
Alarm
Lpbk
Carrier
Alarm
Lpbk
4
3
2
1
Console
SYSTEM
Encrypt
Run
Load
Test
Status
Forward
Reset
Power /Fault
T1/E1 Ports (RJ-48C) and Carrier, Alarm, and Lpbk LEDs
10/100/1000 Ethernet Ports (RJ-45) and Status LEDs
Console Port (DB-9)
System Status LEDs
Reset Button

base_module_A

The GGM 8000 base module provides the following features:

- **T1/E1 ports and LEDs** – Two T1/E1 CSU/DSU ports.
- **Ethernet ports and LEDs** – Four 10/100/1000 Mbps Ethernet ports.
- **Console port** – Use this port to connect the GGM 8000 to a PC, terminal, or modem.
- **System LEDs** – These LEDs indicate the status of the system as a whole.
- **Reset button** – Press and hold this button for approximately 3 seconds to reboot the GGM 8000.

WARNING: Use only a non-conductive object, such as a plastic stylus, to press the reset button. Do not use the tip of a pencil. Graphite particles from the pencil may cause you to receive an electric shock and may damage components on the motherboard.

The USB port was removed from the GGM 8000 base module in 2013. This change does not affect the functionality of the module. The new base module can be installed in a GGM 8000 with either a new chassis design (two TORX® screws on the top of the chassis; see Figure 2: GGM 8000 Base Unit with two TORX screws on top on page 31) or an old chassis design (no TORX® screws on the top of the chassis; see Figure 3: GGM 8000 Base Unit without TORX screws on top on page 32).

CAUTION: For system releases before an ASTRO® 25 7.14 system release, the new GGM 8000 base module (no USB port) is not compatible with EOS software versions lower than the following:

- ASTRO® 25 7.13 - EOS software version 16.4.0.97
- ASTRO® 25 7.12 - EOS software version 16.3.0.98
- ASTRO® 25 7.11 - EOS software version 16.2.0.63
- ASTRO® 25 7.9 - EOS software version 16.0.1.69

If you install a new base module in a GGM 8000 that is running an EOS software version below the required minimum, or if an EOS software version below the required minimum is loaded on a GGM 8000 with a new base module, the GGM 8000 will not startup successfully (the base module will not complete the boot process when it attempts to execute the EOS software). If this happens, contact the Motorola Solutions Support Center (SSC) for recovery instructions.

1.2.2 Expansion Module

The GGM 8000 expansion module is a carrier card that integrates various interface modules (daughterboards) with the GGM 8000 platform. It features three slots into which optional daughterboards can be installed: one analog slot and two I/O slots. In addition, status LEDs indicate the operational status of the expansion module.

The expansion module is powered from 12 VDC (nominal) supplied by the GGM 8000 power subsystem. It includes circuitry that:

- Prevents the expansion module from powering up until it is fully seated in the GGM 8000 chassis and the base module has finished powering up.
- Limits peak current draw during power-up.
- Electrically disconnects the expansion card from the power supply as soon as the expansion card is removed from the chassis.

The added power-on control circuitry is designed to prevent disruption to the operation of the GGM 8000 base module when the expansion module is installed or removed. Two DC-to-DC (switching) converters are built into the expansion card and provide 3.3 V and 5.0 V power to the daughterboards on the expansion module.

The GGM 8000 expansion module supports the following daughterboards:

- Analog/V.24 interface kit (consists of a four-wire E&M module and a DSP SIMM installed in the analog slot and two V.24 daughterboards installed in the I/O slots)
- FlexWAN daughterboards (one port per daughterboard; supported in one or both I/O module slots)

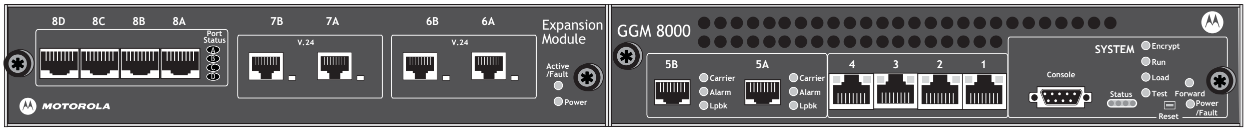
1.2.2.1 GGM 8000 Daughterboards

The GGM 8000 expansion module supports the following daughterboards:

- Analog/V.24 interface kit that consists of one 4-wire E&M daughterboard and a DSP SIMM installed in the expansion card analog slot, and two V.24 daughterboards installed in the expansion module I/O slots.
- FlexWAN daughterboard(s) that are installed in one or both expansion module I/O slots.

The following figure illustrates GGM 8000 configured with the expansion module supporting the analog/ V.24 interface kit:

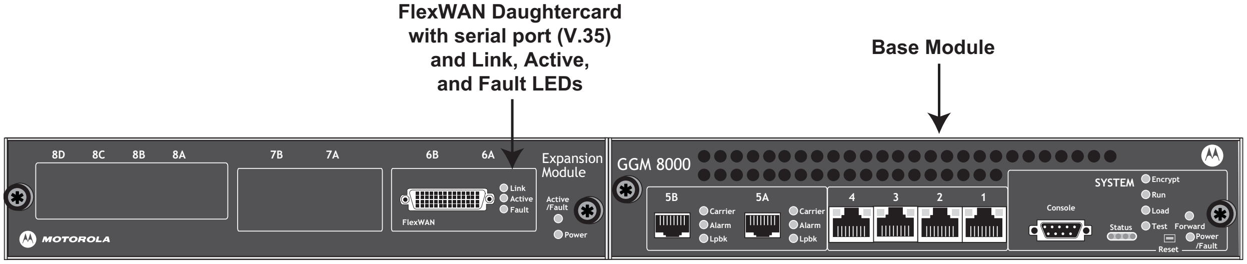
Figure 5: GGM 8000 Supporting the Analog/V.24 Kit



expansion_E_M_V24_no_callouts_A

The following figure illustrates GGM 8000 configured with the expansion module supporting one FlexWAN daughterboard:

Figure 6: GGM 8000 Supporting the FlexWan Daughterboard



expansion_FlexWAN_A

1.2.3 GGM 8000 Enhanced Conventional Channel Gateway Modules

The GGM 8000 Enhanced Conventional Gateway module:

- Consolidates the functionality of the analog/V.24 interface kit onto a single circuit board.
  Before the introduction of the Enhanced Conventional Gateway module, the GGM 8000 CCGW hardware implementation required that the expansion module loaded with the analog/V.24 interface kit be added to the base configuration to support CCGW functionality other than IP conventional channels, which require only a GGM 8000 base unit. The analog/V.24 interface kit implementation requires that five separate boards (the expansion module, the E&M daughterboard, two V.24 daughterboards, and a DSP SIMM) be added to the base configuration to create the CCGW configuration. The Enhanced Conventional Gateway module creates the CCGW configuration with a single I/O module (no expansion module is required).
- Maintains the V.24 signal interface functionality provided by the analog/V.24 interface kit and incorporates hardware design enhancements to the V.24 universal synchronous/asynchronous receivers/transmitters (USARTs) to substantially reduce interrupt overhead.
- Supports a second set of analog connectors that provides a separate audio output on each connector for audio logging recorders, as well as additional signaling capabilities.

GGM 8000 can be configured with the Low Density Enhanced Conventional Gateway and High Density Enhanced Conventional Gateway modules. The Low Density Enhanced Conventional Gateway provides support for four analog and four V.24 interfaces. The High Density Enhanced Conventional Gateway provides support for 8 analog and eight V.24 interfaces.

Table 2: Enhanced Conventional Gateway Analog Interface to RJ-45 Port Mapping

Hardware Platform	Analog Interface	Audio E&M Port	Analog/IO Port
Low Density Enhanced Conventional Gateway and High Density Enhanced Conventional Gateway	1	8A	9A
	2	8B	9B
	3	8C	9C
	4	8D	9D
High Density Enhanced Conventional Gateway	5	12A	13A
	6	12B	13B
	7	12C	13C
	8	12D	13D

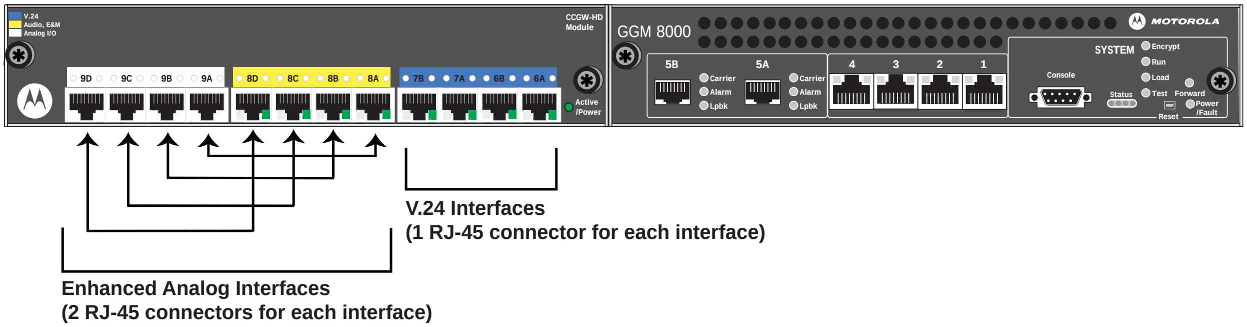
1.2.3.1

Low Density Enhanced Conventional Gateway Module

The Low Density Enhanced Conventional Gateway supports:

- Four enhanced analog interfaces, with two RJ-45 connectors per interface.
  - The first RJ-45 connector (located in the middle (yellow) group of connectors, which is labeled “Audio, E&M” on the Enhanced Conventional Gateway module front panel, supports 4-wire, 2-wire, or 4-wire/2-wire audio.
  - The second RJ-45 connector (located in the left (white) group of connectors, which is labeled “Analog I/O” on the Enhanced Conventional Gateway module front panel, supports additional audio and signaling functions.
- Four V.24 interfaces, with one RJ-45 connector per interface, located in the right (blue) group of connectors, which is labeled “V.24” on the Enhanced Conventional Gateway module front panel.

Figure 7: Low Density Enhanced Conventional Gateway



SD_ECCGW_interface_pairs_A

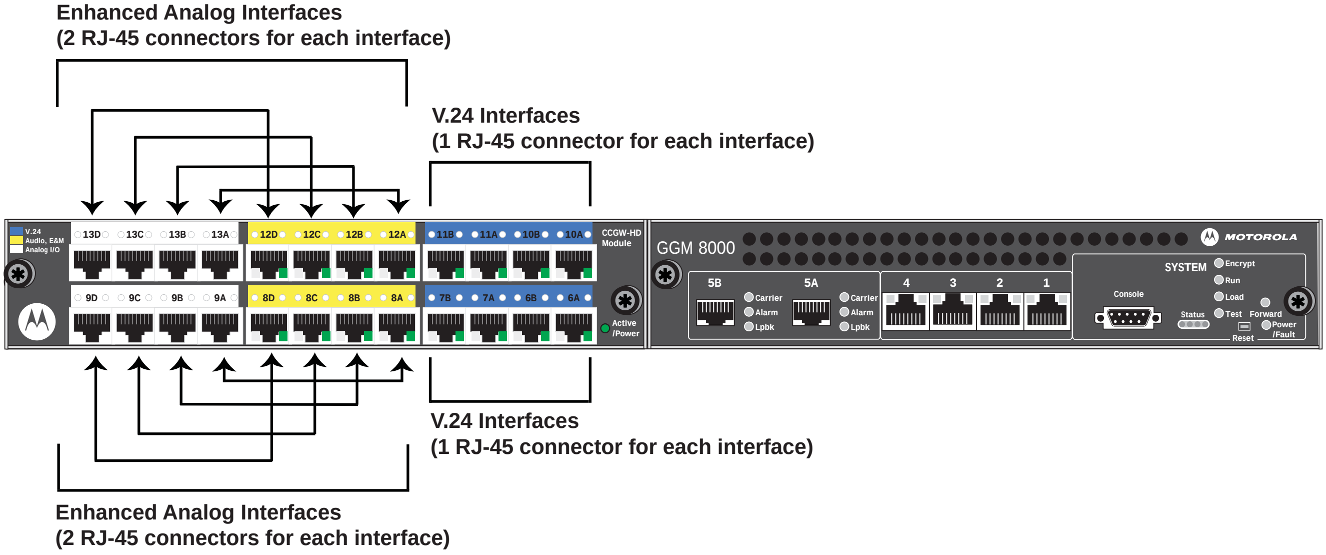
See Table 2: Enhanced Conventional Gateway Analog Interface to RJ-45 Port Mapping on page 35 for a list of the RJ-45 connector pair port numbers for each analog interface supported on the Low Density Enhanced Conventional Gateway.

1.2.3.2 High Density Enhanced Conventional Gateway Module

The High Density Enhanced Conventional Gateway supports:

- Eight enhanced analog interfaces, with two RJ-45 connectors per interface.
  - The first RJ-45 connector (located in the middle (yellow) group of connectors, which is labeled “Audio, E&M” on the Enhanced Conventional Gateway module front panel, supports 4-wire, 2-wire, or 4-wire/2-wire audio.
  - The second RJ-45 connector (located in the left (white) group of connectors, which is labeled “Analog I/O” on the Enhanced Conventional Gateway module front panel, supports additional audio and signaling functions.
- Eight V.24 interfaces, with one RJ-45 connector per interface, located in the right (blue) group of connectors, which is labeled “V.24” on the Enhanced Conventional Gateway module front panel.

Figure 8: High Density Enhanced Conventional Channel Gateway



HD_ECCGW_interface_pairs_A

See Table 2: Enhanced Conventional Gateway Analog Interface to RJ-45 Port Mapping on page 35 for a list of the RJ-45 connector pair port numbers for each analog interface supported on the Low Density Enhanced Conventional Gateway.

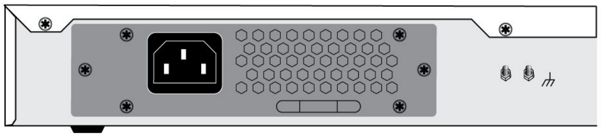
1.2.4 Power Subsystem Module

GGM 8000 supports a removable AC or DC power subsystem module, which occupies a slot in the rear of the chassis.

- The AC power subsystem module provides a single AC power receptacle.
- The DC power subsystem module provides two DC power entry connectors.

The following figure shows the GGM 8000 AC power subsystem module installed in the rear of the chassis.

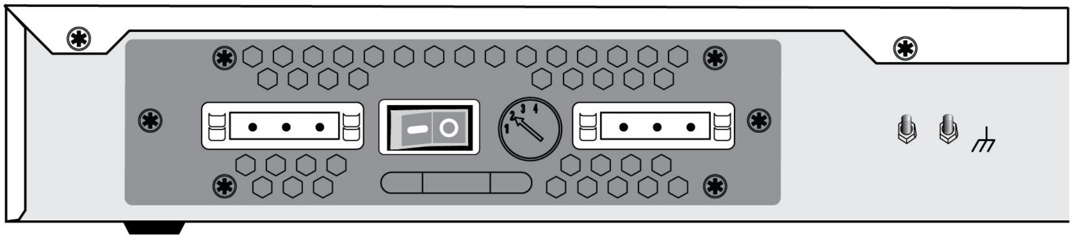
Figure 9: GGM 8000 AC Power Subsystem Module



ac_power

The following figure shows the GGM 8000 DC power subsystem module installed in the rear of the chassis.

Figure 10: GGM 8000 DC Power Subsystem Module



dc_power

1.2.5
Physical Specifications

Table 3: GGM 8000 Physical Specifications

Specification	Value
Dimensions (width x height x depth)	44 cm (17.3 in) x 4.3 cm (1.7 in) x 37 cm (14.6 in)
Weight	7.3 kg (16 lb)

1.2.6
Environmental/Operating Specifications

Table 4: GGM 8000 Environmental/Operating Specifications

Specification	Value
Temperature	-30 °C to 60 °C (-22 °F to 140 °F) operating for base unit installed in open rack
	-30°C to 55°C (-22°F to 131°F) operating for base unit installed in cabinet with doors
	0 °C to 50 °C (32 °F to 122° F) operating for base unit configured with optional daughterboards or Enhanced Conventional Gateway module installed in open rack
	0 °C to 45°C (32 °F to 113° F) operating for base unit configured with optional daughterboards or Enhanced Conventional Gateway module installed in cabinet with doors

Specification	Value
	-40 °C to 85 °C (-40 °F to 185°F) non-operating
Humidity	5% to 95% non-condensing
Heat Dissipation	134 BTU/hour (maximum)
Power Consumption	48 Watts (maximum)
AC power operating range	100 VAC to 230 VAC (-10%, +6%), 50/60 Hz
AC power current draw	Less than 0.50 A at 120 VAC; less than 0.25 A at 220 VAC
DC power operating range	24 VDC to 48 VDC (source); 20 VDC to 60 VDC (maximum)
DC power current draw	Less than 2.0 A at 24 VDC; less than 1.0 A at 48 VDC

1.3 ASTRO 25 Flexible Channel Capacity

The number of channels supported on the GGM 8000 depends on the CCGW hardware and **SiteType** configured in the LDAP database, through Provisioning Manager.

The GGM 8000 with the Low Density Enhanced Conventional Gateway option requires the site type to be configured as Combination-HD. This configuration supports:

- Up to four channels using an analog interface.
- Up to four channels using a V.24 interface.
- Up to 16 IP conventional channels.

The GGM 8000 with the High Density Enhanced Conventional Gateway option requires the site type to be configured as Combination-HD. This configuration supports:

- Up to eight channels using an analog interface.
- Up to eight channels using a V.24 interface.
- Up to 16 IP conventional channels.

The Conventional Channel Gateway (GGM 8000 with analog/V.24 interface kit) requires **SiteType** to be configured as **Combination**. This configuration supports:

- Up to four channels using an analog interface.
- Up to four channels using a V.24 interface.
- Up to ten IP conventional channels.

NOTICE: Site Gateways (Conventional Channel Interface) are required in order for the system to support the maximum capacity of 1000 conventional channels in a multi-zone system and 300 in single-zone systems.

Table 5: CCGW Interface Used By Channel Type

Channel Type	Interface
Analog conventional	One analog interface
Digital convenitonal	One V.24 interface
IP conventional	One Ethernet interface
Mixed mode	One analog interface + One V.24 or One IP (Ethernet) interface
MDC 1200	One analog interface

Channel Type	Interface
ACIM	One analog interface + One V.24 interface

Where:

- **Analog interface** on the Enhanced Conventional Gateway module, consists of:
  - A pair of RJ-45 ports.
  - One port (8A-D or 12A-D) that supports analog audio.
  - The paired port (9A-D or 13A-D) that supports additional audio and signaling functions.

  On the E&M daughterboard included as part of the analog/V.24 interface kit, it consists of one RJ-45 port.
- **Ethernet interface** in IP conventional channels, is not bound to any physical ports on the GGM 8000.
- **Mixed mode** is a single channel type from the perspective of the LDAP server; however, the GGM 8000 supports two types of mixed mode channels, with different underlying signaling functionality, running over different digital interfaces: V.24 mixed mode and IP mixed mode.

Table 6: Maximum Number of Channels Supported for Available CCGW Hardware Platforms

Channel Type	High Density Conventional Channel Gateway	Low Density Conventional Channel Gateway	GGM 8000 Base Unit	GGM 8000 with Expansion Module and Analog/ V.24 Interface Kit
Analog	8	4	0	4
Digital conventional	8	4	0	4
Mixed Mode	8	4	0	4
MDC 1200	8	4	0	4
ACIM	8	4	0	4
IP Conventional	16	16	16	10
Maximum number of Channels per Chassis	32	24	16	14

Where:

- **Mixed Mode Channel** can be either analog + V.24 (V.24 mixed mode) or analog + IP (IP mixed mode).
- **32 High Density Conventional Channels** consist of eight channels that use an analog interface, eight channels that use a V.24 interface, and 16 IP conventional channels.
- **24 Low Density Conventional Channels** consist of four channels that use an analog interface, four channels that use a V.24 interface, and 16 IP conventional channels.
- **14 GGM 8000 with Expansion Module and Analog/V.24 Interface Kit Channels** consist of ten IP conventional channels and four channels of any other type.
- **16 GGM 8000 Base Unit Channels** are supported when SiteType is configured as Combination-HD; when SiteType is configured as Combination, the GGM 8000 base unit supports ten (IP conventional) channels.

NOTICE: The GGM 8000 base unit with SiteType Combination-HD supports 16 IP conventional channels, while the GGM 8000 base unit with SiteType Combination supports ten IP conventional channels.

For more information, see Conventional Channel Gateway – Supported Channels and Sites on page 46.

1.3.1 Conventional Channel Gateway Utilization

GGM 8000 is available as a Conventional Channel Gateway (CCGW) interface device in a variety of different hardware configurations to support various types of conventional channels in your system.

1.3.1.1 Conventional Channel Gateway – Port-to-Channel Mapping

The port-to-channel mapping differs for a High Density Enhanced Conventional Gateway and Low Density Enhanced Conventional Gateway as compared to GGM 8000 equipped with the expansion module and analog/V.24 interface kit.

NOTICE: The GGM 8000 CCGW implementation based on the expansion module and analog/ V.24 interface kit statically maps the GGM 8000 ports to channel types and channel IDs. Since the physical port-based channel types (analog, MDC 1200, mixed mode, and ACIM) share the same channel IDs, they cannot be configured at the same time. The CCGW implementation, on the other hand, statically maps the GGM 8000 ports to channel types and interface IDs but does not statically map the channel IDs.

Low and High Density Enhanced Conventional Gateways

Table 7: Low and High Density Enhanced Conventional Gateways Port-To-Channel Mapping

Port/Path Number	Analog or MDC 1200 Channel Number	Digital Channel Number	Mixed Mode or ACIM Channel Number
Low Density Enhanced Conventional Gateway			
13D + 12D	1-32	N/A	N/A
13C + 12C	1-32	N/A	N/A
13B + 12B	1-32	N/A	N/A
13A + 12A	1-32	N/A	N/A
11B	N/A	1-30	N/A
11A	N/A	1-30	N/A
10B	N/A	1-30	N/A
10A	N/A	1-30	N/A
13D + 12D + 11B	N/A	N/A	1-30
13C + 12C + 11A	N/A	N/A	1-30
13B + 12B + 10B	N/A	N/A	1-30
13A + 12A + 10A	N/A	N/A	1-30
High Density Enhanced Conventional Gateway			
9D + 8D	1-32	N/A	N/A
9C + 8C	1-32	N/A	N/A

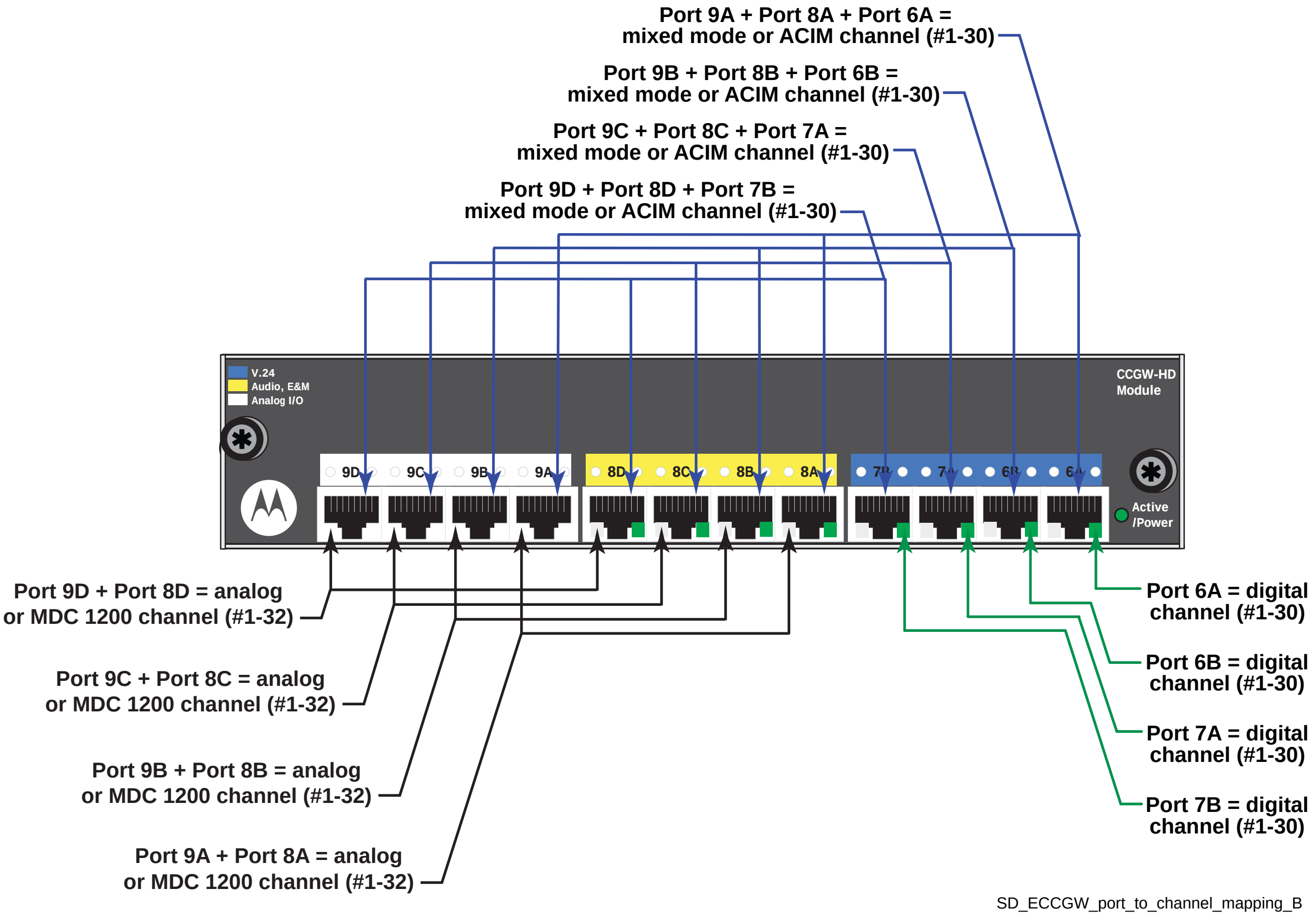
Port/Path Number	Analog or MDC 1200 Channel Number	Digital Channel Number	Mixed Mode or ACIM Channel Number
9B + 8B	1-32	N/A	N/A
9A + 8A	1-32	N/A	N/A
7B	N/A	1-30	N/A
7A	N/A	1-30	N/A
6B	N/A	1-30	N/A
6A	N/A	1-30	N/A
9D + 8D + 7B	N/A	N/A	1-30
9C + 8C + 7A	N/A	N/A	1-30
9B + 8B + 6B	N/A	N/A	1-30
9A + 8A + 6A	N/A	N/A	1-30

Where:

- Allowable analog or MDC 1200 channel IDs are 1-32, but only one channel can be configured at a time on each analog interface.
- Allowable digital channel IDs are 1-30, but only one channel can be configured at a time on each digital interface.
- Allowable mixed mode or ACIM channel IDs are 1-30, but only one channel can be configured at a time on each analog/digital interface pair.

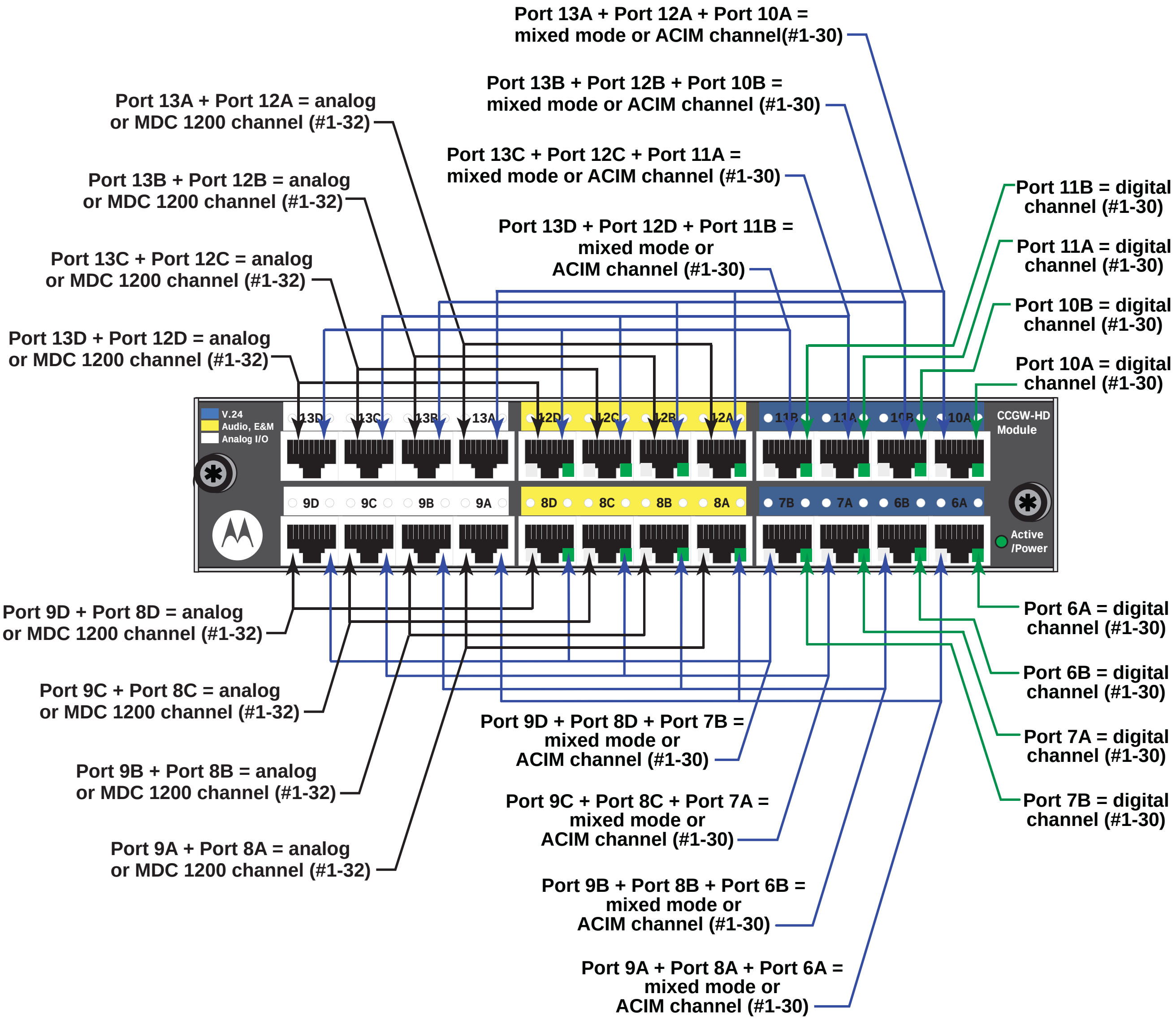
NOTICE: Non-data capable channels (analog, MDC 1200) can have channel IDs in the range 1-32 and data capable channels (digital, IP conventional, mixed mode, or ACIM) can have IDs in the range 1-30.

Figure 11: GGM 8000 Low Density CCGW Port Numbering and Port-to-Channel Mapping


Port 9A + Port 8A + Port 6A = mixed mode or ACIM channel (#1-30)
Port 9B + Port 8B + Port 6B = mixed mode or ACIM channel (#1-30)
Port 9C + Port 8C + Port 7A = mixed mode or ACIM channel (#1-30)
Port 9D + Port 8D + Port 7B = mixed mode or ACIM channel (#1-30)
V.24
Audio, E&M
Analog I/O
CCGW-HD Module
9D
9C
9B
9A
8D
8C
8B
8A
7B
7A
6B
6A
Active /Power
Port 9D + Port 8D = analog or MDC 1200 channel (#1-32)
Port 9C + Port 8C = analog or MDC 1200 channel (#1-32)
Port 9B + Port 8B = analog or MDC 1200 channel (#1-32)
Port 9A + Port 8A = analog or MDC 1200 channel (#1-32)
Port 6A = digital channel (#1-30)
Port 6B = digital channel (#1-30)
Port 7A = digital channel (#1-30)
Port 7B = digital channel (#1-30)

SD_ECCGW_port_to_channel_mapping_B

Figure 12: GGM 8000 High Density CCGW Port Numbering and Port-to-Channel Mapping


Port 13A + Port 12A + Port 10A = mixed mode or ACIM channel(#1-30)
Port 13B + Port 12B + Port 10B = mixed mode or ACIM channel (#1-30)
Port 13C + Port 12C + Port 11A = mixed mode or ACIM channel (#1-30)
Port 13D + Port 12D + Port 11B = mixed mode or ACIM channel (#1-30)
Port 13A + Port 12A = analog or MDC 1200 channel (#1-32)
Port 13B + Port 12B = analog or MDC 1200 channel (#1-32)
Port 13C + Port 12C = analog or MDC 1200 channel (#1-32)
Port 13D + Port 12D = analog or MDC 1200 channel (#1-32)
Port 11B = digital channel (#1-30)
Port 11A = digital channel (#1-30)
Port 10B = digital channel (#1-30)
Port 10A = digital channel (#1-30)
V.24
Audio, E&M
Analog I/O
13D
13C
13B
13A
12D
12C
12B
12A
11B
11A
10B
10A
CCGW-HD Module
9D
9C
9B
9A
8D
8C
8B
8A
7B
7A
6B
6A
Active /Power
Port 9D + Port 8D = analog or MDC 1200 channel (#1-32)
Port 9C + Port 8C = analog or MDC 1200 channel (#1-32)
Port 9B + Port 8B = analog or MDC 1200 channel (#1-32)
Port 9A + Port 8A = analog or MDC 1200 channel (#1-32)
Port 9D + Port 8D + Port 7B = mixed mode or ACIM channel (#1-30)
Port 9C + Port 8C + Port 7A = mixed mode or ACIM channel (#1-30)
Port 9B + Port 8B + Port 6B = mixed mode or ACIM channel (#1-30)
Port 9A + Port 8A + Port 6A = mixed mode or ACIM channel (#1-30)
Port 6A = digital channel (#1-30)
Port 6B = digital channel (#1-30)
Port 7A = digital channel (#1-30)
Port 7B = digital channel (#1-30)

HD_ECCGW_port_to_chanel_mapping_B

GGM 8000 with Analog/V.24 Interface Kit

Table 8: GGM 8000 analog/V.24 Port-To-Channel Mapping

Port/Path Number	Analog or MDC 1200 Channel Number	Digital Channel Number	Mixed Mode or ACIM Channel Number
8D	4	N/A	N/A
8C	3	N/A	N/A
8B	2	N/A	N/A
8A	1	N/A	N/A
7B	N/A	4	N/A
7A	N/A	3	N/A

Port/Path Number	Analog or MDC 1200 Channel Number	Digital Channel Number	Mixed Mode or ACIM Channel Number
6B	N/A	2	N/A
6A	N/A	1	N/A
8D + 7B	N/A	N/A	4
8C + 7A	N/A	N/A	3
8B + 6B	N/A	N/A	2
8A + 6A	N/A	N/A	1

1.3.1.2

Conventional Channel Gateway – Functional Description

The Conventional Channel Gateway provides the interface between the IP network and conventional sites in ASTRO® 25 system by translating the voice and data into the format needed for each individual site type.

The Conventional Channel Gateway serves as the control point between the master site and the site devices (for example, the GGM 8000 comparator, the GTR 8000 Base Radio, and the GPW 8000 Receiver). The CCGW application also communicates with the Zone Controller at the master site for proxy control of the site device, and the Conventional Channel Gateway passes voice and signaling payload between the MCC 7500 VPM dispatch console(s) and the site device and between the MCC 7500 VPMs and the consolettes. For packet data, the Conventional Channel Gateway passes control information and packet data payload between the Radio Network Gateway (RNG) and the stations and comparators.

The Conventional Channel Gateway supports 4-wire or 2-wire (Enhanced Conventional Gateway only) analog interfaces to conventional base stations. The analog interfaces can support analog-only channels, MDC 1200 channels, or the analog side of mixed mode or ACIM channels.

1.3.1.3

Conventional Channel Gateway – Analog (E&M) Interface Overview

The E&M physical interfaces included in the analog/V.24 interface kit were developed for use in the analog tie trunks used to interconnect PBXs. The interface has two line control signals (the E-lead and the M-lead) and separate signals for audio. In the CCGW implementation, the E&M interface controls the state of the E-lead and monitors the state of the M lead, while the other side of the connections monitors the E-lead and controls the M-lead. The specific logical state of either the E-lead or the M-lead control lines correspond to whether electrical current is flowing (the Off-Hook state) or not flowing (the On-Hook state) through the leads.

IMPORTANT: The definitions for the E-lead and M-lead used on the CCGW are the reverse of most other pieces of network equipment.

Five different E&M signaling schemes are defined (E&M Types I, II, III, IV, and V), although only Types I, II, III, and V are in common use. The CCGW E&M interface is configured to operate in E&M Type II mode.

The GGM 8000 Enhanced Conventional Gateway module adds the following functionality on the analog interfaces:

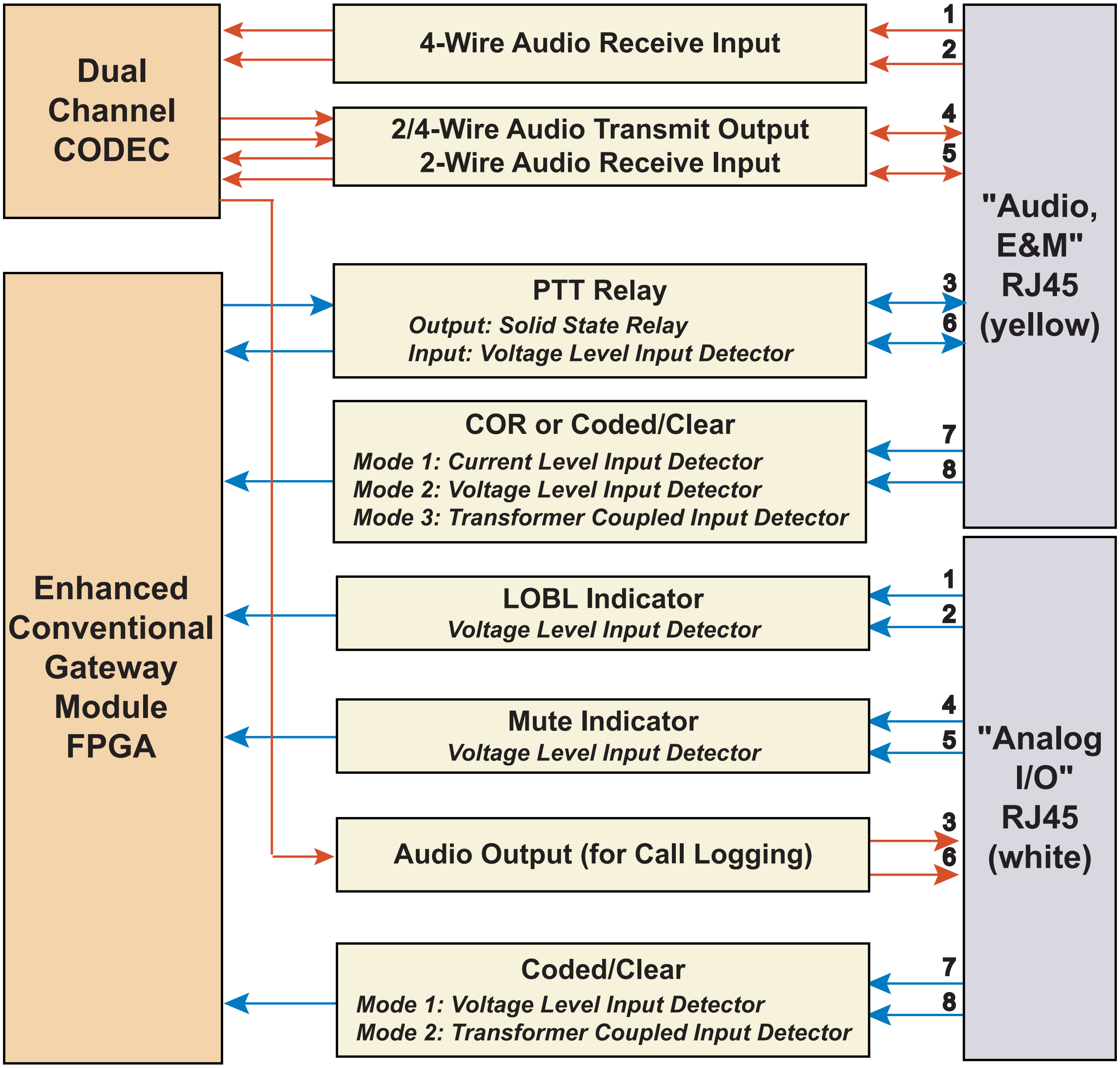
- Support for additional electrical interface types.
  - In addition to the 4-wire interface that is also supported on the analog/V.24 interface kit, the Enhanced Conventional Gateway supports a 2-wire interface and a 2-wire and 4-wire interface. In 4-wire audio mode, audio is transmitted on one signal pair and received on another signal pair. In 2-wire audio mode, audio is transmitted and received on one signal pair.

  - The 4-wire, 2-wire, and 4-wire and 2-wire analog interfaces on the Enhanced Conventional Gateway module support software-selectable termination impedance settings. In addition, the output gain setting for the audio pair (in either 2-wire, 4- wire, or 2-wire and 4-wire mode) is maintained over a wide range of line termination impedances (audio output gain does not vary due to variations in line/load impedance).
- A second set of analog connectors provides a separate audio output on each connector for audio logging recorders, as well as additional signaling capabilities, including:
  - Mute input for the 2-wire, 4-wire, or 2-wire and 4-wire analog interfaces on pins 4 and 5. The mute inputs from the Enhanced Conventional Gateway analog interface can be used to mute the channel associated with that interface without removing the analog capability of the channel.
  - Support for summed audio logging on pins 3 and 6.
  - Detection of an externally controlled digital line operated busy light (LOBL) signal on pins 1 and 2 through either voltage detection or contact closure.
  - Support for a coded/clear signal call indication generated by a base station on pins 7 and 8.
- Enhanced Inbound AGC type settings – The inbound AGC type can be configured as either Dynamic Level Memory (DLM), AGC or AGC off. DLM means that the AGC gain adjustment is only active when the AGC detects voice activity.

Table 13: Pin Functions for Analog/V.24 Interface Kit on page 80describes the pin functions for analog base station connections to GGM 8000 when GGM 8000 is equipped with an Enhanced Conventional Gateway module. GGM 8000 supports four pairs of analog connectors per chassis (two connectors per analog interface) when equipped with the Low Density Enhanced Conventional Gateway module and eight pairs of analog connectors per chassis (two connectors per analog interface) when equipped with the High Density Enhanced Conventional Gateway module.

The following figure summarizes the signal functions on the Enhanced Conventional Gateway module RJ-45 analog connectors.

Figure 13: Enhanced CCGW – Analog Interface Signal Functions


Dual Channel CODEC
Enhanced Conventional Gateway Module FPGA
4-Wire Audio Receive Input
2/4-Wire Audio Transmit Output
2-Wire Audio Receive Input
PTT Relay
Output: Solid State Relay
Input: Voltage Level Input Detector
COR or Coded/Clear
Mode 1: Current Level Input Detector
Mode 2: Voltage Level Input Detector
Mode 3: Transformer Coupled Input Detector
LOBL Indicator
Voltage Level Input Detector
Mute Indicator
Voltage Level Input Detector
Audio Output (for Call Logging)
Coded/Clear
Mode 1: Voltage Level Input Detector
Mode 2: Transformer Coupled Input Detector
1
2
4
5
3
6
7
8
"Audio, E&M" RJ45 (yellow)
1
2
4
5
3
6
7
8
"Analog I/O" RJ45 (white)

ECGW_analog_signal_functions_A

1.3.1.4 Conventional Channel Gateway – Supported Channels and Sites

The GGM 8000 conventional channel interface (also referred to as the CCGW) supports a number of channel and site types.

NOTICE: Channel types are configured in the LDAP server database, through Provisioning Manager.

Supported Channels

The GGM 8000 Conventional Channel Gateway supports the following channel types:

Analog conventional
Interfaces analog audio connections (across LAN or WAN links) with certain types of Motorola Solutions public safety network equipment that support analog audio connections.

Digital conventional (digital over V.24 interface)
Interfaces V.24 ports carrying digital audio (across LAN or WAN links) with certain types of Motorola Solutions public safety network equipment that support digital audio connections.

IP conventional (digital over IP interface)
Supports IP connectivity between the CCGW and conventional IP base stations and comparators (in IP simulcast systems). An IP conventional channel functions as an IP interface between the base station and the console, creating an IP link between the CCGW and the base station using Motorola’s proprietary link management protocol. Typically, IP conventional runs over the Ethernet interface.

Mixed mode
Processes audio over the analog E&M interface and the signaling related to this call over the digital interface. The CCGW supports mixed mode channels over V.24 and IP digital interfaces:

- **V.24 mixed mode** – Binds an analog interface and a V.24 digital interface as a single channel. The CCGW associates the signaling information processed over the digital V.24 interface with the voice processed over the corresponding analog E&M interface.
- **IP mixed mode** – Binds an analog interface and an IP digital interface as a single channel. The IP interface is used for call signaling and control and digital audio for digital calls, while the analog interface is used for call signaling and control and analog audio for analog calls. Each direction is independent of the other.

MDC 1200
Integrates MDC 1200 and analog conventional signaling. An MDC channel is a channel where audio and call control are processed over the analog E&M interface.

ACIM
Enables connection of the Motorola Solutions consolette to the CCGW via the ACIM link serial control protocol. This topology allows a console site to have access to talkgroups when its link to the zone core has failed. It also enables wireless connection to systems utilizing a variety of over-the-air protocols.

Supported Sites

The GGM 8000 CCGW supports the following site types:

Combination
GGM 8000 equipped with an analog/V.24 interface kit requires that the SiteType be configured as Combination. A GGM 8000 base unit can also be configured with the Combination SiteType.

Combination-HD
GGM 8000 equipped with an Enhanced Conventional Gateway module requires that the SiteType be configured as Combination-HD. A GGM 8000 base unit can also be configured with the Combination-HD SiteType.

1.3.1.4.1 Conventional Gateway Interfaces

The Conventional Channel Gateway (CCGW) acts a gateway between various site devices and the rest of the system. CCGW translates voice and data into the format needed for each individual site type. CCGWs support the following channel types: digital, analog, mixed-mode, MDC1200, and ACIM.

NOTICE: The GGM 8000 supports digital channels with either V.24 or IP site links.

CCGW IP Conventional Channels

CCGW support up to ten IP-based conventional channels and additionally can support up to four V.24-based or four analog conventional channels.

CCGW is supported in any of the site types that may contain conventional channels and may reside on the site gateway in non-redundant site gateway configurations. Since sites can support up to three or ten CCGWs, additional GGM 8000 gateways may be necessary to support the CCGW application. Each CCGW at a physical site is considered a separate logical conventional site and the site devices that it communicates with are the conventional channels.

CCGW serves as the control point between the Master Site and the site devices (that is, GCM 8000 Comparator, GTR 8000 Base Radio, and GPW 8000 Receiver). The CCGW application also communicates with the ZC at the Master Site for proxy control of the site devices. The CCGW passes voice and signaling payload between the MCC 7500 VPM Dispatch Console(s) and the site devices. In a different setup involving the consolette, CCGW passes voice and signaling payload between the MCC 7500 VPM Dispatch Console(s) and the consolettes. For packet data, CCGW passes control information and packet data payload between the RNG and the stations and comparators.

Digital CCGW with v.24 Module

A GGM 8000 gateway can support up to four digital conventional sources. If the number of stations, receivers, or comparators at a site exceeds the capacity of the gateway, additional gateways can be added to support more digital connections.

The GGM 8000 CCGW is able to support up to four non-IP conventional channels of any type, Analog, Digital, Mixed-Mode, and MDC1200. For these non-IP channels, the interface between the CCGW and the stations are either 4-wire, V.24, a hybrid 4-wire/V.24 or 4-wire respectively. In addition, GGM 8000 can support up to ten IP-digital conventional channels, where the interface between GGM 8000 and the digital station is over an IP link.

Analog CCGW with E&M Module

The GGM 8000 CCGW can also support the 4-wire E&M module. If GGM 8000 is equipped with the CCGW option, it automatically includes the 4-Wire module, which can support up to four analog 4-wire interfaces to conventional stations. These 4-wire interfaces can be used for analog-only, MDC1200 or the analog side of a Mixed Mode conventional channel. This 4-Wire module is included in the hardware configuration of GGM 8000 along with the V.24 daughterboards for the digital interfaces to digital conventional and Mixed Mode channels.

1.4 ACIM Interface on GGM 8000

The following sections describe the ASTRO Control Interface Module (ACIM) feature on GGM 8000.

1.4.1 ACIM Interface – Functional Description

The ACIM feature adds the serial control protocol to GGM 8000 in order to allow exchanging control information between an MCC 7500 VPM console and a Motorola Solutions consolette. The consolette enables a console site to have access to resources when its link to the zone core has failed. The consolette can also enable wireless connection to systems utilizing a variety of over-the-air protocols (such as analog, analog with MDC-1200, ASTRO Conventional, and 3600 Trunking) that may be not accessible otherwise.

The consolette is connected to the Conventional Channel gateway via a V.24 and 4-wire connector constituting an ACIM conventional channel. GGM 8000 configured with the analog/V.24 interface kit or the Low Density Enhanced Conventional Gateway module can support up to four ACIM conventional channels in each topology. The GGM 8000 configured with the High Density Enhanced Conventional Gateway module can support up to eight ACIM conventional channels in each topology. One analog and one V.24 (digital) port on the Conventional Channel Gateway are needed to connect to the Motorola Solutions consolette. Each analog port contains the following inputs and outputs:

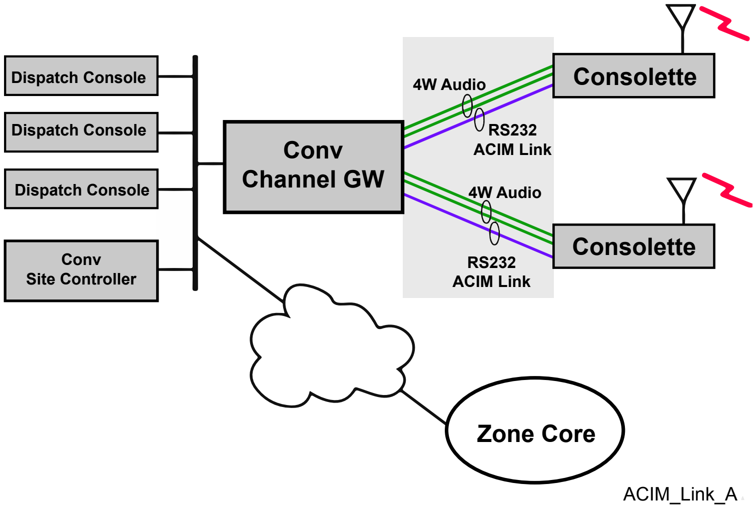
- 600 Ohm balanced analog audio input – Used to accept radio audio from the consolette
- 600 Ohm balanced analog audio output – Used to send console transmit audio to the consolette
- 1 Amp, 24 VDC relay output – Used to diagnose relay keying capability at the M-lead

The audio connections on the E&M port consist of one signal pair for each direction (4-wire audio). The audio signals on the CCGW E&M card are designed for 600Ω resistively terminated interfaces and it is recommended that the terminators on the consolette be configured appropriately (either 600 or 10K).

The CCGW provides an RJ-45 connector for standard 9600 baud RS-232 asynchronous cable connection to the consolette for the control signaling over the V.24 card port. The RS-232 link uses 8 bits, one stop bit and no parity.

The following diagram shows the Conventional Channel Gateway used with two ACIM conventional channels.

Figure 14: ACIM Conventional Channel



For more information on the ACIM conventional channel, see the *RF Site Technician Reference Guide* manual.

For more information on Motorola Solutions consolettes, see one of the following manuals:

- *APX 7500 Multi-Band Consolette Detailed Service Manual*
- *ASTRO Digital XTL 5000 Consolette Instruction Manual*

1.4.1.1 ACIM Consolette

The APX 7500 Multi-Band Motorola Solutions consolette and the ASTRO® 25 Digital XTL 5000 Consolette can connect to the MCC 7500 VPM through the GGM 8000 Conventional Channel Gateway (CCGW). This capability provides the high tier set of features such as Console Initiated Calls, Subscriber Initiated Calls and Extended Messaging features such as Call Alert, Radio Disable/Enable, Remote Monitor, Status Query/Response, and Message Update. The Extended Messaging feature set is available only with the Motorola Solutions 7500 Consolette and not with the ASTRO® 25 Digital XTL 5000 Consolettes. The consolette connects to the GGM 8000 CCGW, using both the 4-wire interface for audio and the V.24 link interface for control messaging.

1.4.2 ACIM Interface – Modules Used

In order to support the ACIM conventional channel, GGM 8000 must be equipped with the analog/V.24 interface kit or an Enhanced Conventional Gateway module.

NOTICE: For more information on the GGM 8000 modules, see Expansion Module on page 33 and GGM 8000 Enhanced Conventional Channel Gateway Modules on page 34.

1.5 ASTRO Advanced SECURENET

Secure communication using Advanced SECURENET® encryption is supported on digital conventional channels using MCC 7500 VPM dispatch consoles in K, L, or M core ASTRO® 25 systems.

Advanced SECURENET® conventional operation allows for secure communication on analog (both with and without MDC 1200) channels with Voice Processor Module-based MCC 7500 VPM Dispatch Consoles in an M3 core ASTRO® 25 system.

1.5.1 Advanced SECURENET on Digital-Capable Channel Types

ASTRO® 25 systems use IC-based digital encryption algorithms. These algorithms are linear functions that operate bit-by-bit; selection of an encryption key variable governs them.

ASTRO® 25 digital technology enhancements to encrypted voice radio systems include:

- No range degradation is in the encrypted mode, regardless of the algorithm employed
- No voice truncation is at the beginning of the voice message
- Provides multiple algorithm capability
- ASTRO® 25 key management facilities support Over-the-Air-Rekeying (OTAR) functions

The following describes a type of encryption called Advanced SECURENET® supported by ASTRO® 25 systems:

Advanced SECURENET® provides Physical Identifier (PID) key management. PID key management identifies a physical memory slot where a key variable is stored in a unit. All products that support PID key management access the same encryption keys dependent on the physical storage capability of the product.

Advanced SECURENET® security is supported on the following digital-capable channels:

- Digital conventional
- IP Conventional
- ASTRO® 25 Control Interface Module (ACIM)

- Mixed Mode conventional (only when operating in Digital Transmit mode)

On these channels, encryption can be performed through Advanced SECURENET® using the following:

- ACIM Consolettes
- Digital Interface Unit (DIU) implementation
- Key Variable Loader (KVL)

The following parameters apply to Advanced SECURENET® digital capabilities. For more information about these parameters, see the manuals and online help for Provisioning Manager and Configuration Manager – Conventional.

Secure Communication Mode
Indicates the security mode capability enabled for the channel (may be **Clear**, **Secure**, or **Both**).

Secure Communication Mode Default
Indicates which security mode is in effect when the channel comes up when **Secure Communication Mode** is set to **Both**.

Common Key Reference Alias List
Lists default Common Key Reference (CKR) assigned to a digital conventional channel configured for secure communication.

Advanced Securenet
Determines if the channel has advanced secure options.

Secure Key In
Enables the console to display the alias of the CKR for the received call

Secure Key Out
Determines if the console user can select from a list of CKRs for use in sending encrypted audio, if Advanced SECURENET® is enabled.

Default CKR
If the console subsystem user does not select the CKR, the default CKR for a given channel is used.

Auto Key
If Secure Key Out is enabled, the Auto Key parameter determines whether the console uses the last received key for the next console transmission. When Auto Key is enabled, the console overwrites the value of the last CKR in the CKR list with the auto key.

Common Key Reference Index List
Selects number of keys to configure for a channel.

In the case of Digital/ACIM/Mixed Mode channels, unlike the Key Numbers for Analog/Mobile Data Communications, CKRs are logical keys shared across the system to which PID-based keys used by Advanced SECURENET® products can be mapped (see “Common Key Reference” in the *Provisioning Manager User Guide*).

1.5.2 Advanced SECURENET Conventional Operation – Analog Channel Types

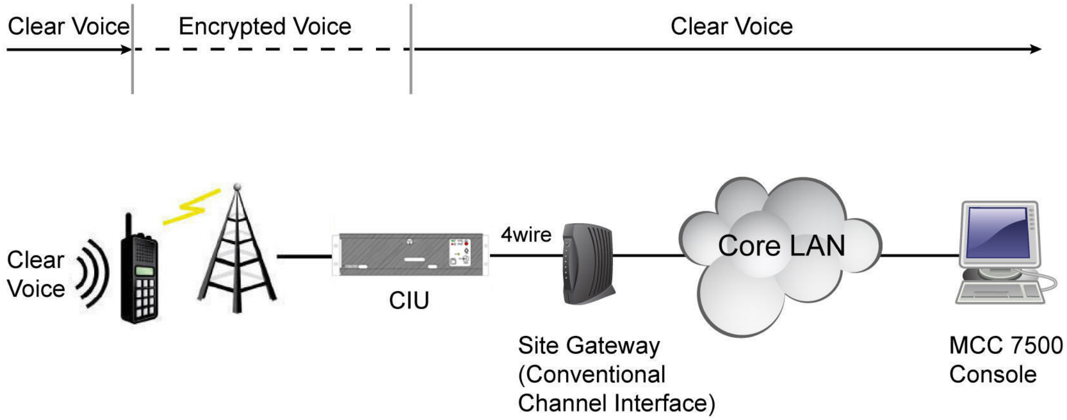
Advanced SECURENET® Conventional Operation on Analog Channel Types requires an existing Advanced SECURENET® Console Interface Unit (CIU) connected to an existing secure-capable base radio to be connected to a GGM 8000 Conventional Channel Interface, to be used by Voice Processor Module (VPM)-based MCC 7500 Dispatch Consoles.

NOTICE: The GGM 8000 Conventional Channel Interface is also known as a Conventional Channel Gateway (CCGW).

The Advanced SECURENET® CIU acts as the station interface to CCGW providing secure decryption for 12 kbit encoded signals. The CIU interface to the CCGW must comply with the same interface specifications as required for a QUANTAR®. For the base station interface specification, see the "Analog Base Stations to Site Gateways (Conventional Channel Interface)" section in the *GGM 8000 Hardware User Guide*. For details regarding the CCGW support of the Advanced SECURENET® feature, see *GGM 8000 Hardware User Guide*.

Regardless of the secure mode (coded or clear) of a call, all audio from the Advanced SECURENET® CIU into the core to the consoles is "clear" audio, assuming the Advanced SECURENET® CIU is able to decrypt a coded call successfully (if not, scrambled digital noise is heard, or is muted by Proper Code detection functions in the CIU).

Figure 15: Secure Voice Using Advanced SECURENET for Analog and MDC 1200 Channels



Call controllers distribute inbound and outbound channel activity to all affiliated consoles. Advanced SECURENET® conventional channels may have inbound calls sourced by various alert tones originating from the channel equipment (as opposed to originating from the radio user). These alert tones are referred to as "Channel Feedback" tones and may include TX or RX clear alerts, or status/ event alerts from the Advanced SECURENET® CIU or transport modems. The Proper Channel Feedback setting (configurable through Provisioning Manager) allows the system administrator to limit tones being heard at the console to operationally critical, as opposed to hearing them all.

Important limitations include:

- Advanced SECURENET® Conventional Operation on Analog Channel Types only works with a QUANTAR® that is version 10 or earlier.
- Advanced SECURENET® Conventional Operation on Analog Channel Types is not supported by GTR 8000 Base Radios.
- Advanced SECURENET® connections to MCC 7500 VPM Dispatch Consoles are only supported in ASTRO® 25 systems with an M3 core.

The following Analog conventional configurations are allowed:

- MDC 1200 configurations
- Main/alt configurations
- M core system that falls back to C-sub operation, because the Conventional Site Controller (CSC) allows Advanced SECURENET® operation to continue
- Systems may contain MCC 7500 VPM Dispatch Consoles or analog consoles enabled for Advanced SECURENET® conventional operation, and other MCC 7500 VPM Dispatch Consoles or analog consoles not enabled for Advanced SECURENET®.

The following parameters apply to the Advanced SECURENET® Analog and MDC 1200 capabilities:

Secure Communication Mode
Indicates the security mode capability enabled for the channel (may be **Clear**, **Secure**, or **Both**).

Secure Communication Mode Default
Indicates which security mode is in effect when the channel comes up (when **Secure Communication Mode** is set to **Both**)

Advanced Securenet
Determines if the channel has advanced secure options.

Secure Key Out
Determines if the console user can select from a list of PID-based keys per channel for use in sending encrypted audio, if Advanced SECURENET® is enabled.

Number of Keys
Selects number of keys to configure for a channel.

Proper Channel Feedback
The CCGW reports the presence of detected channel feedback audio in a bit and only passes feedback tones from the channel to the console.

NOTICE: For information about defining a list of Keys when Secure Key Out is enabled, see "Common Key Reference" in the *Provisioning Manager User Guide* or online help.
For information about setting up Momentary Override CKRs to override default keys for Advanced SECURENET® channels, see "Momentary Override CKR" in the *Provisioning Manager User Guide*.

Additionally, see *Elite Dispatch User Guide* for the following information:

- Instructions on using the dispatch console functions that support Advanced SECURENET® (see the sections about Transmit Mode Select, Outbound Secure Key, and Momentary Override).
- Instructions on changing the way these functions are presented on the dispatch console (see the sections about editing the order of drop-down items and editing the stack).

NOTICE: If a site using the Key Management Controller (KMC) for Advanced SECURENET® is added to a system with the current ASTRO® 25 system Key Management Facility (KMF), the KMC can still be used at its site, but map the relationship between keys in the KMC and keys in the KMF to avoid confusion.

1.5.3 Implementing Advanced SECURENET for Conventional Operation

Perform the following procedure to implement Advanced SECURENET® for conventional operation.

Prerequisites: Verify that you have the following items:

- Existing base radio configured for Advanced SECURENET® (QUANTAR® only, because GTR 8000 Base Radios do not support Advanced SECURENET®)
- Existing Advanced SECURENET® Conventional Interface Unit (CIU)

  NOTICE: For information on CIU, see the *CIU Instruction Manual* (6881066E95).

- Advanced SECURENET® CIU manuals
- GGM 8000 with Analog/V.24 Interface Kit (GGM 8000 Conventional Channel Interface, also known as Conventional Channel Gateway (CCGW))
- MCC 7500 Dispatch Console with Voice Processor Module (VPM)
- User credentials to log on to Provisioning Manager
- Elite Dispatch manual
- LAN Switch – to deploy a LAN switch, see the *System LAN Switches Feature Guide*.

Process:

1. Set up MCC 7500 VPM Dispatch Consoles and CCGWs and connect to site switch. Power up and confirm manager access to these components. For more details, see the *Provisioning Manager User Guide*.
2. Plan which Advanced SECURENET® channels connect to which CCGW. You can connect up to four CIUs to each CCGW (four E&M analog ports available). Use Provisioning Manager to configure up to four ASN channels on each CCGW. Ports not used for Advanced SECURENET® channels may be used for other analog channel types. See the *Provisioning Manager User Guide*.
3. Configure MCC 7500 VPM Dispatch Consoles from Provisioning Manager to enable console and station capabilities supported on Advanced SECURENET® channels.
   a. CIU with MDC 1200 signaling (Advanced SECURENET®)
   b. CIU without MDC 1200 signaling (Advanced SECURENET®)

   See the *Provisioning Manager User Guide*.
4. **(Motorola Solutions personnel only)** First set of four CIUs: power down CIU and make physical config changes to enable coded/clear indication function (make wire connection on Interconnect board backplane, and change position of a user jumper). For the details on jumper settings and a diagram, see the “Cabling the E&M (Analog) Connector(s)” section in the *Motorola GGM 8000 Hardware User Guide*, accessible on Motorola Online.
5. Power up CIUs.

Configured Advanced SECURENET® Channel resources initialize on MCC 7500 VPM Dispatch Consoles.

Postrequisites: Verification.
When calls are active on the channel:

- When the CIU is configured for Tx Clear Alerts and outbound clear calls are made, CIU feedback tones should be heard at console speakers.
- MDC 1200 messages should display in MCC 7500 VPM Dispatch Console GUI, if applicable.
- Cross mode indication should display in dispatch GUI if applicable.
- ZoneWatch scrolling log viewer should show DCP protocol.
- Logging Recorder should show teleservice messages with coded/clear indication. Station Control Commands should show Outbound Key Selected.
- 12 kbit and MDC 1200 messages can be heard from sniffer tool, line analyzer, and RF Comm analyzer as described in the diagram captions.

1.5.4 GGM 8000 Conventional Channel Interface Connections to Console Interface Unit (CIU)

See “Connecting the GGM 8000 E&M Interface to a CIU for Advanced SECURENET Support Connecting the GGM 8000 Analog Interface to a CIU for Advanced SECURENET Support” in *Motorola GGM 8000 Hardware User Guide*. For instructions on how to access the *Motorola GGM 8000 Hardware User Guide*, see Related Information on page 27.

1.6 Installation

Obtain:

- Pan-head screws (4) for rack-mounting
- TORX® screws for rack-mounting (provided with the rack-mount kit). Eight screws are needed to secure a GGM 8000 with two TORX® screws on top of the chassis. Four screws are needed to secure a GGM 8000 with no TORX screws on top of the chassis. See Physical Description on page 30.
- TORX® driver set
- Electrostatic discharge (ESD) wrist strap (Motorola Solutuions part number RSX4015A, or equivalent)
- For AC power connections:
    - AC power cord (supplied with the GGM 8000)
    - #6 AWG grounding (earthing) wire, terminated with UL-listed two-hole rectangular grounding lugs on both ends

        NOTICE: If the length of the grounding wire must exceed 4 meters before it is terminated, grounding wire larger than #6 AWG is required. See the *Standards and Guidelines for Communication Sites* manual for details.

        NOTICE: The grounding wire is required only if your network topology requires an additional ground on the chassis, separate from the AC ground.
    - Two (2X) M6 hex nuts for attaching the grounding wire to the chassis (supplied with the GGM 8000)
- For DC power connections:
    - 2.5 mm flat blade screwdriver for setting the low voltage disconnect level (LVDL) rotary selector switch
    - GGM 8000 tray cable (part number DKN6145A). This three-wire cable is constructed from #14 AWG UL-listed tray cable wiring (Type TC-ER)
        + One end of the cable is factory-terminated with a polarity-keyed, 3-pin latching female connector that mates with the DC power entry connector on the GGM 8000 power subsystem module.
        + One end of the cable is unterminated and must be cut to length and suitably terminated, as required for the connection with the centralized DC power source.

            NOTICE: If you connect GGM 8000 to two DC power sources, you need two GGM 8000 tray cables.

        If you want to build your own DC-to-DC cable for use with the GGM 8000, refer to GGM 8000 Tray Cable Assembly Details on page 55 for important cable construction details.
    - Wire-stripping tools
    - Wire-crimping tool
    - Appropriate terminals to terminate the three wires that comprise the GGM 8000 tray cable for connection to a centralized DC power source.

        NOTICE: A wire-crimping tool and terminals are not required if you connect GGM 8000 to a DC power source with compression-style terminals.

1.6.1 GGM 8000 Tray Cable Assembly Details

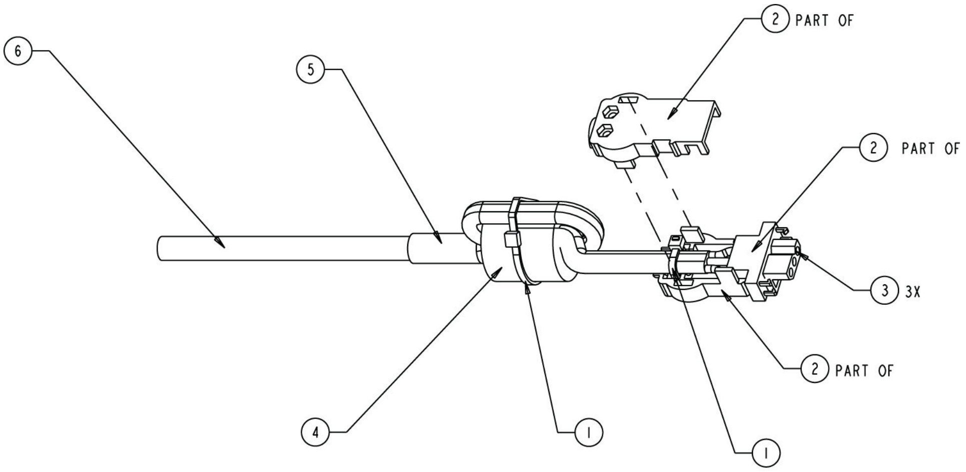
This section illustrates and describes the assembly of the GGM 8000 tray cable (Motorola Solutions part number DKN6145A). Use this information if you want to build your own DC-to-DC cable for use with the GGM 8000.

IMPORTANT: Follow these requirements when constructing a DC-to-DC cable for use with the GGM 8000:

- Interpret all dimensions, tolerances, and practices per ANSI Y14.5M-1194.
- For workmanship standards, see ANSI/IPC-A-610.
- All wiring harnesses must be constructed with UL-recognized and CSA-certified materials.
- Suppliers must be UL and CSA approved.
- Cable must be tested, point-to-point, at minimum, and stamped to indicate such testing.
- The end-to-end length of the unsupported cable (from the cable tray to the GGM 8000) must be no more than 1830 mm (6 feet).
- Only one physical connector per pin is allowed.
- Install connectors per manufacturer specifications.
- Refer to Figure 16: GGM 8000 Tray Cable Assembly Drawing on page 56 and tightly wind item 6 with item 5 on item 4 one and a half (11/2) turns prior to installing item 1 on the cable assembly.
- Refer to Figure 16: GGM 8000 Tray Cable Assembly Drawing on page 56 and secure the cable assembly to the connector shell (item 2) with the cable tie (item 1).

The following figure shows the assembly drawing for the GGM 8000 tray cable.

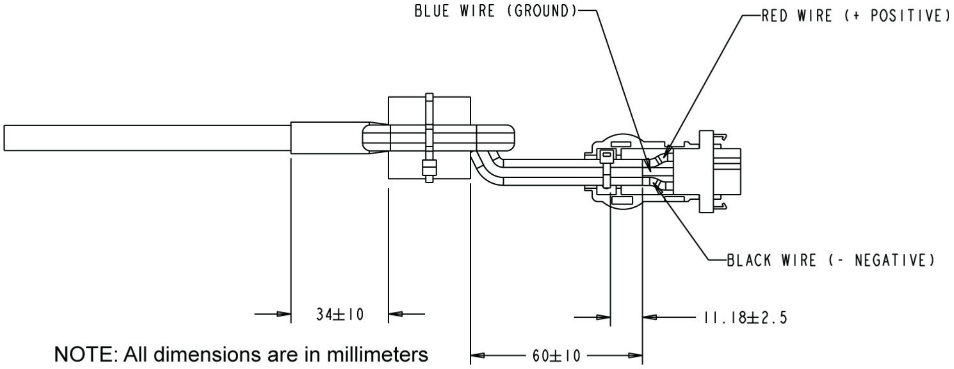
Figure 16: GGM 8000 Tray Cable Assembly Drawing



tray_cable_ad

The following figure provides a view with the connector cover removed to show the construction detail.

Figure 17: GGM 8000 Tray Cable (Connector Cover Removed)



NOTE: All dimensions are in millimeters

tray_cable_no_cover

The following table lists the manufacturer part numbers for the required GGM 8000 tray cable components. The item numbers correspond to the numbers in the assembly drawing shown in Figure 16: GGM 8000 Tray Cable Assembly Drawing on page 56.

Table 9: GGM 8000 Tray Cable Required Components

Item #	Manufacturer	Manufacturer Part Number	Quantity	Description
1	Panduit	PLT1.5M	2	Cable tie
2	Anderson Power	PM103FOOLCH	1	Connector
3	Anderson Power	PM16S1416S32	3	Female pin socket
4	Fair-Rite	2643101902	1	Toroid
5	Tyco	RNF–100 3/8–BK	260 mm	Heat shrinkable tubing
6	General Cable	235050	1830 mm	Cable

1.6.2

General Safety Guidelines

Observe the following general safety precautions during all phases of operation, service, and repair of the equipment described in this manual. Follow the safety precautions listed and all other warnings and cautions necessary for the safe operation of the equipment. Because of the danger of introducing additional hazards, do not install substitute parts or perform any unauthorized modifications of the equipment.

Always follow all applicable safety procedures, such as Occupational Safety and Health Administration (OSHA) requirements, National Electrical Code (NEC) requirements, local code requirements, safe working practices, and good judgment.

General safety practices include, but are not limited to, the following:

- Read and follow all warning notices and instructions marked on the product or included in this manual before installing, servicing, or operating the equipment. Retain these safety instructions for future reference.
- All equipment must be properly grounded in accordance with the *Standards and Guidelines for Communication Sites* manual.
- Only a qualified technician familiar with similar electronic equipment must service this equipment.
- Never store combustible materials in or near equipment racks. The combination of combustible material, heat, and electrical energy increases the risk of a fire safety hazard.

1.6.3 Rack-Mounting the GGM 8000

IMPORTANT: Follow these precautions when rack-mounting the GGM 8000:

- **Elevated Operating Ambient** – If installed in a closed or multi-unit rack assembly, the ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer.
- **Reduced Air Flow** – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.
- **Circuit Overloading** – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- **Reliable Grounding (Earthing)** – Reliable grounding of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (use of power strips).

The procedure for rack-mounting the GGM 8000 chassis varies, depending on the chassis design:

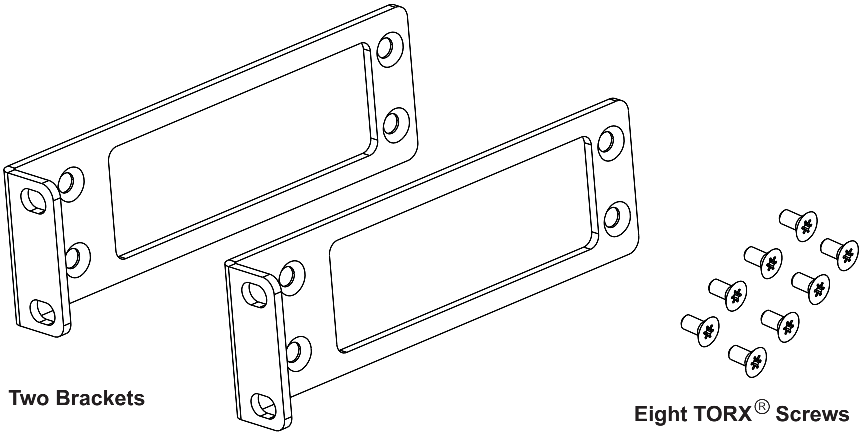
- If the GGM 8000 chassis has two TORX® screws on top, perform the procedure in one of the following sections:
  - Rack-Mounting the GGM 8000 (Chassis with the TORX Screws) – Front-Mount on page 58
  - Rack-Mounting the GGM 8000 (Chassis with the TORX Screws) – Mid-Mount on page 61
- If the GGM 8000 chassis does not have TORX® screws on top, perform the procedure in section Rack-Mounting the GGM 8000 (Chassis without the TORX Screws) on page 64.

1.6.3.1 Rack-Mounting the GGM 8000 (Chassis with the TORX Screws) – Front-Mount

Prerequisites: Obtain:

- Pan-head screws (4) for rack-mounting
- TORX® screws (8) for rack-mounting (provided with the rack-mount kit)
- TORX® driver set
- Rack-mounting kit

Figure 18: GGM 8000 Rack-Mounting Kit Contents



rack-mount-kit-revised_A

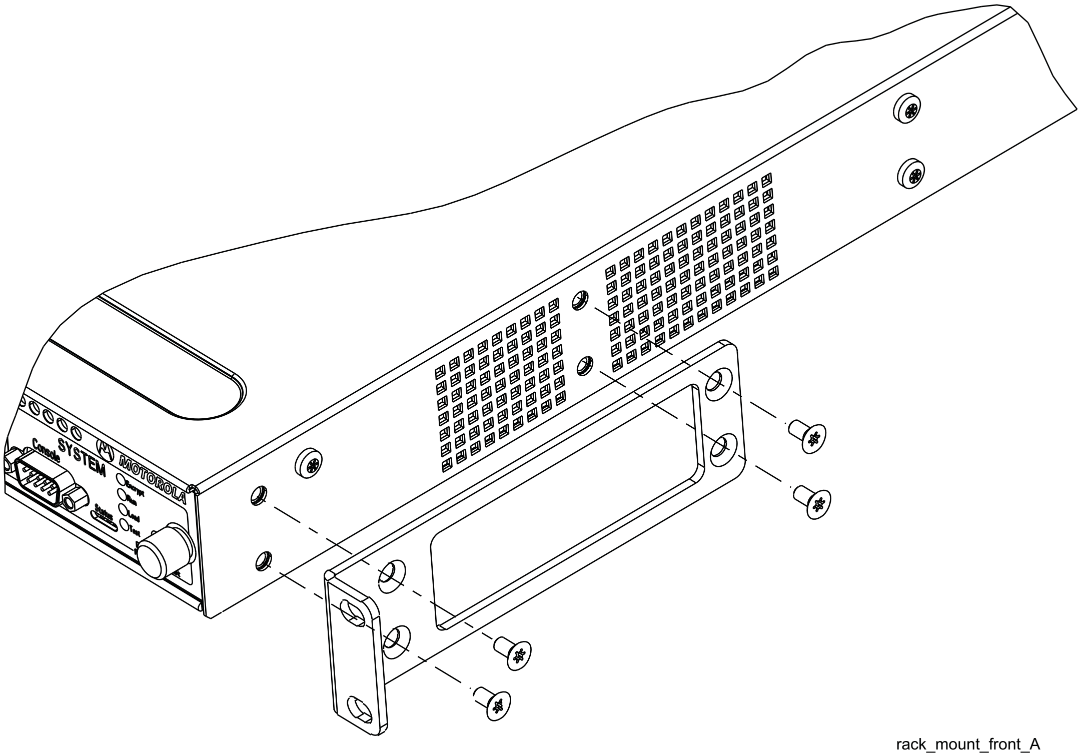
CAUTION: Do not restrict air flow around the sides, front, and back of the GGM 8000.

When and where to use: Use the procedure for the GGM 8000 with the two TORX® screws on the top of the chassis. See Physical Description on page 30.

Procedure:

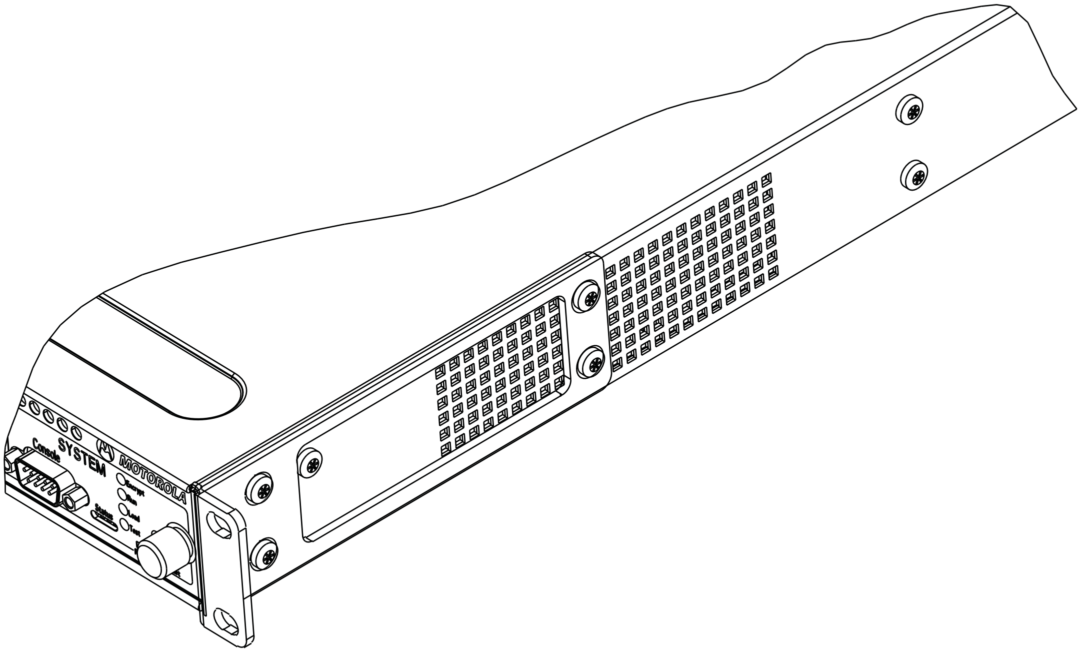
1 Using four of the TORX® screws provided in the rack-mount kit, attach one of the rack-mount brackets in the front-mount position.

Figure 19: Attaching the Rack-Mount Bracket to the Chassis (Front-Mount Applications)



rack_mount_front_A

Figure 20: Rack-Mount Bracket Attached to the Chassis (Front-Mount Applications)



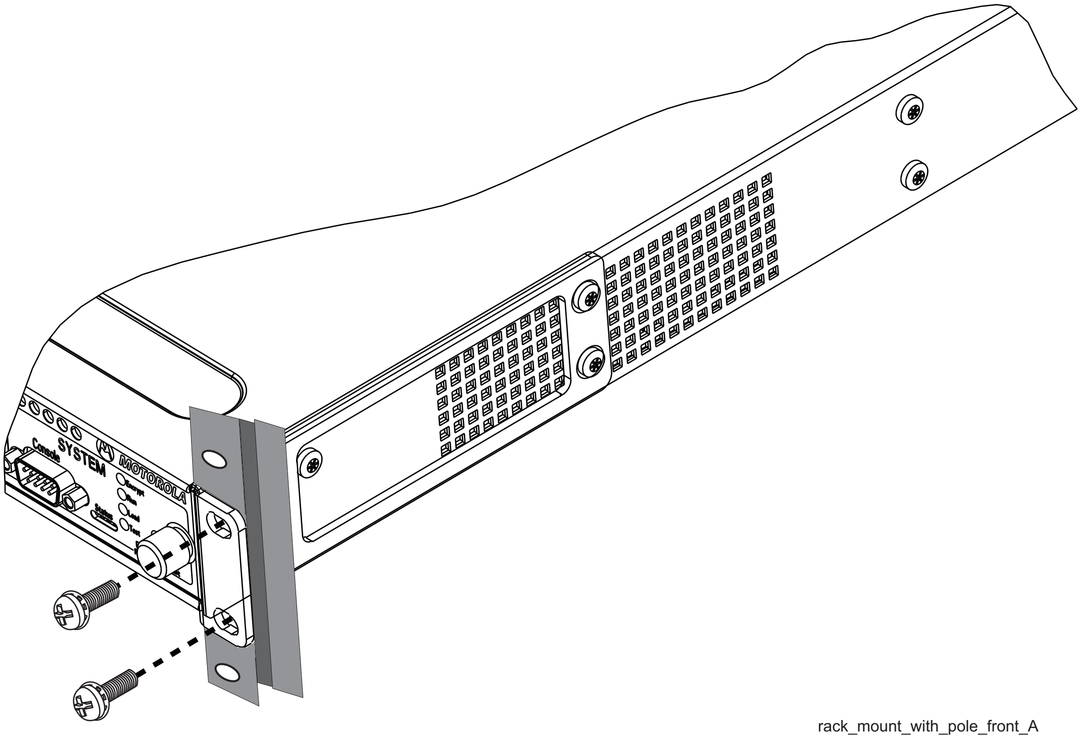
rack_mount_bracket_attached_front_A

2 Repeat step 1 to attach the other rack-mount bracket to the other side of the chassis using the four remaining TORX® screws provided in the rack-mount kit.

3 Hold the chassis between the poles of the rack and attach the brackets to the rack using two pan-head screws on each side (you must provide these screws).

⚠ **CAUTION:** Using fewer than two screws on each side to secure the brackets to the rack may cause the GGM 8000 to fall and sustain damage not covered by the warranty.

Figure 21: Securing the GGM 8000 in the Rack (Front-Mount Applications)



rack_mount_with_pole_front_A

4 Tighten each screw securely.

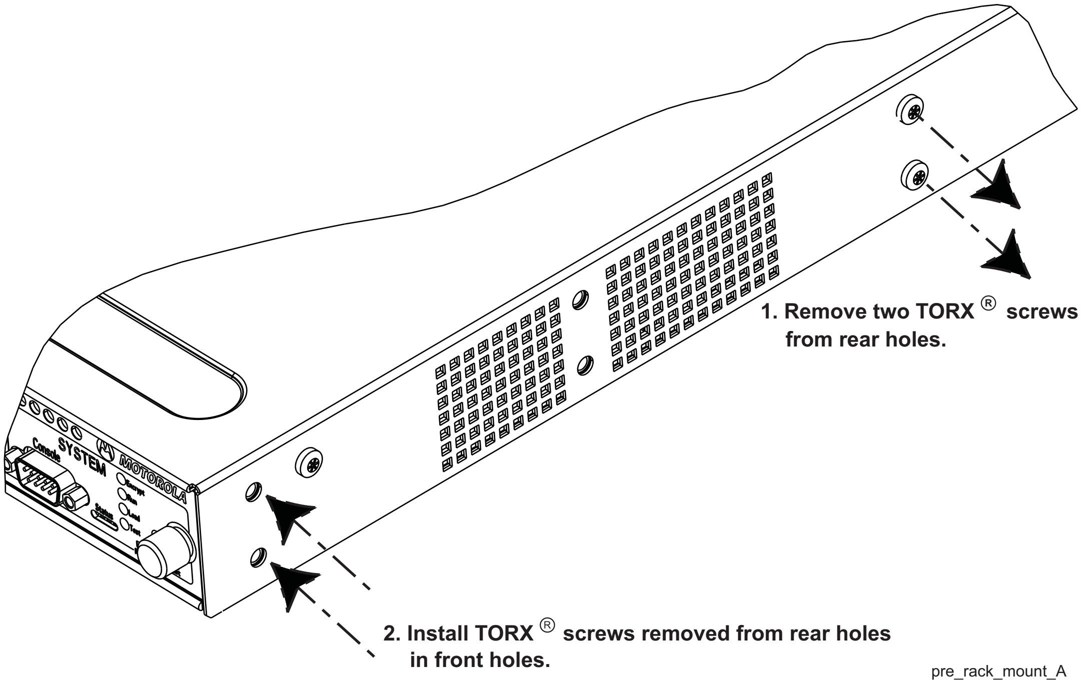
1.6.3.2
Rack-Mounting the GGM 8000 (Chassis with the TORX Screws) – Mid-Mount

When and where to use: Use the procedure for the GGM 8000 with the two TORX® screws on the top of the chassis. See Physical Description on page 30.

Procedure:

1 On one side of the chassis, remove the two TORX® screws installed in the pair of holes closest to the rear of the chassis and re-install them in the pair of holes closest to the front of the chassis.

Figure 22: Move the Pre-Installed TORX Screws to Prepare for Mid-Mount Rack Mounting


1. Remove two TORX ® screws from rear holes.
2. Install TORX ® screws removed from rear holes in front holes.
Console
SYSTEM
MOTOROLA
pre_rack_mount_A

2 Using four of the TORX® screws provided in the rack-mount kit, attach one of the rack-mount brackets in the mid-mount position.

Figure 23: Attaching the Rack-Mount Bracket to the Chassis (Mid-Mount Applications)

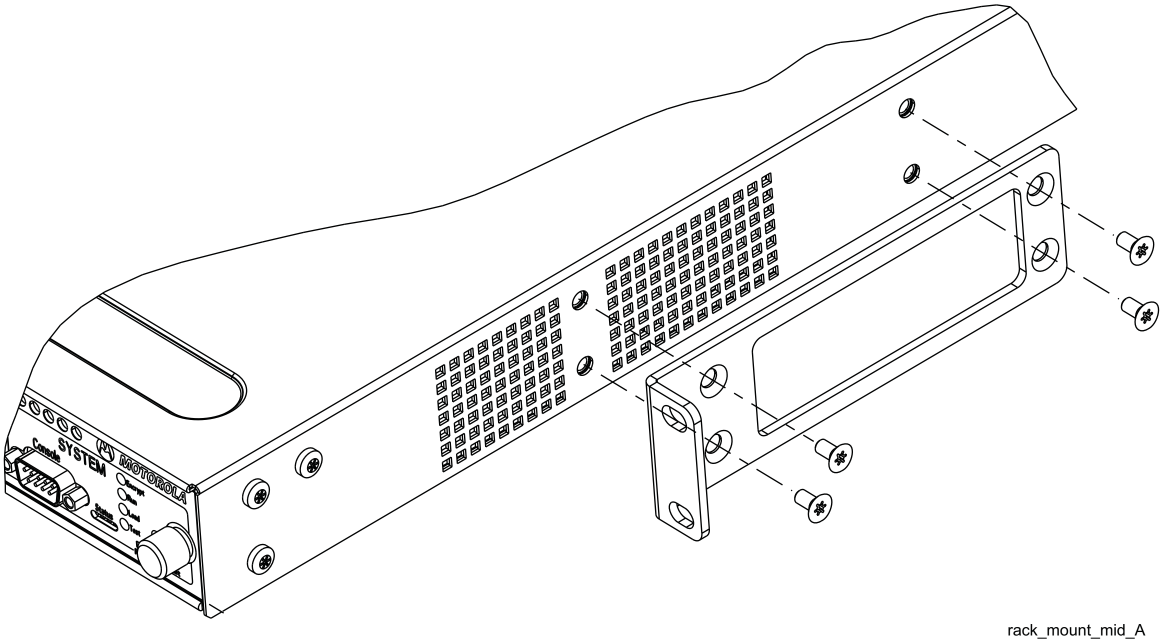
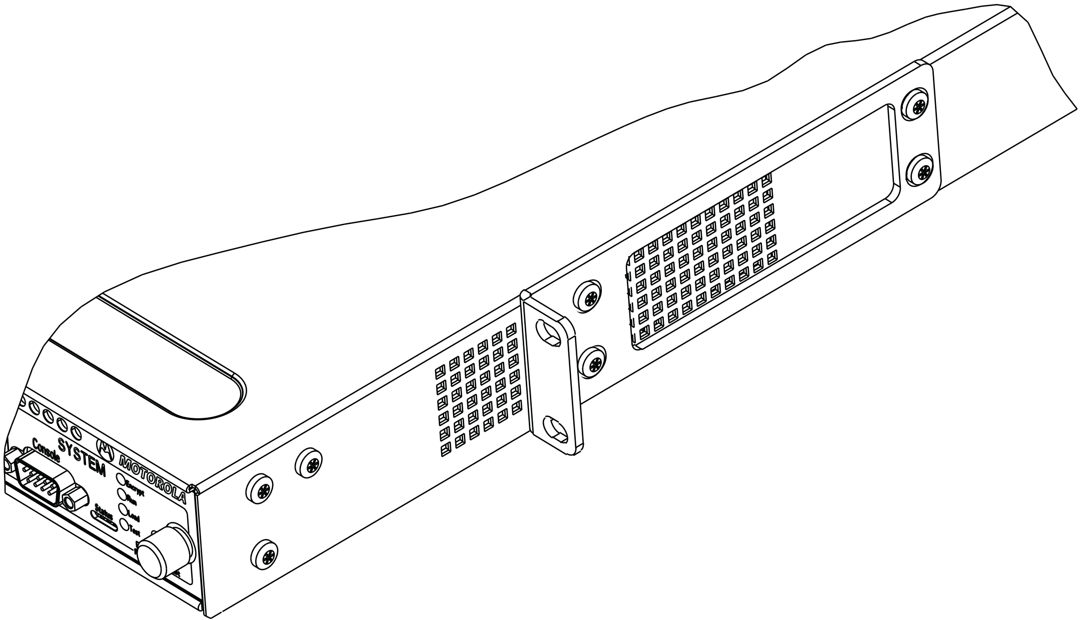


Figure 24: Rack-Mount Bracket Attached to the Chassis (Mid-Mount Applications)



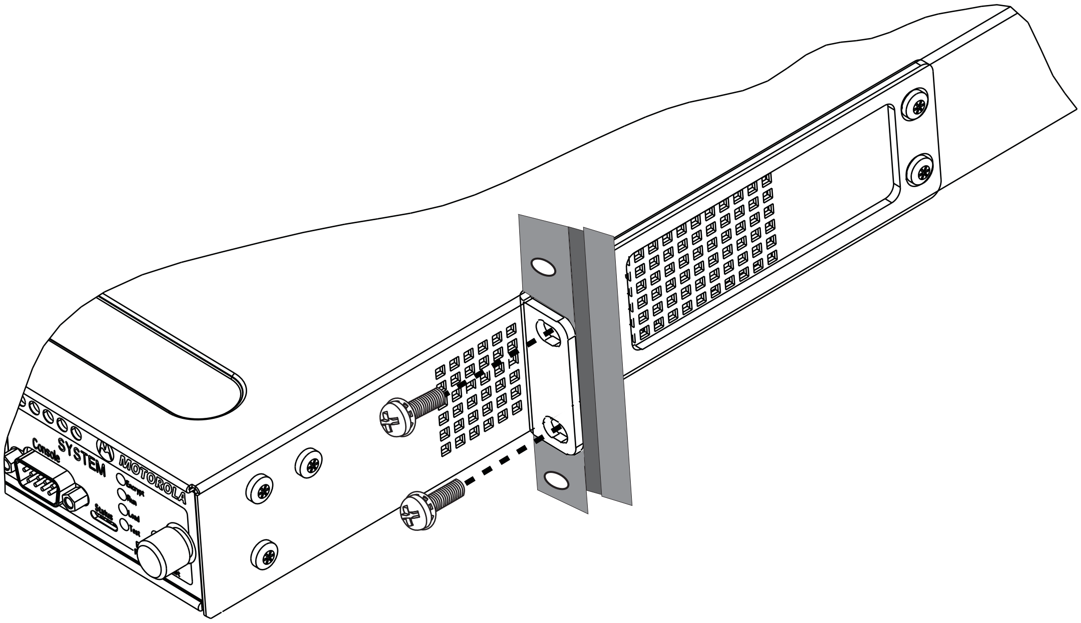
rack_mount_bracket_attached_mid_A

3 Repeat step 1 and step 2 to move the pre-installed TORX® screws from the rear holes to the front holes and to install the other rack-mount bracket on the other side of the chassis using the four remaining TORX® screws provided in the rack-mount kit.

4 Hold the chassis between the poles of the rack and attach the brackets to the rack using two pan-head screws on each side (you must provide these screws).

⚠ **CAUTION:** Using fewer than two screws on each side to secure the brackets to the rack may cause the GGM 8000 to fall and sustain damage not covered by the warranty.

Figure 25: Securing the GGM 8000 in the Rack (Mid-Mount Applications)



rack_mount_with_pole_mid_A

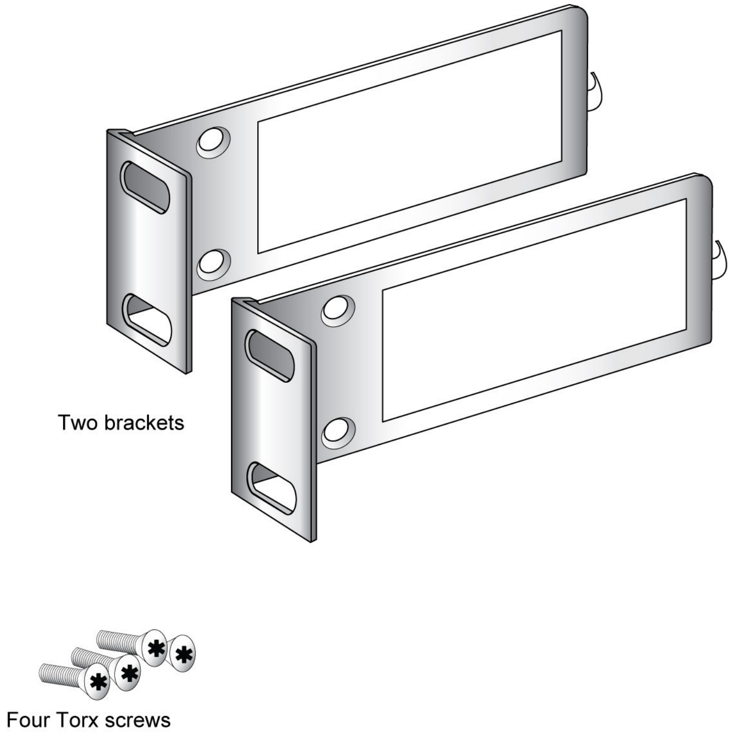
5 Tighten each screw securely.

1.6.3.3 Rack-Mounting the GGM 8000 (Chassis without the TORX Screws)

Prerequisites: Obtain:

- Pan-head screws (4) for rack-mounting
- TORX® screws (4) for rack-mounting (provided with the rack-mount kit)
- TORX® driver set
- Rack-mounting kit

Figure 26: GGM 8000 Rack-Mounting Kit Contents



rack_mnt_kit

CAUTION: Do not restrict air flow around the sides, front, and back of the GGM 8000.

When and where to use: Use the procedure for the GGM 8000 without the two TORX® screws on the top of the chassis. See Physical Description on page 30.

Procedure:

1 Hook the tab of one of the rack-mount brackets into a venting hole on the side of the GGM 8000 chassis.

  - For front-mount applications, align the holes on the bracket with the threaded holes toward the front of the chassis, as shown in Figure 27: Aligning the Rack-Mount Bracket for Front-Mount Applications on page 65.
  - For mid-mount applications, align the holes on the bracket with the threaded holes toward the middle of the chassis, as shown in Figure 28: Aligning the Rack-Mount Bracket for Mid-Mount Applications on page 65.

Figure 27: Aligning the Rack-Mount Bracket for Front-Mount Applications

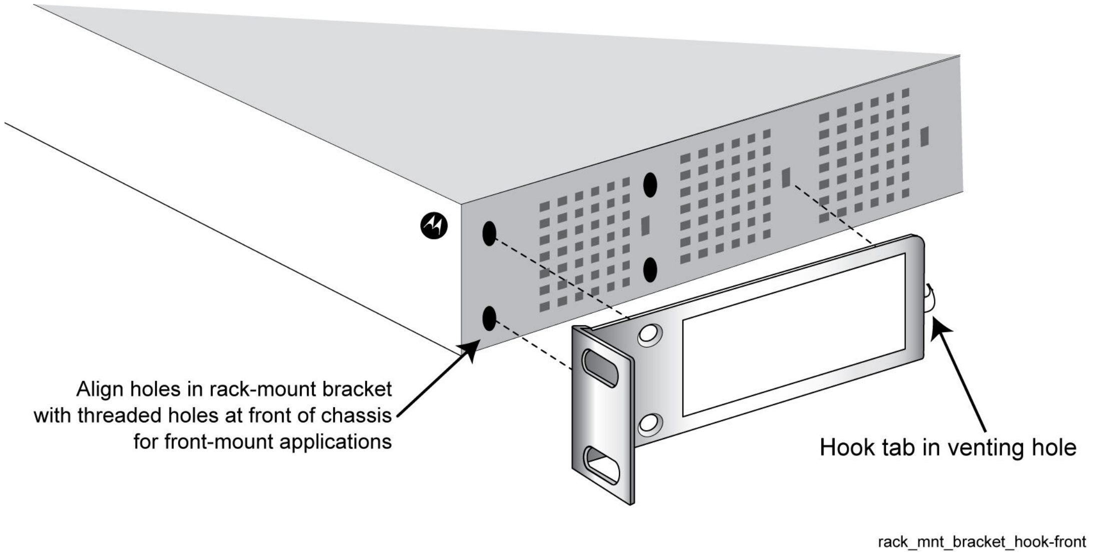
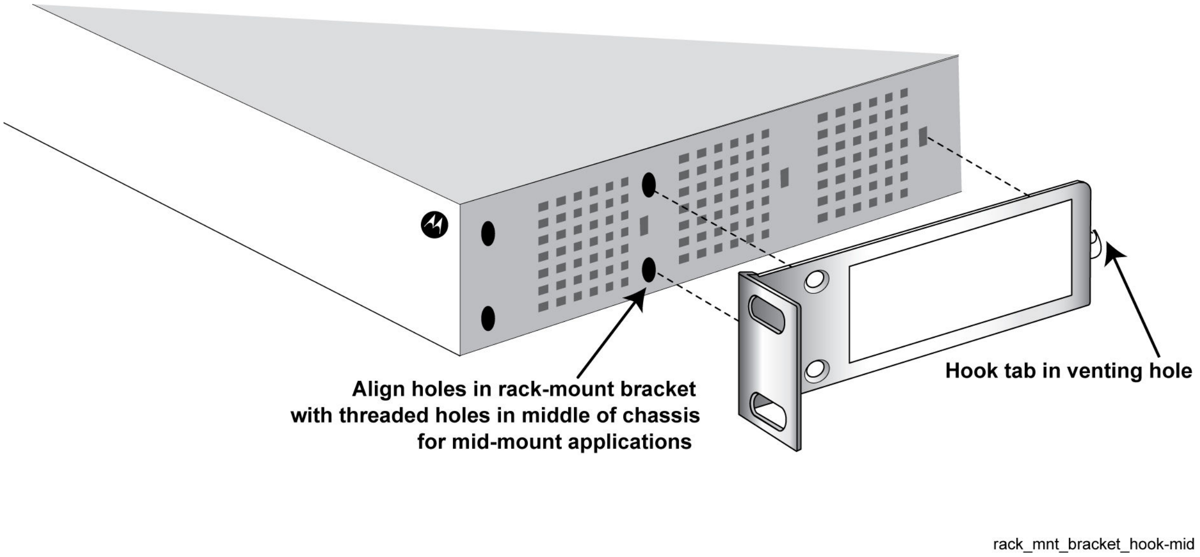
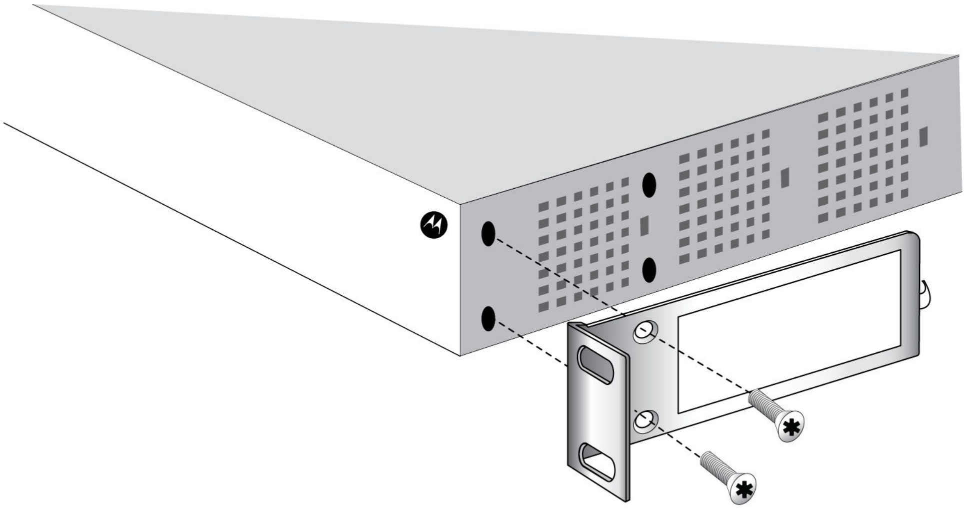

Align holes in rack-mount bracket
with threaded holes at front of chassis
for front-mount applications
Hook tab in venting hole
rack_mnt_bracket_hook-front

Figure 28: Aligning the Rack-Mount Bracket for Mid-Mount Applications


Align holes in rack-mount bracket
with threaded holes in middle of chassis
for mid-mount applications
Hook tab in venting hole
rack_mnt_bracket_hook-mid

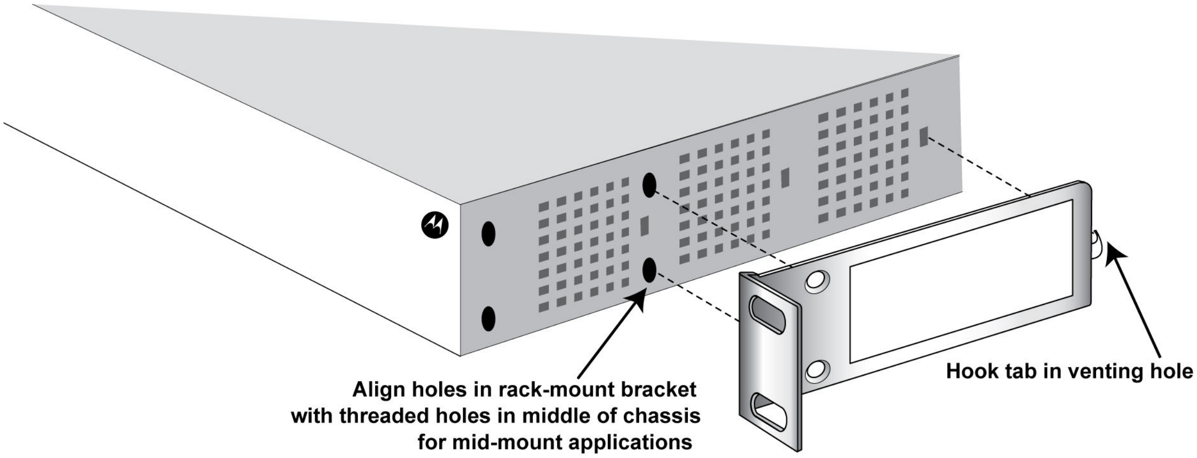
2 Secure the rack-mount bracket to the side of the chassis using two TORX® screws, as illustrated in Figure 29: Securing the Rack-Mount Bracket (Front-Mount Applications) on page 66 and Figure 30: Securing the Rack-Mount Bracket (Mid-Mount Applications) on page 66.

Figure 29: Securing the Rack-Mount Bracket (Front-Mount Applications)



rack_mnt_bracket_front

Figure 30: Securing the Rack-Mount Bracket (Mid-Mount Applications)


Align holes in rack-mount bracket
with threaded holes in middle of chassis
for mid-mount applications
Hook tab in venting hole

rack_mnt_bracket_hook-mid

3 Repeat step 1 and step 2 to attach the other rack-mount bracket to the other side of the GGM 8000 chassis.

4 Hold the chassis between the poles of the rack and attach the brackets to the rack using two panhead screws on each side (you must provide these screws), as illustrated in Figure 31: Securing the GGM 8000 in the Rack (Front-Mount Applications) on page 67 and Figure 32: Securing the GGM 8000 in the Rack (Mid-Mount Applications) on page 67.

⚠ **CAUTION:** Using fewer than two screws on each side to secure the brackets to the rack may cause the GGM 8000 to fall and sustain damage not covered by the warranty.

Figure 31: Securing the GGM 8000 in the Rack (Front-Mount Applications)

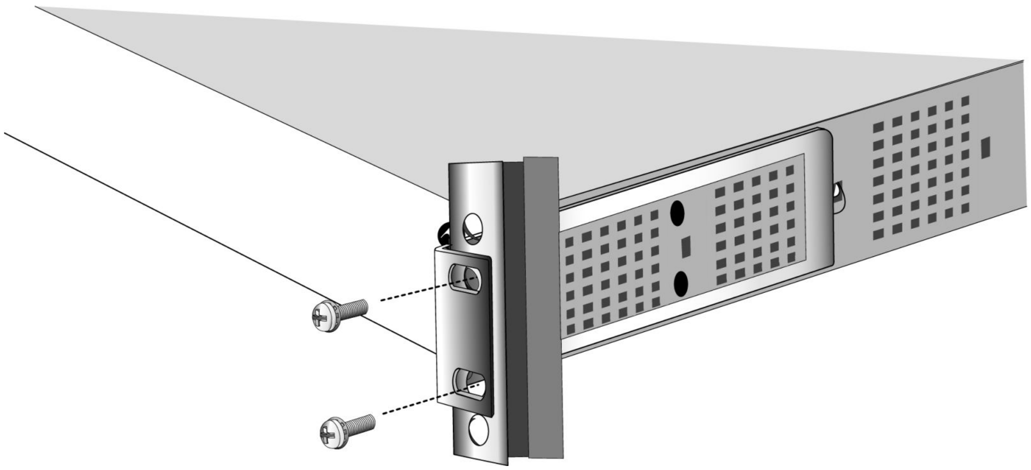
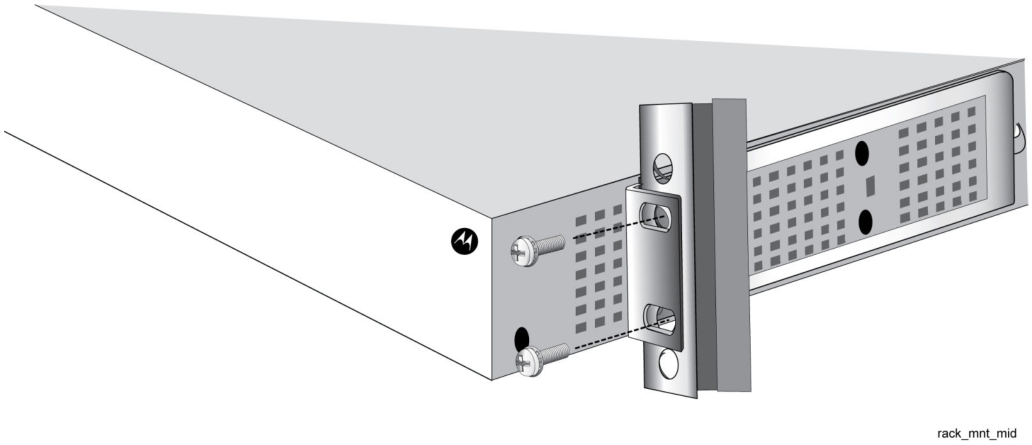


Figure 32: Securing the GGM 8000 in the Rack (Mid-Mount Applications)



5 Tighten each screw securely.

1.6.4 Connecting the GGM 8000 to a Power Source

The GGM 8000 supports a removable AC or DC power subsystem module.

- The AC power subsystem module provides a single power receptacle.
- The DC power subsystem module provides two DC power entry connectors.

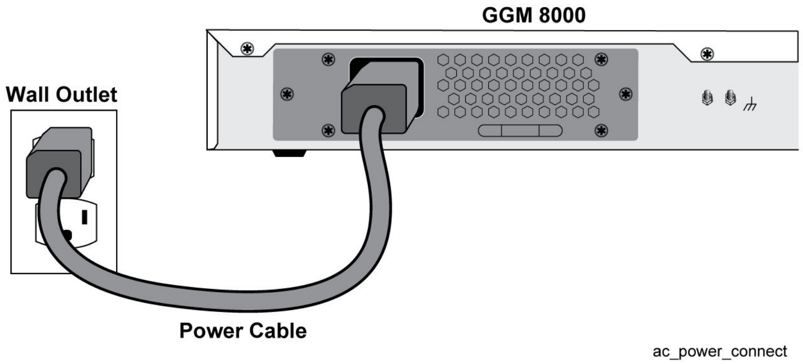
For details about how to replace a GGM 8000 power subsystem module, see Replacing the GGM 8000 Power Subsystem Module on page 137.

1.6.4.1 Connecting the GGM 8000 to an AC Power Source

Procedure:

1. Attach the female end of the power cable to the power connector on the GGM 8000 power subsystem module, located on the rear panel of the GGM 8000.
2. Attach the male end of the power cable to a wall outlet, as illustrated in the following figure.

Figure 33: Cabling the GGM 8000 AC Power Subsystem Module



1.6.4.1.1 Connecting a Chassis Ground

When and where to use: Some network topologies require an additional earth ground connection to the equipment chassis that is separate from the AC safety ground. If this type of grounding (earthing) is required for your topology, follow this procedure to connect a separate ground cable to the GGM 8000 chassis.

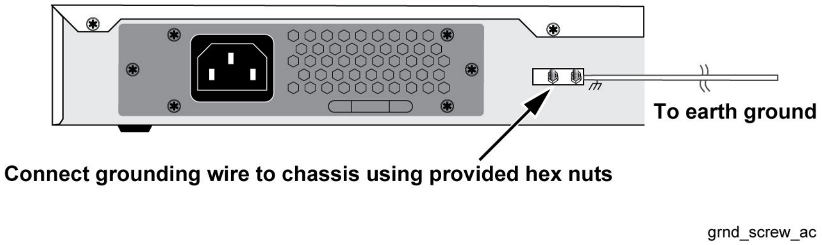
NOTICE: See the *Standards and Guidelines for Communication Sites* manual for additional information on proper bonding and ground at a site.

Procedure:

1. Remove the two M6 lock nuts from the studs on the rear of the chassis and set them aside.
2. Using #6 AWG grounding wire terminated with UL-listed two-hole rectangular grounding lugs on both ends, position the grounding lug on one end of the wire over the studs on the rear of the GGM 8000 chassis.

   NOTICE: If the length of the grounding wire must exceed 4 meters before it is terminated, grounding wire larger than #6 AWG is required. See the *Standards and Guidelines for Communication Sites* manual for details.
3. Attach the lock nuts that you removed in step 1 to the chassis studs, tightening the nuts to attach the ground cable lug to the rear of the chassis, as illustrated in the following figure.

Figure 34: Grounding the GGM 8000 (AC Power Subsystem Module)



4. Terminate the other end of the wire on a permanently-connected protective grounding conductor.

1.6.4.2 GGM 8000 to a Centralized DC Power Source Connection

Read this section completely before making the DC power connections.

IMPORTANT: To reduce the risk of electric shock or energy hazards, follow the guidelines outlined in the DC input power connection caution notice below.

CAUTION: DC INPUT POWER CONNECTION GUIDELINES:

1. Only trained and qualified personnel should be allowed to install or replace this equipment.
2. Before working on equipment that is connected to power, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal objects to the terminals.
3. For a centralized DC power connection (battery bank), the GGM 8000 is to be installed only in Restricted Access Locations (Dedicated Equipment Rooms, Equipment Closets, or the like) in accordance with Articles 110.26 and 110.27 of the National Electrical Code, ANSI/ NFPA 70 (2008).
4. Damage may result if power is connected improperly.

The GGM 8000 DC power subsystem module is designed to operate from a DC output power source with a nominal output level of 24 V to 48 V DC. A GGM 8000 equipped with a DC power subsystem module can be deployed as a standalone device that is powered by a centralized DC power source provided the following installation criteria are met:

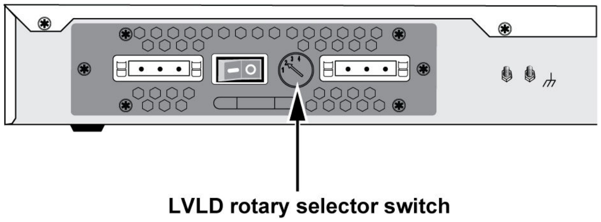
- The GGM 8000 must be deployed within a Restricted Access Location (RAL). An RAL is a location where access can only be gained by service personnel by using a special tool, lock, and key, or other means of security, and is controlled by the authority responsible for the location.
- The current rating of the circuit breaker in the DC branch circuit must be 15A or less.
- The GGM 8000 should be connected to the DC power source via the GGM 8000 DC power tray cable (part number DKN6145A) or equivalent.
- The GGM 8000 DC power tray cable should be supported by a cable tray and securely fastened to the tray as described in Connecting the GGM 8000 to a Centralized DC Power Source on page 70.

  IMPORTANT: Provide proper strain relief for the DC power tray cable. Route and secure the cable to protect it from strain and external forces. Careful cable routing and securing the cable with tie wraps (or other devices) is one way to provide this protection.

1.6.4.2.1 Setting the LVLD Level

The GGM 8000 supports a low voltage local disconnect (LVLD) feature that electronically disconnects the GGM 8000's DC power subsystem from the DC power source when the DC input voltage level drops below a specified level. You set the LVLD level using the four-position rotary selector switch. This switch is located on the GGM 8000 power subsystem module, as shown in the following figure.

Figure 35: LVLD Rotary Selector Switch on GGM 8000 DC Power Subsystem Module



rotary_switch_location

The LVLD feature safeguards against potential battery damage when the DC power is being provided directly by batteries. Without the LVLD feature, the batteries could be damaged by excessive discharge when the DC input voltage level drops below a certain level. When the GGM 8000 DC power subsystem disconnects due to low supply voltage, the subsystem draws less than 1ma of current.

For details about how to set the rotary selector switch, see Connecting the GGM 8000 to a Centralized DC Power Source on page 70.

1.6.4.2.2

Connecting the GGM 8000 to a Centralized DC Power Source

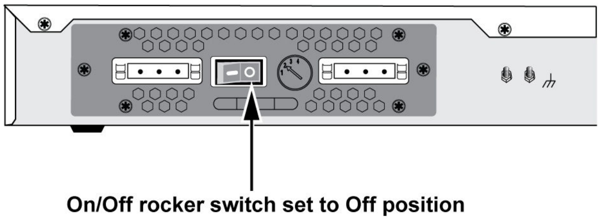
Prerequisites:

IMPORTANT: Before connecting the GGM 8000 to a centralized DC power source, read Setting the LVLD Level on page 69 and fulfill all requirements mentioned in GGM 8000 to a Centralized DC Power Source Connection on page 69.

Procedure:

1. Ensure that the On/Off rocker switch on the GGM 8000 DC power subsystem module is set to the Off position, as illustrated in the following figure.

   Figure 36: Setting the On/Off Rocker Switch to the Off Position

   dc_off

2. Using a 2.5 mm flat blade screwdriver, turn the recessed arrow to set the LVLD rotary selector switch to the setting corresponding to the DC output level of your battery-based DC power supply, as illustrated in the following figure. Table 10: Correlation Between Rotary Selector Switch and LVLD Levels on page 71 correlates the switch settings with the LVLD levels and corresponding nominal battery voltages.

   NOTICE: The supply voltage first must come up to the "Nominal Battery Voltage" before the GGM 8000 DC power subsystem module will start operating. Once the power subsystem module is operational, if the "Nominal Battery Voltage" drops to its "LVLD Level" or below, it will disconnect.

Figure 37: Setting the GGM 8000 LVLD Rotary Selector Switch

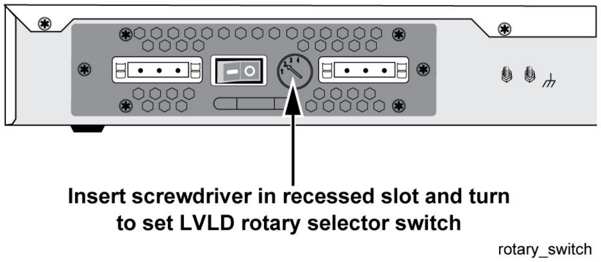

Insert screwdriver in recessed slot and turn
to set LVLD rotary selector switch
rotary_switch

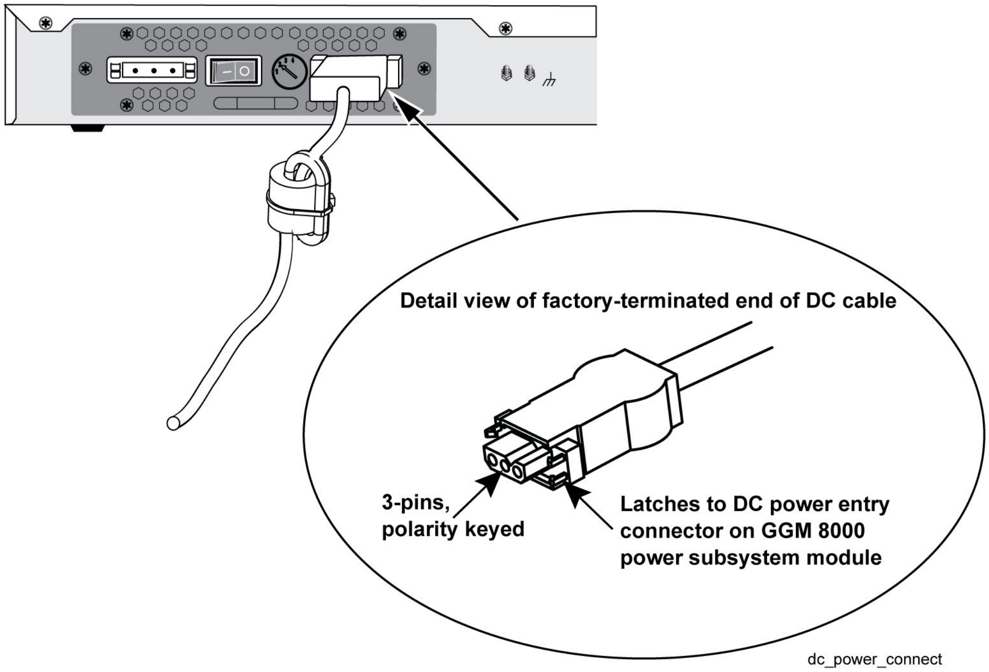
Table 10: Correlation Between Rotary Selector Switch and LVLD Levels

Switch Setting	LVLD Level	Nominal Battery Voltage
1	19 V	24 VDC
2	23 V	28 VDC
3 (Not Used)	N/A	N/A
4	42 V	48 VDC

3 Plug the connector on the terminated end of the GGM 8000 power tray cable into one of the two DC power entry connectors on the GGM 8000 DC power subsystem module, as shown in the following figure.

IMPORTANT: Make certain the connector on the power cable latches securely with the DC power entry connector on the power subsystem module.

Figure 38: Connecting the DC Power Tray Cable to the GGM 8000 DC Power Subsystem Module



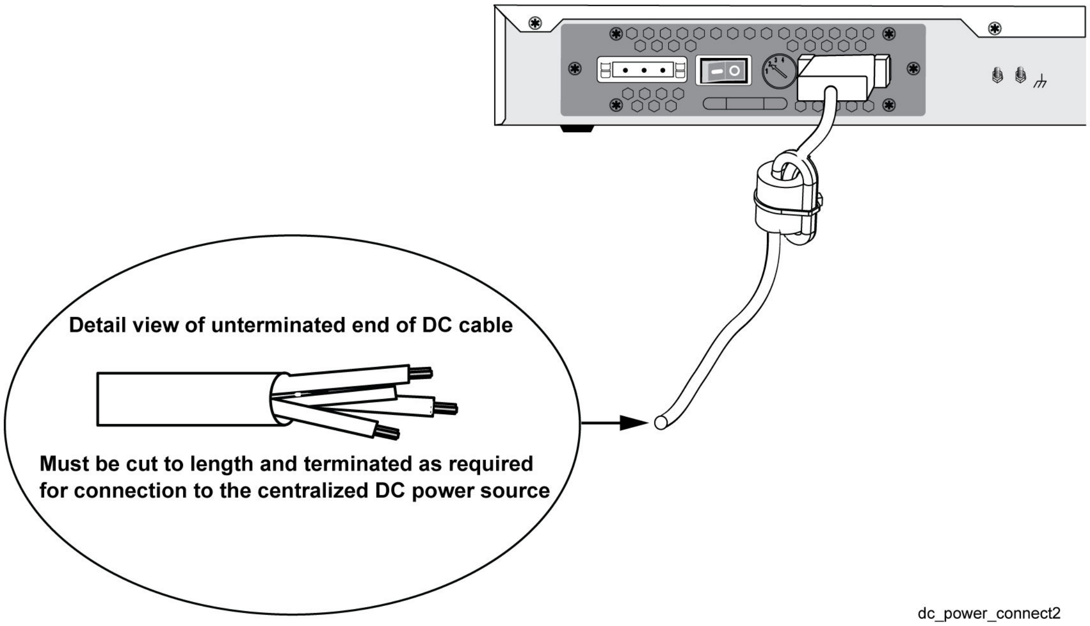
4 If you connect GGM 8000 to two DC power sources, repeat step 3 to connect a second GGM 8000 power tray cable to the other DC power entry connector on the GGM 8000 power subsystem module.

5 Support the GGM 8000 DC power tray cable(s) in a cable tray and secure the cable(s) to the cable tray near the rack framework using multiple cable ties to minimize the chance of connections being disturbed by casual contact with the wiring.

CAUTION: Use at least four cable ties separated by 4 inches, with the first tie located within six inches of the GGM 8000 DC power entry connector. Also take care to minimize tight bending radii; the bending radius should not be smaller than 4 times the cable diameter.

6 Cut the unterminated end of the GGM 8000 power tray cable(s), illustrated in the figure below, to length and terminate the wire ends for the connection to the DC power source(s).

Figure 39: Preparing the DC Power Tray Cable for Connection to the DC Power


Detail view of unterminated end of DC cable
Must be cut to length and terminated as required for connection to the centralized DC power source
dc_power_connect2

a Using a wire-stripping tool, strip each of the three wires on the unterminated end of the GGM 8000 power tray cable(s) to the appropriate length for the terminal.

WARNING: Do not strip more than the amount of wire required to accommodate the terminal. Stripping more than the required amount of wire can create a safety hazard by leaving exposed wire on the terminal block.

b Using a wire-crimping tool, crimp the terminals to the wires.

NOTICE: Crimping the terminals to the wires is not required if the DC power source(s) have compression-style terminals.

7 Confirm that there is no power present on the DC power source(s) before proceeding to connect the GGM 8000 to the power source(s). Use appropriate disconnection means and lock-out, tag-out procedures as necessary.

8 Identify the positive, safety/earth ground, and negative terminals on the DC power source(s).

9 Connect the terminated wire ends from the GGM 8000 tray cable to the DC power source(s):

WARNING: Make the connections in accordance with all applicable safety regulations, such as the national electrical codes, as well as any other locally-applicable safety standards.

a Connect the wire from the middle connector (pin 2) on the DC power entry connector to the safety/earth ground terminal on the DC power source.

WARNING: When connecting the DC power to the GGM 8000, always ensure that the GGM 8000 tray cable safety/earth ground wire is connected to the power source first.

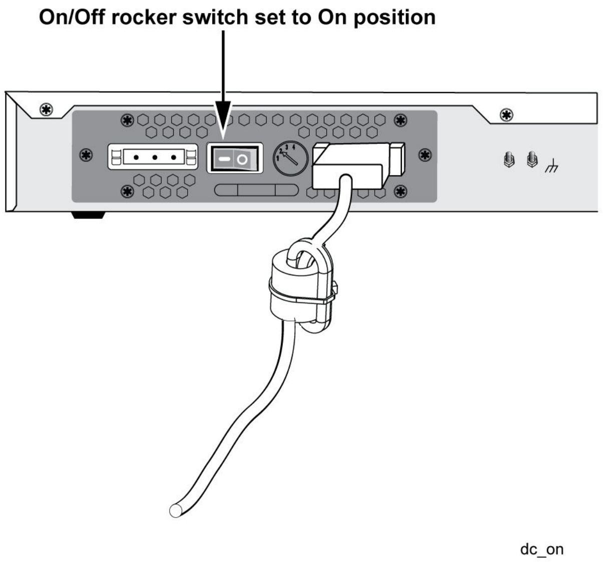
b Connect the other two wires (from pins 1 and 3) on the GGM 8000 DC power entry connector to the positive (+) and negative (-) output terminals on the DC power source. It does not matter which wire you connect to the positive terminal and which wire you connect to the negative terminal the GGM 8000 supports either polarity.

c If you connect GGM 8000 to two DC power sources, repeat steps a and b for the second power source.

10 Restore power to the DC power sources.

11 Set the On/Off rocker switch on the GGM 8000 DC power subsystem module to the On positions, as illustrated in the following figure.

Figure 40: Setting the On/Off Rocker Switch to the On Position



1.6.5
Conventional Channel Gateway – Installation

When and where to use: Follow this process to install any Conventional Channel Gateway.

Process:

1 If necessary, install the CCGW hardware in the GGM 8000.

- For details about how to install the analog/V.24 interface kit, see Replacing Daughterboards on the GGM 8000 on page 129.
- For details about how to install the Enhanced Conventional Gateway module, see Replacing the GGM 8000 ECGW Module on page 134.

NOTICE: If the GGM 8000 is ordered with an analog/V.24 kit or an Enhanced Conventional Gateway module, the optional hardware is mounted at the factory.

2. Install the Conventional Channel Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
3. Connect the Conventional Channel Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
4. If necessary, ground the Conventional Channel Gateway. See Connecting a Chassis Ground on page 68.
5. Configure the Conventional Channel Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

   IMPORTANT: Last 3 steps of Downloading a Stored Configuration File to the GGM 8000 on page 93 do not apply to configurations without the UNC application.

6. Connect the site equipment to the Conventional Channel Gateway. See one of the following:
   - Conventional Conduit Hub Site – GGM 8000 Installation on page 235
   - Conventional Hub Site – GGM 8000 Installation on page 238
   - Conventional Base Radio Site – GGM 8000 Installation on page 244

1.6.5.1 Software Installation

No additional software programs need installing, in addition to the software installed as part of the routine installation procedures. The Conventional Channel Gateway (CCGW) ships with all the necessary software pre-installed. The software includes both the MNR ASTRO® Smart/Zone Software Upgrade and the Enterprise Operating System (EOS). If a firmware downgrade is necessary due to an MNR replacement, check the version of the firmware. Additional steps may be required depending on the firmware version. See Performing a Firmware Downgrade on page 273.

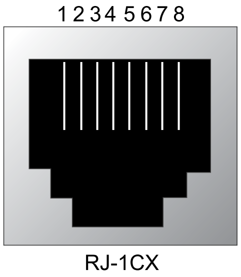
EOS enables the GGM 8000 Gateway to coexist as a CCGW, and enables the CCGW to be configured for conventional operation. Conventional operation is achieved by executing commands that are contained in a configuration file (boot.cfg) that is executed when the gateway is booted up. Once these commands have been executed, EOS initializes the CCGW, enabling it to communicate with the Network Management system LDAP service. EOS configures the CCGW based on the LDAP configuration.

A CCGW configuration file (CCGWDB) is created on the EOS flash. This file contains the latest CCGW configuration from the network management LDAP server. It is updated when changes are received from the Network Management LDAP server after the CCGW has been rebooted and is used for boot-up persistence. If the CCGW cannot communicate with the LDAP server, it reads the configuration from the EOS flash.

1.6.5.2 E&M (Analog) Connections

When configured with the optional analog/V.24 interface kit, the GGM 8000 supports four 4-wire E&M (analog) connectors, labeled 8D, 8C, 8B, and 8A on the expansion module analog slot. The following figure illustrates the pin locations on the connector.

Figure 41: GGM 8000 E&M (Analog) Connector



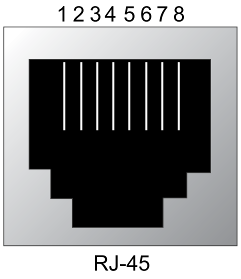
The following table lists the connector pinouts.

Table 11: GGM 8000 E&M (Analog) Connector Pinouts

Pin Number	Name
1	Tip-2
2	Ring-2
3	E-Lead
4	Ring-1
5	Tip-1
6	SG (Signal Ground)
7	M-Lead
8	SB (Signal Battery)

When configured with the optional Enhanced Conventional Gateway module, the GGM 8000 supports eight (Low Density Enhanced Conventional Gateway) or 16 (High Density Enhanced Conventional Gateway) RJ-45 connectors, functioning in pairs to support four (Low Density Enhanced Conventional Gateway) or eight (High Density Enhanced Conventional Gateway) analog interfaces. The following figure illustrates the pin locations on the connectors.

Figure 42: GGM 8000 Enhanced Conventional Gateway Module Connector



The following table describes the signal assignments.

Table 12: GGM 8000 Enhanced Analog Interface Signal Assignments

Connector Group	Pins	Function
Audio, E&M (yellow)	1/2	4-wire audio receive input
	3/6	E-Lead (PTT output)

Connector Group	Pins	Function
	4/5	2-wire audio receive input/ output 4-wire audio transmit output
	7/8	M-Lead (COR or CIU coded/ clear)
Analog I/O (white)	1/2	LOBL (voltage-level or contact closure input detector)
	4/5	Mute (contact closure input detector)
	3/6	Audio output (for audio logging detector)
	7/8	Base station coded/clear (contact closure input detector)

1.6.5.2.1 QUANTAR to Site Gateways (Conventional Channel Interface)

Figure 43: QUANTAR Base Station Interconnections – 4-Wire Interface on page 79 shows the recommended wiring scheme for directly connecting a Conventional Channel Gateway to a QUANTAR® base station (one of the more commonly used types of base station) through the Analog Conventional ports. For the specific port number on the base station that is used to connect the 4W interface cable, refer to the documentation supplied with the particular base station.

While the figure shows a 5 V supply output on the base station as the voltage source for the current detector on the base station, the CCGW safely accepts any voltage source between ±60 VDC. However, the voltage output of the source must not cause the optically isolated current detector on the base station to exceed its maximum current rating.

1.6.5.2.2 GGM 8000 Analog Interfaces to a QUANTAR or GTR 8000 Base Station Connections

The GGM 8000 is physically connected to an analog base station through one or more of the analog interface ports:

- For a GGM 8000 equipped with an Enhanced Conventional Gateway module, channels can be configured to interpret the analog audio from pins 1, 2, 4, and 5 on the middle (yellow) bank of RJ-45 connectors (labeled “Analog audio, E&M”) as either a 2-wire, a 4-wire, or a 2-wire/4-wire audio connections.
- A GGM 8000 equipped with an expansion module and analog/V.24 interface kit supports 4-wire audio connections only.

When configured for 4-wire audio connections, the GGM 8000 analog interface operates in E&M Type II mode. In E&M Type II mode, the two line-control functions are implemented with two current loops. Each side of an E&M Type II connection has a relay, a voltage source, and a current detector:

- The relay/switch function in the GGM 8000 analog interface is provided on the E and SG signals. The E and SG signals are connected to a voltage source and an optically-isolated current detector on the base station to form a current loop controlled by the GGM 8000. The base station detects GGM 8000 relay closure with its current detector. See Figure 43: QUANTAR Base Station Interconnections – 4-Wire Interface on page 79.

- The contacts of the base-station-controlled relay are interconnected with the M and SB signals on the GGM 8000 to form a current loop that is controlled by the base station. The GGM 8000 SB signal provides the low voltage source for the current loop and the current detector (on the GGM 8000 M-lead) detects base station relay closure.

The audio connections on the analog port consist of one signal pair for each direction (4-wire audio). The control signal pairs are designed to interoperate with E&M signals meeting the TIA/EIA-464 specification. According to this specification, the voltages on the line control signals must adhere to the following limits:

- The continuous working voltages on the E&M line control signals must not exceed 60 V in magnitude (nominal working voltage is -48VDC).
- Transient peaks of up to 300 V are permitted (for inductive or capacitive ringing).
- A level of 80 V is sustained for no more than 10 milliseconds.

Termination Impedance Recommendations

The audio signals on the GGM 8000 E&M module (included as part of the analog/V.24 interface kit) are designed for 600Ω resistively-terminated interfaces, and that the terminators on the base station be configured appropriately. The audio signals on the Enhanced Conventional Gateway module, on the other hand, can be configured for 600Ω, 900Ω, or 10KΩ impedance. In most cases where there is one device at the end of the connection, both ends of the analog audio signal connection should be terminated with 600Ω. In certain cases, however, other settings may be appropriate:

- The call logging signal output pair (pins 3/6 on the “Analog I/O” (white) connector has a fixed source impedance of 600Ω and ideally the device at the other end of the connection should also have a termination impedance of 600Ω.
- For the 4-wire signal pair input (pins 1/2 on the “Audio, E&M” (yellow) connector), the 600Ω termination impedance setting is normally used. The 10KΩ setting should only be used when more than one device is connected to the same end of the same signal line as the CCGW. 600Ω and 10KΩ are the only settings supported on this signal pair.
- For the 2-wire (bi-directional) signal pair (pins 4/5 on the “Audio, E&M” (yellow) connector), both ends of the connection should normally be configured to have 600Ω impedance. The other impedance settings (900Ω and 10KΩ) are used in the following scenarios:
    - With long cable runs, the characteristic line impedance of the cabling can be closer to 900Ω than to 600Ω. As a result, better performance (signal quality) can sometimes be obtained by configuring both ends of the connection to 900Ω.

        NOTICE: Long cable runs should be used only with the 2-wire (bi-directional) signal pair interface.

    - When more than one device is connected to the same signal line at the same end of the cable as the 2-wire signal interface, the 10KΩ setting may be needed.

NOTICE: The 10KΩ termination option actually disconnects the onboard termination network. This option is required only when more than one device is connected to the same signal pair at one end of the connection. In this case:

- Only one of the devices (at each end of the connection) must be configured to terminate the line.
- Alternatively, a separate external line terminator can be used at one or both ends of the cable.

CAUTION: For a GGM 8000 configured with the analog/V.24 interface kit or an Enhanced Conventional Gateway module on which pins 7/8 on either the “Analog I/O” or the “Audio, E&M” connector are configured as a voltage-level input detector, the analog interface of the GGM 8000 is designed to connect directly to analog stations that are physically located in the same room or building, or via a connection provided by a microwave link. If analog lines are used to connect the GGM 8000 to an analog station at another location, a primary surge suppression device must be installed. This limitation does not apply to a GGM 8000 configured with an Enhanced Conventional Gateway module on which pins 7/8 on either the “Analog I/O” or the “Audio, E&M” connector are configured as a transformer-coupled input detector. In this case, pins 7/8 provide a distance input buffer (DIB) which supports base stations in other buildings up to 4000 ft away.

1.6.5.2.3
GGM 8000 Analog Interface to a QUANTAR Base Station Connection

The cable pinouts vary, depending on whether the channel is configured to interpret the analog audio on pins 1, 2, 4, and 5 as a 4-wire interface or a 2-wire interface.

NOTICE: While QUANTAR® base stations do not specifically implement a standard E&M interface, they do include all the components (voltage supplies, relays, and current detectors) necessary to interoperate with the E&M interface on the GGM 8000.
It may be necessary to connect additional circuitry to accommodate various unique base station applications.

To achieve reliable relay/switch closure detection on pins 7 and 8 and pins 3 and 6, the base station must be colocated on the same premises as the GGM 8000

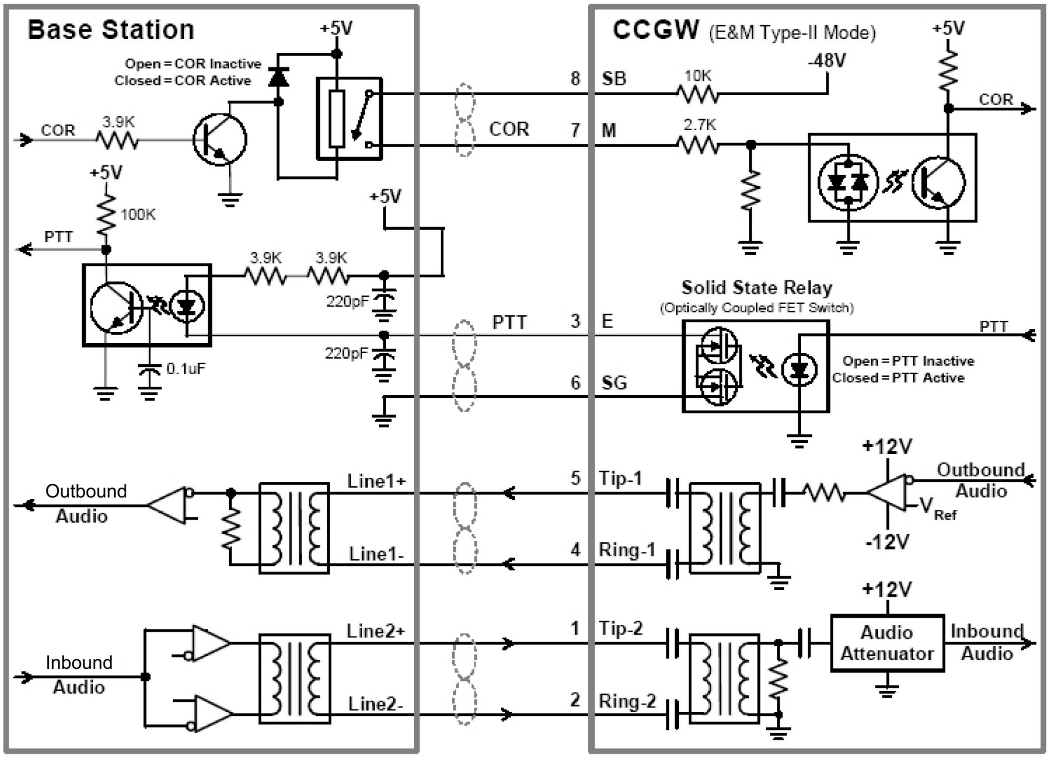
Connecting GGM 8000 Analog Interface to a QUANTAR Base Station 4–Wire Mode

To connect GGM 8000 analog ports configured as 4-wire interfaces to a QUANTAR® base station, connect the signals on the GGM 8000 analog port(s) to the base station as illustrated in the figure below. For the specific port number on the base station that is used to connect the 4-wire interface cable, refer to the documentation supplied with the base station. The GGM 8000 4-wire analog ports are:

- Ports 8D, 8C, 8B, 8A, 12D, 12C, 12B, and 12A on the High Density Enhanced Conventional Gateway.
- Ports 8D, 8C, 8B, and 8A on the Low Density Enhanced Conventional Gateway.
- Ports 8D, 8C, 8B, and 8A on the E&M daughterboard included as part of the analog/V.24 interface kit.

NOTICE: The following figure shows a 5-Volt supply output on the base station as the voltage source for the current detector on the base station. However the GGM 8000 safely accepts any voltage source between +/- 60 VDC, providing that the voltage output of the source does not cause the optically-isolated current detector on the base station to exceed its maximum current rating.

Figure 43: QUANTAR Base Station Interconnections – 4-Wire Interface



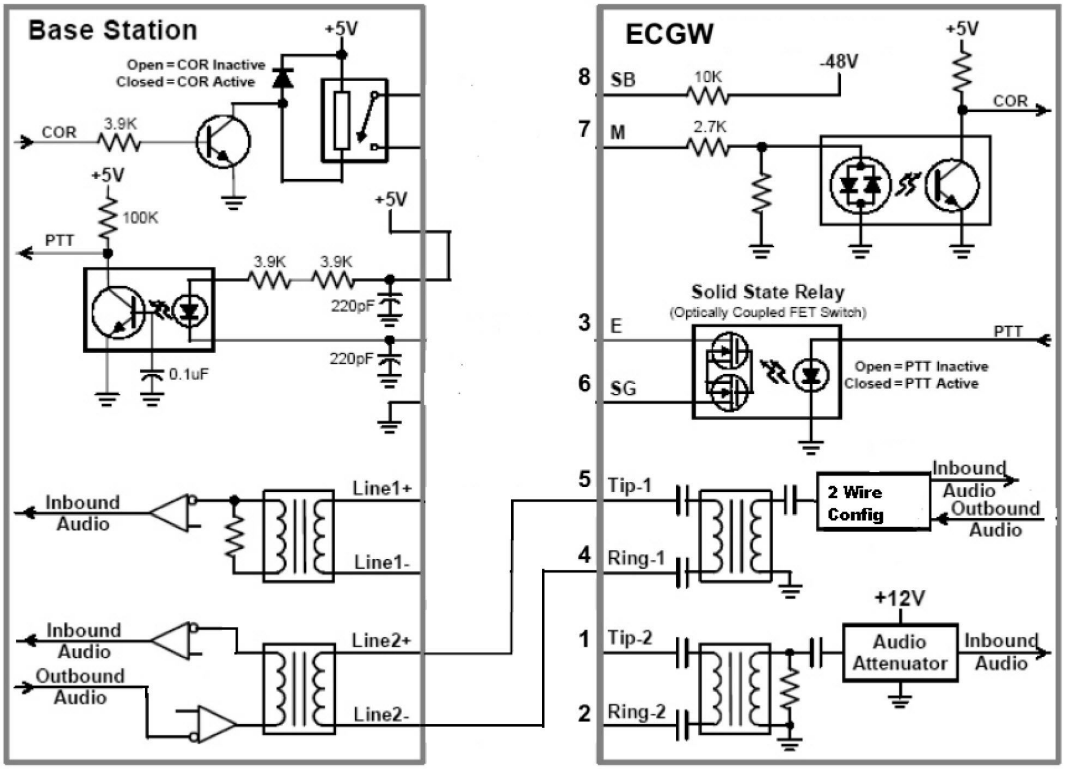
Connecting GGM 8000 Analog Interface to a QUANTAR Base Station 2–Wire Mode

To connect GGM 8000 analog ports configured as 2-wire interfaces to a QUANTAR® base station, connect the signals on the GGM 8000 analog port(s) to the base station as illustrated in the figure below. For the specific port number on the base station that is used to connect the 2-wire interface cable, refer to the documentation supplied with the base station. The GGM 8000 2-wire analog ports are:

- Ports 8D, 8C, 8B, 8A, 12D, 12C, 12B, and 12A on the High Density Enhanced Conventional Gateway.
- Ports 8D, 8C, 8B, and 8A on the Low Density Enhanced Conventional Gateway.

NOTICE: The E&M daughterboard included as part of the analog/V.24 interface kit does not support 2-wire mode.

Figure 44: QUANTAR Base Station Interconnections – 2-Wire Interface



1.6.5.3

GGM 8000 to Analog Base Station Pin Functions

Pin functions are different for analog base station connections to GGM 8000 equipped with an expansion module, analog/V.24 interface kit, and an Enhanced Conventional Gateway module.

1.6.5.3.1

Expansion Module and Analog/V.24 Interface Kit Pin Functions

The following table describes the pin functions for analog base station connections to the GGM 8000 when GGM 8000 is equipped with an expansion module and analog/ V.24 interface kit. In this case, GGM 8000 supports four analog connectors per chassis (one connector per analog interface).

NOTICE: The relay/switch closure detection function provided on pins 7 and 8 and the relay/ switch function provided on pins 3 and 6 is only possible if the equipment connected is collocated on the same premises as GGM 8000.

Table 13: Pin Functions for Analog/V.24 Interface Kit

Pin Function	Description
COR or coded/clear (pins 7 and 8)	Pins 7 and 8 are normally used as part of a current loop that is controlled by the attached equipment. Pin 8 provides a current-limited –48 VDC supply to drive the current loop, while pin 7 detects when the relay/switch on the attached equipment is closed. The current detector on pin 7 detects currents of 2 mA or greater and is used in circuits with average signal levels ranging between ±60 V. The Thyristor Surge Protection Devices that are included in

Pin Function	Description
	this circuit trigger when the signal significantly exceeds 60 V in magnitude and as a result contribute to the overall signal settling time for signals exceeding 60 V.
PTT Relay Output (pins 3 and 6)	Pins 3 and 6 are normally used to control (open and close) a current loop that is monitored by the attached equipment. The Conventional Channel Gateway uses a solid-state relay to control the current loop. The solid-state relay on the Conventional Channel Gateway switches as much as 1 A. However the current through pins 3 and 6 should not average more than 0.5 A, or significantly exceed 1 A peak, else the self-healing polymer “fuses” that are included in this circuit triggers. The average voltage level must not exceed 60 V in magnitude for much longer than 10 ms, to avoid damaging the Transient Voltage Suppressors in the circuit. The solid-state relay has a worst-case off-state leakage current of 10 µA, when open. Pins 3 and 6 are not protected against high voltage. If your particular application warrants it, however, you may add your own surge protection devices.
Outbound Audio (pins 4 and 5)	The analog audio from the Conventional Channel Gateway is carried (differentially) on pins 4 and 5. The source impedance of the outbound audio circuit is 600 Ω and the receiving end of the line is terminated with a load impedance of 600 Ω (to maintain specified output gain levels). It is recommended that the terminators on the receiving equipment be configured appropriately, if multiple termination options are available. The outbound audio circuit is designed to drive an analog audio tone with average levels as high as +11 dBm (±3.9 V peak-to-peak) into a 600 Ω load without clipping. Transient Voltage Suppressors on the secondary side of the isolation transformer clips signals significantly exceeding 8 V (differential) and Thyristor Surge Protection Devices on the primary side of the transformer trigger when the differential voltage significantly exceeds 25 V.
Inbound Audio (pins 1 and 2)	The analog audio into the Conventional Channel Gateway is carried (differentially) on pins 1 and 2. Normally the Conventional Channel Gateway is configured to provide a termination impedance of 600 Ω across these pins. The Conventional Channel Gateway has a software option (referred to as the high-impedance option, the non-terminated option, or, alternatively, the 10K-Ohms loading option) to disconnect the terminating load, on a port-by-port basis, for cases where another piece of equipment (attached to the same signal pair) is configured to provide the 600 Ω termination. **NOTICE:** The resulting termination impedance is greater than 10K-Ohms. The inbound audio circuit is designed to receive an analog audio tone with average levels as high as +11 dBm (±3.9 V peak-to-peak) without clipping. Transient Voltage Suppressors on the secondary side of the isolation transformer clips signals significantly exceeding 8 V (differential) and Thyristor Surge Protection Devices on the primary side of the transformer trigger when the differential voltage significantly exceeds 25 V.

1.6.5.3.2 Enhanced Conventional Gateway Module Pin Functions

The following table describes the pin functions for analog base station connections to the GGM 8000 when the GGM 8000 is equipped with an Enhanced Conventional Gateway module. When equipped with a Low Density Enhanced Conventional Gateway module, GGM 8000 supports four pairs of analog connectors per chassis (two connectors per analog interface). When equipped with a High Density Enhanced Conventional Gateway module, GGM 8000 supports eight pairs of analog connectors per chassis (two connectors per analog interface).

NOTICE: The relay/switch closure detection function provided on pins 7 and 8 and the relay/switch function provided on pins 3 and 6 is only possible if the equipment connected is collocated on the same premises as GGM 8000.

Table 14: Pin Functions for the Enhanced Conventional Gateway Module

Pin Function	Description
E&M Connector	
COR or coded/clear (pins 7 and 8)	The detection mode used from the control signal input on pins 7 and 8 is software-configurable for relay closure detection or long-distance transformer coupled detector. When configured for relay closure detection, the description for pins 7 and 8 on the E&M connector for the analog/V.24 interface kit applies.
PTT Relay Output (pins 3 and 6)	Pins 3 and 6 are normally used to control (open and close) a current loop that is monitored by the attached equipment. GGM 8000 uses a solid-state relay to control the current loop. The solid-state relay on GGM 8000 switches as much a 1 A. However the current through pins 3 and 6 should not average more than 0.5 A, or significantly exceed 1 A peak; otherwise, the self-healing polymer “fuses” that are included in this circuit trigger. The average voltage level must not exceed 60 V in magnitude for much longer than 10 milliseconds to avoid damaging the transient voltage suppressors in the circuit. The solid-state relay has a worst-case off-state leaking current of 10 μA when open. Pins 3 and 6 are not protected against high voltage. If your particular application warrants it, however, you may add your own surge protection devices.
4-wire Outbound Audio 2-wire Inbound/Outbound Audio (pins 4 and 5)	The differential analog audio signal interface on pins 4 and 5 can be used to send and receive audio. GGM 8000 can be configured for a termination impedance of 600Ω, 900Ω, or 10KΩ (unterminated) across these pins. In certain circumstances the 900Ω setting may provide better performance with lengthy cable runs (both ends of the connection should be configured to have 900Ω impedance in this case). The 10KΩ impedance setting is used when the signal line is terminated by a different device or an external terminator. The outbound audio circuit is designed to drive an analog tone with average levels as high as +9 dBm (+/- 3.9 V peak-to-peak) into a 600Ω load without clipping. Transient voltage suppressor on the secondary side of the isolation transformer clips signals significantly exceeding 8 V (differential) and surges suppression devices on the primary side of the transformer trigger when the differential voltage significantly exceeds 25 V.

Pin Function	Description
4-wire Inbound Audio (pins 1 and 2)	The analog audio into GGM 8000 is carried (differentially) on pins 1 and 2. Normally GGM 8000 is configured to provide a termination impedance of 600Ω across these pins.
Analog I/O connector	
LOBL Indicator (pins 1 and 2)	CCGW employs a voltage detector circuit to detect the LOBL signal on pins 1 and 2. The voltage detector interoperates with two different types of signal inputs, either a relay-based input, using contact closure and a balanced 2-wire connection, or a voltage driver input, using a single-ended connection. The impedance settings on pins 1 and 2 can be configured for 600Ω or 10KΩ.
Mute Indicator (pins 4 and 5)	CCGW employs a voltage detector circuit to detect the mute signal on pins 4 and 5. The voltage detector interoperates with two different types of signal inputs, either a relay-based input, using contact closure and a balanced 2-wire connection, or a voltage driver input, using a single-ended connection.
Summed Audio Logging Output (pins 3 and 6)	Each of the analog interfaces includes a dedicated differential analog audio output signal designed for use with call logging recorders. The inbound and outbound audio conversations on the analog interface are combined and output at an average level of -10dBm into a load of 600Ω.
COR or coded/clear (pins 7 and 8)	The detection mode used from the control signal input on pins 7 and 8 is software-configurable for relay closure detection or long-distance transformer coupled detector. When configured for relay closure detection, the description for pins 7 and 8 on the E&M connector applies.

Pins 7 and 8, on both the E&M connector and the Analog I/O connector, also support a transformer-coupled input detector. The transformer coupled input detector detects contact closures over large distances (up to 4000 ft) and over AC coupled lines (where the use of direct current is not an option).

For more information about pin functions, see *Motorola GGM 8000 Hardware User Guide*.

1.6.5.4 Digital Base Stations to Conventional Channel Gateway

The conventional channel gateway provides V.24 ports for standard network cables to connect to digital conventional RF equipment.

When configured with the optional analog/V.24 interface kit or the optional Low Density Enhanced Conventional Gateway module, the GGM 8000 supports four RJ-45 connectors, labeled 7B, 7A, 6B, and 6A. When configured with the optional High Density Enhanced Conventional Gateway module, the GGM 8000 supports eight RJ-45 connectors, labeled 7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A.

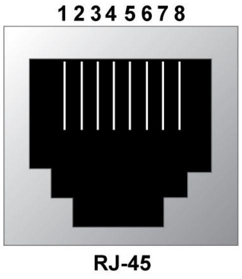
How you cable the V.24 ports on the GGM 8000 depends on the device being connected:

- To connect directly to a base station, follow Connecting the V.24 Conventional Channel Interface Directly to a Base Station on page 85.
- To connect to a modem, follow Connecting the V.24 Conventional Channel Interface to a Modem on page 86.
- To connect to a Subrate Data (SRU) card, follow Connecting the V.24 Conventional Channel Interface to a Subrate Data (SRU) Card on page 88.

In addition, ensure that the clock source is set appropriately. For details, see Setting the Clock Source in the Provisioning Manager on page 89.

The following figure illustrates the pin locations on the GGM 8000 V.24 connector.

Figure 45: GGM 8000 V.24 Connector (RJ-45)



v24_conn

IMPORTANT: To maintain product certifications, shielded cables must be used for connections to the GGM 8000 V.24 ports.

NOTICE: The pin functions described in the following table apply to internal clock applications (colocated links with direct connections to a base station). When configuring the V.24 conventional channel interface for an external clock application (external links connected via a modem or SRU), an external clock signal (TCLK-EXT) must be brought in on pin 2 of the GGM 8000 V.24 port interface. For details, see Connecting the V.24 Conventional Channel Interface to a Modem on page 86 or Connecting the V.24 Conventional Channel Interface to a Subrate Data (SRU) Card on page 88.

Table 15: GGM 8000 V.24 Connector Pin Functions

Pin Number	Direction	Signal Name	Description
1	Input	RCLK	Receive Clock (synchronous mode)
2	Input	CD	Carrier Detect (or a second clock input for modem or SRU connections) Where: Synchronous RS-232 modems and SRUs are designed to supply both the transmit clock and the receive clock to the attached device. As a result, separate clock inputs are needed in these cases, as the clocks provided by the modem or SRU may not necessarily in phase or in synch with each other.
3	Output	TCLK	Transmit Clock (synchronous mode)
4		SGND	Signal Ground
5	Input	RXD	Receive Data
6	Output	TXD	Transmit Data
7	Input	CTS	Clear to Send
8	Output	RTS	Request to Send

1.6.5.4.1 V.24 Port Numbering

The GGM 8000 V.24 module supports two V.24 serial ports. The ports on the V.24 module are labeled "Port 1" and "Port 2". However, the software reserves the following port numbers for ASTRO® 25 Conventional V.24 ports:

- If the V.24 module is installed in port 6, the software uses port numbers 6A and 6B.
- If the V.24 module is installed in port 7, the software uses port numbers 7A and 7B.

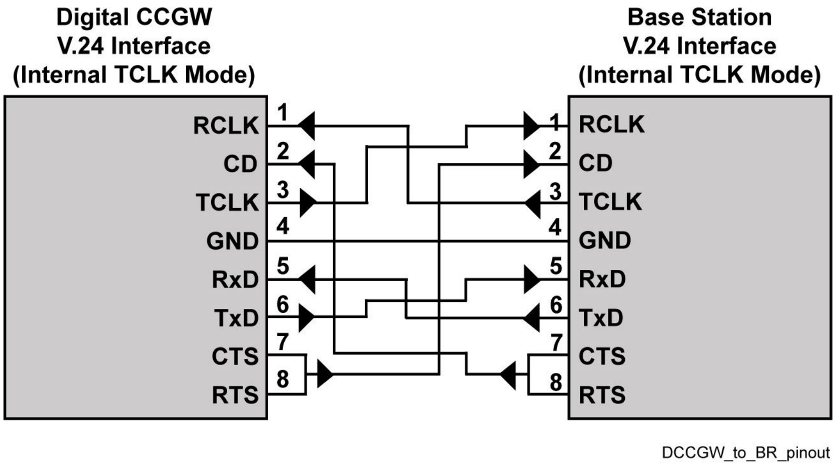
NOTICE: The software supports twoV.24 module per GGM 8000.

1.6.5.4.2 Connecting the V.24 Conventional Channel Interface Directly to a Base Station

When and where to use:
If you connect the GGM 8000 V.24 connector directly to a base station, make the connection using a shielded port-to-port (V.24 null modem) cable with shielded RJ-45 plugs at both ends and wired as illustrated in the following figure.

NOTICE: The interface interconnection illustrated in in the following figure can also be achieved by using the pre-built cable designed for use with the GGM 8000 V.24 module (part number DKN6143A-A).

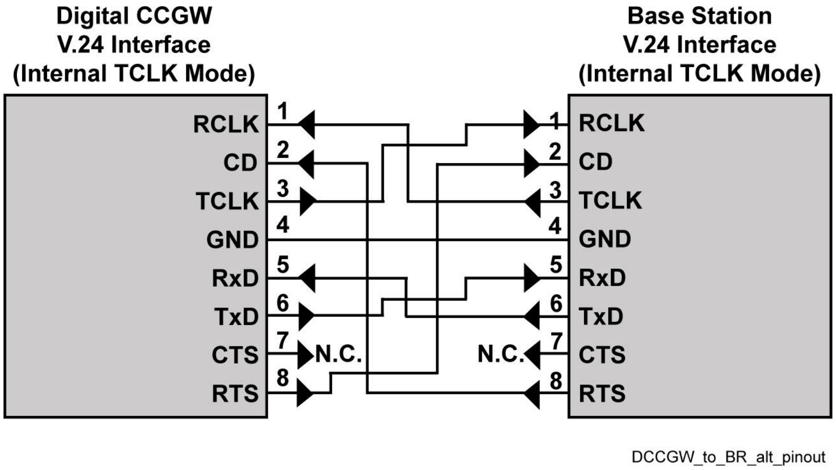
Figure 46: Signal Diagram: V.24 Conventional Channel Interface to Base Station



Alternatively, you can connect the GGM 8000 to the base station using a shielded port-to-port (V.24 null modem) cable with shieldedRJ-45 plugs at both ends and wired as illustrated in the following figure.

NOTICE: The interface interconnection illustrated in the following figure can also be achieved by using a pre-built cable, such as ASTRO-TAC™ null cable (part number 30C83271X14).

Figure 47: Alternative Signal Diagram: V.24 Conventional Channel Interface to Base Station



In addition to interconnecting the GGM 8000 and the base station as illustrated in Figure 46: Signal Diagram: V.24 Conventional Channel Interface to Base Station on page 85 or Figure 47: Alternative Signal Diagram: V.24 Conventional Channel Interface to Base Station on page 86, follow these best practice recommendations to ensure that the port clock is configured appropriately:

⚠ **CAUTION:** Incorrect settings will cause data bit errors that damage the link packets and result in packet loss with the data transfers to and from the GGM 8000.

- Configure the V.24 port interface on the GGM 8000 to synchronize the transmission of its serial data (TXD) using an internally-generated reference clock.
- Configure the V.24 port interface on the base station to synchronize the transmission of its serial data (TXD) using an internally-generated reference clock.
- Connect the transmit clock output signal (TCLK) from the V.24 port of one device to the receive clock input signal (RCLK) on the V.24 port of the other device.

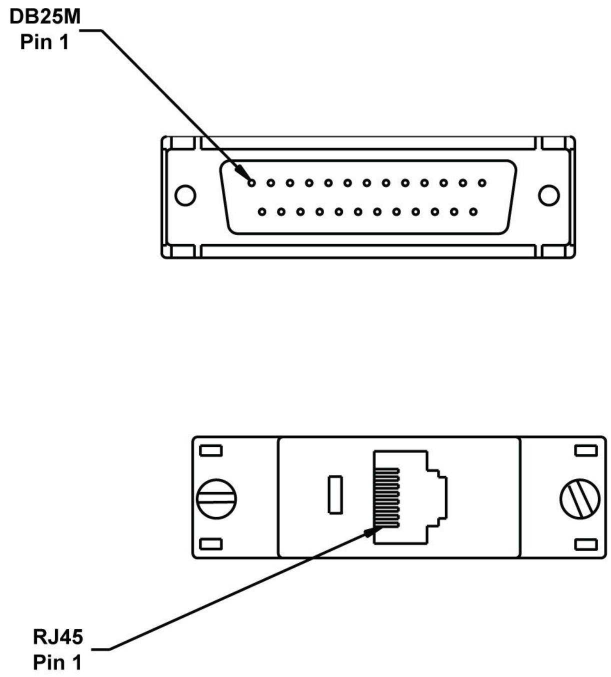
Procedure:

1. Attach one end of the shielded port-to-port (V.24 null modem) cable to the GGM 8000 V.24 port.
2. Attach the other end of the shielded V.24 null modem cable to the base station port.

1.6.5.4.3
Connecting the V.24 Conventional Channel Interface to a Modem

When and where to use:
If you connect the GGM 8000 V.24 connector to a modem, you must attach a shielded RJ-45-to-25-pin "D" cable adapter to the modem port. The following figure shows the pin locations for the cable adapter.

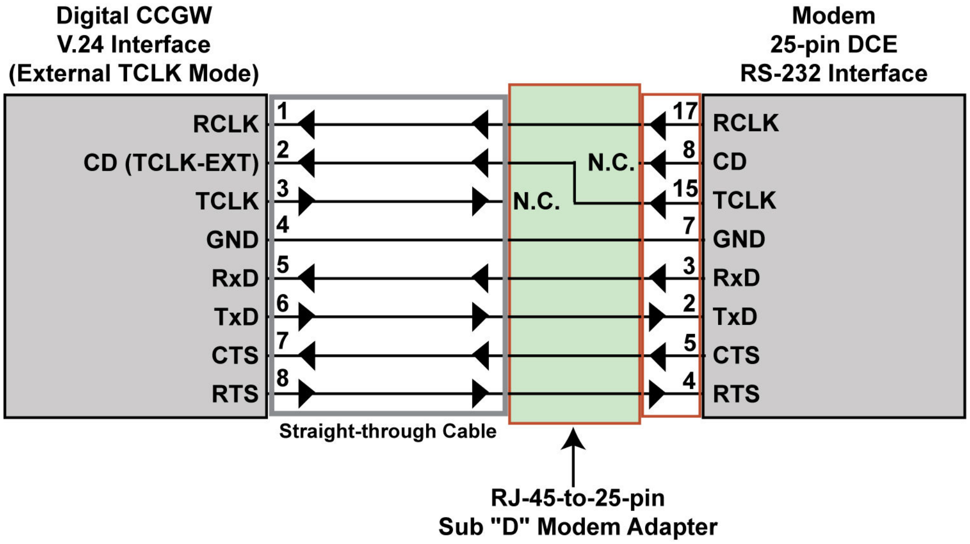
Figure 48: RJ45-to-25 "D" Cable Adapter Pin Locations



v24adaptor

Connect the V.24 connector to the modem adapter using a shielded straight-through cable wired as illustrated in the following figure.

Figure 49: Signal Diagram: V.24 Conventional Channel Interface to Modem (with Cable Adapter)



DCCGW_to_Modem_pinout

In addition to interconnecting the GGM 8000 and the modem as illustrated in Figure 49: Signal Diagram: V.24 Conventional Channel Interface to Modem (with Cable Adapter) on page 87, follow these best practice recommendations to ensure that the port clock is configured appropriately:

CAUTION: Incorrect settings will cause data bit errors that damage the link packets and result in packet loss with the data transfers to and from the GGM 8000.

- Configure the DB-25 interface connection on the modem to supply both the transmit and the receive clock signals to the V.24 port interface on the GGM 8000.
- Configure the V.24 port interface on the GGM 8000 to use the externally-supplied clock signal from the modem to synchronize the transmission of serial data.
- Connect the TCLK-EXT input signal on the V.24 port interface on the GGM 8000 to the TCLK output signal on the DB-25 interface connection on the modem.

Procedure:

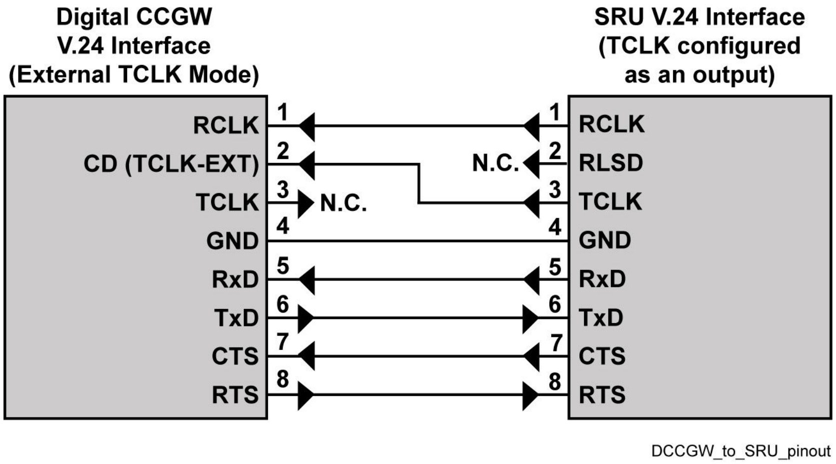
1. Attach a shielded RJ-45-to-25-pin "D" cable adapter (CLN8488A) to the modem port.
2. Attach one end of the shielded RJ-45-to-RJ-45 straight-through cable to the GGM 8000 V.24 port.
3. Attach the other end of the shielded RJ-45-to-RJ-45 straight-through cable to the cable adapter on the modem port.

1.6.5.4.4
Connecting the V.24 Conventional Channel Interface to a Subrate Data (SRU) Card

When and where to use:
If you connect GGM 8000 V.24 connector to an SRU card, connect the two ports using a shielded 8-conductor cable with shielded RJ-45 plugs at both ends and wired as illustrated in the following figure.

CAUTION: The two ends of the cable are not interchangeable and should be marked accordingly.

Figure 50: Signal Diagram: V.24 Conventional Channel Interface to SRU



In addition to interconnecting the GGM 8000 to the SRU as illustrated in Figure 50: Signal Diagram: V.24 Conventional Channel Interface to SRU on page 88, follow these best practice recommendations to ensure that the port clock is configured appropriately:

CAUTION: Incorrect settings will cause data bit errors that damage the link packets and result in packet loss with the data transfers to and from the GGM 8000.

- Configure the V.24 port interface on the SRU to supply both the transmit and the receive clock signals to the V.24 port interface on the GGM 8000.
- Configure the V.24 port interface on the GGM 8000 to use the externally-supplied clock signal from the SRU to synchronize the transmission of serial data.
- Connect the TCLK-EXT input signal on the V.24 port interface on the GM 8000 to the TCLK output signal on the V.24 port interface on the SRU.

Procedure:

1. Attach the appropriate end of the shielded 8-conductor cable to the GGM 8000 V.24 port.
2. Attach the other end of the shielded 8-conductor cable to the SRU card port.

1.6.5.4.5 Setting the Clock Source in the Provisioning Manager

In addition to interconnecting the devices as described in the previous sections, follow these best practice recommendations to configure the clock mode on the GGM 8000 V.24 ports:

- If you connect GGM 8000 directly to a base station, the clock source for the V.24 communication link should be set to internal (the transmit clock is generated internally in the GGM 8000).
- If you connect GGM 8000 to a modem, the clock source for the V.24 communications link should be set to external (the transmit clock is generated by an external device; in this case, the modem).
- If you connect GGM 8000 to a subrate data (SRU) card, the clock source for the V.24 communications link should be set to external (the transmit clock is generated by an external device; in this case, the SRU card).

You configure the clock source in the Provisioning Manager. Clock Source is one of the fields included when you configure a digital conventional channel, a mixed mode conventional channel, or an ACIM conventional channel. For more information about how to use the Provisioning Manager to configure these conventional channel types, see the *Provisioning Manager User Guide* and the *Provisioning Manager OLH*.

IMPORTANT: A reboot is required in order for changes made in Provisioning Manager to be adopted permanently by GGM 8000.

1.6.5.5 Analog Comparator to Conventional Channel Gateway

MLC 8000 comparators and link converters can be implemented along with GGM 8000s to provide the interface for conventional analog and mixed mode conventional site architectures. For details, see the *MLC 8000 Setup Guide*. It includes site diagrams and complete implementation sequences with steps for all the devices.

1.6.5.5.1 Making a Physical 4-W Connection on MLC 8000 Analog Comparator to CCGW

Prerequisites: To accomplish this task you need:

- A cross-over cable, Category 5 or higher.
- Access to the *Motorola GGM 8000 Hardware User Guide* (for access instructions, see Related Information on page 27).
- Access to the *MLC 8000 Comparator Feature Guide* manual.

- Access to the *MLC 8000 Setup Guide*.

Procedure:

1. Connect the RJ45 “MLC8000” side of the cable to the “R1 4W E&M” port at the MLC 8000 Comparator.
2. Connect the RJ45 “CCGW” side of the cable to the configured “4W E&M” port at the CCGW.

Postrequisites: Verify the link status. Check the LED for the corresponding port on the GGM 8000 hardware that you used for establishing the connection with the MLC 8000 Analog Comparator.

NOTICE: For the details on the GGM 8000 LED indicators information, refer to E&M Module LEDs on page 111.

1.6.6

ACIM Interface – Installation

Process:

1. If necessary, install the CCGW hardware in the GGM 8000.
   - For information about installing the analog/V.24 interface kit, see Replacing Daughterboards on the GGM 8000 on page 129
   - For information about installing the Enhanced Conventional Gateway module, see Replacing the GGM 8000 ECGW Module on page 134

   NOTICE: If the GGM 8000 is ordered with an analog/V.24 kit or an Enhanced Conventional Gateway module, the optional hardware is mounted at the factory.
2. Create and configure the ACIM conventional channel in the system. Depending on your configuration, do one of the following:
   - Create an ACIM conventional channel in the Provisioning Manager application. See “Creating Records” in the Provisioning Manager manual.
   - Create a configuration record in the Configuration Manager application. See the “Creating a Configuration Record” section in the *Configuration Manager for Conventional Systems User Guide*.
3. Configure the consolette(s) for the ACIM operation and then power up the consolette(s). For details, see one of the following manuals:
   - *APX 7500 Multi-Band Consolette Detailed Service Manual*
   - *ASTRO Digital XTL 5000 Consolette Instruction Manual*
4. Connect the consolette(s) to the Conventional Channel Gateway. Depending on the model of the consolette, do one of the following:
   - Follow Connecting the GGM 8000 to an APX Consolette on page 91.
   - Follow Connecting the GGM 8000 to an XTL Consolette on page 92.

   NOTICE: The connection between the Conventional Channel Gateway and the consolette for ACIM conventional channel support is an asynchronous connection and does not require setting the clock source.

Postrequisites: Verify the link status on the consolette(s).

1.6.6.1 ACIM Interface – Cabling

ACIM link support requires both an RS-232 link and a 4-wire link between the GGM 8000 and the consolette. In order to connect the GGM 8000 to a consolette for ACIM link support, you must connect both the V.24 interface and the corresponding analog (4-wire) interface.

Table 16: GGM 8000 with ACIM Interface – Cabling

Gateway		Port	Device/Function
Conventional Channel Gateway	Base module	LAN 1-4	Site LAN Switch, Backhaul Switch
	Analog/V.24 interface kit	4-wire analog ports (8A to 8D)	Connections to up to 4 colocated Motorola Solutions consolettes.
		V.24 digital ports (6A, 6B, 7A, 7B)	
	Low Density Enhanced Conventional Gateway module	4-wire analog ports (paired ports 9D+8D to 9A+8A)	Connections to up to 4 colocated Motorola Solutions consolettes
		V.24 digital ports (7B, 7A, 6B, 6A)	
	High Density Enhanced Conventional Gateway module	4-wire analog ports (paired ports 9D+8D to 9A+8A and 13D +12D to 13A+12A)	Connections to up to 8 colocated Motorola Solutions consolettes
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	

For more information about the Enhanced Conventional Gateway modules, see GGM 8000 Enhanced Conventional Channel Gateway Modules on page 34.

1.6.6.2 Connecting the GGM 8000 to an APX Consolette

Procedure:

1. Attach the appropriate end of the V.24 CCGW-to-APX console cable (an 8-conductor cable with standard RJ45 plugs at both ends) to the GGM 8000 V.24 port.

   NOTICE: See V.24 CCGW-to-APX Console Cable on page 92 for details on how to wire the V.24 CCGW-to-APX console cable.

2. Attach the other end of the V.24 CCGW-to-APX cable to the RJ45 connector labeled **ACIM** on the back of the APX consolette.
3. Attach the appropriate end of the 4-wire CCGW-to-APX console cable (an RJ45-to-RJ45 cable) to the GGM 8000 E&M port.

   NOTICE: See 4-Wire CCGW-to-APX Console Cable on page 92 for details on how to wire the 4-wire CCGW-to-APX console cable.

4. Attach the other end of the 4-wire CCGW-to-APX console cable to the RJ45 connector labeled **Wireline** on the back of the APX consolette.

1.6.6.2.1
V.24 CCGW-to-APX Console Cable

Table 17: V.24 CCGW-to-APX Console Cable Wiring

RJ45 – GGM 8000			RJ45 – Consolette	
Signal	**Pin#**	**Pair**	**Pin#**	**Signal**
TxD	6	Green	4	RxD
RxD	5	White-Green	6	TxD
GND	4	Orange	8	GND

1.6.6.2.2
4-Wire CCGW-to-APX Console Cable

Table 18: 4-Wire CCGW-to-APX Console Cable Wiring

RJ45 – GGM 8000			RJ45 – Consolette	
Signal	**Pin#**	**Pair**	**Pin#**	**Signal**
TIP2	1	White-Green	3	TIP2
RING2	2	Green	6	RING2
TIP1	4	White-Blue	4	TIP1
RING1	5	Blue	5	RING1

1.6.6.3
Connecting the GGM 8000 to an XTL Consolette

Procedure:

1 Attach the appropriate end of the V.24 CCGW-to-XTL console cable (an 8-conductor cable with standard RJ45 plugs at both ends) to the GGM 8000 V.24 port.

NOTICE: See V.24 CCGW-to-XTL Console Cable on page 93 for details how to wire the V.24 CCGW-to-XTL console cable.

2 Attach the other end of the V.24 CCGW-to-XTL cable to the RJ45 connector labeled **Accessory 1** on the back of the XTL Consolette.

3 Attach the appropriate end of the 4-wire CCGW-to-XTL console cable (an RJ45-to-RJ45 cable) to the GGM 8000 port.

NOTICE: See 4-Wire CCGW-to-XTL Console Cable on page 93 for details how to wire the 4-wire CCGW-to-XTL console cable.

4 Attach the other end of the 4-wire CCGW-to-XTL cable to the RJ45 connector labeled **Accessory 2** on the back to the XTL Consolette.

1.6.6.3.1 V.24 CCGW-to-XTL Console Cable

Table 19: V.24 CCGW-to-XTL Console Cable Wiring

RJ45 – GGM 8000			RJ45 – Consolette	
Signal	**Pin#**	**Pair**	**Pin#**	**Signal**
TxD	6	Green	4	RxD
RxD	5	White-Green	6	TxD
GND	4	Orange	8	GND

1.6.6.3.2 4-Wire CCGW-to-XTL Console Cable

Table 20: 4-Wire CCGW-to-XTL Console Cable Wiring

RJ45 – GGM 8000			RJ45 – Consolette	
Signal	**Pin#**	**Pair**	**Pin#**	**Signal**
TIP2	1	White-Green	4	TIP2
RING2	2	Green	5	RING2
TIP1	4	White-Blue	3	TIP1
RING1	5	Blue	6	RING1

1.7 GGM 8000 Configuration

GGM 8000 gateways are configured at the factory. No additional configuration is required other than restoring gateways in the event of a break-fix situation.

⚠ **CAUTION:** Do not tamper with the factory configuration settings without consulting your system manager. Factory configuration settings include software configuration, firmware release, and physical connections. Motorola Solutions has configured and connected these devices to meet specific performance requirements. Tampering with the configuration settings for these devices may result in unpredictable system performance or a catastrophic failure.

NOTICE: For information about how to configure a GGM 8000 with IPLC functionality, see the *GGM 8000 with IP Link Converter (IPLC) Functionality User Guide*.

1.7.1 Downloading a Stored Configuration File to the GGM 8000

Prerequisites: Obtain:

- A PC loaded with a TFTP server application (such as the 3Com TFTP server application) and a terminal emulation program (such as ProComm or Hyperterminal).
- An Ethernet crossover cable to establish the LAN connection between the PC and the gateway.
- A DB9 null modem cable to establish console access between the PC and the gateway.

- Access to the appropriate configuration file(s) (such as the boot.cfg, StaticRP.cfg, and acl.cfg) for the gateway you are installing or replacing. These files are located either on the media containing the electronic version of your system documentation, backed up on your PC, or obtained in another way from the factory.
- IP addresses for the gateway. Contact your system administrator for this information.
- Account logins and passwords. Contact your system administrator for this information.

IMPORTANT: If you load a configuration file that changes the system IP address on a gateway, the SNMPv3 credentials must be re-established with that gateway. Therefore, if SNMPv3 users were configured on the gateway prior to the system IP address change, issue the ResetV3 command to reset the SNMPv3 data, then reconfigure the SNMPv3 users with the appropriate privilege levels. For details, see “Configuring MNR Routers and GGM Gateways for SNMPv3” in the *SNMPv3 Feature Guide*.

When and where to use: Follow this procedure if you replace GGM 8000 and the replacement gateway was not configured at the factory, or if you need to load a configuration file on a new gateway during installation.

NOTICE: This process does not apply to Border Gateways in ASTRO/LTE CEN configuration. In this case the Border Gateways should be configured manually using a configuration document. For details concerning Border Gateways in ASTRO/LTE CEN configuration see Border Gateway – Functional Description on page 255.

Procedure:

1 Assign the following IP address and subnet mask to the LAN card on the PC you are using to perform the configuration:
   - **IP Address:** 20.0.0.1
   - **Subnet Mask:** 255.255.255.0

2 Connect the following cables between the PC and the gateway:
   - Ethernet crossover cable between the LAN card on the PC and LAN port 1 on the gateway.

     NOTICE: The crossover cable crosses over pins 1 and 2 to pins 3 and 6.
   - Null modem cable between the serial port on the PC and the console port on the gateway.

3 Power up the gateway and connect to this gateway by using a terminal emulation program (such as ProComm or Hyperterminal).

4 In the terminal emulation program, perform the following actions:

   a Enter: `9600 baud rate`

   b Enter: `8 bit`

   c Enter: `No parity`

   d Enter: `1 stop bit`

   Then press ENTER several times until the `NetLogin:` prompt appears.

5 At the `NetLogin:` prompt, enter `root`. Press ENTER.

6 At the `password:` prompt, press ENTER.

7 Verify that the gateway is unconfigured (no IP addresses are assigned to any of the ports):

   a Enter: `sh -ip net`

   b If any IP addresses are listed, enter:

```
del !<portlist> -ip net <ip_address>
```

8 To configure the IP address for the gateway, enter: `setd !1 -ip net = 20.0.0.2 255.255.255.0`

NOTICE: The IP addresses assigned to the PC LAN card and the gateway are chosen so that the gateway's IP address is on the same subnet as the PC used to configure this gateway.

9 Select and run the **3Com TFTP** application from the Windows Program menu.

The **3Com 3C Server** window appears.

10 From the **TFTP** toolbar, click **Setup**.

The **3C Server Configuration** dialog box opens.

11 Select the **TFTP Configuration** tab.

The **TFTP Configuration** tab appears.

12 Verify that the gateway configuration files are present on the PC and that you know their location.

13 Select the gateway configuration file directory:

a Click **Browse Directories** in the **TFTP Configuration** tab.

b Select the directory containing the configuration files, click **OK**.

14 Transfer the configuration fields required by the gateway you are configuring to the gateway:

a Return to the terminal program and locate the `EnterpriseOS#` prompt.

b Perform the following actions:

Enter: `copy 20.0.0.1:`***`<.cfg_filename>`***` a:/primary/boot.cfg`

Enter: `copy 20.0.0.1:`***`<.cfg_filename>`***` a:/primary/StaticRP.cfg`

Enter: `copy 20.0.0.1:`***`<.cfg_filename>`***` a:/primary/acl.cfg`

NOTICE: Where ***`<.cfg_filename>`*** is the name of the configuration file specific to the gateway you are replacing. For example, the configuration file for the Site Gateway (Console Site) in zone 1 is z001ds001r1_10.1.1.254.cfg.

The configuration files are transferred to the gateway and renamed as boot.cfg, StaticRP.cfg, and acl.cfg respectively.

15 Verify that the account password is set to the same value as the gateway.

16 Reboot the gateway:

a Return to the terminal program.

b At the `EnterpriseOS#` prompt, type `rb` and press Enter.

The gateway reboots and processes the configuration files. Once the processing is complete, the following message is displayed: `System Initialized and Running`

17 Verify that the gateway did reboot and is running the new configuration:

a After the `System Initialized and Running` message is displayed, log on to the gateway.

b At the `EnterpriseOS#` prompt, enter: `cd`

c At the `EnterpriseOS#` prompt, enter: `cat boot.cfg`

d Compare the Timestamp and Config Summary sections to the original file on the PC.

e Enter: Enter to quit the display of the boot.cfg file.

f Follow steps **d** to **e** for the StaticRP.cfg and acl.cfg files.

The gateway prompt now displays the system name of the gateway rather than `EnterpriseOS#` and the information in the boot.cfg, StaticRP.cfg, and acl.cfg files matches the original files.

18 Power down the gateway, disconnect the TFTP computer, and connect all system communication cables to the gateway.

19 Power up the gateway.

The gateway reboots using the boot.cfg, StaticRP.cfg, and acl.cfg files. The IP address you assigned to the gateway is replaced with the IP address specific to that gateway in your system.

20 On systems with MAC port locking, disable the locking on the switch, and then re-enable the locking on the switch with the MAC address of the new gateway. For instructions on how to disable and enable MAC port locking, refer to the *MAC Port Lockdown Feature Guide*.

21 On systems with link encryption, enter the correct pre-shared keys (PSKs) for the new gateway so it can be authenticated by its encryption peer. For instructions, see the *Link Encryption and Authentication Feature Guide*.

22 On systems that required SSH, generate a key for the new gateway to enable the SSH. For instructions, see the *Securing Protocols with SSH Feature Guide* .

23 For the centralized authentication feature, the RADIUS sources are already set up in the gateway configuration files by Motorola Solutions. The only RADIUS configuration you need to perform on the GGM 8000 Gateways is to enter the secret key that matches the shared secret from the properties for this RADIUS client on the RADIUS server. For instructions, see the *Authentication Services Feature Guide*.

24 Configure SNMPv3 passphrases. For instructions, see the *SNMPv3 Feature Guide*.

25 On systems with protocol authentication, enter the correct OSPF/PIM keys for the new gateway so it can authenticate with its neighbor. For instructions see the *Link Encryption and Authentication Feature Guide*.

26 Discover the router in the UNC (if the UNC application is present in the system). For instructions, see the *Unified Network Configurator User Guide*.

27 Upload the device configuration and hardware information from the router to the UNC. Perform the “Scheduling the Pull of Device Configurations”procedure in the *Unified Network Configurator User Guide*.

Postrequisites: Print out all the gateway configurations in your system from the UNC and store them in a secure location. If any gateway upgrades are made, print out the new configurations and replace those gateways' records in your records. This provides specific address information for the individual gateways. For details, see the *Unified Network Configurator User Guide*.

NOTICE: For security purposes, all default passwords have to be changed prior to operational use. Those include both 'root' and 'admin' user passwords.

1.7.2 Restoring or Changing a Gateway Configuration

If you need to restore a previous gateway configuration, then perform a Rollback Configuration procedure, as described in the *Unified Network Configurator User Guide*.

If you need to change a current gateway configuration and send the new configuration to the gateways, then perform a Configuration Change procedure, as described in the *Unified Network Configurator User Guide*.

1.7.3 Preparing the Gateway for Management

For information about how to prepare the gateway for management, see the “Configuration Management” section in the *Unified Network Configurator User Guide*.

1.7.4 Backing up the Gateway Configuration

You can create a backup of the gateway’s running configuration files and execution image by copying the contents of the gateway’s primary directory either to the gateway’s secondary directory or to a TFTP server. This backup includes the Motorola Solutions-provided configuration files as well as other manually-entered configuration, such as pre-shared keys. In the event that the contents of the gateway’s primary directory are corrupted, you can restore the configuration files and execution image from the backup.

Use these procedures to create backups which you can use to recover the gateway configuration in the event of a failure.

NOTICE: The backups created by these procedures are specific to the physical motherboard from which the primary directory contents are copied. In other words, these backups work only if the motherboard from which you copied the configuration files and execution image is installed in the device you are restoring. You cannot use the backups created by these procedures if you are swapping one device for another or if you are replacing a motherboard.

1.7.4.1 Creating a Local Backup

To create a local backup, use the following procedure to copy the contents of the gateway’s primary directory to the gateway’s secondary directory.

Prerequisites: PC with a terminal emulation program.

Procedure:

1. At the `EnterpriseOS#` prompt, enter the following command to clean up the previous backup:

   ```
   RF a:/secondar/*.*
   ```

2. Enter the following command to make a copy of the current running configuration and execution image:

   ```
   COPY a:/primary/*.* a:/secondar
   ```

3. Check if there are any subdirectories of the **a:/primary** directory. If so, repeat steps 1 and 2 above for each subdirectory, replacing `a:/primary/` with the path to the subdirectory in the `COPY a:/primary/*.* a:/secondar` command.

4. To subsequently restore the gateway configuration from the backup in the secondary directory in the event that the contents of the primary directory have become corrupted, follow these steps:

   a. From the `EnterpriseOS#` prompt, enter `SF 7` to open the **SysconF** command Boot Sources menu.

   b. Enter 3 to direct the gateway to boot from the secondary directory.

   c. Reboot the gateway.

1.7.4.2 Backing Up to a TFTP Server

To back up the contents of the gateway's primary directory to a TFTP server, use the following procedure.

Prerequisites: Dedicated site PC or laptop with TFTP server application.

Procedure:

1. Connect a straight-through Ethernet cable between the gateway and a hub or switch port that is in the same subnet as the TFTP server.
2. At the `EnterpriseOS#` prompt, enter the following commands to configure the gateway to access the TFTP server:

   ```
   SETDefault !3 -IP NETaddr = <IP address> [<network mask>]
   ```

   Where ***<IP address>*** is the IP address you want to assign to the gateway's Ethernet port and ***<network mask>*** is the subnet mask.

   ```
   SETDefault !3 -PAth CONTrol = Enable
   ```

   ```
   SETDefault !3 -POrt CONTrol = Enable
   ```

   ```
   ADD -IP ROUte <IP address> <mask> <gateway> <metric>
   ```

   Where ***<IP address>*** is the subnet address for the TFTP server, ***<mask>*** is the subnet mask, ***<gateway>*** is the gateway IP address, and ***<metric>*** represents the number of hops required for a packet to reach its destination.

   Step example:

   ```
   SETDefault !3 -IP NETaddr = 10.79.130.128 255.255.255.0
   ```

   ```
   SETDefault !3 -PAth CONTrol = Enable
   ```

   ```
   SETDefault !3 -POrt CONTrol = Enable
   ```

   ```
   ADD -IP ROUte 10.79.0.0 255.255.0.0 10.79.130.1 0
   ```
3. Enter the following command to generate a list of files in the gateway's primary directory: **`DF a:/primary`**
4. Use the list of file names generated in step 3 to create a list of copy commands, one command for each file name, and enter them one at a time until all the files in the list have been copied.

   Step example:
   For example, if the list returned by the DF command consists of a boot.ppc file and a boot.cfg file, enter the following commands to copy the files to a directory named backup1 on the TFTP server with IP address 10.79.0.2:

   ```
   copy a:/primary/boot.ppc 10.79.0.2:/backup1
   ```

   ```
   copy a:/primary/boot.cfg 10.79.0.2:/backup1
   ```

   NOTICE: If the list returned by the DF command includes other files in addition to the boot.ppc and the boot.cfg files, then you must enter additional copy commands (one command for each file), substituting the filename(s) of the additional files for boot.ppc or boot.cfg in the examples above.
5. To subsequently restore the gateway configuration files and execution image from the backup on the TFTP server in the event that the contents of the gateway's primary directory have become corrupted, follow these steps:

   a. From the `EnterpriseOS#` prompt, enter a copy command for each file in the backup directory. For example, if backup directory backup1 on the TFTP server with IP address 10.79.0.2 includes a boot.ppc file and a boot.cfg file, enter the following commands:

```
copy 10.79.0.2:/backup1/boot.ppc a:/primary
```

```
copy 10.79.0.2:/backup1/boot.cfg a:/primary
```

NOTICE: If the backup directory includes other files in addition to the boot.ppc and the boot.cfg files, then you must enter additional copy commands (one command for each file), substituting the filename(s) of the additional files for boot.ppc or boot.cfg in the examples above.

b Reboot the gateway.

1.7.5

Updating Access Control List Files to Support System Expansions

System expansions require that you update the gateway access control list (ACL) files (`acl.cfg`) in different scenarios.
These scenarios are:

- Console site expansion – When you add a console site to a trusted group, you must update the `acl.cfg` file for all gateways in the trusted group.
- Zone core expansion – When you add a zone core, you must update the `acl.cfg` file for all gateways.

Prior to the ASTRO® 25 7.13 system release, the ACL update procedure involved copying the new `acl.cfg` file to the routers and rebooting the gateways. The ASTRO®25 7.13 system release introduces the `antiacl.cfg` file, a file that completely removes the current `acl.cfg` settings from a gateway. By copying the `antiacl.cfg` file and the new `acl.cfg` file to a gateway, you can update the current ACL/firewall settings without a reboot. You can perform the update procedure manually and automatically.

When and where to use: Update the ACL files in one of the following ways:

- Automatically, in the UNC (M core, or L core systems). For more information, see Automatically Updating Access Control List Files on page 100.

  NOTICE: Downtime cannot be avoided for L1 and M1 systems.

- Manually, using the gateway command line (K core systems). For more information, see Manually Updating Access Control List Files on page 100.

The following basic process steps are common for manual and automatic ACL updates.

NOTICE: The ACL file distribution and file activation can be implemented as two separate processes and executed at different times.

Process:

1. Distribute the antiacl.cfg and new `acl.cfg` files to the gateways.
2. Activate the antiacl.cfg and new `acl.cfg` files.
3. Delete the antiacl.cfg file.
4. For a console site expansion, reboot the core router or routers. For a zone core expansion, reboot the exit router or routers.

   NOTICE: For systems that are redundant in the core, you must reboot both routers in the core or exit router pair. The gateway router does not require a reboot.

Related Links

Automatically Updating Access Control List Files on page 100
Manually Updating Access Control List Files on page 100

1.7.5.1
Automatically Updating Access Control List Files

You can use Unified Network Configurator (UNC) to automatically update Access Control List (ACL) files. You update the files without rebooting the gateway.

Prerequisites:
Familiarize yourself with the overview information. See Updating Access Control List Files to Support System Expansions on page 99.

Obtain the `antiacl.cfg` and new `acl.cfg` files, from your Motorola Solutions field representative.

When and where to use: Perform this process to support console site expansion or zone core expansions for ASTRO® 25 systems that employ the M core or L core zone cores.

Process:

1. Load the antiacl.cfg and new `acl.cfg` files to the UNC workspace. See the *Unified Network Configurator User Guide* for information about uploading the configurations for transport devices in the UNC Wizard.
2. Distribute the antiacl.cfg and new `acl.cfg` files to the impacted gateways using UNC. Refer to the *Unified Network Configurator User Guide* for information about distributing configurations for transport devices by using the UNC Wizard.

   NOTICE: You can schedule many distributions of the configuration files. However, when you schedule a very large number of distributions, you may delay other UNC operations.
3. Clear old ACL and activate new ACL files using the UNC Save Command. Refer to the *Unified Network Configurator User Guide* for information about activating new ACL files.
4. Check the Activation Status of the ACL file. See the *Unified Network Configurator User Guide* for information about accessing and executing existing saved commands.

Return to Process

Updating Access Control List Files to Support System Expansions on page 99

Related Links

Manually Updating Access Control List Files on page 100

1.7.5.2
Manually Updating Access Control List Files

You can use Unified Network Configurator (UNC) to manually update Access Control List (ACL) files. You update the files without rebooting the gateway.

Prerequisites:
Familiarize yourself with the overview information. See Updating Access Control List Files to Support System Expansions on page 99.

Obtain the `antiacl.cfg` and new `acl.cfg` files from your Motorola Solutions field representative.

When and where to use: Perform this process on each of the impacted gateways to support Console Site Expansion or Zone Core Expansions for ASTRO®25 systems that employ the K core.

Procedure:

1. Use TFTP (non-secure) or PuTTY secure copy protocol (SCP) (secure) to transfer `antiacl.cfg` and `acl.cfg` files to the impacted gateways.

   See Downloading a Stored Configuration File to the GGM 8000 on page 93
2. Establish a Telnet (non-secure) or SSH (secure) connection to the gateway.

3. Activate the antiacl.cfg file. From the gateway command line, enter:

   ```
   cd
   lc antiacl.cfg ie
   ```

4. Check the status of the antiacl.cfg file activation. From the gateway command line, enter:

   ```
   cat config.log | grep -i error
   ```

5. Activate the new `acl.cfg` file. From the gateway command line, enter:

   ```
   cd
   lc acl.cfg ie
   ```

6. Check the status of the `acl.cfg` file activation by repeating step 4.
7. Delete the `antiacl.cfg` file. From the gateway command line, enter:

   ```
   rf antiacl.cfg
   ```

8. Perform one of the following actions:
   - For a console site expansion, reboot the core router or routers.
   - For a zone core expansion, reboot the exit router or routers.

Return to Process

Updating Access Control List Files to Support System Expansions on page 99

Related Links

Automatically Updating Access Control List Files on page 100

1.7.6 Conventional Channel Gateway – Configuration

The configuration through Provisioning Manager interface is preceded by initial device setup by the Motorola Solutions Support Center (SSC). To add a Conventional Channel Gateway (CCGW) to a new or existing site, your organization needs to contact Motorola Solutions field personnel to initiate the request to perform the initial setup with the SSC. Once the SSC has completed the initial device setup, your organization can proceed with the Provisioning Manager configuration of the CCGW. The SSC upon the initial configuration assigns an instance ID to the CCGW; this ID must match the CCGW ID configured through Provisioning Manager interface, and your organization must obtain this information before the configuration through Provisioning Manager interface can occur.

1.7.6.1 Configuring the Conventional Channel Gateway at an MCC 7500 VPM Dispatch Console (NM/Dispatch) Site

The Conventional Channel Gateways (CCGWs) are located as part of the MCC 7500 VPM Dispatch Console site and resides on the subnet for the MCC 7500 VPM Dispatch Console site. Individual CCGWs are assigned an IP address on the subnet, and the host part of the IP address is determined through the uniquely assigned CCGW ID configured from the NM configuration subsystem. The CCGW ID has a valid range of 1-10. The CCGW ID must be assigned uniquely to the CCGWs for each MCC 7500 VPM Dispatch Console site to avoid the same IP address being assigned to two or more CCGWs. This implies the following rules must be enforced by system administrators:

```
CCGW IP Address = 10.zone.NMDispConv.CCGW ID+84 (i.e. 10.1.1.85 for CCGW ID
= 1, zone = 1, NMDispConv = MCC 7500 Site ID-1000 = 1001-1000 = 1)
```

In this example, **NMDispConv** is the physical site number.

The customer configuration through NM interface is preceded by initial device setup by the SSC. To add a CCGW to a new or existing customer site, the customer needs to contact Motorola Solutions field personnel to initiate the request to perform the initial setup with the SSC. Once the SSC has completed the initial device setup, the customer can proceed with the NM configuration of the CCGW. The SSC upon the initial configuration assigns an instance ID to the CCGW; this ID must match the CCGW ID configured through NM interface, and the customer must obtain this information before the configuration through NM interface can occur.

NOTICE: If the device ID and the Provisioning Manager-configured ID do not match, conventional is inoperable.

For CCGWs co-located at the trunked RF sites (Trunking Repeater Site or Simulcast Prime), the host part of the IP address remains the same except that there can be up to two CCGWs co-located at the trunked RF sites, so the CCGW ID should be chosen to be unique in the range of 1-2.

For CCGWs co-located at the IP-based conventional-only RF sites, the host part of the IP address remains the same except that there can be up to three CCGWs co-located at the RF sites, so the CCGW ID should be chosen to be unique in the range of 1-3:

```
CCGW Domain Name = ccgwGI.nmdS.zoneZ (i.e. ccgw01.nmd1.zone1 for GI = 1, S =
MCC 7500 Site ID-1000 = 1001-1000=1, Z = 1)
```

1.7.6.2 Configuring the Conventional Channel Gateway in a Distributed Conventional Subsystem

Conventional Subsystems utilize dynamic IP address pools for addressing devices in the conventional subsystems. The conventional subsystems are placed in the UCS domain for DNS purposes; it is not possible to derive zone information from the IP address or fully qualified domain name for devices in a conventional subsystem. The Network Management suite also uses information in the MIB variable “sysName” to determine and display relationship information in the managers, i.e. which BR and Conventional Channel Gateway (CCGW) are related. This is important to note since configuration of CCGWs in Provisioning Manager for a conventional subsystem differs from that at an NM Dispatch site.

The following parameters are used in Provisioning Manager when configuring CCGWs for a conventional subsystem:

- **CSub# = 1 through 47**
- **ConvLoc# = 2001 through 2255**
- **CCGW ID = 1 through 10**

A system may have up to 47 conventional subsystems (CSub#); each must have a unique number in the system (1 – 47). The conventional subsystems contain up to 255 conventional locations (ConvLoc#) which are a combination of Hubs and BR Sites; each must have a valid number in the conventional system (2001 – 2255). The ConvLoc# must be unique within a conventional subsystem but it does not need to be unique across all conventional subsystems in the zone. The combination of CSub# and ConvLoc# will ensure that Provisioning Manager can uniquely identify every conventional location in the system.

The CCGW ID has a valid range of 1-10. Individual CCGWs are assigned an IP address on the hub subnet, and the host part of the IP address is determined through the uniquely assigned CCGW ID configured from the NM configuration subsystem. The CCGW ID must be assigned uniquely to the CCGWs for each MCC 7500 VPM Dispatch Console site to avoid the same IP address being assigned to two or more CCGWs. This implies the following rules must be enforced by system administrator.

The customer configuration through NM interface is preceded by initial device setup by the SSC. To add a CCGW to a new or existing customer site, the customer needs to contact Motorola Solutions field personnel to initiate the request to perform the initial setup with the SSC. Once the SSC has completed the initial device setup, the customer can proceed with the NM configuration of the CCGW. The SSC upon the initial configuration assigns an instance ID to the CCGW; this ID must match the CCGW ID configured through NM interface, and the customer must obtain this information before the configuration through NM interface can occur.

1.7.6.3 Configuring Audio Levels for the Analog Conventional Channel Gateway

Conventional Channel Gateway (CCGW) analog conventional channel audio level parameters are listed in the *MCC 7500 Dispatch Console with VPM User Guide* and *RF Site Technician Reference Guide*. The audio level parameters must be configured separately for each analog channel in the CCGW. These parameters are configured through the Network Manager.

NOTICE: Digital Conventional devices do not require level settings.

CCGW Outbound Path Parameters

Outbound Alignment Tone Level – This parameter controls the analog output level from the CCGW channel.

CCGW Inbound Path Parameters

Average Inbound G.728 Audio Level – This parameter tells the CCGW the target audio level going to the consoles. This is the target output level of the CCGW’s inbound AGC.

NOTICE: DLM is only valid with the Enhanced Conventional Gateway module.

1.7.7 ACIM Interface – Configuration

The Network Management consider ACIM conventional channels to be a new type of conventional channels and allow the capability to configure this new channel type by the operator.

NOTICE: ACIM conventional channel enabled with the MDC-1200 Signaling Capability can be configured for the "Limited ID Space" capability, if the customer uses Unit ID that is limited to the decimal range.

1.8 GGM 8000 Operation

To power up the GGM 8000, connect AC or DC power to the GGM 8000 as described in one of the following procedures:

- Connecting the GGM 8000 to an AC Power Source on page 68
- Connecting the GGM 8000 to a Centralized DC Power Source on page 70

1.8.1 Successful Startup Verification

The startup process takes a few seconds. When the startup process has successfully completed, the LEDs on the front panel should be on or off as described in the following table. If the LEDs on your

GGM 8000 appear differently than indicated in the table, reboot the GGM 8000. If the LEDs still appear differently than indicated in the table, see Troubleshooting on page 114 for further guidance.

Table 21: LED Status at Successful Startup

Port	LED	Status
Ethernet LAN (on the base system) **NOTICE:** For Ethernet LEDs to display properly, an appropriate device must be connected to the GGM 8000 via a cable of the appropriate type, and this device must be powered on.	Left/Right	Green/Off (10 Mbps full duplex mode) Orange/Off (10 Mbps half duplex mode) Off/Green (100 Mbps full duplex mode) Off/Orange (100 Mbps half duplex mode) Green/Green (1000 Mbps full duplex mode) Orange/Orange (1000 Mbps half duplex mode)
T1/E1 (on the base system)	Carrier	On
	Alarm	Off
	Lpbk	Off
V.24(on the optional expansion module (analog/V.24 interface kit) daughterboard(s) and optional Enhanced Conventional Gateway module)	Port Status	**Green** - The V.24 port is connected, the link to Station/Comparator/Receiver is up, and the digital channel corresponding to this port is enabled and idle. **Blinking Green** – The V.24 port is connected, the link to the Station/Comparator/Receiver is up, the digital channel corresponding to this port is enabled, and audio packets are flowing. **NOTICE:** For the V.24 module port status LEDs to light green, the conventional channel interface service must be enabled in the Enterprise Operating System (EOS) software and the site type must be configured as “digital” or “combination” from the Lightweight Directory Access Protocol (LDAP) server. **Yellow** - The conventional channel interface service is enabled in the EOS software and the corresponding channel is configured to use the V.24 port (it is a digital, mixed mode, or the ASTRO Control Interface Module (ACIM) channel), but the V.24 port is not connected. **Off** - The conventional channel interface service is disabled in the EOS software, or the corresponding channel is not configured to use the V.24 port (it is an analog or MDC 1200 channel).

Port	LED	Status
		NOTICE: If the site type is configured as "analog" from the LDAP server, the digital channel is disabled, and the port status LED is off.
E&M Voice Card (analog)(on the optional expansion module (analog/V.24 interface kit) daughterboard and optional Enhanced Conventional Gateway module)	Port Status	**Green** - Steady if the analog channel is idle; blinking if audio packets are flowing. **Off** - Conventional Channel Gateway (CCGW) functionality is enabled, but the channel corresponding to this port is disabled or is not configured to use an E&M port (for example, it is a V.24 digital channel). **Yellow** - CCGW functionality is not enabled; the Digital Signal Processor (DSP) is out of service; or a fault has been detected on the analog channel corresponding to this port. **NOTICE:** When the GGM 8000 boots up, the E&M port LEDs are yellow until the first analog channel is configured. When an analog channel is configured, if an enabled/active channel fails, the E&M port LEDs are off and turn yellow. If the channel is configured as mixed mode and the E&M port LED is yellow while the corresponding V.24 port LED is green, the mixed mode channel is partially available.
FlexWAN Serial **NOTICE:** For FlexWAN serial LEDs to display properly, an appropriate device must be connected to the GGM 8000 via a cable of the appropriate type, and this device must be powered on.	Link	On
	Active	On
	Fault	Off
System	Status	All off
	Encrypt	**Off** – If the GGM 8000 is not configured with an encryption module. **On** – If encryption capability is enabled. • For units shipped before the ASTRO® 25 7.12 system release (EOS software version 16.0 and 16.2), encryption support requires the presence of an encryption daughtercard. • For units shipped for the ASTRO® 25 7.12 system release and after (EOS software version 16.3 and higher), encryption support requires

Port	LED	Status
		successful feature authentication. For details, see “Secure Feature Authentication” in *Motorola GGM 8000 Hardware User Guide*. **Off** – If the encryption capability is not enabled.
	Run	On
	Load	Off
	Test	Off
	Forward	Off or blinking
	Power/ Fault	Green
Expansion Module	Power/ Fault	Green
	Power	Green

1.8.2

Backing up and Restoring the Secure Feature Authentication File

The secure feature authentication (features.cfg) file is a unique feature configuration file that is generated and loaded by manufacturing for each GGM 8000 gateway. The file is signed with a private key to create a cryptographic signature (the signature value) which protects the file from modification. The GGM 8000 software authenticates the signature value during bootup to allow (or disallow) utilization of the information in the configuration file. If the file is modified, it will not pass authentication when it is booted.

When and where to use:
For GGM 8000 not managed by VoyenceControl, backup the secure feature authentication file so you can restore this file in the event of file corruption or loss.

NOTICE: For GGM 8000 managed by VoyenceControl, the features.cfg file is backed up and restored through the Unified Network Configurator (UNC).
The names EMC Smarts® Network Configuration Manager and VoyenceControl are used interchangeably for this product.

1.8.2.1

Backing up the Secure Feature Authentication File

Prerequisites: Obtain:

- Null modem serial cable
- Service laptop
- Ethernet straight-through cable
- Serial number of the GGM 8000 gateway

NOTICE: You can obtain the serial number by issuing the `SysInfo` command from the GGM 8000 command-line interface.

When and where to use: Back up the `features.cfg` file for GGM 8000 gateways that implement encryption through the embedded encryption engine in the Freescale processor and are not managed by VoyenceControl.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1. Connect the laptop to the GGM 8000 console port by using the serial cable.
2. Connect the laptop's Ethernet card to port 4 (!4) on the GGM 8000 by using the Ethernet cable.
3. Log on to the gateway by using the username (root) and appropriate password.
4. Point the TFTP (or FTP) server to the location where you want to store the features.cfg file.
5. Assign an IP address (for example 10.0.0.1) to the laptop with the appropriate subnet mask (for example 255.255.255.0).
6. To set the port 4 IP address (for example 10.0.0.2), disable the loopback system IP feature for the PING and TFTP services, and enable port/path 4, perform the following actions:
   - **a** In the GGM 8000 command line, enter: `SETDefault !4 -IP NETaddr = 10.0.0.2 255.255.255.0`
   - **b** In the GGM 8000 command line, enter: `SETDefault -SYS UseSystemIP = NPING`
   - **c** In the GGM 8000 command line, enter: `SETDefault -SYS UseSystemIP = NTFTP`
   - **d** In the GGM 8000 command line, enter: `SETDefault !4 -POrt CONTrol = Enable`
   - **e** In the GGM 8000 command line, enter: `SETDefault !4 -PAth CONTrol = Enable`

   NOTICE: This procedure uses TFTP for the file transfer. You can also use FTP, in which case you should replace `SETDefault -SYS UseSystemIP = NTFTP` with `SETDefault -SYS UseSystemIP = NFTP` in the command sequence above.
7. To ensure that port 4 is up and ping the laptop's IP address to ensure connectivity, enter `SHow -IP NETaddr`
8. Change to the directory on the GGM 8000 where the features.cfg file is located and make sure that you see the features.cfg file:
   - **a** Enter: `cd a:/certs`
   - **b** Enter: `df`
9. Copy the features.cfg file from the gateway to the TFTP server directory, renaming the file with the gateway's serial number. Enter:

   `copy a:/certs/features.cfg 10.0.0.1:`***`<gateway_serial #>`***`.cfg`
   Where ***`<gateway_serial #>`*** is the GGM 8000 serial number.

   NOTICE: If you use FTP to transfer the file, enter:
   `put a:/certs/features.cfg 10.0.0.1:`***`<gateway_serial #>`***`.cfg`
10. Store the file in a secure place for future use.

    NOTICE: The features.cfg file is unique for each GGM 8000 and cannot be used with any other GGM 8000.
11. Remove the ethernet cable.
12. Reboot the gateway.

1.8.2.2 Restoring the Secure Feature Authentication File

Prerequisites: Obtain:

- Null modem serial cable

- Service laptop
- Ethernet straight-through cable
- Serial number of the GGM 8000 gateway

NOTICE: You can obtain the serial number by issuing the `SysInfo` command from the GGM 8000 command-line interface.

When and where to use: After you back up the `features.cfg` file for GGM 8000 gateways, restore a lost or corrupted `features.cfg` file. This corrupted or missing `features.cfg` file may cause the following secure feature authentication failure:

- An `ERROR: Not FIPS` compliant log message
- An mnrCryptoSelfTestFailed trap in the Network Manager
- An error string (for example: `Error retrieving config file!`) in the “Certificate Information” section of the SysInfo Command output

Procedure:

1. Connect the laptop to the GGM 8000 console port by using the serial cable.
2. Connect the laptop’s Ethernet card to port 4 (!4) on the GGM 8000 by using the Ethernet cable.
3. Log on to the gateway by using the username (root) and appropriate password.
4. Point the TFTP (or FTP) server to the appropriate secure feature authentication file (the `features.cfg` file) that you renamed as ***<gateway_serial #>*** .cfg, where ***<gateway_serial #>*** is the serial number of GGM 8000 for which you want to restore the `features.cfg` file.
5. Assign an IP address (for example 10.0.0.1) to the laptop with the appropriate subnet mask (for example 255.255.255.0).

   NOTICE: The IP address must be on the same subnet as the GGM 8000’s Ethernet port 4 interface.

6. To set the port 4 IP address (for example 10.0.0.2), disable the loopback system IP feature for the PING and TFTP services, and enable port/path 4, perform the following actions:
   - **a** In the GGM 8000 command line, enter `SETDefault !4 -IP NETaddr = 10.0.0.2 255.255.255.0`
   - **b** In the GGM 8000 command line, enter `SETDefault -SYS UseSystemIP = NPING`
   - **c** In the GGM 8000 command line, enter `SETDefault -SYS UseSystemIP = NTFTP`
   - **d** In the GGM 8000 command line, enter `SETDefault !4 -POrt CONTrol = Enable`
   - **e** In the GGM 8000 command line, enter `SETDefault !4 -PAth CONTrol = Enable`

   NOTICE: This procedure uses TFTP for the file transfer. You can also use FTP, in which case you should replace: `SETDefault -SYS UseSystemIP = NTFTP` with `SETDefault -SYS UseSystemIP = NFTP` in the command sequence above.

7. To ensure that port 4 is up and ping the laptop’s IP address to ensure connectivity, enter `SHow -IP NETaddr`
8. Change to the directory on the GGM 8000 where the `features.cfg` file is located and make sure that you see the `features.cfg` file. Perform the following actions:
   - **a** Enter: `cd a:/certs`
   - **b** Enter: `df`
9. Verify the presence of the `features.cfg` file. Perform one of the following actions:

- If no `features.cfg` file exists, continue with step 10.
- If a `features.cfg` file exists, but you believe it may be corrupted, enter `ReName features.cfg features.bak`. Continue with step 10.

10 Copy the ***<gateway_serial #>***.cfg file from the TFTP server directory to the gateway, renaming the file to `features.cfg`. Enter:

```
copy 10.0.0.1:<gateway_serial #>.cfg a:/certs/features.cfg
```

Where ***<gateway_serial #>*** is the GGM 8000 serial number.

> **NOTICE:** If you use FTP to transfer the file, enter:
> `get 10.0.0.1:<gateway_serial #>.cfg a:/certs/features.cfg`

11 Remove the Ethernet cable.

12 Reboot the gateway.

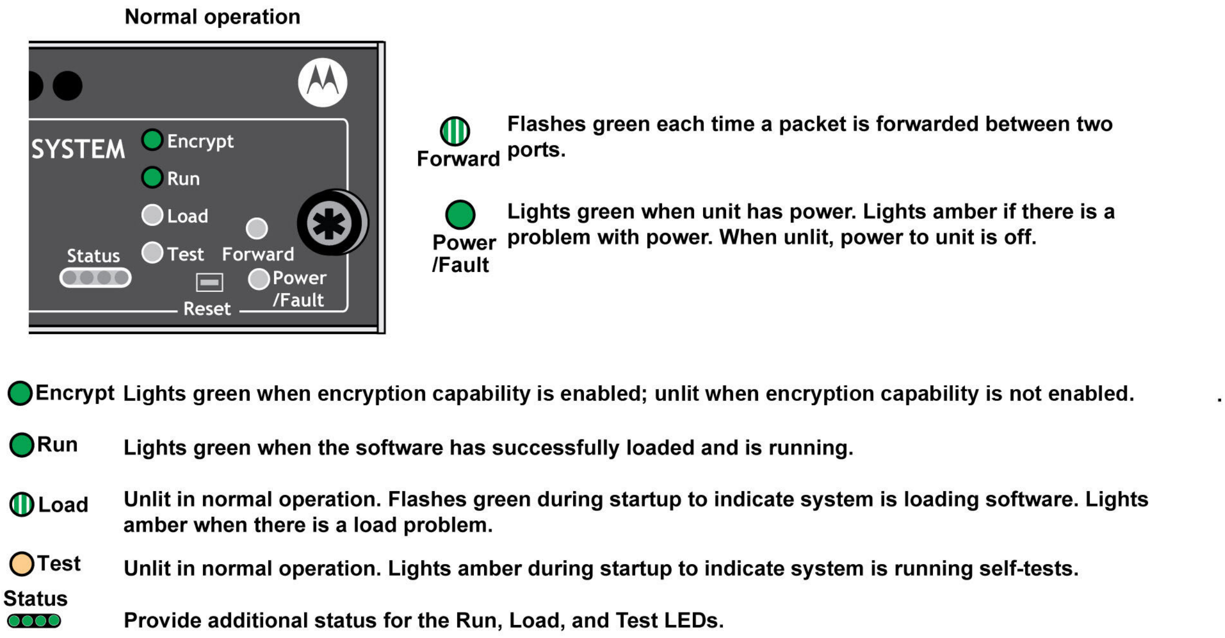
1.8.3 GGM 8000 LEDs

This section describes the GGM 8000 LEDs. For suggestions about troubleshooting actions to take based on the GGM 8000 LED status, see Troubleshooting GGM 8000 Using Status LEDs on page 116.

1.8.3.1 System LEDs

The system LEDs indicate the overall condition of the GGM 8000, including its operating status, power conditions, and fault conditions. The following figure describes the system LEDs.

Figure 51: GGM 8000 System LEDs



Forward Flashes green each time a packet is forwarded between two ports.

Power /Fault Lights green when unit has power. Lights amber if there is a problem with power. When unlit, power to unit is off.

Encrypt Lights green when encryption capability is enabled; unlit when encryption capability is not enabled.

Run Lights green when the software has successfully loaded and is running.

Load Unlit in normal operation. Flashes green during startup to indicate system is loading software. Lights amber when there is a load problem.

Test Unlit in normal operation. Lights amber during startup to indicate system is running self-tests.

Status Provide additional status for the Run, Load, and Test LEDs.

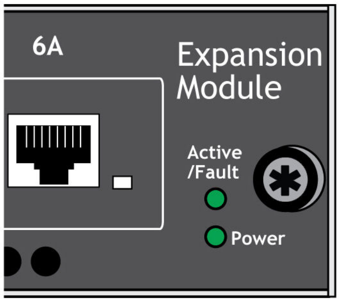
GGM8000_SystemLEDs_B

1.8.3.2 Expansion Module LEDs

The following figure describes the expansion module status LEDs.

Figure 52: GGM 8000 Expansion Module LEDs

Normal operation



🟢 **Active/ Fault** **Lights green when the software has released the expansion module from the reset state.**

🟢 **Power** **Lights green when the expansion module has power.**

🟠 **Active/ Fault** **Lights amber when the software detects a problem on the expansion module.**

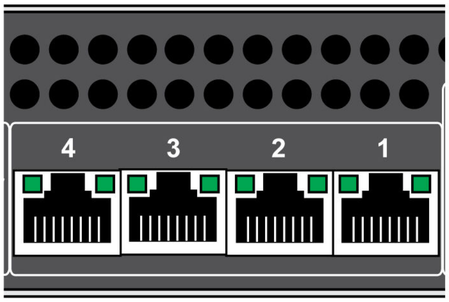
expansion_LEDs

1.8.3.3 Ethernet LEDs

The following figure describes the GGM 8000 Ethernet port LEDs.

Figure 53: GGM 8000 Ethernet LEDs

Normal Operation



🟩 ⬜ **Left LED green; Right LED off:**
Indicates 10 Mbps full duplex mode

🟧 ⬜ **Left LED orange; Right LED off:**
Indicates 10 Mbps half duplex mode

⬜ 🟩 **Left LED off; Right LED green:**
Indicates 100 Mbps full duplex mode

⬜ 🟧 **Left LED off; Right LED orange:**
Indicates 100 Mbps half duplex mode

🟩 🟩 **Both LEDs green:**
Indicates 1000 Mbps full duplex mode

🟧 🟧 **Both LEDs orange:**
Indicates 1000 Mbps half duplex mode

enet_LEDs

1.8.3.4 T1/E1 LEDs

The following figure describes the GGM 8000 T1/E1 LEDs.

The following table lists the T1/E1 LED definitions for the GGM 8000.

Table 22: T1/E1 LED Definitions

Operational State	Carrier	Alarm	Lpbk
Normal operation	ON	OFF	OFF
Loss of Signal	OFF	ON	OFF
Link Failure (no LOS)	OFF	ON	OFF
Remote Initiated Loopback	No Change	OFF	ON
Path or Port Disabled	OFF	OFF	OFF

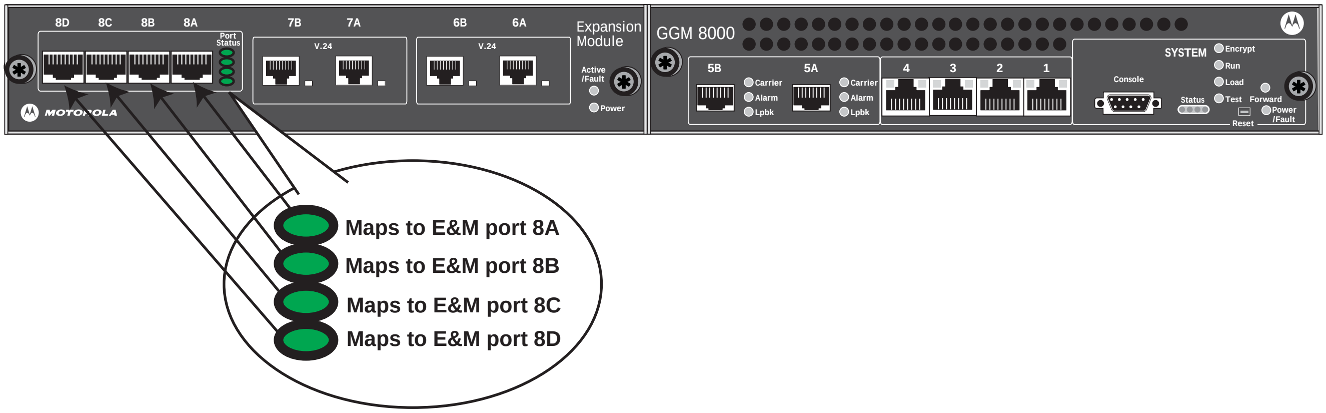
1.8.3.5 Analog/V.24 Interface Kit LEDs

The GGM 8000 analog/V.24 interface kit consists of an E&M module (and DSP SIMM) and two V.24 modules.

1.8.3.5.1 E&M Module LEDs

The GGM 8000 E&M module features four port status LEDs, as illustrated in the following figure.

Figure 54: GGM 8000 E&M Module LEDs



GGM8000_CCGW_LEDs_A

Each LED indicates the status of one of the four E&M ports as follows:

Steady Green
The analog channel corresponding to this port is enabled and idle.

Blinking Green
The analog channel corresponding to this port is enabled, and audio packets are flowing.

Yellow
The conventional channel interface functionality is not enabled; the DSP is out of service; or a fault has been detected on the analog channel corresponding to this port.

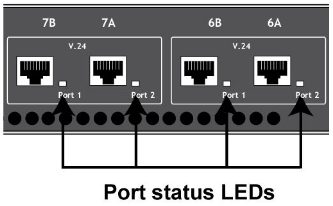
NOTICE: When the GGM 8000 boots up, the E&M port LEDs are yellow until the first analog channel is configured. Once an analog channel is configured, the E&M port LEDs are off and turn yellow if an enabled/active channel fails.
If the channel is configured as mixed mode and the E&M port LED is yellow while the corresponding V.24 port LED is green, then the mixed mode channel is partially available.

For information about analog LEDs on the Enhanced Conventional Gateway module, see Enhanced Conventional Gateway Module V.24 Interface Status LEDs on page 113.

1.8.3.5.2
V.24 Module LEDs

Each of the two ASTRO (V.24 digital) modules included in the analog/V.24 interface kit features two port status LEDs, for a total of four LEDs, as illustrated in the following figure.

Figure 55: GGM 8000 V.24 Module LEDs



v24_LEDs

Each LED indicates the status of one of the four V.24 ports as follows:

- **Steady Green** - The V.24 port is connected, the link to Station/Comparator/Receiver is up, and the digital channel corresponding to this port is enabled and idle.
- **Blinking Green** - The V.24 port is connected, the link to the Station/Comparator/Receiver is up, the digital channel corresponding to this port is enabled, and audio packets are flowing.

  NOTICE: In order for the V.24 module port status LEDs to light green, the conventional channel interface service must be enabled in the EOS software and the site type must be configured as “digital” or “combination” from the LDAP server.
- **Yellow** - The conventional channel interface service is enabled in the EOS software and the corresponding channel is configured to use the V.24 port (it is a digital, mixed mode, or ACIM channel), but the V.24 port is not connected.

For more information about V.24 LEDs on the Enhanced Conventional Gateway module, see Enhanced Conventional Gateway Module V.24 Interface Status LEDs on page 113.

1.8.3.6
Enhanced Conventional Gateway Module LEDs

The Enhanced Conventional Gateway module features a bi-color (green/amber) LED in the lower right corner that indicates the overall operational status of the module as well as two bi-color (green/amber) LEDs for each analog and each V.24 interface.

1.8.3.6.1
Enhanced Conventional Gateway Module Analog Interface Status LEDs

Each analog interface on the Enhanced Conventional Gateway module features two bi-color status LEDs located in the lower left and right corners of the “Audio, E&M” (yellow) RJ45 connectors.

NOTICE: The corresponding “Analog I/O” (white) RJ45 connectors do not feature LEDs.

Each analog interface status LED indicates the status of one of the four analog interfaces as follows:

Steady Green
The analog channel corresponding to this interface is enabled and idle.

Blinking Green
The analog channel corresponding to this interface is enabled, and audio packets are flowing.

Yellow

CCGW functionality is not enabled, the DSP is out of service, or a fault has been detected on the analog channel corresponding to this interface.

NOTICE: When the GGM 8000 boots up, the analog interface status LEDs are amber until the first analog channel is configured. Once an analog channel is configured, the analog interface LEDs are off and turn amber if an enabled/active channel fails.

NOTICE: If the channel is configured as mixed mode and the analog interface status LED is amber while the corresponding V.24 interface LED is green, then the mixed mode channel is partially available.

Off

CCGW functionality is enabled, but the channel corresponding to this interface is disabled or is not configured to use an analog interface (for example, it is a V.24 digital channel).

For information about how the GGM 8000 analog interface status LEDs should appear when all supported channels are in service, depending on the channel type, see “Conventional Channel Gateway (CCGW) LEDs” in *Motorola GGM 8000 Hardware User Guide*.

1.8.3.6.2 Enhanced Conventional Gateway Module V.24 Interface Status LEDs

Each V.24 interface on the Enhanced Conventional Gateway module features two bi-color (green/ amber) status LEDs in the lower left and right corners of the “V.24” (blue) RJ45 connectors. Only the right-hand LED is operational. The left-hand LED is always off.

Each V.24 interface status LED indicates the status of one of the V.24 interfaces as follows:

Steady Green

The V.24 interface is connected, the link to the base station/comparator/receiver is up, and the digital channel corresponding to this interface is enabled and idle.

Blinking Green

The V.24 interface is connected, the link to the base station/comparator/receiver is up, the digital channel corresponding to this interface is enabled, and audio packets are flowing.

NOTICE: In order for the Enhanced Conventional Gateway module V.24 interface status LEDs to light green, the CCGW service must be enabled in the EOS software, and the site type must be configured as combination-HD from the LDAP server.

Yellow

The CCGW service is enabled, and the corresponding channel is configured to use the V.24 interface (it is a digital, mixed mode, or ACIM channel), but the V.24 interface is not connected).

Off

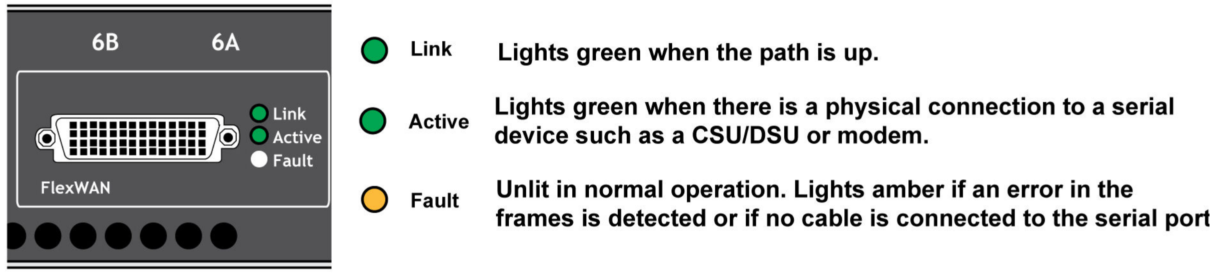
The CCGW service is disabled or the corresponding channel is not configured to use the V.24 interface (it is an analog or MDC 1200 channel).

For details about how the GGM 8000 V.24 interface status LEDs should appear when all supported channels are in service, depending on the channel type, see “Conventional Channel Gateway (CCGW) LEDs” in *Motorola GGM 8000 Hardware User Guide*.

1.8.3.7 FlexWAN Serial LEDs

The following figure describes the LEDs on the optional FlexWAN daughterboard.

Figure 56: GGM 8000 FlexWAN LEDs



● Link — Lights green when the path is up.

● Active — Lights green when there is a physical connection to a serial device such as a CSU/DSU or modem.

● Fault — Unlit in normal operation. Lights amber if an error in the frames is detected or if no cable is connected to the serial port

Normal operation

ser_LED

1.8.4
ACIM Interface – Operation

For operation information about GGM 8000 used with conventional channels, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

1.9
GGM 8000 Maintenance

There are no serviceable parts in the GGM 8000 gateway that require maintenance or calibration. Exterior cleaning using a clean, lint-free cloth or a soft brush is sufficient. Ensure that the ventilation ports are kept clean at all times.

Monitor the GGM 8000 LEDs periodically to ensure that the gateway is operating properly. In the event of a gateway failure, see Troubleshooting on page 114 or contact Motorola Solutions for support.

1.10
Troubleshooting

This section provides fault management and troubleshooting information relating to the GGM 8000 Gateway.

The following resources are available for troubleshooting problems with the GGM 8000 Gateway:

- Unified Network Configurator
- Unified Event Manager
- InfoVista
- Local Gateway Administration

See the *Provisioning Manager OLH* for details about the gateway alarms.

1.10.1
Troubleshooting General Connectivity Problems

Prerequisites: The following procedure assumes that the GGM 8000 gateway is already installed and configured.

When and where to use: Use the following steps to troubleshoot the GGM 8000 gateway's connectivity problems related to the LAN connection.

NOTICE: The Border Gateway does not support the UNC/UEM procedures. You can perform the same tasks locally using the gateway administration menus.

Procedure:

1. Perform the following actions:
   - **a** In the Unified Event Manager (UEM), check the conditions and alarms for the gateway.
   - **b** In the Unified Network Configurator (UNC), check the gateway configuration and router log information.
   - **c** Verify that the IP address, MAC address, and other configuration settings are correct.
2. Using UEM, check the alarms for other critical network devices on the LAN. Also verify the configuration of LAN switch.
3. Check the physical connection to the LAN port on the gateway. Verify that the cabling is properly connected and in good condition. Check for sharp bends in cabling and cabling that is longer than the specification (for example 100 meters for 10BASE-T).
4. Try to reboot the gateway through Provisioning Manager or cycle power to the gateway. See the *Provisioning Manager User Guide* for more information.
5. If the connection fails, power down the gateway and test the Ethernet cable for continuity, attenuation, and excessive crosstalk. Replace the cable if necessary.
6. If the connection still fails, try to reload the EOS software and configuration files to the gateway locally.
7. If the gateway still fails to operate properly, replace the gateway.

   See FRU/FRE Procedures on page 125 for replacement instructions.

1.10.2 Troubleshooting General Performance Problems on the LAN

Prerequisites: The following procedure assumes that the GGM 8000 gateway is already installed and configured.

When and where to use: Use the following steps to troubleshoot the GGM 8000 gateway's performance problems on the LAN.

NOTICE: The Border Gateway does not support the UEM procedures. You can perform the same tasks locally using the gateway administration menus.

Procedure:

1. In UEM, check the condition of the LAN switch and all affected devices and links. Verify that all gateways are operational.
2. Using Historical Reports and Performance Reports, check the overall loading of calls and activities on the LAN. Verify that the loading is within the maximum loading specifications for the system.
3. Using InfoVista, generate performance and traffic reports for the gateways. Look for anomalies, heavy volumes of traffic, or high CPU utilization or other device resources.
4. Run ping, traceroute, and pathping commands and loopback testing across any troubled links or between any suspected devices.
5. Verify that the address tables, subnet masks, and default gateways are set appropriately in the GGM 8000 gateway and other networked devices.

6 Physically verify that the LAN switch is operating properly. Check LEDs and physical connections and verify that all cabling conforms to standard. Check for sharp bends in cabling and cabling that is too long for specification (such as 100 meters for 10Base-T).

7 Check troubled cabling for noise, attenuation, continuity, and crosstalk. Verify that communication cabling is routed apart from all power cabling and power sources. Verify that cabling is also clear from any test equipment that is causing interference.

8 As applicable, verify that any service provider connections are providing the appropriate throughput for your system.

9 Identify the bottleneck points in the system. Check and reload device configurations as necessary, or replace any suspected switching or routing devices that are not performing to specification.

10 Revise the configurations, services, and permissions for the subscribers as necessary.

11 Purchase additional equipment to handle the additional load of traffic (more gateways or sites). Contact Motorola Solutions for assistance.

1.10.3 Troubleshooting GGM 8000 Using Status LEDs

This section suggests troubleshooting actions to take based on GGM 8000 LED status.

The system LEDs indicate the overall condition of GGM 8000, including its operating status, power conditions, and fault conditions. The table below provides details about troubleshooting actions to take based on the state of the system LEDs.

Table 23: Troubleshooting Using the System LEDs

LED	Purpose	Appearance	Troubleshooting Action
Encrypt	Indicates whether or not encryption capability is enabled.	Green	Encryption capability is enabled; no action is necessary.
		OFF	Encryption capability is not enabled. If GGM 8000 is not used in a network position or application that requires encryption, no action is necessary. If GGM is being used in a network position or application that requires encryption, perform the following checks: • Make sure that the proper EOS software package is loaded. GGM 8000 encryption requires the EOS XS software package. To view the software package and version number, enter `SHow -SYS SOftwareInfo /primary/boot.ppc` • For units shipped prior to the ASTRO® 25 7.12 system release (EOS software version 16.0 and 16.2), encryption support requires the presence of an encryption daughtercard. To verify that an encryption daughtercard is present, enter `SysInfo` The returned information should include the following entry for slot 8: `Cavium Nitrox PX :`

LED	Purpose	Appearance	Troubleshooting Action
			• For units shipped for the ASTRO® 25 7.12 system release and after (EOS software version 16.3 and higher), encryption support requires successful feature authentication. Check for the following, which indicate a secure feature authentication failure: - An `ERROR: Not FIPS compliant` log message - An `mnrCryptoSelfTestFailed` in the network manager - An error string (for example `Error retrieving config file!`) in the “Certificate Information” section of the SysInfo command output For details about the secure authentication mechanism, see the *Motorola GGM 8000 Hardware User Guide*.
Run	Indicates whether the software has successfully loaded and GGM 8000 is running	Solid Green	All startup diagnostics have passed and GGM 8000 is operating normally; no action is necessary.
		OFF	GGM 8000 is not powered or is not running properly. • Using the Provisioning Manager, check the alarms for GGM 8000. • Verify that the Power/Fault LED is solid green and the Load LED is off. - If the Power/Fault LED is off, there may be a problem with the power input. - If the Load LED is illuminated, there may be a software loading problem. See the descriptions of the Power/Fault and Load LEDs later in this table for further details.
Load	Indicates the software loading status for GGM 8000	OFF	GGM 8000 software is loaded and operating properly; no action is necessary.
		Flashing Amber	GGM 8000 is initializing; no action is necessary.
		Solid Amber	GGM 8000 is experiencing a software loading problem. Typically, the Power/Fault LED is also solid amber in this case. The status LEDs indicate the specific type of loading problem. You can also take these troubleshooting actions: • Using the Provisioning Manager, check the alarms for GGM 8000. • Cycle power to GGM 8000.

LED	Purpose	Appearance	Troubleshooting Action
			• If GGM 8000 continues to iterate through the boot process without finally moving into the run mode (indicated by the Run LED turning solid green), contact the Motorola Solutions Support Center (SSC) for assistance.
Test	Indicates that GGM 8000 is running self tests	OFF	GGM 8000 is operating normally; no action is required.
		Solid Amber	GGM 8000 is performing self tests; no action is necessary.
Forward	Indicates that traffic is being forwarded on GGM 8000	Flashing Green	Packets are being forwarded; no action is necessary.
Power / Fault	Indicates the power or fault condition of GGM 8000	Solid Green	GGM 8000 is properly powered and is not reporting a fault condition; no action is necessary.
		Solid Amber	GGM 8000 is reporting a fault condition. Troubleshoot GGM 8000 according to System Status LED Failure Codes on page 119. • Check the Load and Status LEDs for additional error indications. Use the troubleshooting steps for the Load LED, earlier in this table or see System Status LED Failure Codes on page 119. • Using the UEM, check the alarms for GGM 8000. • Try rebooting GGM 8000 through the UNC or cycle power to GGM 8000. - If GGM 8000 does not boot properly, try reloading the EOS software and configuration files. - If GGM 8000 still does not run properly, replace GGM 8000. See FRU/FRE Procedures on page 125 for replacement instructions.
		OFF	GGM 8000 is not powered. • Using the UEM, check the alarms for GGM 8000. • Verify that the power cabling is firmly connected on the rear of GGM 8000. • Connect GGM 8000 to a different power source. **NOTICE:** If possible, maintain redundant GGM 8000s on separate circuits.

LED	Purpose	Appearance	Troubleshooting Action
			• If GGM 8000 still does not boot up, replace GGM 8000. See FRU/FRE Procedures on page 125 for details.

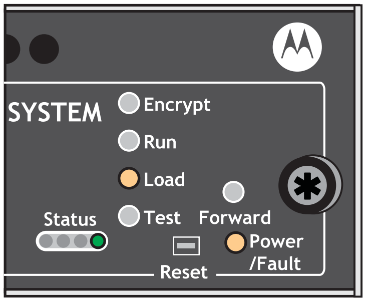
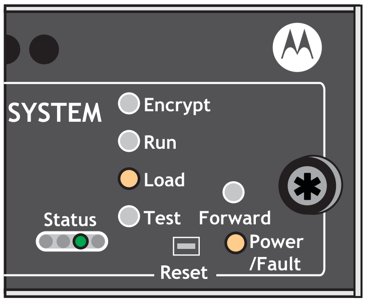
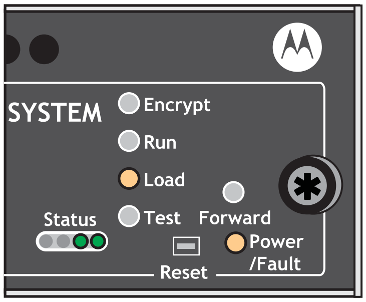
1.10.3.1

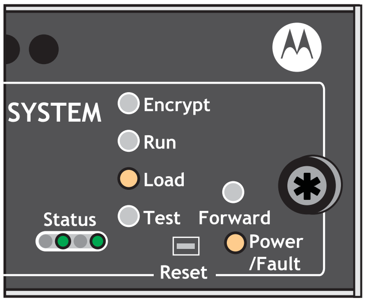
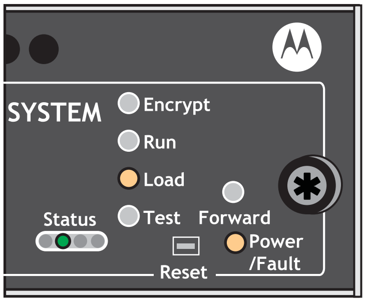
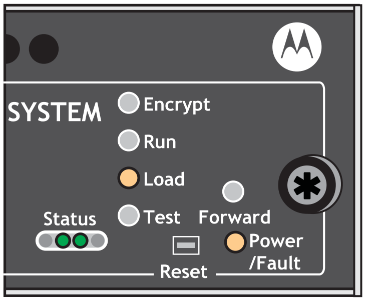
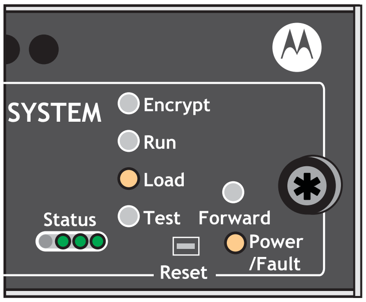
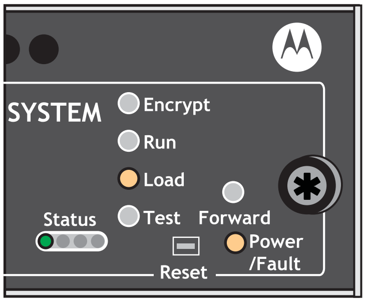
System Status LED Failure Codes

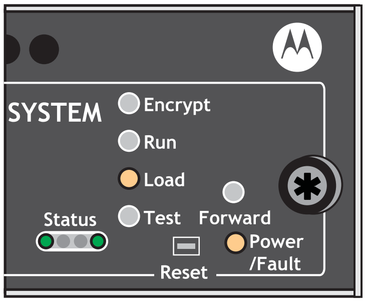
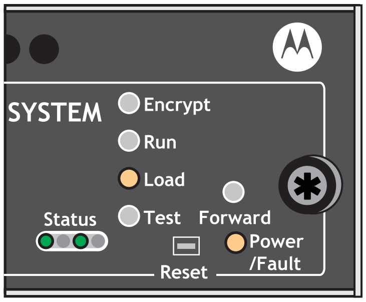
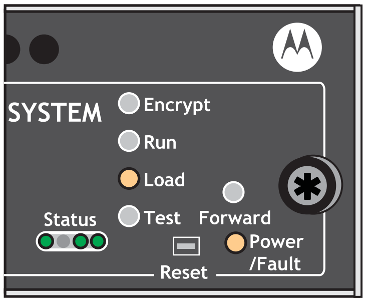
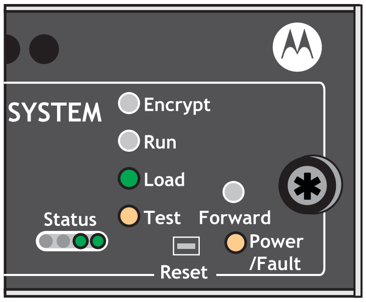
If the system Load and Power/Fault LEDs light amber, a problem occurred during the system software load phase. When a failure occurs, the four status LEDs can also indicate a failure code that defines the particular problem.

Compare the status LEDs on your GGM 8000 with the examples provided in the table below and follow the corresponding instructions for troubleshooting. If the suggested troubleshooting measures do not solve the problem, contact the Motorola Solutions Support Center (SSC) for assistance.

Table 24: System Status LED Failure Codes and Troubleshooting Actions

System LED Appearance	Meaning	Troubleshooting Action
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The GGM 8000 file system is empty.	Try reloading the EOS software and configuration files.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	Possible read-only memory corruption.	Cycle power to the GGM 8000 and try reloading the EOS software and configuration files.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The software image file has been deleted or the boot source and image names do not match.	Cycle power to the GGM 8000 and see if the problem is resolved. If the problem is not resolved, try reloading the EOS software and configuration files. If the problem is not resolved, replace the GGM 8000 or contact the Motorola Solutions Support Center (SSC).

System LED Appearance	Meaning	Troubleshooting Action
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The image file is larger than available memory.	Cycle power to the GGM 8000 and see if the problem is resolved. If the problem is not resolved, try reloading the EOS software and configuration files. If the problem is not resolved, replace the GGM 8000 or contact the Motorola Solution Support Center (SSC).
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	There was an error either reading the image files or decompressing it.	Cycle power to the GGM 8000 and try reloading the EOS software and configuration files.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	A file checksum detection error has been detected.	Cycle power to the GGM 8000 and try reloading the EOS software and configuration files.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	An unspecified fatal error has occurred.	Cycle power to the GGM 8000 and see if the problem is resolved. If the problem is not resolved, try reloading the EOS software and configuration files. If the problem is not resolved, replace the GGM 8000 or contact the Motorola Solutions Support Center (SSC).
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The GGM 8000 is unable to transmit a BOOTP request.	Verify that the Ethernet cabling to the GGM 8000 is properly connected and in good condition. If necessary, cycle power to the GGM 8000. If the GGM 8000 does not boot properly, try reloading the EOS software and configuration files.

System LED Appearance	Meaning	Troubleshooting Action
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The GGM 8000 is not receiving a response to a BOOTP request. The BOOTP server is not present or may be configured incorrectly.	Check the Trivial File Transfer Protocol (TFTP)/BOOTP server configuration and verify the media access control (MAC) address of the GGM 8000.
		Cycle power to the GGM 8000 to retry the system software load. If the GGM 8000 does not boot properly, contact the Motorola Solutions Support Center (SSC) for assistance.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The GGM 8000 is not receiving a response to an address resolution protocol (ARP) request from the TFTP server. The TFTP server is not present or may be incorrectly configured.	Check the TFTP server configuration and verify the MAC address of the GGM 8000.
		Cycle power to the GGM 8000 to retry the system software load. If the GGM 8000 does not boot properly, contact the Motorola Solutions Support Center (SSC) for assistance.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	The GGM 8000 is not receiving a response to a TFTP request. The TFTP server is not present, the incorrect file was downloaded, or the file in incorrectly configured.	Check the TFTP server configuration and verify the MAC address of the GGM 8000.
		Cycle power to the GGM 8000 to retry the system software load. If the GGM 8000 does not boot properly, contact the Motorola Solutions Support Center (SSC) for assistance.
 SYSTEM Encrypt Run Load Status Test Forward Power /Fault Reset	When the software load is complete, the system begins the test phase. If the Test LED lights amber, as illustrated to the left, a problem occurred during the system test phase; for example, an EEPROM checksum test failed.	Contact the Motorola Solutions Support Center (SSC).

1.10.4

Conventional Channel Gateway – General Maintenance and Troubleshooting

This section contains troubleshooting information pertaining to the GGM 8000 used to support Conventional Channel Gateway (CCGW) functionality.

1.10.4.1 CCGW Serviceability

The CCGW serviceability interface enables technicians to view and query logged information and to enable/disable system/device options. Access to the serviceability interface may be either local (through a local configuration management terminal) or remote.

Refer to the “Using the Command-line Interface” and “Using the Menu-Driven Interface” sections in *Motorola GGM 8000 Hardware User Guide*. More information is also available in the “Serviceability of Console Sites” section in the *Console Sites Reference Guide* for the information that is accessible through the CCGW serviceability interface.

1.10.4.2 Troubleshooting CCGW with Network Management Components

You can use the following network management applications to troubleshoot the CCGWs:

ZoneWatch

ZoneWatch data that is specific to conventional calls is noted in the MCC 7500 VPM manuals and *RF Site Technician Guide*. For a full discussion of the use of ZoneWatch for troubleshooting, refer to the ZoneWatch documentation.

Affiliation Display

Affiliation Display data that is specific to conventional calls is noted in the MCC 7500 VPM manuals and *RF Site Technician Guide*. For a full discussion of the use of Affiliation Display for troubleshooting, see the Affiliation Display documentation.

Air Traffic Router

The messages from the ATR that are specific to conventional calls are noted in the MCC 7500 VPM manuals and *RF Site Technician Guide*. For a full discussion of the use of ATR for troubleshooting, refer to the Air Traffic Router documentation.

1.10.4.3 Failures Reported

The following types of failures for conventional are reported to the fault management system through SNMP:

- Link failures:
  - CCGW links (control paths) to and from the zone controller (ZC), that is ZC-CCGW CP and CCGW-ZC CP
  - Console site link (control path) to ZC
  - CCGW link to LAN switch
- CCGW internal failures
- Digital link loss between CCGW and digital capable RF equipment

Internal failures in CCGW (for example, DSP, E&M, or v.24 module failures) are reported to the fault management system as if they were failures of the conventional channel, although the reason code in the trap indicates the actual module that failed.

1.10.4.3.1 Conventional Gateway to Zone Controller

Each CCGW maintains an independent control link with the zone controller. If two or more CCGWs are located at an RF site, the link between each CCGW and the zone controller is reported independently. Failures of a CCGW to ZC and ZC to CCGW control link are detected and reported in two ways. In the event of a failure of the link, the failure is detected within 10 seconds during the periods of inactivity and within 1.5 seconds when there is an active voice call (inbound or outbound) on any of the conventional channels served by CCGW. The same is true when a Conventional Site Controller is managing CCGW.

1.10.4.3.2 GGM 8000 to GTR 8000 Base Radio/GPW 8000 Receiver

The CCGW will detect a link failure with a GTR 8000 Base Radio/GPW 8000 Receiver. Any voice calls active on the link during a link failure will end immediately when the link is lost. The channel will be displayed as failed after a short period of time. This time window allows for the link to encounter a brief burst of link errors or microwave fades that may cause lost packets without flashing link failures too frequently to system operators.

1.10.4.3.3 Mixed Mode Conventional Channels

Hybrid links are used for Mixed Mode channels. When in analog mode, Conventional Mixed Mode channels use the analog 4-Wire port on the CCGW and base radio for audio transmission, and use the digital v.24 interface for all call control signaling. When in digital transmission mode the Conventional Mixed Mode channels use the same v.24 resources and signaling as v.24 digital conventional channels.

To support Conventional Mixed Mode channels, a new channel state was added to reflect the channels' ability to support digital transmission while being unable to provide analog. This situation arises when the analog 4-Wire interface is inoperable, or base station or the comparator is not connected properly, and the digital v.24 port is available. This state is called “Partially Available” and is determined through the use of a continuity tone provided by the CCGW and base station on the transmit side of the 4-Wire interface. This tone is called the Analog Link Monitor Tone (ALMT).

1.10.4.3.4 ALMT

The ALMT is supported on Conventional Mixed Mode with the V.24 interface. It is not supported on Conventional Mixed Mode with the Ethernet interface and is not supported on analog conventional channels.

When the CCGW detects that there is no ALMT signal on the 4-Wire interface and that it has not received a “start” signal on the associated v.24 interface it will report that the 4-Wire interface is down (e.g. “ALMT un-detect”). An alarm will be sent to Provisioning Manager for the channel associated with the 4-Wire. The status of the Mixed Mode channel associated with that 4-Wire interface will be reported as “Partially Available” (assuming that the v.24 interface for that channel remains available). The “Partially Available” status is reported to and displayed at the consoles so that the console operators know when selecting the Conventional Mixed Mode channel that the channel is incapable of transmitting audio in analog mode, but that the channel can function properly in digital mode (for example, that the v.24 is available).

Table 25: Channel State for the Conventional Mixed Mode

4-Wire Port	V.24 Port	Mixed Mode Channel Status/ Interface
Available	Available	In Service
Unavailable	Unavailable	Out Of Service
Unavailable	Available	Partially Available
Available	Unavailable	Out Of Service

NOTICE: Conventional Mixed Mode channels can also be placed in the Partially Available state when the CCGW detects a DSP failure. The DSP in the CCGW is critical to the operation of analog operation. A failure of a DSP will render the associated analog channels Out Of Service. However, the digital components of the Conventional Mixed Mode channel may still be available and usable based on the states in the table above.
Analog Conventional 4–Wire interfaces alone provide no link failure capability.

1.10.4.4 ACIM Interface – Troubleshooting & Maintenance

For maintenance and troubleshooting information about GGM 8000 used with conventional channels, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

NOTICE: The Conventional Channel Gateway reports the status of the ACIM conventional channel to the NM using the same method that it uses for ASTRO conventional channels.

1.10.4.5 Relay Keying For Diagnostics

Prerequisites: Prepare:

- CAT 5 network cable
- Wire stripper
- Ohm meter with audible indicator

When and where to use:
Relay keying is a new service functionality added to the GGM 8000. It can be used as an additional diagnostic tool for the ACIM conventional channel, digital conventional and mixed mode channels, or for keying a transmitter over the relay closure. The relay keying feature allows you to use the M-lead on the gateway E&M card as a diagnostic tool to monitor the base station's or consolette's keyed state.

Relay keying is supported on digital conventional, mixed mode, and ACIM conventional channel. For these three channel types, the E&M card is used for transmission and reception of audio, but the E-lead and M-lead signals on each port are unused since all control signaling uses the digital command link, and keying is performed through digital messaging across the V.24 interface. When the M-lead is not being used to key the base station or consolette, it can be used as a diagnostic tool to monitor the base station or consolette's keyed state.

NOTICE: For current and voltage rating of the relay keying, refer to GGM 8000 to Analog Base Station Pin Functions on page 80.

Procedure:

1. Cut one end of the network cable off to approximately one foot in length.
2. Strip back the outer jacket approximately two inches to expose the 4-wire pairs.
3. Select and untwist the pair of wires that are connected to pins 3 and 6 of the RJ45 plug.
4. Strip approximately 1/4 inch off the ends of the untwisted wires.
5. Connect an Ohm meter with an audible indicator to the exposed conductors.

   When the M-lead is actuated (base station or consolette is keyed), the Ohm meter registers a low (single digit) reading and sounds the audible indicator.

1.11 FRU/FRE Procedures

This section lists the field replaceable units (FRUs) and filed replaceable entity (FRE) for the GGM 8000 and provides replacement instructions.

The following table lists the GGM 8000 FRE and part number.

Table 26: GGM 8000 FRE List

FRE Description	Part Number
GGM 8000 Base Unit (no power supply) – new base module (no USB port)	TYN4001B
GGM 8000 Base Unit (no power supply)	TYN4001A
GGM 8000 Base Unit (no power supply) – new base module (no USB port), encryption enabled	TYN4010B
GGM 8000 Base Unit (no power supply) – encryption enabled	TYN4010A

The following table lists the GGM 8000 FRUs and part numbers.

Table 27: GGM 8000 FRU List

FRU Description	Part Number
GGM 8000 encryption module **NOTICE:** New GGM 8000 devices ordered from Motorola Solutions do not require an encryption module in order for encryption to be enabled.	TYN4000A
GGM 8000 analog/V.24 interface kit	TYN4002A
GGM 8000 AC power supply	TPN6210A
GGM 8000 DC power supply	TPN6211A
GGM 8000 E&M daughterboard and DSP SIMM	TYN4003A
GGM 8000 V.24 daughterboard	TYN4004A
GGM 8000 expansion module	TYN4005A
GGM 8000 FlexWAN module	TYN4007A
GGM 8000 base (router) module – new base module (no USB port)	TYN4006B
GGM 8000 base (router) module	TYN4006A
GGM 8000 base (router) module – new base module (no USB port)	TYN4009B
GGM 8000 base (router) module – encryption enabled	TYN4009A
GGM 8000 High Density Enhanced Conventional Gateway Module	TYN4011A
GGM 8000 Low Density Enhanced Conventional Gateway Module	TYN4012A

1.11.1
Required Tools and Equipment for GGM 8000 Replacement

Take the following items to the site when replacing a GGM 8000 FRE or FRU:

- ESD wrist strap (Motorola Solutions part number RSX4015A, or equivalent)
- Laptop with terminal emulation program such as Hyperterminal or ProComm+
- Ethernet crossover cable
- DB9 null modem cable
- Set of TORX® drivers

CAUTION: When removing or installing modules, take the following precautions to prevent ESD (electrostatic discharge) from damaging the internal components of the GGM 8000:

- Always wear a properly-grounded anti-static wrist strap. Always wear a properly-grounded anti-static wrist strap.
- Transport static-sensitive components in anti-static packaging.
- Keep static-sensitive components in their anti-static packaging until you are ready to install them.
- Just before removing components from their anti-static packaging, discharge static electricity from your body by touching an unpainted metal surface.
- When you handle modules, place them printed circuit side down on a non-conducting, static-free, flat surface.

1.11.2
Replacing a GGM 8000

Prerequisites: Before replacing a GGM 8000 unit, ensure that you have access to the appropriate GGM 8000 configuration (`boot.cfg`, `StaticRP.cfg`, and `acl.cfg`) files for the unit you are replacing.

NOTICE: You can either find the configuration files on the media device containing the electronic version of the system-specific documentation provided by Motorola Solutions when your system was commissioned or upgraded, or download the files to your PC from the UNC.

WARNING: The GGM 8000 contains dangerous voltages, which may cause electric shock or damage to the equipment. Turn off the GGM 8000 and remove the power cabling when servicing this unit.

Prior to beginning the replacement procedure, ensure that the replacement GGM 8000 has the same hardware installed in the left-hand slot. Possible hardware includes:

- Blank filler panel
- Enhanced Conventional Gateway module (High Density (8 analog ports and 8 V.24 ports) or Low Density (4 analog ports and 4 V.24 ports))
- Expansion module equipped with one of the following:
  - analog/V.24 interface kit (E&M daughterboard and two V.24 daughterboards)
  - FlexWAN daughterboard(s)

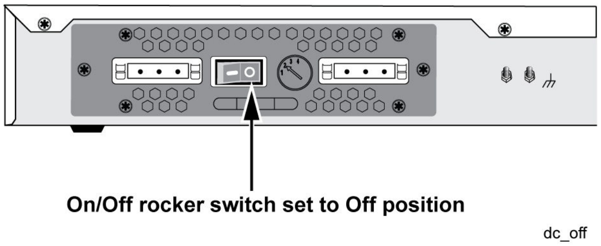
NOTICE: One way to test that the hardware configurations match is to make sure that there is a connector on the replacement unit for each of the cables connected to the existing unit.

When and where to use: Use this procedure when replacing a GGM 8000 as a unit.

Procedure:

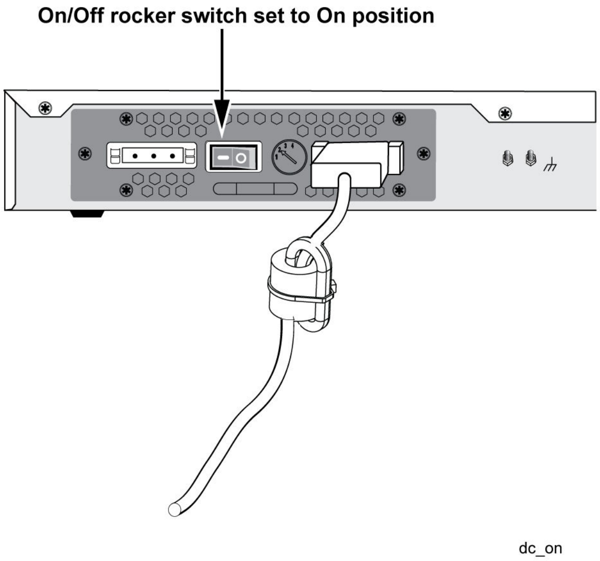
1. Wear an ESP strap and connect its cable to a verified good ground. This strap must be worn throughout this procedure to prevent ESD damage to any components.
2. Power down the existing GGM 8000.
   - For a GGM 8000 with an AC power subsystem: Turn off the power at its source.
   - For a GGM 8000 with a DC power subsystem: Set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the Off position, as illustrated in the following figure.

   Figure 57: Setting the On/Off Rocker Switch to the Off Position

3. Remove the existing GGM 8000:
   - **a** Label and disconnect all communication cabling from the GGM 8000.
   - **b** Disconnect the ground cable from the rear of the chassis.
   - **c** Remove the screws securing the GGM 8000 to the rack.
   - **d** Pull the GGM 8000 out through the front of the rack.
4. Remove the mounting brackets from the existing GGM 8000 and install the brackets on the replacement GGM 8000.
5. Install the replacement GGM 8000:
   - **a** Install the replacement GGM 8000 into the rack and secure the gateway with the screws that were previously removed.
   - **b** Secure the ground cable to the ground location on the rear of the chassis.
   - **c** Attach all communication cabling to the GGM 8000.
6. Power on the replacement GGM 8000.
   - For a GGM 8000 with an AC power subsystem: Restore the power at its source.
   - For a GGM 8000 with a DC power subsystem: Set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the On position, as illustrated in the following figure.

Figure 58: Setting the On/Off Rocker Switch to the On Position



7 Proceed to configure the GGM 8000 as described in the configuration section of this chapter.

8 Enable RADIUS authentication on the GGM 8000. See the *Authentication Services Feature Guide* for details.

9 On system with MAC port locking, disable the locking and then re-enable the locking with the MAC address of the GGM 8000. For instructions on how to disable and enable MAC port locking, refer to the *MAC Port Lockdown Feature Guide*.

10 On system with link encryption or protocol authentication, enter the correct keys for the new GGM 8000 so that it can be authenticated by its encryption or authentication peer. For instructions, see the *Link Encryption and Authentication Feature Guide*.

11 On systems with SNMPv3 enabled, enable passphrase information. For instructions, see the *SNMPv3 Feature Guide*.

12 Find this device in the VoyenceControl devices list. Execute the saved command called **Clear USM Cache** from the list of saved commands under **System** → **Motorola** → **SNMPv3**. For instructions on accessing and executing saved commands for a device, see “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator User Guide*.

NOTICE: The names EMC Smarts® Network Configuration Manager and VoyenceControl are used interchangeably for this product.

13 Test the device credentials with the **Test Credentials** quick command. For more details, see “Executing Quick Commands” in the *Unified Network Configurator User Guide*.

14 Right-click the device, from the context menu select **Pull** → **Pull All**.

15 Go to the Schedule Manager to approve the remedy job that resulted from the Pull operation. For more details, see the “Approving Configuration Changes” section in the *Unified Network Configurator User Guide*.

16 Compare the version of the EOS software that is running on the replacement GGM 8000 with the version that was running on the replaced device by running the Compare function in the hardware history in UNC. For instructions, see the *Unified Network Configurator User Guide*.

NOTICE: If the replacement GGM 8000 needs a software upgrade, then upgrade software as described in the *Unified Network Configurator User Guide*.

17 Check the version of the firmware if performing a firmware downgrade. If the version is 16.8.0.19 or higher for an NMR, additional steps are necessary. See Performing a Firmware Downgrade on page 273.

18 Compare the configuration of the replacement GGM 8000 with the configuration of the replaced device by running the Compare function in the configuration history in UNC. For instructions, see the *Unified Network Configurator User Guide*.

> **NOTICE:** If necessary, perform a Rollback Configuration procedure as described in the *Unified Network Configurator User Guide*.

19 Verify that the replacement GGM 8000 is operating properly.

1.11.3

Replacing Daughterboards on the GGM 8000

Prerequisites: Obtain a size T15 TORX® screwdriver.

> **IMPORTANT:** In order to replace a daughterboard, you must remove the expansion module. If the GGM 8000 is secured with tamper evidence labels, removing the expansion module will break one of these labels. You must either return the unit to Motorola Solutions for daughterboard replacement or obtain new tamper evidence labels (part number TYN4008A) and follow the instructions provided with the labels to install a new tamper evidence label after you have replaced the daughterboard.

When and where to use: Use this procedure when replacing an optional daughterboard on the GGM 8000 expansion module. The expansion module can be removed, and the daughterboards replaced, without removing the GGM 8000 from the rack.
The GGM 8000 expansion module provides two I/O slots and one analog slot. For the ASTRO® 25 system, the GGM 8000 supports daughterboards as follows:

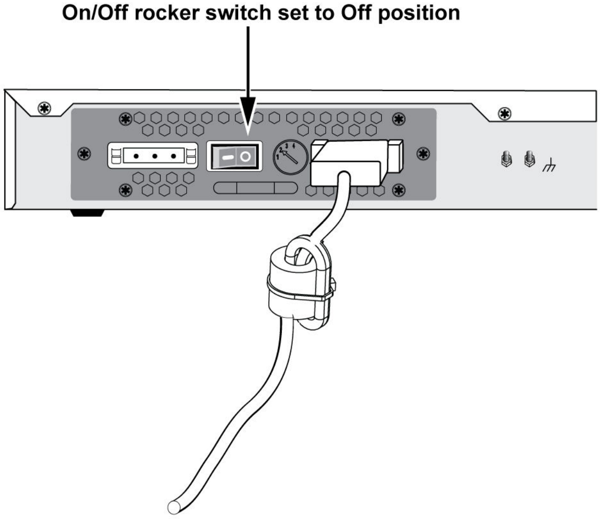
- Analog/V.24 interface kit
  - Two V.24 daughterboards supported in the I/O slots.
  - E&M daughterboard and DSP SIMM, supported in the analog slot.

  > **NOTICE:** The GGM 8000 requires DSP version 5416 to support conventional channel mixed mode and MDC 1200 functionality. If you install an earlier DSP version, the GGM 8000 command will display “No DSP”.
- FlexWAN daughterboard supported in one or both I/O slots.

Procedure:

1. Wear an ESP strap and connect its cable to a verified good ground. This strap must be worn throughout this procedure to prevent ESD damage to any components.
2. Power down the GGM 8000:
   - If GGM 8000 has an AC power subsystem, turn off the power at its source.
   - If GGM 8000 with a DC power subsystem, set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the Off position, as illustrated in the following figure.

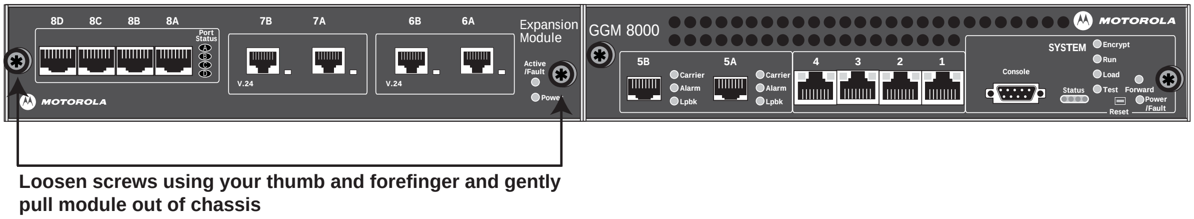
Figure 59: Setting the On/Off Rocker Switch to the Off Position



dc_off_remove_replace

3 Use your thumb and index finger to loosen the captive screws on the front of the expansion module and remove the module from the GGM 8000 chassis, as illustrated in the following figure:

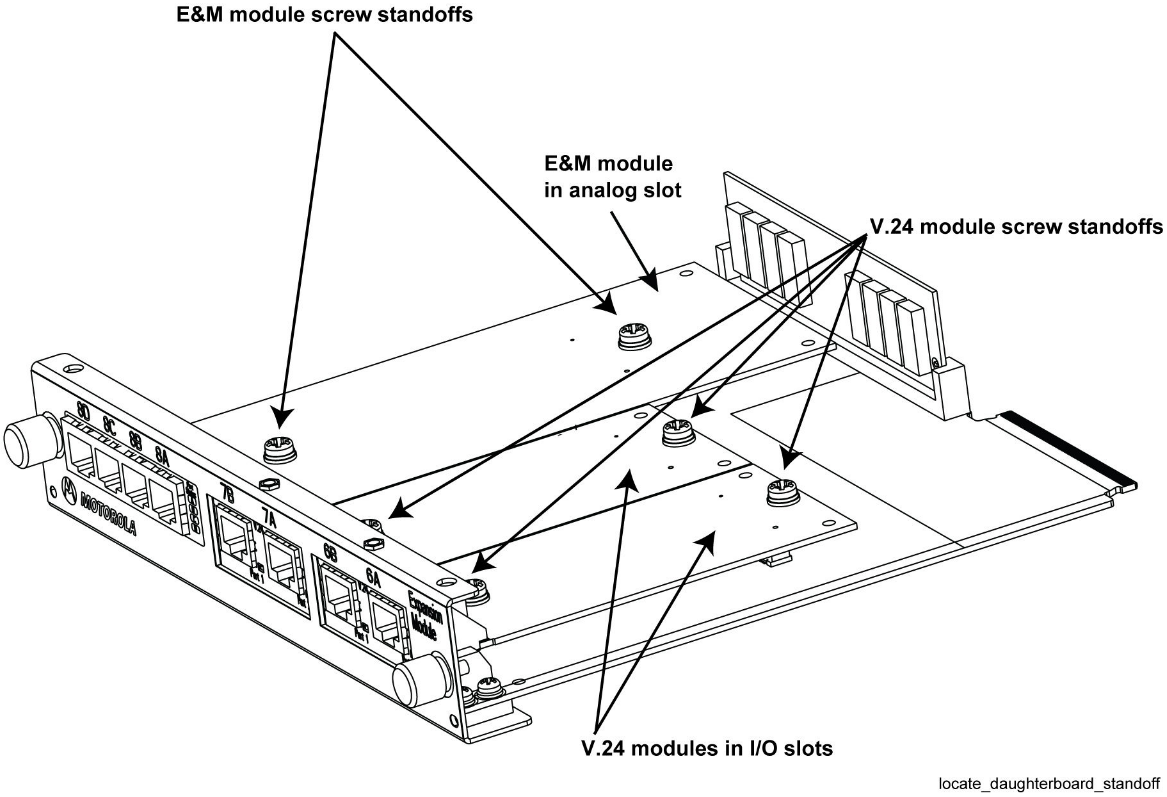
Figure 60: Removing the Expansion Module from the GGM 8000 Chassis



loosen_expansion_replace_A

4 Use the following figure as a guide to locate the daughterboard you want to replace on the expansion module and remove the TORX screws from the standoffs by using a size T15 TORX® screwdriver. Set the screws aside, as you will need them later in this procedure.

Figure 61: Daughterboard and Screw Standoff Locations on the Expansion Module

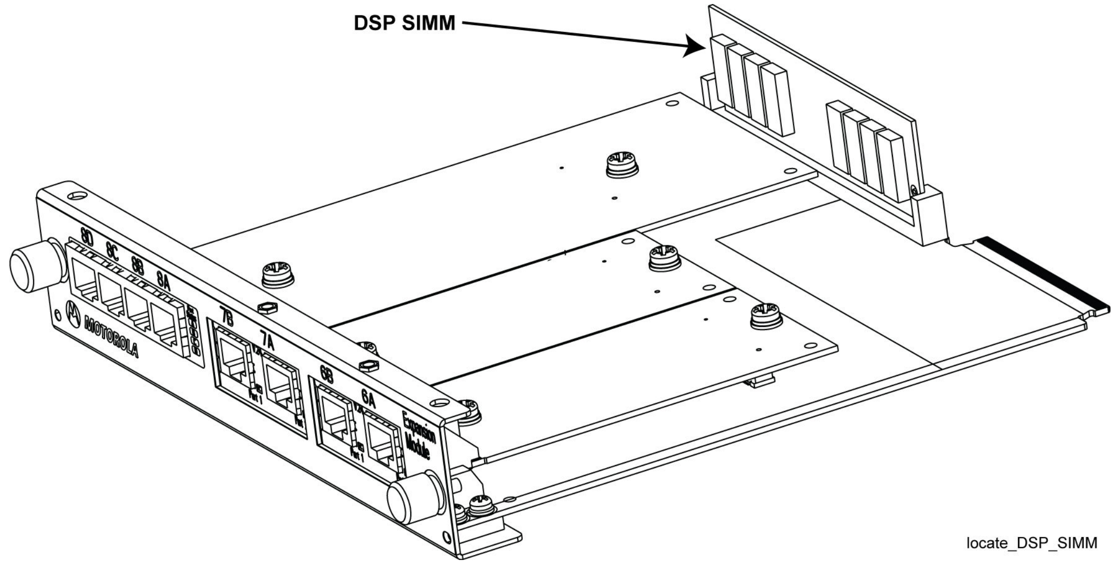

E&M module screw standoffs
E&M module in analog slot
V.24 module screw standoffs
V.24 modules in I/O slots
8D
8C
8B
8A
7B
7A
6B
6A
MOTOROLA
Expansion Module
locate_daughterboard_standoff

5 Gently remove the daughterboard from the connector pins on the expansion module by pulling the connector up and off.

6 If you replace DSP SIMM, perform the following actions:

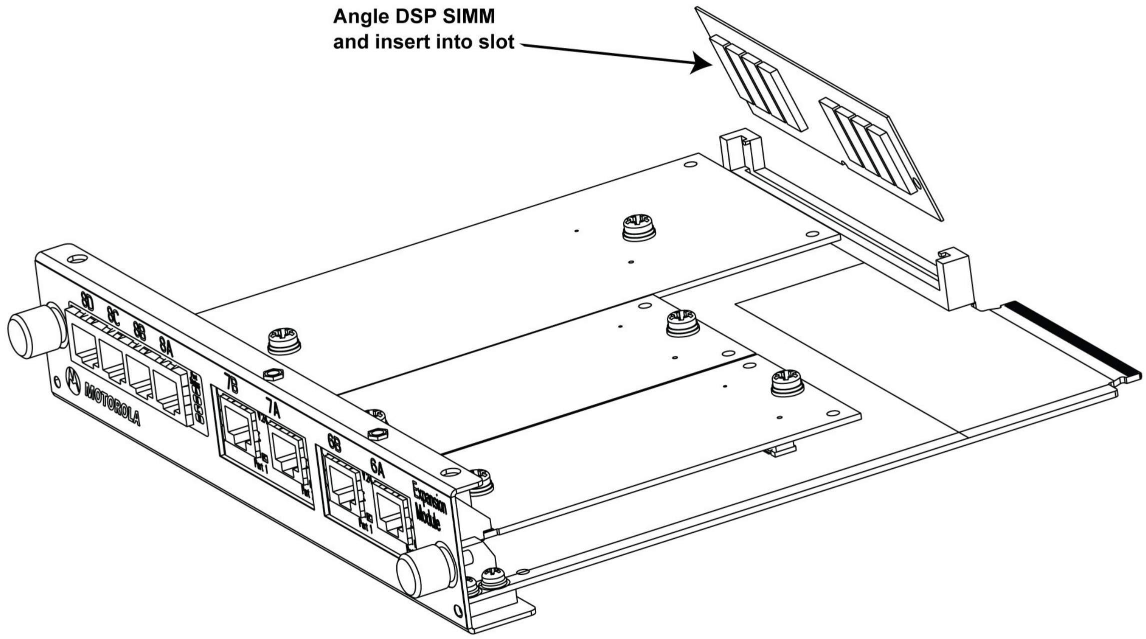
   a Use the following figure as a guide to locate DSP SIMM and gently remove it.

   Figure 62: SIMM Location on the Expansion Module



   b Insert the new DSP SIMM into the slot at a 30 degree angle, with the SIMM angled forward (toward the front of the chassis), as shown in the following figure:

Figure 63: Inserting the DSP SIMM

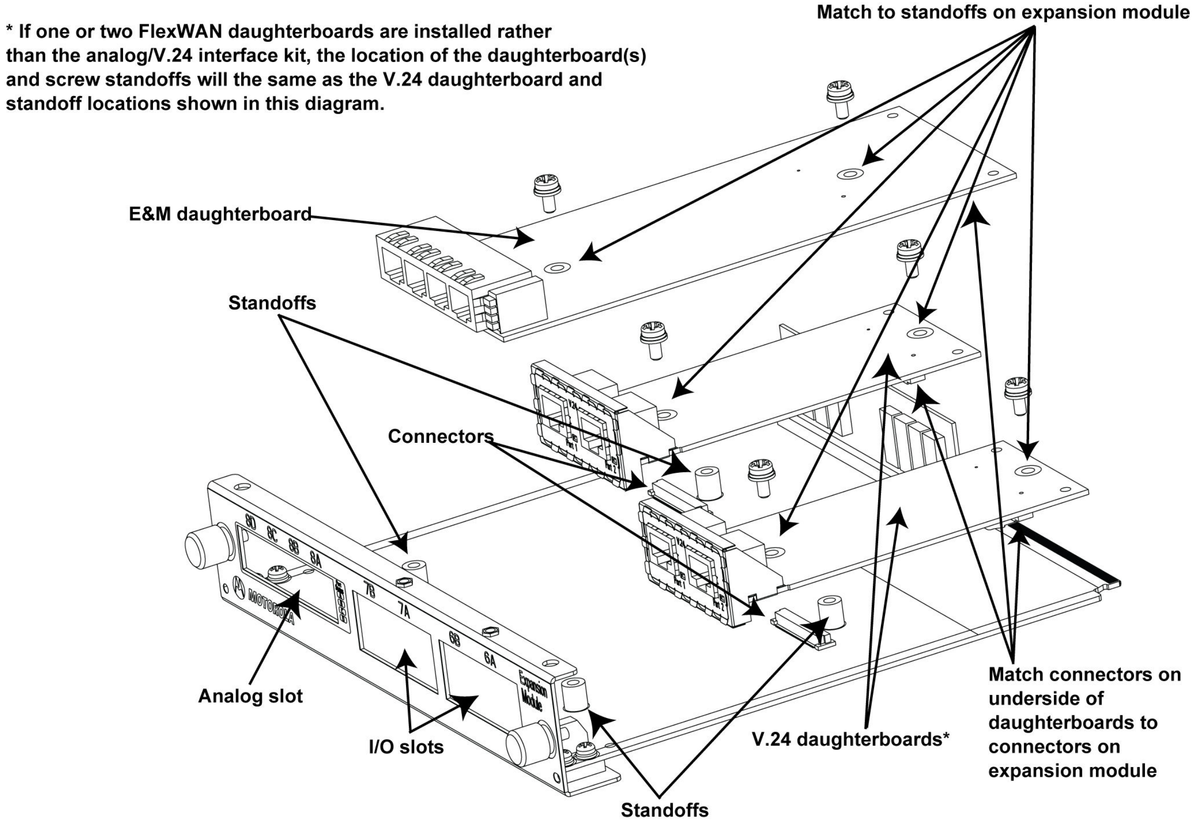


insert_DSP_SIMM

c Press back on the SIMM to seat it into position. The socket clips automatically engage the SIMM as you move it into position.

7 Use the following figure as a guide to insert the new daughterboard:

Figure 64: Inserting the Daughterboard in the Expansion Module


* If one or two FlexWAN daughterboards are installed rather than the analog/V.24 interface kit, the location of the daughterboard(s) and screw standoffs will the same as the V.24 daughterboard and standoff locations shown in this diagram.

insert_daughterboard

a Coming from the back of the expansion module, insert the front of the daughterboard through the front panel of the expansion module.

b Line up the connector pins carefully.

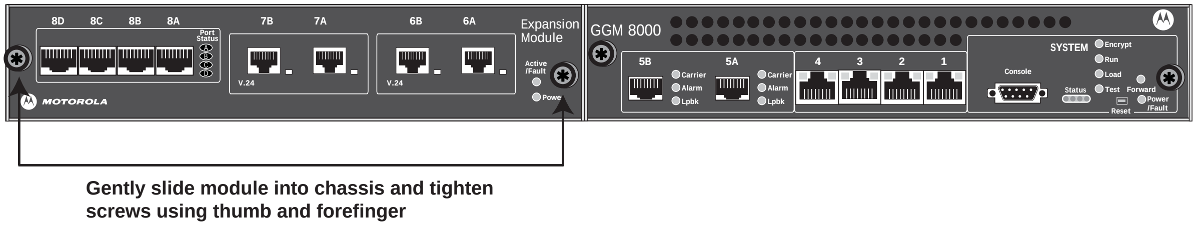
c Press down gently on the daughterboard.

8 Use a size T15 TORX® screwdriver to install the screws you removed in step 4 on the standoffs to secure the daughterboard.

> **IMPORTANT:** Be sure to use the TORX screws you removed earlier in this procedure. **Do not secure the daughterboard with the screws and washers that are shipped with the daughterboard.**
> To ensure that the daughterboard is seated properly, tighten the screws to a torque of 7.5 to 9.8 centimeter-kilograms.

9 Gently slide the expansion module back into the GGM 8000 chassis and tighten the captive screws by using your thumb and index finger, as illustrated in the following figure.

Figure 65: Re-Inserting the Expansion Module in the GGM 8000 chassis

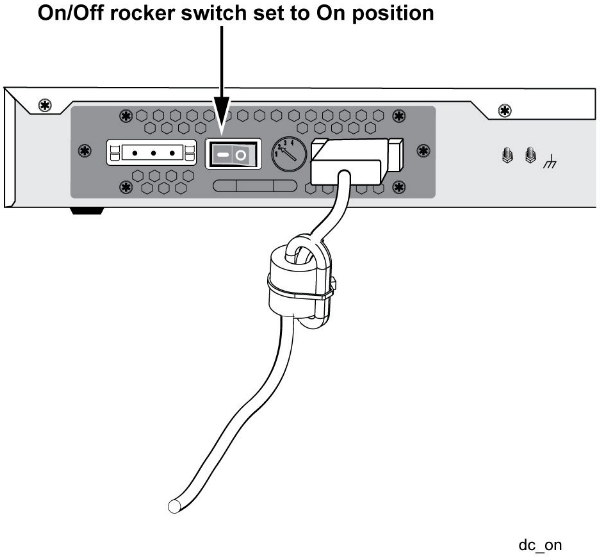


tighten_expansion_screws_A

10 Power on the GGM 8000:

- If GGM 8000 has an AC power subsystem, restore the power at its source.
- If GGM 8000 has a DC power subsystem, set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the On position, as illustrated in the following figure.

Figure 66: Setting the On/Off Rocker Switch to the On Position



1.11.4

Replacing the GGM 8000 ECGW Module

You can replace the ECGW module without removing GGM 8000 from a rack.

IMPORTANT: If the GGM 8000 is secured with tamper evidence labels, removing the ECGW module will break these labels. You must either return the unit to Motorola Solutions for ECGW module replacement or follow instructions about securing the GGM 8000 with tamper evidence labels in *Motorola GGM 8000 Hardware User Guide* to install new tamper evidence labels after you have replaced the ECGW module.

When and where to use: Review the following ESD (electrostatic discharge) precautions:

CAUTION: When removing or installing modules, take the following precautions to prevent ESD from damaging the internal components of the GGM 8000:

- Always wear a properly-grounded anti-static wrist strap.
- Transport static-sensitive components in anti-static packaging.
- Keep static-sensitive components in their anti-static packaging until you are ready to install them.
  - Just before removing components from their anti-static packaging, discharge static electricity from your body by touching an unpainted metal surface.
  - When you handle modules, place them printed circuit side down on a nonconducting, static-free, flat surface.

Procedure:

1 Power down GGM 8000:
   - If GGM 8000 has an AC power subsystem, turn off the power at its source.

- If GGM 8000 has a DC power subsystem, set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the Off position.

2. Use your thumb and index finger to loosen the captive screws on the front of the ECGW module and remove the module from the GGM 8000 chassis.
3. Gently slide the replacement ECGW module back into the GGM 8000 chassis and tighten the captive screws by using your thumb and index finger.
4. Power on GGM 8000:
   - If GGM 8000 has an AC power subsystem, restore the power at its source.
   - If GGM 8000 has a DC power subsystem, set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the On position.

1.11.5 Replacing the GGM 8000 Base Module

Prerequisites:

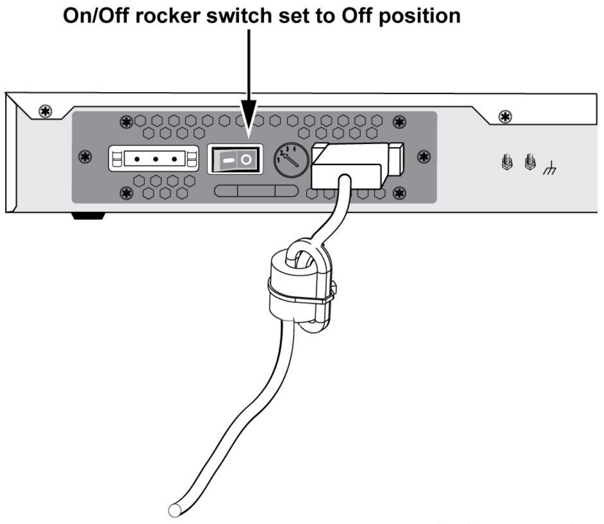
IMPORTANT: If the GGM 8000 is secured with tamper evidence labels, removing the base module will break these labels. You must either return the unit to Motorola Solutions for base module replacement or obtain new tamper evidence labels (part number TYN4008A) and follow the instructions provided with the labels to install new tamper evidence labels after you have replaced the base module.

When and where to use: Use this procedure when replacing the GGM 8000 base module. The base module can be replaced without removing the GGM 8000 from the rack.

Procedure:

1. Wear an ESP strap and connect its cable to a verified good ground. This strap must be worn throughout this procedure to prevent ESD damage to any components.
2. Power down the GGM 8000.
   - For a GGM 8000 with an AC power subsystem: Turn off the power at its source.
   - For a GGM 8000 with a DC power subsystem: Set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the Off position, as illustrated in the following figure.

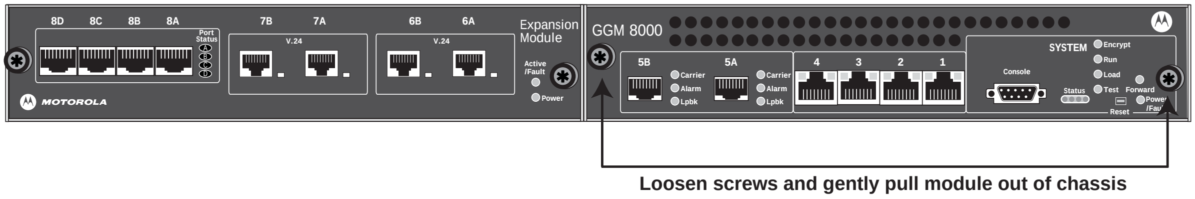
Figure 67: Setting the On/Off Rocker Switch to the Off Position



dc_off_remove_replace

3 Use your thumb and index finger to loosen the captive screws on the front of the base module and remove the module from the GGM 8000 chassis, as illustrated in the following figure.

Figure 68: Removing the Base Module from the GGM 8000 Chassis



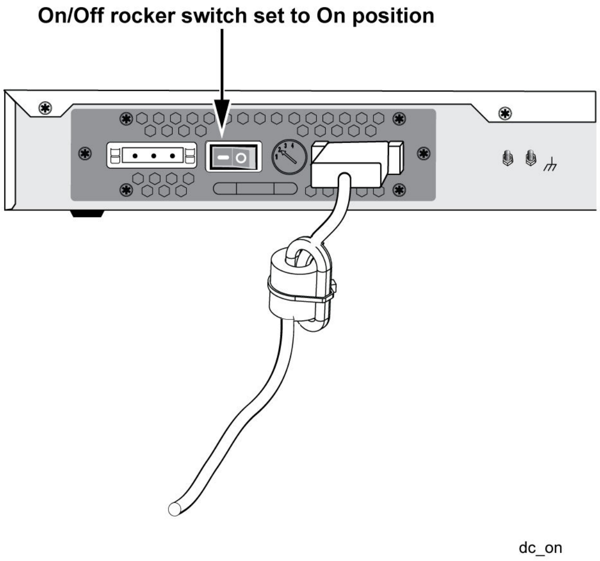
loosen_expansion_screws_base_A

4 Gently slide the replacement base module into the chassis and tighten the captive screws by using your thumb and index finger.

5 Power on the GGM 8000.

- For a GGM 8000 with an AC power subsystem: Restore the power at its source.
- For a GGM 8000 with a DC power subsystem: Set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the On position, as illustrated in the following figure.

Figure 69: Setting the On/Off Rocker Switch to the On Position



1.11.6 Replacing the GGM 8000 Power Subsystem Module

This section describes how to replace a GGM 8000 AC or DC power subsystem module. The power subsystem module can be installed or removed while the unit remains mounted in the rack.

1.11.6.1 Replacing the GGM 8000 AC Power Subsystem Module

Prerequisites:

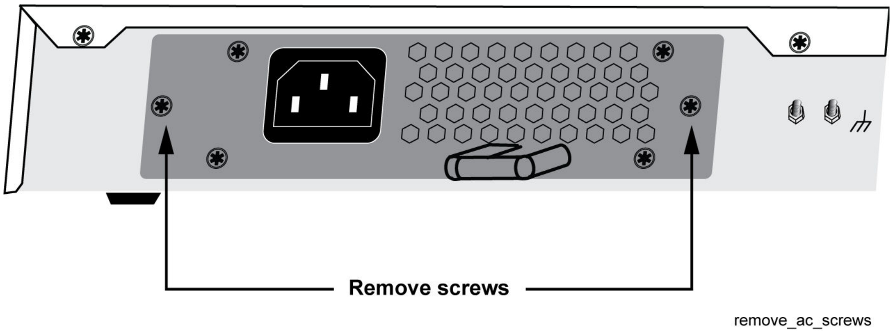
IMPORTANT: If the GGM 8000 is secured with tamper evidence labels, removing the power subsystem module will break one of these labels. You must either return the unit to Motorola Solutions for power subsystem module replacement or obtain new tamper evidence labels (part number TYN4008A) and follow the instructions provided with the labels to install a new tamper evidence label after you have replaced the power subsystem module.

When and where to use: Follow this procedure to replace and reconnect a GGM 8000 AC power subsystem module.

Procedure:

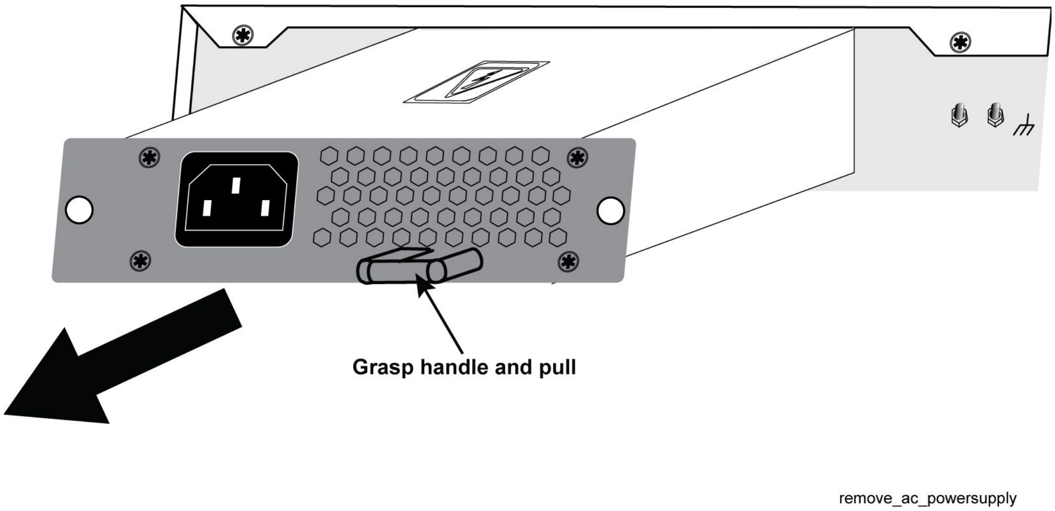
1. Wear an ESP strap and connect its cable to a verified good ground. This strap must be worn throughout this procedure to prevent ESD damage to any components.
2. Turn the power off at its source.
3. Remove the power cord from the power connector on the rear of the GGM 8000.
4. Using a TORX screwdriver, remove the two screws that secure the power subsystem module to the GGM 8000 chassis, as shown in the following figure.

Figure 70: Removing the Screws that Secure the AC Power Subsystem Module to the Chassis



5 Grasp the handle on the power subsystem module and pull the module out of the chassis, as shown in the following figure.

Figure 71: Removing the AC Power Subsystem Module from the Chassis



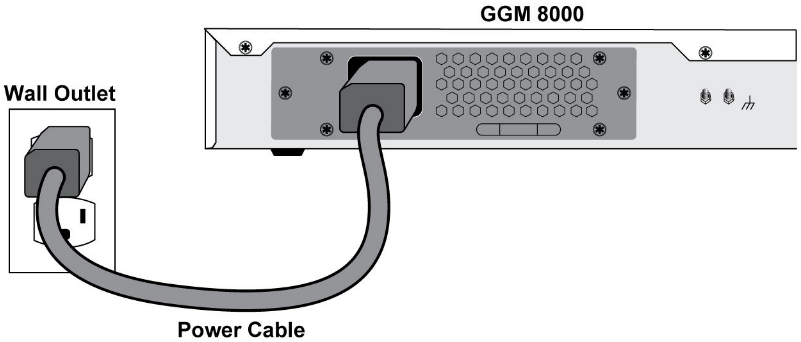
6 Insert the new power subsystem module into the chassis and gently push it in. When correctly inserted, the module should be flush with the GGM 8000 rear panel.

7 Secure the power subsystem module in the chassis using the two screws you removed earlier in this procedure.

8 Attach the female end of the power cable to the power connector on the GGM 8000 power subsystem module.

9 Attach the male end of the power cable to a wall outlet, as illustrated in the following figure.

Figure 72: Connecting the GGM 8000 AC Power Subsystem Module



ac_power_connect

10 Restore the power at its source.

1.11.6.2
Replacing the GGM 8000 DC Power Subsystem Module

Prerequisites:

CAUTION: To reduce the risk of an electric shock, follow these guidelines:

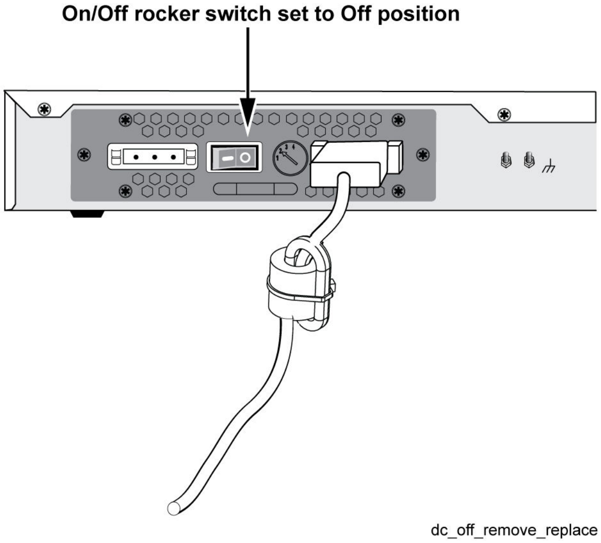
- Only trained and qualified personnel should be allowed to install or replace this equipment.
- Before working on equipment that is connected to power, remove jewelry, including rings, necklaces, and watches. Metal objects heat up when connected to power and ground and can cause serious burns or weld the metal objects to terminals.
- For a centralized DC power connection (battery bank), the GGM 8000 is to be installed only in Restricted Access Locations (dedicated equipment rooms, equipment closets, or the like) in accordance with Articles 110.26 and 110.27 of the National Electrical Code, ANSI/NFPA 70 (2008).
- Damage may results if power is connected improperly.

When and where to use: Follow this to replace and reconnect a GGM 8000 DC power subsystem module.

Procedure:

1 Ensure that the On/Off rocker switch on the GGM 8000 power subsystem module is set to the Off position, as illustrated in the figure below.

Figure 73: On/Off Rocker Switch



2 Confirm that there is no power present on the DC power source(s) before proceeding to disconnect the GGM 8000 from the power source(s). Use appropriate disconnection means and lock-out, tag-out procedures as necessary.

3 Disconnect the GGM 8000 tray cable(s) from the DC power source(s):

⚠ **WARNING:** Disconnect the wires from the DC power source terminals in accordance with all applicable safety regulations, such as the national electrical codes, as well as any locally-applicable safety standards or regulations.

a Disconnect the wires from the positive (+) negative (-) output terminals on the DC power source.

b Disconnect the wire from the safety/earth ground terminal on the DC power source.

⚠ **WARNING:** When disconnecting DC power from the GGM 8000, always ensure that the GGM 8000 tray cable safety/earth ground wire is disconnected from the power source last.

c If the GGM 8000 is connected to two centralized DC power sources, repeat steps **a** and **b** above for the second power source.

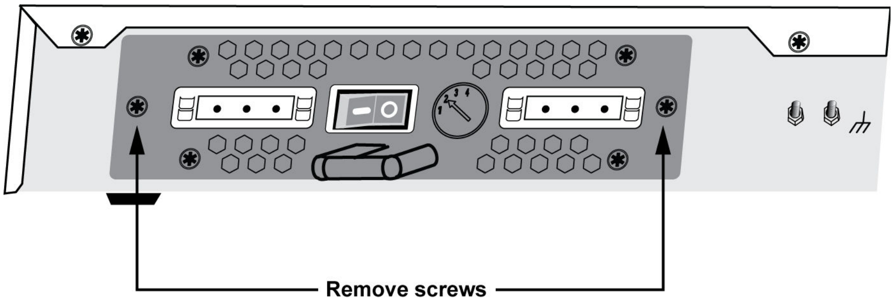
⚠ **WARNING:** If the GGM 8000 is connected to two DC power sources, disconnect the wires from both power sources, as described in steps a and b above, in order to completely remove power from the GGM 8000.

4 Disconnect the GGM 8000 tray cable connector from the DC power entry connector on the GGM 8000 DC power subsystem module. To do this, squeeze the spring clips on both sides of the cable connector and disconnect the cable from the DC power entry connector on the chassis.

5 If the GGM 8000 is connected to two DC power sources, repeat step 4 to remove the tray cable connector from the other DC power entry connector.

6 Using a TORX screwdriver, remove the two screws that secure the power subsystem module to the GGM 8000 chassis, as shown in the following figure.

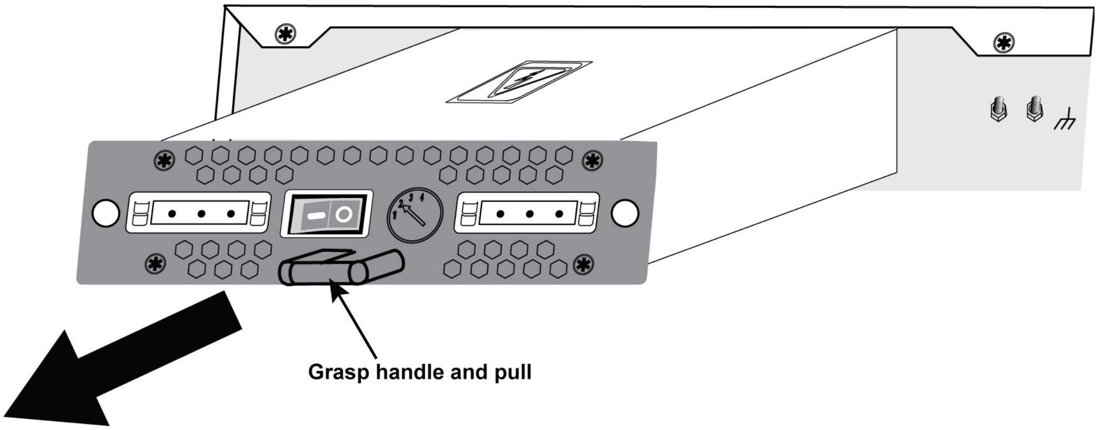
Figure 74: Removing the Screws that Secure the DC Power Module to the Chassis



remove_dc_screws

7 Grasp the handle on the power subsystem module and pull the module out of the chassis, as shown in the following figure.

Figure 75: Pulling out the Module



remove_dc_powersupply

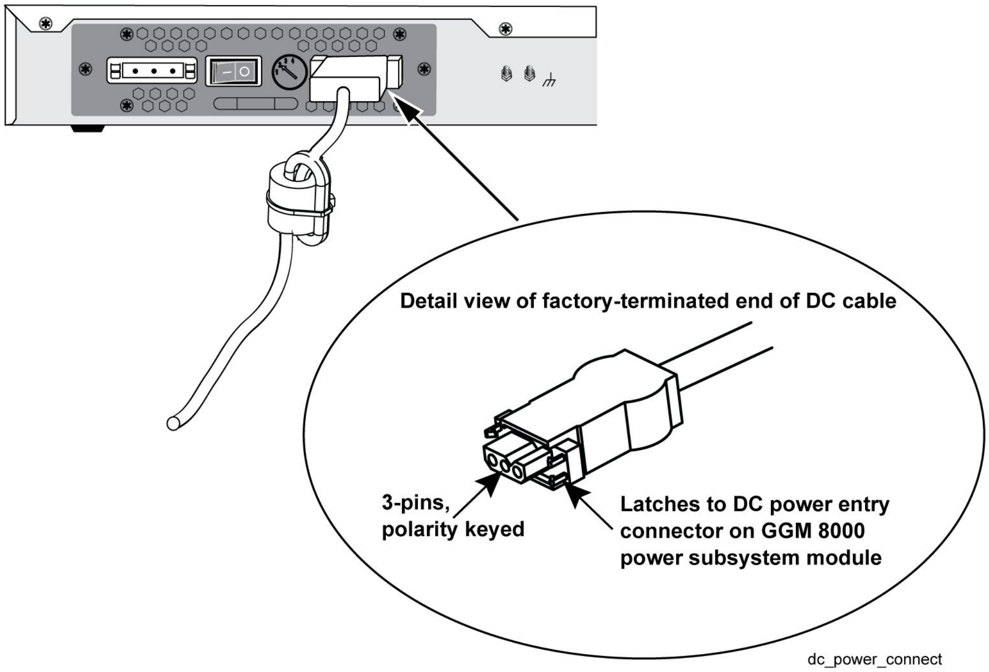
8 Insert the new power subsystem module into the chassis and gently push it in. When correctly inserted, the module should be flush with the GGM 8000 rear panel.

9 Secure the power subsystem module in the chassis using the two screws you removed earlier in this procedure.

10 Plug the connector end of the GGM 8000 power tray cable into one of the two DC power entry connectors on the GGM 8000 DC power subsystem module, as shown in the following figure.

IMPORTANT: Make certain the connector on the power cable latches securely with the DC power entry connector on the power subsystem module.

Figure 76: Connecting the DC Power Tray Cable to the GGM 8000 DC Power Subsystem Module



11 If you connect GGM 8000 to two centralized DC power sources, repeat step 10 to connect the second GGM 8000 power tray cable to the other DC power entry connector on the GGM 8000 power subsystem module.

12 Identify the positive, safety/earth ground, and negative terminals on the centralized DC power source.

13 Connect the terminated wire ends from the GGM 8000 tray cable to the DC power source(s):

⚠ **WARNING:** Make the connections in accordance with all applicable safety regulations, such as the national electrical codes, as well as any other locally-applicable safety standards or regulations.

a Connect the wire from the middle conductor (pin 2) on the GGM 8000 power entry connector to the safety/earthy ground terminal on the DC power source.

⚠ **WARNING:** When connecting DC power to the GGM 8000, always ensure that the GGM 8000 tray cable safety/earth ground wire is connected to the power source first.

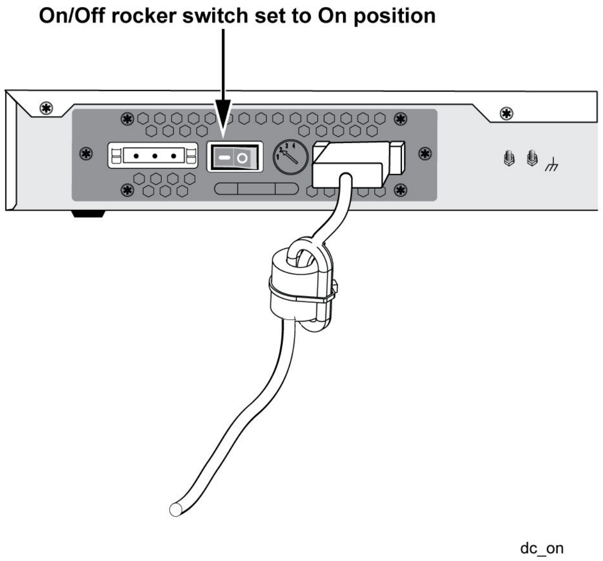
b Connect the other two wires (from pins 1 and 3) on the GGM 8000 DC power entry connector to the positive (+) and negative (-) output terminals on the DC power source. It does not matter which wire you connect to the positive terminal and which wire you connect to the negative terminals the GGM 8000 supports either polarity.

c If you connect the GGM 8000 to two DC power sources, repeat steps 1 and 2 above for the second power source.

14 Restore power to the DC power source.

15 Set the On/Off rocker switch on the GGM 8000 power subsystem module on the On position, as illustrated in the following figure.

Figure 77: Setting the On/Off Rocker Switch to the On Position



1.11.6.3

Replacing the GGM 8000 Encryption Card

Prerequisites:
For units shipped for the ASTRO® 25 7.12 system release and after, the encryption card is no longer required, and successful secure feature authentication determines whether or not encryption is enabled on the GGM 8000. However, only GGM 8000s manufactured for the ASTRO® 25 7.12 system release and after include the required BID in write-once flash. No previously-shipped GGM 8000s will be upgraded to include the BID and feature configuration file. To upgrade pre-ASTRO® 25 7.12 GGM 8000s to include encryption, you must order and install an encryption daughtercard. EOS 16.3 and later software detects the presence of a Cavium chip on an installed daughtercard and accepts that as a pseudo-certificate for the embedded Freescale encryption engine. EOS 16.0 and 16.2 software uses the encryption daughtercard as the encryption engine.

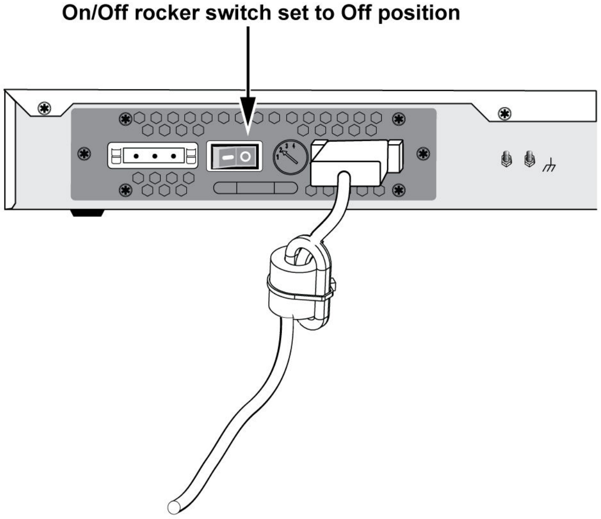
IMPORTANT: If the GGM 8000 is secured with tamper evidence labels, removing the power subsystem module will break one of these labels. You must either return the unit to Motorola Solutions for power subsystem module replacement or obtain new tamper evidence labels (part number TYN4008A) and follow the instructions provided with the labels to install a new tamper evidence label after you have replaced the power subsystem module.

When and where to use: Follow this procedure to replace a GGM 8000 encryption card. The encryption card can be replaced without removing the GGM 8000 from the rack.

Procedure:

1. Power down the GGM 8000.
   - For a GGM 8000 with an AC power subsystem, turn off the power at its source.
   - For a GGM 8000 with a DC power subsystem, set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the Off position, as illustrated in the following figure.

Figure 78: Setting the On/Off Rocker Switch to the Off Position

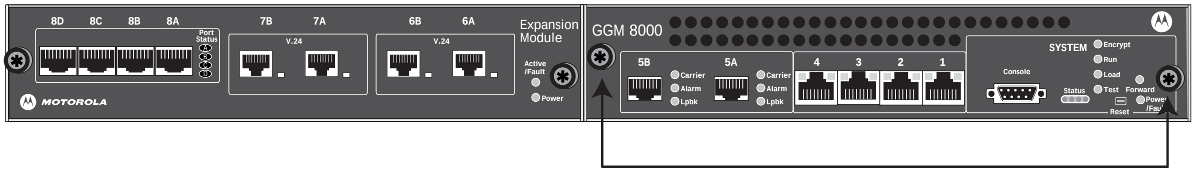


On/Off rocker switch set to Off position

dc_off_remove_replace

2 Use your thumb and index finger to loosen the captive screws on the front of the base module and remove the base module from the GGM 8000 chassis, as illustrated in the following figure.

Figure 79: Removing the Base Module from the GGM 8000 Chassis



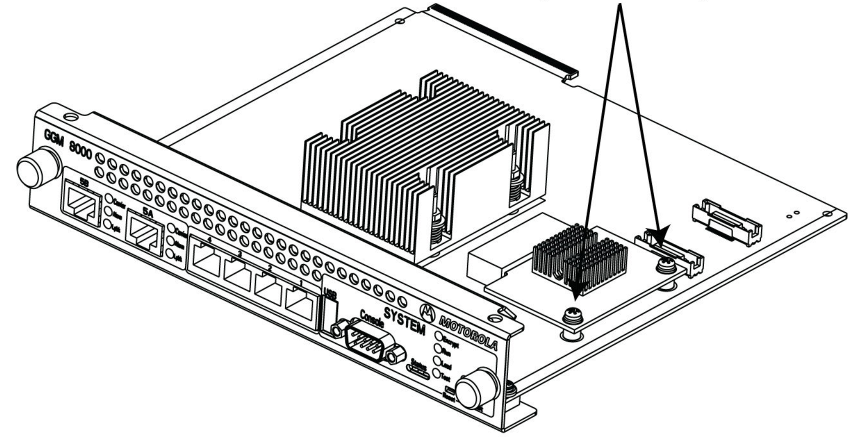
Loosen screws and gently pull module out of chassis

loosen_expansion_screws_base_A

3 Using the following figure as a guide, locate the encryption card on the base module and remove the TORX screws from the standoffs. Set the screws aside, as you will need them later in this procedure.

Figure 80: Encryption Card and Screw Standoff Locations on the Base Module

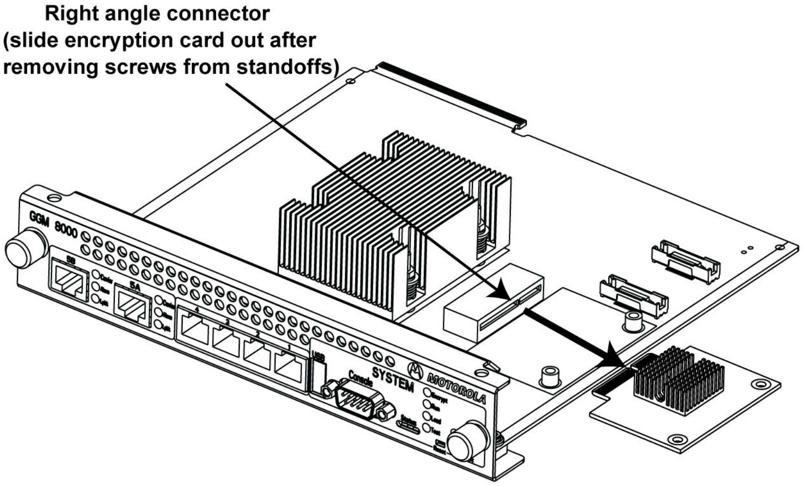
Encryption card standoffs (remove screws)



encrypt_connector_standoffs

4 Gently slide the encryption card out of the right angle connector on the base module, as shown in the following figure.

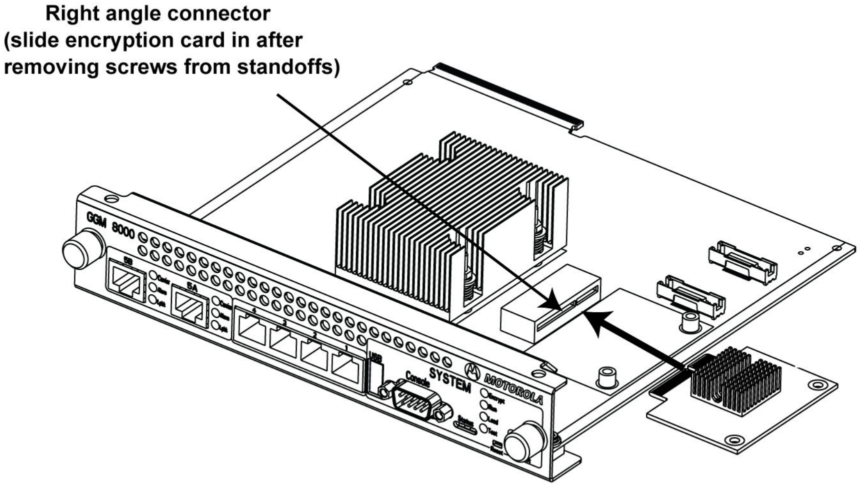
Figure 81: Removing the Encryption Card from the Base Module


Right angle connector
(slide encryption card out after
removing screws from standoffs)
GGM 8000
SYSTEM
Console
MOTOROLA

remove_encrypt_card

5 Gently slide the replacement encryption card into the right angle connector on the base module, as shown in the following figure.

Figure 82: Installing a New Encryption Card on the Base Module


Right angle connector
(slide encryption card in after
removing screws from standoffs)
GGM 8000
SYSTEM
Console
MOTOROLA

install_encrypt_card

6 Install the screws you removed earlier in this procedure on the standoffs to secure the encryption card.

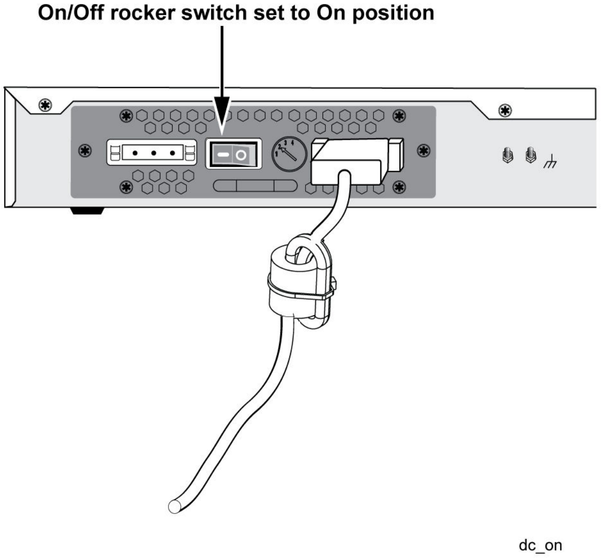
IMPORTANT: To ensure that the encryption card is seated properly, tighten the screws to a torque of 7.5 to 9.8 centimeter-kilograms.

7 Gently slide the base module back into the GGM 8000 chassis and tighten the captive screws using your thumb and index finger.

8 Power on the GGM 8000.

- For a GGM 8000 with an AC power subsystem: Restore the power at its source.
- For a GGM 8000 with a DC power subsystem: Set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the On position, as illustrated in the following figure.

Figure 83: Setting the On/Off Rocker Switch to the On Position



9 Verify the installation:

a From the EOS command-line interface, issue the SysInfo command.

b In the SysInfo display, locate the `Encryption Card Information` line.

- If the `Encryption Card Information` line lists the name of the encryption card, the encryption card has been successfully installed.
- If the `Encryption Card Information` lists `Unavailable`, the GGM 8000 is not recognizing the encryption card. Make sure that you have installed EOS software version 16.0 or higher (XS package).

1.11.7 Replacing an S6000 Router with a GGM 8000 Site Gateway

Prerequisites: Ensure that you have access to the appropriate GGM 8000 Gateway configuration (boot.cfg, StaticRP.cfg, and acl.cfg) files for the S6000 Router you are replacing.

NOTICE: The configuration files can be found on the Motorola Solutions media device that contains the electronic version of the system-specific documentation. If you do not have access to this media device, contact your system administrator.

Pull the configuration and hardware information from the router into the Unified Network Configurator User Guide (UNC) by performing a “Pull All” procedure from the UNC. See the “Scheduling the Pull of Device Configurations” procedure, in the *Unified Network Configurator User Guide*.

If a “Pull All” procedure is not possible because communication is lost between the router and UNC, or if the router is not managed by UNC, or if the system is supported by a K core, perform any one of the following:

- Use the last known good configuration files from the UNC
- Extract the configuration files from the router directly
- Use the Motorola Solutions configuration files on the Electronic Build Book media

In any case, copy the configuration files to a service PC/laptop with TFTP software enabled.

WARNING: The S6000 Router contains dangerous voltages, which may cause electric shock or damage to the equipment. Turn off the router and remove the power cabling when servicing this unit.

When and where to use: Replacing an S6000 Router with a GGM 8000 Site Gateway consists of removing the existing router, installing the GGM 8000 hardware, and then configuring the GGM 8000 for its intended function. This procedure applies to the replacement of an S6000 Router with a GGM 8000 for the following functions:

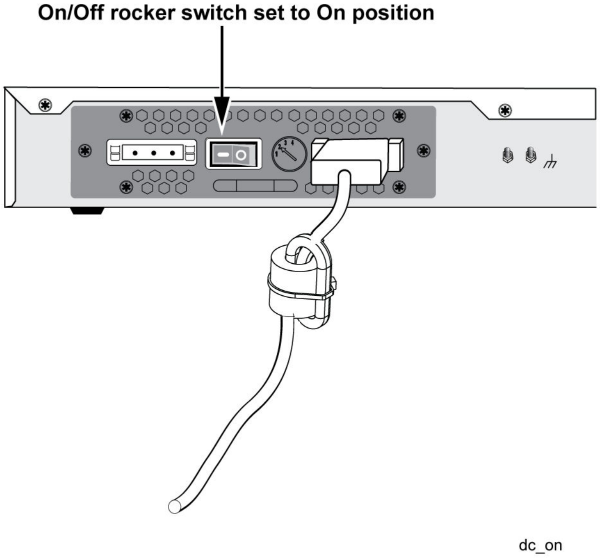
- Replacing an S6000 GGSN with the GGM 8000 GGSN
- Replacing an S6000 Core and Exit Router (Ethernet Link Only) with the GGM 8000 Core and Exit Site Gateway
- Replacing an S6000 Gateway Router with the GGM 8000 Gateway

NOTICE: If redundant site links are supported, powering down an active site router causes the redundant site router to route the full load of traffic for the site, and communication is not affected. However, if redundant site links are not supported, powering down the site router causes the site to enter site trunking mode until the router is operational again.
Do not use this procedure to replace S6000 Routers which use the Cooperative WAN Routing (CWR) device configuration with GGM 8000 Site Gateway devices.

Procedure:

1. Wear an ESP strap and connect its cable to a verified good ground. This strap must be worn throughout this procedure to prevent ESD damage to any components.
2. Power down the existing S6000 Router:
   - **a** Disconnect the power cable from the router.
   - **b** Remove any cables installed on the chassis.
3. Remove the existing S6000 Router:
   - **a** Label and disconnect all communication cabling from the router.
   - **b** Disconnect the ground cable from the rear of the chassis.
   - **c** Remove the screws securing the router to the rack.
   - **d** Pull out the router through the front of the rack.
4. Remove the mounting brackets from the existing S6000 Router and install the brackets on the replacement GGM 8000.
5. Install the replacement GGM 8000. See Rack-Mounting the GGM 8000 on page 58:
   - **a** Install the replacement GGM 8000 into the rack and secure the gateway with the screws that were previously removed.
   - **b** Secure the ground cable to the ground location on the rear of the chassis.
6. Cable the GGM 8000. Perform one of the following:
   - GGM 8000 Gateway (M Zone Core) – Site-Specific Cabling on page 153
   - Core Gateway (M Zone Core) – Site-Specific Cabling on page 158
   - Exit Gateway (M1 DSR and M3 Zone Core) – Site-Specific Cabling on page 161
   - GGSN Gateway – Site-Specific Cabling on page 165
7. Power on the replacement GGM 8000.
   - For a GGM 8000 with an AC power subsystem: Restore the power at its source.
   - For a GGM 8000 with a DC power subsystem: Set the On/Off rocker switch on the GGM 8000 power subsystem module on the rear of the chassis to the On position, as shown in the following figure.

Figure 84: Setting the On/Off Rocker Switch to the On Position



8 Proceed to configure the GGM 8000 as described in the configuration section of this chapter.

9 Enable RADIUS authentication on the GGM 8000. See the *Authentication Services* manual for details.

10 On a system with MAC port locking, disable the locking and then re-enable the locking with the MAC address of the GGM 8000. For instructions on how to disable and enable MAC port locking, see the *MAC Port Lockdown Feature Guide*.

11 On a system with link encryption or protocol authentication, enter the correct keys for the new GGM 8000 so that it can be authenticated by its encryption or authentication peer. For instructions, see the *Link Encryption and Authentication Feature Guide*.

12 On systems with SNMPv3 enabled, enable passphrase information. For instructions, see the *SNMPv3 Feature Guide*.

13 Find this device in the VoyenceControl devices list. Execute the saved command called **Clear USM Cache** from the list of saved commands under **System** → **Motorola** → **SNMPv3**. For instructions on accessing and executing saved commands for a device, see “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator User Guide*.

NOTICE: The names EMC Smarts® Network Configuration Manager and VoyenceControl are used interchangeably for this product.

14 Test the device credentials with the **Test Credentials** quick command. For more details, see “Executing Quick Commands” in the Unified Network Configurator User Guide.

15 Right-click the device, from the context menu select **Pull** → **Pull All**.

16 Go to the Schedule Manager to approve the remedy job that resulted from the Pull operation. For more details, see the “Approving Configuration Changes” section in the Unified Network Configurator User Guide.

17 Compare the version of the Enterprise Operating System (EOS) software that is running on the GGM 8000 with the version that was running on the replaced router device by using the Compare function in the hardware history in UNC. For instructions, see “Comparing Device Configuration Versions” in the *Unified Network Configurator User Guide*.

NOTICE: If the GGM 8000 needs a software upgrade, perform the upgrade. See “Operating System and Software Upgrade” in the *Unified Network Configurator User Guide*.

18 Compare the configuration of the GGM 8000 with the configuration of the replaced device by running the Compare function in the configuration history in UNC. For instructions, see the *Unified Network Configurator User Guide*.

NOTICE: If the previous configuration needs to be restored, see “Rolling Back to a Previous Version” in the *Unified Network Configurator User Guide*. If the current configurations are changed and sent to the GGM 8000, see “Device Update with a Download of Configuration Changes” in the *Unified Network Configurator User Guide*.

19 Verify that the GGM 8000 is operating properly.

Chapter 2

ASTRO 25 Master Site (M Zone Core)

This chapter provides information on the GGM8000 in an ASTRO® 25 system master site.

2.1 Master Site Gateways – Functional Description

This chapter explains how the master site GGM 8000 Gateways work in the context of your system.

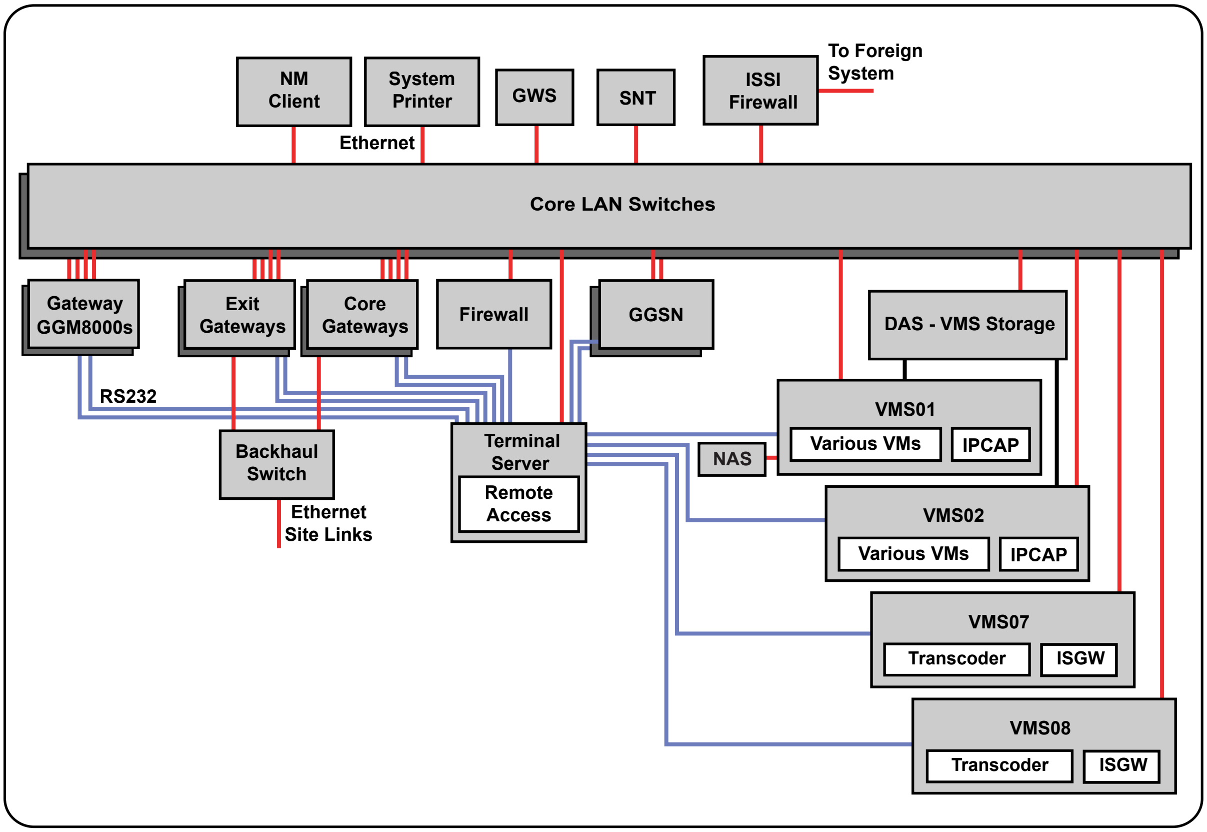
If the Dynamic System Resilience (DSR) feature is implemented on your system, refer to the *Dynamic System Resilience Feature Guide* for details. Dynamic System Resilience allows a system to continue to operate without loss of function on the failure or destruction of any controlling master site within a single or multizone by providing geographically redundant Fixed Network Equipment.

2.1.1 Master Site Gateways – Network Connections

GGM8000 Gateways are installed at the master site interface with certain components.

The following figure provides an example of an M3 configuration. See the *Master Site Infrastructure Reference Guide* for additional zone core architecture diagrams.

Figure 85: Master Site Gateways



S_A717_M3_Primary_System_Zone_Core_Config_Gateways_A

2.1.2 Enterprise Operating System Functions

The GGM 8000 Gateway uses basic routing and IP features in the Enterprise OS (EOS) software including the following:

- IP Routing
- 10/100 Ethernet
- Static Routes
- Frame Relay
- Fragmentation

The GGM 8000 Gateway uses the following protocols and interfaces:

- Simple Network Management Protocol (SNMP)
- Type of Service (TOS)
- Network Time Protocol (NTP)
- Multicast

NOTICE: Network transport devices (gateways, switches, firewalls and others) are pre-configured to support systems with and without a TRAK 9100 NTP Server, so the primary NTP Server is set to ntp02, which is always present in the system. For details regarding the Network Time Protocol (NTP) Server, as well as the primary and secondary NTP source for devices in your system, see the *Network Time Protocol Server Feature Guide*.

2.2 Master Site Gateways – Installation and Configuration

Prerequisites: Ensure that you have the required cabling and connectors.

Process:

1. Install the Master Site Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Master Site Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Master Site Gateway. See Connecting a Chassis Ground on page 68.
4. Connect the equipment to the Master Site Gateway. For Master Site Gateway cable connections, see the following site-specific cabling:
   - GGM 8000 Gateway (M Zone Core) – Site-Specific Cabling on page 153
   - Core/Exit Gateway (M1 and M3 Zone Core) – Site-Specific Cabling on page 155
   - Core Gateway (M Zone Core) – Site-Specific Cabling on page 158
   - Exit Gateway (M1 DSR and M3 Zone Core) – Site-Specific Cabling on page 161
   - GGSN Gateway – Site-Specific Cabling on page 165
5. Configure the Master Site Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

2.3 Master Site Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

2.3.1 Master Site Gateways – General Troubleshooting

This section discusses troubleshooting steps for general problems with the GGM 8000 Gateways.

NOTICE: See the *Flexible Site and InterZone Links Feature Guide* for troubleshooting information relating to Ethernet LAN links.

NOTICE: In systems with the Dynamic System Resilience (DSR) feature installed, there is one more level of redundancy for network transport routers, resulting in a lower number of connectivity problems and less troubleshooting required. For more information on the Dynamic System Resilience feature, see the *Dynamic System Resilience Feature Guide*.

2.4 GGM 8000 Gateway (M Zone Core)

The GGM 8000 Gateway can replace the S6000 Gateway Router used in the zone core to route traffic to and from the zone controller, the Motorola Solutions MCC 7500 VPM/MCC 7500E/MCC 7100 Consoles, and the Packet Data Gateway (PDG) devices in the system.

2.4.1 GGM 8000 Gateway (M Zone Core) – Functional Description

The GGM 8000 Gateway serves as the single access interface for all information intended for the zone controller, MCC 7500 VPM/MCC 7500E/MCC 7100 Dispatch Consoles, and the Packet Data Gateway (PDG). Any traffic to and from these devices is routed through the GGM 8000 Gateway.

A GGM 8000 Gateway functions as a data and control gateway and its functions include:

- Providing an audio switch interface and network management functionality
- Providing a level of isolation for the zone controller and the PDG
- Supporting multicast traffic, allowing the zone controller to send control packets to multiple points in the zone

Two GGM 8000 Gateways are installed on the Local Area Network (LAN).

GGM 8000 Gateways are used for devices that require network redundancy and are multicasting beyond their local LAN. GGM 8000 Gateways provide support for the following:

- Zone Controller (control router functionality)
- MCC 7500 VPM/MCC 7500E/MCC 7100 Dispatch Console
- Packet Data Gateway (PDG router functionality)
- Network Management

GGM 8000 Gateways provide several benefits for the zone master site:

- Provide a single access point or gateway to access the core and exit routers.
- Isolate multicast traffic from the various hosts they are servicing.
- Provide redundant connections for hosts with redundant interfaces (zone controller).

Each GGM 8000 Gateway has two 100Base-TX connections to one of the master site LAN switches. One GGM 8000 Gateway connects to TLAN 1 and the other connects to TLAN 2. Any traffic to and from the zone controllers and the PDG is routed by one of the GGM 8000 Gateways. Each GGM 8000 Gateway has an RS232 connection to the terminal server, allowing router administration by PC clients over the LAN.

NOTICE: See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

See Master Site Gateways – Network Connections on page 150 for a network transport diagram showing the GGM 8000 Gateway.

2.4.2 GGM 8000 Gateway (M Zone Core) – Installation

When and where to use: Follow this process to install the GGM 8000 Gateway.

Process:

1. Install the GGM 8000 Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the GGM 8000 to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the GGM 8000 Gateway. See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the GGM 8000 Gateway. See the following table in section GGM 8000 Gateway (M Zone Core) – Site-Specific Cabling on page 153.
5. Configure the GGM 8000 Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

2.4.2.1 GGM 8000 Gateway (M Zone Core) – Site-Specific Cabling

The following table lists GGM 8000 Gateway port assignments when used in an M Zone Core configuration.

Table 28: GGM 8000 Gateways Cabling – M1 Zone Core Configuration

GGM 8000 Gateway	Port	Device/Function
GGM 8000 Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	RS-232	Terminal Server or Local Serial Access

Table 29: GGM 8000 Gateways Cabling – M2 and M3 Zone Core Configuration

GGM 8000 Gateway	Port	Device/Function
GGM 8000 Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access
GGM 8000 Gateway 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access

2.4.3 GGM 8000 Gateway (M Zone Core) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

2.4.4 GGM 8000 Gateway (M Zone Core) – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

2.4.5 GGM 8000 Gateway (M Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

2.4.5.1 GGM 8000 Gateway (M Zone Core) – Failures

A failure of a single GGM 8000 Gateway is transparent to the user, as the redundant gateway takes over. A failure of both GGM 8000 Gateways would mean that local devices within a zone are no longer able to communicate with each other and intra-zone traffic stops.

2.5 Core/Exit Gateway (M1 and M3 Zone Core)

Depending on performance and capacity requirements and considerations for the zone core, a single gateway transport device may be deployed as a single-function device or dual-function device.

2.5.1 Core/Exit Gateway (M1 and M3 Zone Core) – Functional Description

The Core/Exit gateway (GGM 8000 platform in a multi-zone system) may be deployed as a dual-function transport (gateway) device for Intra-Zone (zone-to-site) network traffic (Core gateway) and Inter-Zone (zone-to-zone) network traffic (Exit gateway).

For details regarding the single-function Core gateway and Exit gateway and their functions, see the following:

- Core Gateway (M Zone Core) on page 156
- Exit Gateway (M1 DSR and M3 Zone Core) on page 159

2.5.1.1 Core/Exit Gateway (M1 and M3 Zone Core) – Network Connections

Each core/exit gateway also has an RS-232 connection to the terminal server, allowing gateway administration by PC clients over the LAN.

See Master Site Gateways – Network Connections on page 150 for a network transport diagram showing the core gateway.

For information on core/exit gateway cabling, see the customized configuration information provided by Motorola Solutions for your system.

NOTICE: See the *Dynamic System Resilience Feature Guide* for additional configurations.

2.5.1.2 Core/Exit Gateway (M1 and M3 Zone Core) – Site Connectivity

The Core/Exit gateway is used for site link connectivity and it interfaces directly to the zone core LAN switch and backhaul switch at the master site to provide an Ethernet interface to the sites in the zone.

2.5.2 Core/Exit Gateway (M1 and M3 Zone Core) – Installation

When and where to use: Follow this process to install the Core/Exit Gateway(s).

Process:

1. Install the Core/Exit Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Core/Exit Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Core/Exit Gateway(s). See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the Core/Exit Gateway(s). See Core/Exit Gateway (M1 and M3 Zone Core) – Site-Specific Cabling on page 155.
5. Configure the Core/Exit Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

2.5.2.1 Core/Exit Gateway (M1 and M3 Zone Core) – Site-Specific Cabling

The following tables list Core/Exit Gateway port assignments when used in M1 and M3 Zone Core configuration.

Table 30: Core/Exit Gateways Cabling – M1 and M3 Zone Core Configuration

Core/Exit Gateway	Port	Device/Function
Core/Exit Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

Table 31: Core/Exit Gateways Cabling – M3 Zone Core Configuration

Core/Exit Gateway	Port	Device/Function
Core/Exit Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Core/Exit Gateway 2	LAN 1	Coret LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

2.5.3 Core/Exit Gateway (M1 and M3 Zone Core) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

2.5.4 Core/Exit Gateway (M1 and M3 Zone Core) – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

2.5.5 Core/Exit Gateway (M1 and M3 Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

2.5.5.1 Core/Exit Gateway (M1 and M3 Zone Core) – Failures

Depending on the configuration, a core/exit gateway failure can have different connotations.

- In an M1 configuration, if a failure of the core/exit gateway occurs, the local devices within a zone are no longer able to communicate with each other and Local Area Network (LAN) traffic to other zones is lost. Both intraZone and InterZone traffic stops.
- In an M3 configuration, if a a failure of one core/exit gateway occurs, the redundant gateway takes over.
- In an M3 configuration, if a failure of both core/exit gateways occur, or are powered down, the local devices within a zone are no longer able to communicate with each other and Local Area Network (LAN) traffic to other zones is lost. Both intraZone and InterZone traffic stops.

Core/Exit gateway failures are reported in the fault management application and additional gateway details are available through the Unified Network Configurator (UNC) application. If a gateway hardware failure is suspected, perform the appropriate field replaceable entity (FRE) replacement procedures.

2.6 Core Gateway (M Zone Core)

The GGM 8000 Core Gateway can replace the S6000 Core Routers (Ethernet only) used in the zone core to route traffic within the zone core and to route traffic to and from between zones (inter-zone links).

NOTICE: For multi-zone systems using Ethernet site links, a Core/Exit gateway deployed as a dual-function transport device provides Intra-Zone (zone-to-site and Inter-Zone (zone-to-zone). See Core/Exit Gateway (M1 and M3 Zone Core) on page 154.

2.6.1 Core Gateway (M Zone Core) – Functional Description

The core gateways route traffic between the master site and remote sites. The core gateway connects to the LAN switch on two 100Base-TX links. A core gateway connects to site links through the RJ-45 connectors to a backhaul switch.

The core gateways used by the system are GGM 8000 Gateways with four 10/100/1000 Mbps Ethernet ports.

The core gateway performs the following tasks:

- Controls data, and network traffic in and out of the master site
- Provides control path redundancy and segregates the network management traffic
- Provides necessary services to the sites
- Provides a proactive fault management system, notifying whenever a redundant core gateway takes control
- Handles network traffic between the master site and remote sites within a zone (intrazone traffic)
- Provides an interface (Ethernet Backhaul Switches) to the Primary Prime Site and Secondary Prime Site to support the Geographically Redundant Prime Site feature.
- Supports Ethernet Site Link Statistics for the Intra-Prime Site link between the Zone Core and Prime Sites to support the Geographically Redundant Prime Site feature. See the *Flexible Site and InterZone Links Feature Guide* for “Ethernet Site Link Statistics – Transport Devices”.

NOTICE: The core gateway interfaces with the Network Management server using Simple Network Management Protocol (SNMP). Network transport devices (gateways, switches, firewalls, and others) are pre-configured to support systems with and without a TRAK 9100 NTP Server, so the primary NTP Server is set to ntp02, which is always present in the system. For details regarding the Network Time Protocol (NTP) Server and the primary and secondary NTP source for devices in your system, see the *Network Time Protocol Server Feature Guide*.

The third Ethernet port on the core gateway is used to make the connection to two core backhaul switches, which then link to the Ethernet backhaul network. See the *Flexible Site and InterZone Links Feature Guide* for details.

2.6.1.1 Core Gateway (M Zone Core) – Network Connections

Each core gateway has two 100Base-TX connections to separate logically defined Transitional LANs (TLANs) on separate switching modules on the LAN switch. A core gateway directs any traffic to other routers or gateways on the LAN, which then forward the traffic to the destination device.

A core gateway interfaces with remote sites through a backhaul switch. The backhaul switch serves the traffic directly to the sites, or sends the traffic through RJ-45 connectors on the Ethernet links to the sites.

If an ISSI.1 Network Gateway is implemented in the system, a connection between a core gateway and the site router of the ISSI.1 Network Gateway is established. See the *ISSI.1 Network Gateway Feature Guide* manual for details.

Each core gateway also has an RS232 connection to the terminal server, allowing gateway administration by PC clients over the LAN.

See Master Site Gateways – Network Connections on page 150 for a network transport diagram showing the core gateway.

For information on core gateway cabling, see the customized configuration information provided by Motorola Solutions for your system.

NOTICE: See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

2.6.1.2 Core Gateway (M Zone Core) – Site Connectivity

Ethernet links are implemented between sites. The third Ethernet port on the two core gateways is used to make the connection to the two core backhaul switches installed at the master site. The switches connect to the Ethernet backbone to provide links to the sites. For details, see the *Flexible Site and InterZone Links Feature Guide*.

2.6.2 Core Gateway (M Zone Core) – Installation

When and where to use: Follow this process to install the Core Gateway(s).

Process:

1. Install the Core Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Core Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Core Gateway(s). See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the Core Gateway(s). See the following table in section Core Gateway (M Zone Core) – Site-Specific Cabling on page 158.
5. Configure the Core Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

2.6.2.1 Core Gateway (M Zone Core) – Site-Specific Cabling

The following table lists Core Gateway port assignments when used in M Zone Core configuration.

Table 32: Core Gateways Cabling – M1 Zone Core Configuration

Core Gateway	Port	Device/Function
Core Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

Table 33: Core Gateways Cabling – M2 and M3 Zone Core Configuration

Core Gateway	Port	Device/Function
Core Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2

Core Gateway	Port	Device/Function
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Core Gateway 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

2.6.3 Core Gateway (M Zone Core) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

2.6.4 Core Gateway (M Zone Core) – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

2.6.5 Core Gateway (M Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information,see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

2.6.5.1 Core Gateway (M Zone Core) – Failures

Core gateways are installed in pairs. Because of this redundancy, failure of one core gateway is transparent to the user.

- If a core gateway fails, the redundant gateway takes over.
- If both core gateways fail or are powered down, local LAN devices within the zone can no longer communicate with each other. However, local devices on the master site LAN still communicate.

Core gateway failures are reported in the fault management application and additional gateway details are available through the Unified Network Configurator (UNC) application. If a gateway hardware failure is suspected, perform the appropriate field replaceable entity (FRE) replacement procedures.

2.7 Exit Gateway (M1 DSR and M3 Zone Core)

The GGM 8000 Exit Gateway can replace the S6000 Exit Routers (Ethernet Only) used in the zone core to route traffic to and from between zones (inter-zone links) and other sites in the system.

NOTICE: For multi-zone systems using Ethernet site and Inter-Zone links, a Core/Exit gateway deployed as a dual-function transport device provides Intra-Zone (zone-to-site) and Inter-Zone (zone-to-zone). See Core/Exit Gateway (M1 and M3 Zone Core) on page 154.

2.7.1 Exit Gateway (M1 DSR and M3 Zone Core) – Functional Description

The exit gateways function as core gateways that manage traffic for the InterZone links. There are four exit gateways in each zone of a multizone system. The exit gateways are installed in the zone to route all inbound and outbound InterZone traffic for the zone.

The exit gateways used by the system are GGM 8000 Gateways with four 10/100/1000 Mbps Ethernet ports.

An exit gateway performs the following tasks:

- Handles InterZone links. As with the core gateways, exit gateways have Ethernet ports that connect into different layer 2 modules on the Local Area Network (LAN) switch and a backhaul switch for InterZone traffic.

  NOTICE: Exit gateways use Border Gateway Protocol (BGP) for InterZone routing.

- Deploys packets among its multiple connections on the LAN interfaces using dynamic routes. The packets destined for the control Ethernet interfaces on the zone controller, as well as the packets for network management, are routed through the Transitional LAN (TLAN) ports of the Ethernet LAN switch using dynamic routes.
- Talks to other zones through the backhaul switch connection. The exit gateways learn about the Permanent Virtual Circuit (PVCs) on the Ethernet connection from the backhaul switch. Each PVC originates on an exit gateway in one zone, and terminates on an associated exit gateway in the adjacent zone.

2.7.1.1 Exit Gateway (M1 DSR and M3 Zone Core) – Network Connections

If Ethernet links are implemented to other zones, the third Ethernet port on the two exit gateways is used to make the connection to the two core backhaul switches installed at the master site. The switches connect to the Ethernet backbone to provide links to the other zones. For details, see the *Flexible Site and InterZone Links Feature Guide*.

Each exit gateway also has an RS232 connection to the terminal server, allowing gateway administration by PC clients over the LAN.

See Master Site Gateways – Network Connections on page 150 for a network transport diagram showing the exit gateway.

For information on exit gateway cabling, see the customized configuration information provided by Motorola Solutions for your system.

NOTICE: See the *Dynamic System Resilience Feature Guide* for additional configurations.

2.7.2 Exit Gateway (M1 DSR and M3 Zone Core) – Installation

When and where to use: Follow this process to install the Exit Gateway(s).

Process:

1 Install the Exit Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.

2. Connect the Exit Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Exit Gateway(s). See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the Exit Gateway(s). See the following table in section Exit Gateway (M1 DSR and M3 Zone Core) – Site-Specific Cabling on page 161.
5. Configure the Exit Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

2.7.2.1
Exit Gateway (M1 DSR and M3 Zone Core) – Site-Specific Cabling

The following table lists Exit Gateway port assignments when used in an M1 DSR and M3 zone core configuration.

Table 34: Exit Gateways Cabling – M1 Zone Core Configuration

Exit Gateway	Port	Device/Function
Exit Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

Table 35: Exit Gateways Cabling – M3 Zone Core Configuration

Exit Gateway	Port	Device/Function
Exit Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Exit Gateway 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

2.7.3
Exit Gateway (M1 DSR and M3 Zone Core) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

2.7.4
Exit Gateway (M1 DSR and M3 Zone Core) – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

2.7.5 Exit Gateway (M1 DSR and M3 Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

2.7.5.1 Exit Gateway (M1 DSR and M3 Zone Core) – Failures

Exit gateways are installed in pairs. Because of this redundancy, failure of one exit gateway is transparent to the user.

- If an exit gateway fails, the redundant gateway takes over.
- If both gateways fail, the network of the connected zone is isolated and InterZone Local Area Network (LAN) traffic to other zones is lost.

Exit gateway failures are reported in the fault management application and additional gateway details are available through the Unified Network Configurator (UNC) application. If a gateway hardware failure is suspected, perform the appropriate field replaceable entity (FRE) replacement procedures.

2.8 GPRS Gateway Support Node (GGSN) Gateway (M Zone Core)

The GGM 8000 can replace the S6000 GGSN Routers used in the zone core for routing data traffic between the Radio Network Infrastructure (RNI) and external networks to support data services. The GGSN tunnels packet data through private networks to mobile subscribers providing them access to Customer Enterprise Networks (CENs).

2.8.1 GGSN Gateway – Functional Description

The GPRS Gateway Support Node (GGSN) gateway enables data capability. The GGSN tunnels packet data through private networks to mobile subscribers, thereby allowing the mobile subscribers to access the Customer Enterprise Networks (CENs) to which they belong.

A mobile subscriber typically consists of a mobile computer attached to a mobile radio through a serial or USB connection. The mobile radio performs all mobility tasks on behalf of the mobile computer.

A GGSN gateway serves as a network interface between the Motorola Solutions radio network and the CEN. One side of the gateway connects to the Motorola Solutions Radio Network Infrastructure (RNI). The other side attaches to a peripheral network to interface with the border routers of the CEN.

The GGSN provides General Packet Radio Service (GPRS) network access to external hosts to communicate with mobile subscribers. The GGSN acts as a fixed relay point between the external hosts and the mobile subscribers.

A GGSN gateway is designed to handle IP routing services for end-to-end data messaging for Trunking and/or Conventional ASTRO® 25 systems that support High Performance Data (HPD) and Integrated Voice and Data (IV&D). The functions of a gateway include the following:

- Network address translation for static and dynamic IP addressing and IP fragmentation
- Secure IP tunneling
- Internet Control Message Protocol (ICMP) error reporting for troubleshooting activities

Each HPD and IV&D system has one GGSN gateway or more per system. The GGSN gateway provides the following HPD and IV&D support functions:

- Isolates wireline and wireless network traffic from the Motorola Solutions RF network

- Facilitates the use of Dynamic Host Configuration Protocol (DHCP) servers as well as the IP plan
- Isolates agencies

A GGSN gateway provides a logical interface to the Packet Data Router (PDR) module in the Packet Data Gateway (PDG). It maintains routing information for all attached packet data users. Routing information is used to tunnel through GPRS Tunneling Protocol (GTP) user datagrams to the current point of attachment of each Mobile Subscriber Unit (MSU). The attachment is the home PDR to the hosts through IP-IP tunnels.

2.8.1.1 Manual GGSN Switchover

Redundant GGSN gateways are used to support HA (High Availability) Data and DSR Data. In the event of failure, redundant GGSN gateways provide an automatic switchover, but the user also has the option to initiate a switchover manually. A manual GGSN gateway switchover is executed from the Unified Network Configurator (UNC) by performing a reboot of the primary GGSN gateway. The reboot causes the redundant GGSN gateway to take over.

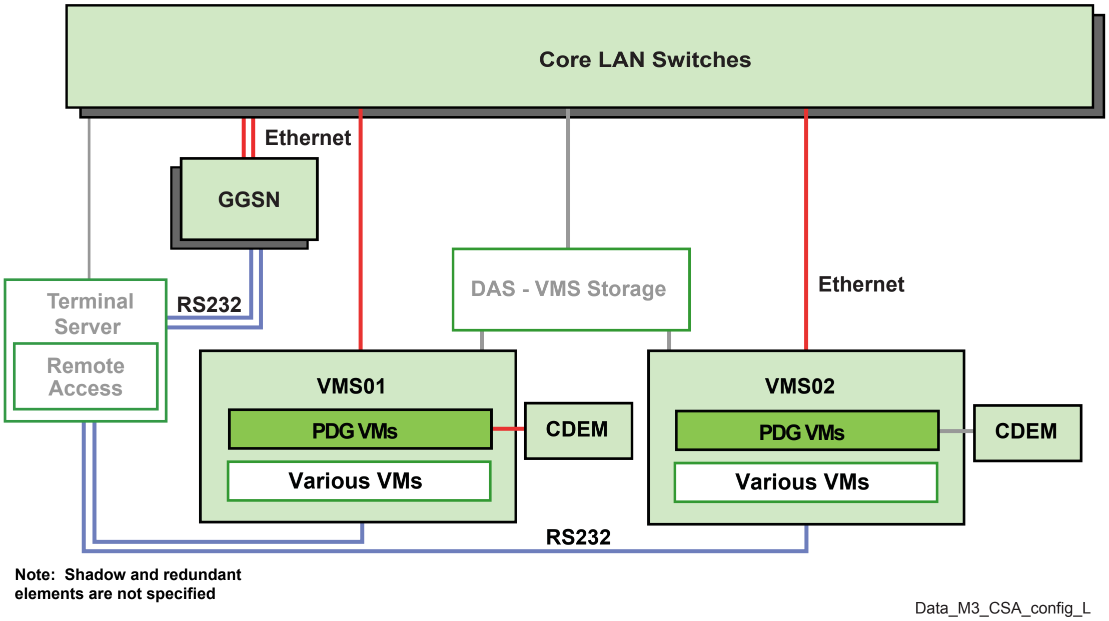
See the *Unified Network Configurator User Guide* for the gateway reboot procedure.

2.8.1.2 GGSN – Network Connections

The GGSN gateway has two 100Base-T connections to the LAN switch to tunnel traffic between the HPD or Trunking and/or Conventional IV&D Packet Data Gateway (PDG) and a border router. The border router routes the traffic for the CEN. It also has a serial connection to the terminal server, enabling router administration.

The diagram below shows the GGSN gateway connections at the master site. See Master Site Gateways – Network Connections on page 150 for a master site diagram showing the GGSN gateways.

Figure 86: GGSN Gateway Connections



NOTICE: This diagram shows the connection of the IV&D PDG to the GGSN through the LAN switch. The placement of the PDG is the same regardless of whether it is an IV&D PDG, HPD PDG or Conv PDG.

See the *Dynamic System Resilience Feature Guide* manual for additional configurations.

2.8.1.3 Charging Gateway Interface

The Charging Gateway provides a mechanism for GGSN to collect usage statistics for data calls and forward them to your organization’s billing interface, which exists outside the ASTRO® 25 system Radio Network Infrastructure (RNI) in the Customer Enterprise Network (CEN). This is achieved by switching on the charging function in the GGSN. The GGSN generates Call Detail Records (CDR), which it then forwards to the Charging Gateway Function (CGF) located in the DMZ, which in turn forwards the data to an external billing system in the CEN for further processing. The external billing system is considered to be part of your system, and is not provided as part of Motorola Solutions Radio Network Infrastructure (RNI).

2.8.1.4 GGSN Functions

The GGSN performs the following specific functions:

- Forwards outbound traffic to the appropriate home HPD or IV&D PDRs
- Sends inbound traffic through Virtual Private Network (VPN) tunnels to the appropriate CEN
- Originates/terminates the GTP tunnels to the Conventional HPD or IV&D PDRs, and the IP-IP tunnels to the CENs
- Sends dynamic updates to the Dynamic Domain Name Service (DDNS) server on the CEN for MSUs after context activation, if configured
- Queries the RADIUS or DHCP server on the CEN for authentication or dynamic addressing, if configured
- Provides local dynamic addressing for MSUs, if configured
- Collects usage statistics for data calls through the Charging Gateway and forwards them to your organization’s billing interface

The GGSN originates IP-IP tunneling to the CENs. The IP-IP tunnels provide secure data delivery traffic to the CENs over the peripheral network. The IP-IP tunneling also provides IP isolation between the system and the CENs to prevent IP address conflicts.

The GGSN is configured with an Access Point Number (APN) for each CEN. The APN is mapped to the physical or virtual ports assigned for each of the CEN border routers. Each MSU is assigned to a particular CEN or APN through the Provisioning Manager application. When the GGSN receives inbound traffic, it forwards the traffic to the appropriate CEN, depending on the APN.

The GGSN is provisioned to interact with RADIUS, DHCP, and DDNS servers on each CEN. The GGSN queries the RADIUS server on the CEN with authentication credentials received from the context-activating MSU. It permits mobile users to authenticate with the CEN during the context activation process.

Depending on the MSU and system configuration, the GGSN also queries the DHCP server on the CEN to receive dynamic addresses for context-activating MSUs. When a RADIUS server is used at the CEN, it operates as both an authentication server and a DHCP server. Otherwise, the GGSN is configured with its own pool of IP addresses to locally provide dynamic addresses to context-activating MSUs.

The GGSN is configured to supply dynamic updates to a DDNS on the CEN. These dynamic updates provide Fully Qualified Domain Name (FQDN) bindings for each context-activating MSU. This FQDN consists of a host name plus the domain name for the MSU (such as: c620100000e0df659f.hpd.cen20). It allows CEN hosts to access the MSUs by using the FQDN associated with an MSU instead of its IP address.

2.8.1.5 GGSN Functional Requirements

Motorola Solutions GGSN functionality requires the following:

- GGM 8000 Gateway with an IP path to each HPD, IV&D PDG, or Conv PDG and your organization's border router
- EOS software certified for this system release, that supports GGSN (GS or GW package)
- EOS software configuration for GGSN service:
  - Virtual ports configured to connect to the CEN domain
  - APN profiles created to configure IP address allocation
  - GGSN control enabled

The PDG consists of the PDR and the Radio Network Gateway (RNG). It performs the functions of a Serving General Packet Radio Service Support Node (SGSN) and mobility. The GGSN software configuration is contained in the `XGSN.cfg` configuration file.

NOTICE: The `XGSN.cfg` file is also known as the `xgsn.cfg` file.

2.8.2 GGSN Gateway – Installation

When and where to use: Follow this process to install the GGSN Gateway(s).

Process:

1. Install the GGSN Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the GGSN Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the GGSN Gateway(s). See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the GGSN Gateway(s). See the following table in section GGSN Gateway – Site-Specific Cabling on page 165.
5. Configure the GGSN Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

2.8.2.1 GGSN Gateway – Site-Specific Cabling

The following table lists GGSN Gateway port assignments when used in an M Zone Core configuration.

Table 36: GGSN Gateways Cabling – M1 Zone Core Configuration

GGSN Gateway	Port	Device/Function
GGSN Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	RS-232	Terminal Server or Local Serial Access

Table 37: GGSN Gateways Cabling – M2 and M3 Zone Core Configuration

GGSN Gateway	Port	Device/Function
GGSN Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access
GGSN Gateway 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access

2.8.3 GGSN Gateway – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply. For comprehensive information on configuring charging parameters, see the “GGSN Router Management” section in the *Unified Network Configurator User Guide*.

2.8.3.1 GGSN Configuration (xgsn.cfg) File Management

When the GGSN gateway is enabled, the gateway supports a GGSN configuration (`xgsn.cfg`) file in addition to the `boot.cfg` and `acl.cfg` configuration files. The `xgsn.cfg` file includes GGSN, virtual port, and APN configurations. The TNCT file, supplied by Motorola Solutions, creates the `xgsn.cfg` file and contains the GGSN configuration parameters and the APN configuration commands for the APNs. When there is no `boot.cfg` file in the GGSN gateway, the `xgsn.cfg` file does not execute. The `boot.cfg` file executes first, then the `xgsn.cfg` file. The Unified Network Configurator (UNC) VoyenceControl application uses templates to manage the `xgsn.cfg` file.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
The `xgsn.cfg` file provides GGSN configuration manageability. When booting a gateway running a software package that supports the GGSN, the `xgsn.cfg` file is used for GGSN configuration commands. It includes GGSN configuration commands in the `boot.cfg` file. A `boot.cfg` file with GGSN configuration commands causes logging errors when used on a gateway running a software package that does not support the GGSN.

See the “GGSN Router Management” section in the *Unified Network Configurator User Guide*.

2.8.3.2 IP Address Allocation for Mobile Subscribers

IP addresses for mobile subscribers can be allocated in one of four ways:

Static subscriber IP address allocation

The IP assigner is set to the local DHCP, but no address pools are configured. All requesting subscribers are assigned statically; the User Configuration Server application (UCS) assigns proposed IP addresses before the Packet Data Protocol (PDP) context create reaches the GGSN.

Dynamic subscriber IP address allocation through a local server

The IP Assigner is set to the local DHCP with address pools configured. The Border gateway assigns the IP addresses from this pool to a requesting mobile subscriber during PDP context establishment. The GGSN gateway allocates one or more sets of IP addresses dynamically from a block of available addresses configured per APN from the CEN’s address space. The GGSN requests an IP address from the Border gateway configured IP pool on behalf of the mobile subscribers. The IP addresses can be assigned dynamically from a configured pool. They can also be reserved and specifically matched to the International Mobile Subscriber Identity (IMSI) numbers.

Dynamic subscriber IP address allocation through a DHCP server

The IP Assigner is set to Remote DHCP. A DHCP server, located within the address space of the CEN, assigns the subscriber addresses dynamically. The GGSN requests IP addresses from the DHCP server on behalf of mobile subscribers.

Dynamic subscriber IP address allocation through a RADIUS server

A RADIUS server, located within the address space of the CEN, assigns the subscriber addresses dynamically. Authentication is performed by the same RADIUS server. Authentication is required when IP addresses are allocated through a RADIUS server. The GGSN requests IP addresses and authentication from the RADIUS server on behalf of mobile subscribers.

2.8.3.3 New APN Configuration Parameters

The Unified Network Configurator (UNC) supports the GGSN DDNS feature. It allows for the retrieval of the IP address of a specific mobile subscriber from the DNS server on the CEN.

In the data flow process, the GGSN does the following:

- Receives a PDP context create message from the PDR during the context activation
- Opens the context when the optional RADIUS authentication process passes
- Stores the IP address of the mobile subscriber in the following ways:
  - Proposes in the context create message
  - Allocates from the Border gateway internal IP address pool
  - Allocates from the external DHCP service
  - Allocates from the external RADIUS services
- Sends out UDP-based dynamic DNS update messages to the DNS server located in the CEN
- Starts a retransmission timer after sending out a dynamic DNS update request

When the dynamic DNS response is not received, the GGSN retransmits the update request three times at five second intervals. It does not deactivate the PDP context. Dynamic DNS update messages sent by the GGSN include:

- A resource record that specifies the IP address of the mobile subscriber for DNS forward lookup.
- A PTR resource record that specifies the FQDN of the mobile subscriber for DNS reverse lookup.

The information about the mobile subscriber is registered by the Fully Qualified Domain Name (FQDN) and the assigned mobile IP address. The formatting for the FQDN is **MSISDN.DDName**.

NOTICE: When the GGSN receives a dynamic DNS update response in the middle of a retransmission, it stops the retransmission and frees up the retransmission timer.

To configure a GGSN gateway for dynamic DNS functionality, specify the IP address of the DNS server and the DDNS server name when configuring the APN on the GGSN. Use the templates in the UNC to create, view, and edit the APN configuration parameters for the GGSN gateway.

See “Creating an APN” and “Access Point Name Management” sections in the *Unified Network Configurator User Guide*.

2.8.3.4

Overload Protection Management (OPM)

The gateway software applications are designed for memory usage and CPU utilization within the acceptable margins, based on the required messages-per-hour rate.

For example: The GGSN application performs adequately by limiting the number of simultaneous contexts open at all times. When a packet or a data storm occurs, the packet rate increases above the stated required maximum. In such cases, limited data loss occurs in arbitrary places in the data pipeline of the router.

The purpose of the Overload Protection Management (OPM) feature is to monitor the following parameters and to inform registered applications (OPM clients) when any of the parameters meet or exceed the configured threshold.

- CPU utilizations
- Memory utilization
- Queue drop

The registered applications limit their activity during overload conditions, thereby preventing potential data loss.

NOTICE: In the initial release of the OPM, queue drops are accumulated for Ethernet ports only.

The initial release of the OPM supports the following two clients: GGSN and SNMP.

The OPM thresholds for each of the monitored parameters can be set to high, medium, or low. Each threshold level (high, medium, or low) is associated with internally configured high-water and low-water marks. OPM clients are called when either of the following events occurs:

- Overload – The parameter meets or exceeds the high-water mark associated with the specified threshold level (high, medium, or low).
- Normal – The parameter falls below the low-water mark associated with the specified threshold level (high, medium, or low).

NOTICE: The EOS implementation of overload protection management incorporates a 30-second Holddown timer, which prevents the gateway from entering or leaving Overload within that time period. For example, if a gateway enters Overload state at 3:30:15, the Holddown timer starts and the gateway cannot exit Overload state until the 30-second Holddown period expires (in this example, at 3:30:45).

The registered GGSN application takes the following appropriate actions when it discovers an overload:

- Reads the number of active PDP contexts (GTP tunnels)
- Freezes the number of active contexts at that value
- Rejects any new context creates until one of the following scenarios occurs:
    - An existing context is dropped when one new context is created for every existing context create.

      NOTICE: The maximum configurations of contexts created is 65,535. When no limit is configured, the default limit is 20,000.

    - A received normal event indicates that the monitored parameter falls below the low-water mark associated with the configured threshold.
- Sends a trap when it receives an Overload or a Normal event

Overload Protection Configuration

To activate the overload protection using Unified Network Configurator (UNC), see “Managing GGSN Router Statistics” section in the *Unified Network Configurator User Guide*.

Overload Protection Statistics Retrieval

You can retrieve the following overload protection statistics:

- CPU Utilization – The current value for CPU utilization.
- Memory Usage – The current value for memory usage.
- Queue Drops – The current value for queue drops.
- The number of times the router has gone into Overload state.
- A log of the last five times the router went into Overload state, including the following information:
  - Start Time – The time at which the router went into Overload state.
  - End Time – The time at which the router exited the Overload state.
  - Duration – The amount of time the router was in the Overload state.
  - Cause In – The reason why the router went into the Overload state (CPU utilization, memory usage, or queue drops).
  - Cause Out – The reason why the router exited the Overload state (CPU utilization, memory usage, or queue drops).

For information on how to manage the overload protection statistics in the Unified Network Configurator (UNC), see the “Managing GGSN Router Statistics” section in the *Unified Network Configurator User Guide*.

2.8.4 GGSN Gateway – Operation

This topic provides user operation procedures for working with Access Point Number (APN) information and viewing statistics for the GGSN.

View and Edit Existing APNs

To view and edit existing GGSN parameters, see the “GGSN Router Configuration File Management” section in the *Unified Network Configurator User Guide*.

View Statistics

You can gather and display the following GGSN GTP statistics:

GTP Peer IP Address
The IP address of the GTP tunnel peer.

State
The operational status of the GTP tunnel (UP or DOWN).

Number of PDP Contexts
The currently configured maximum number of PDP contexts supported on the GGSN gateway.

Received Control Packets
The total number of control packets received from all IV&D, HPD, or Conv PDGs (Packet Data Gateways).

Sent Control Packets
The total number of control packets sent to any CEN.

Received Data Packets
The total number of data packets received from all IV&D, HPD, or Conv PDGs

Received Data Bytes
The total number of data bytes received from all IV&D, HPD, or Conv PDGs

Sent Data Packets
The total number of data packets sent to any CEN.

Sent Data Bytes
The total number of data bytes sent to any CEN.

Mobile IP Services
The total number of mobile node registrations sent from all Conv PDGs and received by any CEN.

APN Statistics

You can gather and display statistics for APN. To view APN statistics, see “Showing APN and RADIUS Statistics” in the *Unified Network Configurator User Guide*.

CEN Statistics for User Data

Sent Packets
The total number of packets sent to CEN through this APN

Rcvd Packets
The total number of packets received from CEN through this APN

Sent Bytes
The total number of bytes sent to CEN through this APN

Rcvd Bytes
The total number of bytes received from CEN through this APN

CEN Statistics for DHCP

Sent DHCP Discover
The number of DHCP discover messages sent to the DHCP server in CEN

Rcvd DHCP Offer
The number of DHCP offer messages received from the DHCP server in CEN.

Sent DHCP Req
The number of DHCP request messages sent to the DHCP server in CEN

Rcvd DHCP Ack
The number of DHCP Ack messages received from the DHCP server in CEN

Sent DHCP Release
The number of DHCP release messages sent to the DHCP server in CEN

Rcvd DHCP Rsp Err
The number of received DHCP response messages indicating an error

DHCP Discover Timeout
The number of DHCP discover messages that were retransmitted and eventually timed out

DHCP Req Timeout
The number of DHCP request messages that were retransmitted and eventually timed out

DHCP Switchover
The number of switchovers from primary to secondary or secondary to primary DHCP servers

DHCP
The IP address of the current external DHCP server

RADIUS Auth.
The IP address of the current RADIUS authentication server

RADIUS Acct.
The IP address of the current RADIUS accounting server

Authentication Statistics

Switchovers
The number of switchovers from primary to secondary or secondary to primary RADIUS authentication servers

Accepts
The number of authentication accept messages received from the RADIUS server

Rejects
The number of authentication reject messages received from the RADIUS server

Timeout
The number of context creation failures caused by authentication timeout

Retries
The number of authentication message retransmissions

Max RoundTrip
The maximum response time from the first authentication request message to the time when the response is received. It may include retransmissions.

Accounting Statistics

Switchovers
The number of switchovers from primary to secondary or secondary to primary RADIUS accounting servers

Success
The number of accounting start response messages received from the RADIUS server

Failure
The number of failures on the accounting start response messages received from the RADIUS server

Timeout
The number of timeouts on accounting start response messages

Duplicated IP
The number of RADIUS-allocated IP addresses, which are duplicated in the GGSN gateway

Max RoundTrip
The maximum response time from the first accounting start response message to the time when the start response is received. It may include retransmissions.

High Availability Statistics

Real Time Contexts Sent to Standby
The number of contexts that the Master GGSN sends to the StandBy GGSN

Number of Times Peer Came Up
A counter that increments after port 1 of the peer GGSN comes back **UP** after being disabled

Number of Times Peer Went Down
A counter that increments after port 1 of the peer GGSN goes **DOWN**

Number of HA Switchovers
This counter increments every time the HA vrrp Mastership gets switched from the Master GGSN to StandBy GGSN and reverse

2.8.5 GGSN Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

2.8.5.1 General Troubleshooting for the GGSN

If there is a failure on the GPRS Gateway Support Node (GGSN) gateway, the system loses the ability to provide data messaging from your data network to the mobile data devices in your system, all IP services are dropped. When a GGSN router fails, the Packet Data Router (which this gateway interfaces to) sends “link down” status information to the Unified Event Manger (UEM) server in that zone. The GGSN Link object in the UEM displays the reported status of the logical link between the PDR and the GGSN gateway.

If Dynamic System Resilience (DSR) is implemented on your system, the gateways support multiple IPIP tunnels per APN for redundancy. This feature supports the GGSN Dynamic System Resilience feature. APN to multiple IPIP binding allows the system to support DSR to multiple Customer Enterprise Networks (CENs). When the link for one of the tunnels fails, the gateways switches over to the other IPIP tunnel, thereby preserving connectivity between the GGSN and the CEN.

NOTICE: Multiple IPIP tunnels are supported only for redundancy, and only one tunnel is active at a time.

To bind an APN to multiple IPIP tunnels, a bidirectional forwarding detection (BFD) gateway IP address (the IP address of the border router) and a priority value for each tunnel is specified when the APN is configured in the UNC. BFD maintains the link status for each tunnel and informs the GGSN software when a link comes up or goes down. When the GGSN receives a status change notification, the GGSN transparently uses the active IPIP tunnel with the highest priority value to connect to the CEN. If that tunnel fails, the GGSN switches over to the other IPIP tunnel until the higher priority link is re-established.

The GGSN sends an alarm to the UEM both when the GGSN connection to the CEN has been established and when the GGSN connection to the CEN goes down.

The data port (V1) on the GGSN has a static IP address and does not send any SNMP traps to the UEM.

For more information on the operation of the UEM, a list of devices managed by the UEM, and alarms managed by the UEM, see the *Unified Event Manager User Guide*.

If High Availability (HA) Data is configured in your system, GGSNs are deployed as a redundant pair. If the active GGSN experiences a failure which makes it unable to provide data service, the redundant GGSN becomes active. Data service is restored within 90 seconds of the failure. In this configuration, the gateways support multiple paths (two for HA Data, four for HA Data with DSR) to the Customer Enterprise Networks (CENs). When the active path to the CEN fails, the gateways switch over to the next highest priority path. For more information about the HA Data feature and for a failure and recovery scenario of GGSN HA Data subsystem gateways, see the *Trunked Data Services Feature Guide*.

Chapter 3

ASTRO 25 Master Site (L Zone Core)

This chapter provides information about the GGM 8000 Gateway in ASTRO® 25 system Small Trunking Configurations (L core).

3.1 Zone Core Transport Devices (L Zone Core) – Functional Description

In ASTRO® 25 system Small Trunking Configurations (L core), the zone core transport devices consists primarily of the following devices:

- Core Gateway
- GGM 8000 Gateway
- GGSN Gateway

The number of zone core transport devices in an L Core depends primarily on redundancy.

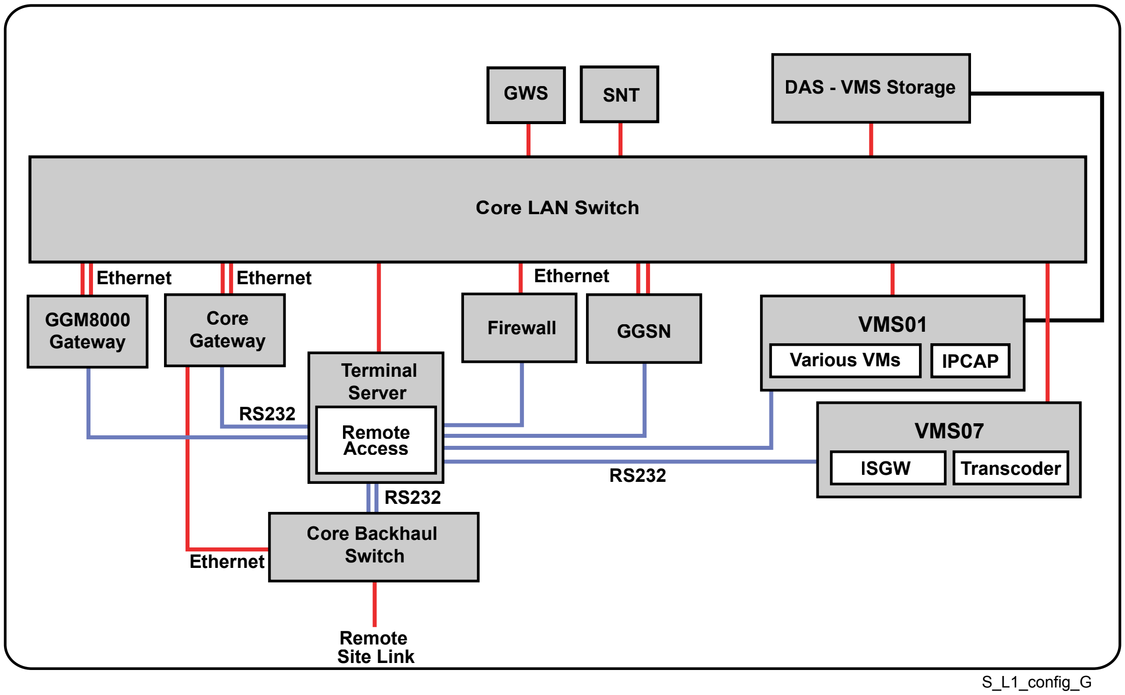
The non-redundant L Core (L1) has one Core Gateway (single-function) and one GGM8000 Gateway. For network traffic between the RNI (Radio Network Infrastructure) and CEN (Customer Enterprise Network) for packet data applications, one GGSN Gateway transport device is added.

The redundant L Core (L2) has two Core Gateways (single-function) and two GGM8000 Gateways. For network traffic between the RNI (Radio Network Infrastructure) and CEN (Customer Enterprise Network) for packet data applications, a GGSN Gateway can be added or two GGSN Gateway transport devices can be added to support HA (High Availability) data.

NOTICE: The GGM 8000 devices ordered from the factory do not require an encryption module for encryption to be enabled. However, the software encryption option must be ordered.

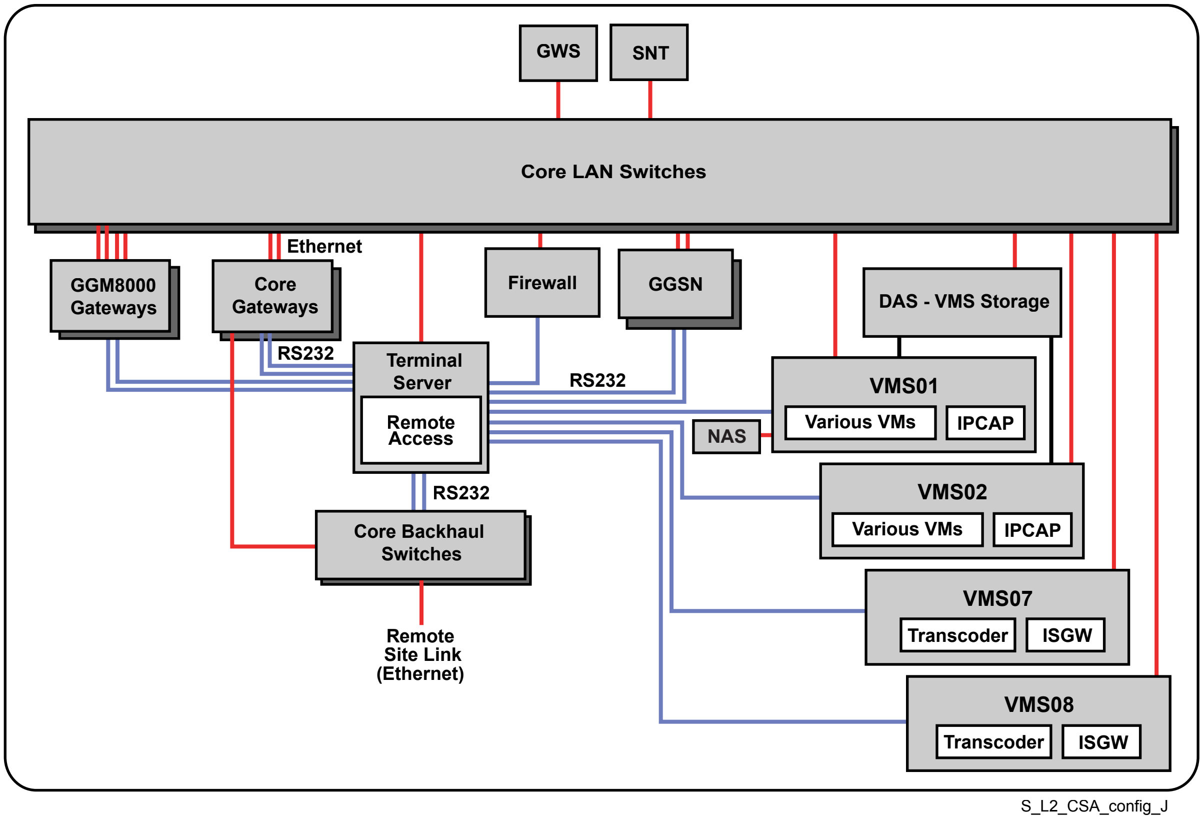
The following figure shows zone core transport devices in the Non-Redundant (L1) zone core configuration.

Figure 87: Non Redundant (L1) Zone Core Configuration



The following figure shows zone core transport devices in the Redundant (L2) zone core configuration.

Figure 88: Redundant (L2) Zone Core Configuration



3.2
Core Gateway (L Zone Core)

The single-function Core Gateway in an L Core provides network transport support for traffic between a zone core and remote sites within a zone (intra-zone traffic).

3.2.1
Core Gateway (L Zone Core) – Installation

When and where to use: Follow this process to install the Core Gateway(s) (L zone core).

Process:

1. Install the Core Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Core Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Core Gateway(s). See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the Core Gateway(s). See one of the following tables in section Core Gateway (L Zone Core) – Site-Specific Cabling on page 175:
    - For L1 configuration, see Table 38: Core Gateway Cabling – L1 Small Trunking Configuration on page 175.
    - For L2 configuration, see Table 39: Core Gateways Cabling – L2 Small Trunking Configuration on page 175.
5. Configure the Core Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

3.2.1.1
Core Gateway (L Zone Core) – Site-Specific Cabling

The following table lists Core Gateway port assignments when used in L1 Small Trunking Configuration.

Table 38: Core Gateway Cabling – L1 Small Trunking Configuration

Core Gateway	Port	Device/Function
Core Gateway 1	LAN 1, 2, 4	Core LAN Switch
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

The following table lists Core Gateway port assignments when used in L2 Small Trunking Configuration.

Table 39: Core Gateways Cabling – L2 Small Trunking Configuration

Core Gateway	Port	Device/Function
Core Gateway 1	LAN 1, 2, 4	Core LAN Switch 1
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access
Core Gateway 2	LAN 1, 2, 4	Core LAN Switch 2

Core Gateway	Port	Device/Function
	LAN 3	Backhaul Switch
	RS-232	Terminal Server or Local Serial Access

3.2.2
Core Gateway (L Zone Core) – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

3.2.3
Core Gateway (L Zone Core) – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

3.2.4
Core Gateway (L Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

3.2.4.1
Core Gateway (L Zone Core) – Failures

Depending on the configuration, a Core Gateway failure can have different connotations:

- In L1 configuration, a failure of the Core Gateway means that local devices within a zone are no longer able to communicate with each other and intra-zone traffic stops.
- In L2 configuration, a failure of a single Core Gateway is transparent to the user, as the redundant gateway takes over. A failure of both Core Gateways would mean that local devices within a zone are no longer able to communicate with each other and intra-zone traffic stops.

3.3
GGM 8000 Gateway (L Zone Core)

The single-function GGM 8000 Gateway in an L Core provides support for zone core network traffic involving the zone controller, Packet Data Gateway, and Consoles.

3.3.1
GGM 8000 Gateway (L Zone Core) – Functional Description

A GGM 8000 Gateway functions as a data and control gateway. Examples include:

- Routing packets for hosts on the various networks in the zone core.
- Supporting multicast traffic by performing the rendezvous point (RP) function for both audio and control messages in the zone.

Two GGM 8000 Gateways are installed on the Local Area Network (LAN).

GGM 8000 Gateways are used for devices that require network redundancy and are multicasting beyond their local LAN. GGM 8000 Gateways provide support for the following:

- Zone Controller (control router functionality)
- Audio RP function (audio duplication for the zone)

- Packet Data Gateway (PDG router functionality)
- Network Management

Each GGM 8000 Gateway has two 100Base-TX connections to one of the master site LAN switches. One GGM 8000 Gateway connects to TLAN 1 and the other connects to TLAN 2. Any traffic to and from the zone controllers and the PDG is routed by one of the GGM 8000 Gateways. Each GGM 8000 Gateway has an RS232 connection to the terminal server, allowing router administration by PC clients over the LAN.

3.3.2 GGM 8000 Gateway (L Zone Core) – Installation

When and where to use: Follow this process to install the GGM 8000 Gateway.

Process:

1. Install the GGM 8000 Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the GGM 8000 to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the GGM 8000 Gateway. See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the GGM 8000 Gateway. See the following table in section GGM 8000 Gateway (L Zone Core) – Site-Specific Cabling on page 177.
5. Configure the GGM 8000 Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

3.3.2.1 GGM 8000 Gateway (L Zone Core) – Site-Specific Cabling

The following table lists GGM 8000 Gateway port assignments when used in an L Zone Core configuration.

Table 40: GGM 8000 Gateways Cabling – L1 Zone Core Configuration

GGM 8000 Gateway	Port	Device/Function
GGM 8000 Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	RS-232	Terminal Server or Local Serial Access

Table 41: GGM 8000 Gateways Cabling – L2 Zone Core Configuration

GGM 8000 Gateway	Port	Device/Function
GGM 8000 Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access
GGM 8000 Gateway 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access

3.3.3 GGM 8000 Gateway (L Zone Core) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

3.3.4 GGM 8000 Gateway (L Zone Core) – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

3.3.5 GGM 8000 Gateway (L Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

3.3.5.1 GGM 8000 Gateway (M Zone Core) – Failures

A failure of a single GGM 8000 Gateway is transparent to the user, as the redundant gateway takes over. A failure of both GGM 8000 Gateways would mean that local devices within a zone are no longer able to communicate with each other and intra-zone traffic stops.

3.4 GPRS Gateway Support Node (GGSN) Gateway (L Zone Core)

The GGSN is used in the zone core for routing data traffic between the Radio Network Infrastructure (RNI) and external networks to support data services. The GGSN tunnels packet data through private networks to mobile subscribers providing them access to Customer Enterprise Networks (CENs).

3.4.1 GGSN Gateway (L Zone Core) – Functional Description

The GPRS Gateway Support Node (GGSN) gateway enables data capability. The GGSN tunnels packet data through private networks to mobile subscribers, thereby allowing the mobile subscribers to access the Customer Enterprise Networks (CENs) to which they belong.

A mobile subscriber typically consists of a mobile computer attached to a mobile radio through a serial or USB connection. The mobile radio performs all mobility tasks on behalf of the mobile computer.

A GGSN gateway serves as a network interface between the Motorola Solutions radio network and the CEN. One side of the gateway connects to the Motorola Solutions Radio Network Infrastructure (RNI). The other side attaches to a peripheral network to interface with the border routers of the CEN.

The GGSN provides General Packet Radio Service (GPRS) network access to external hosts to communicate with mobile subscribers. The GGSN acts as a fixed relay point between the external hosts and the mobile subscribers.

A GGSN gateway is designed to handle IP routing services for end-to-end data messaging for Trunking and/or Conventional ASTRO® 25 systems that support High Performance Data (HPD) and Integrated Voice and Data (IV&D). The functions of a gateway include the following:

- Network address translation for static and dynamic IP addressing and IP fragmentation
- Secure IP tunneling

- Internet Control Message Protocol (ICMP) error reporting for troubleshooting activities

Each HPD and IV&D system has one GGSN gateway or more per system. The GGSN gateway provides the following HPD and IV&D support functions:

- Isolates wireline and wireless network traffic from the Motorola Solutions RF network
- Facilitates the use of Dynamic Host Configuration Protocol (DHCP) servers as well as the IP plan
- Isolates agencies

A GGSN gateway provides a logical interface to the Packet Data Router (PDR) module in the Packet Data Gateway (PDG). It maintains routing information for all attached packet data users. Routing information is used to tunnel through GPRS Tunneling Protocol (GTP) user datagrams to the current point of attachment of each Mobile Subscriber Unit (MSU). The attachment is the home PDR to the hosts through IP-IP tunnels.

3.4.1.1 Manual GGSN Switchover (L Zone Core)

Redundant GGSN gateways are used to support HA (High Availability) Data and DSR Data. In the event of failure, redundant GGSN gateways provide an automatic switchover, but the user also has the option to initiate a switchover manually. A manual GGSN gateway switchover is executed from the Unified Network Configurator (UNC) by performing a reboot of the primary GGSN gateway. The reboot causes the redundant GGSN gateway to take over.

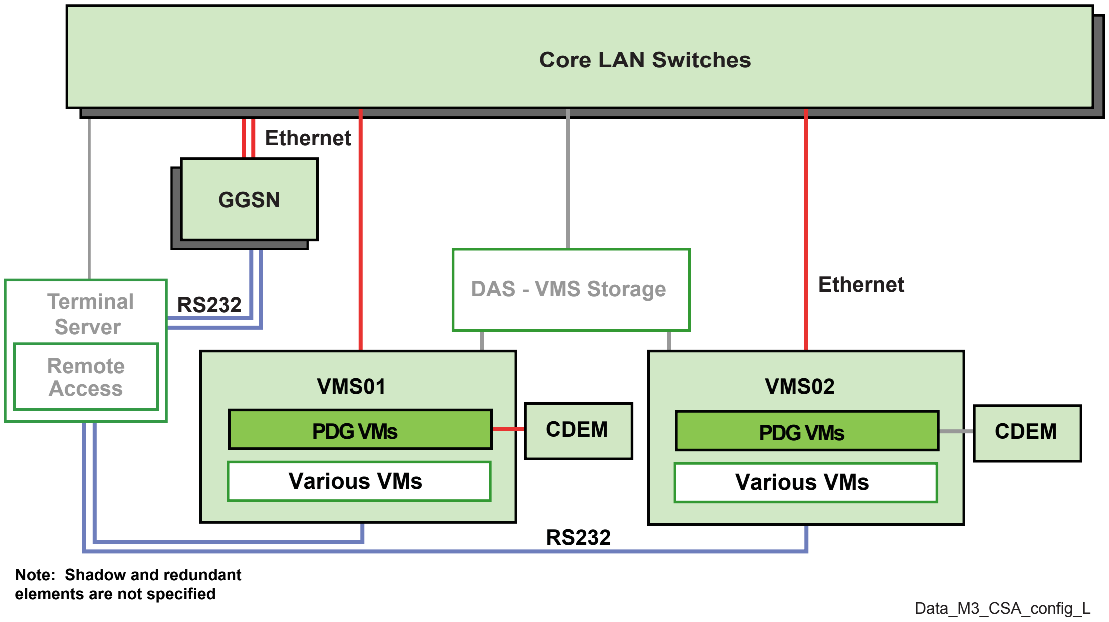
See the *Unified Network Configurator User Guide* for the gateway reboot procedure.

3.4.1.2 GGSN – Network Connections (L Zone Core)

The GGSN gateway has two 100Base-T connections to the LAN switch to tunnel traffic between the HPD or Trunking and/or Conventional IV&D Packet Data Gateway (PDG) and a border router. The border router routes the traffic for the CEN. It also has a serial connection to the terminal server, enabling router administration.

The following diagram shows the GGSN gateway connections at the master site.

Figure 89: GGSN Gateway Connections



NOTICE: This diagram shows the connection of the IV&D PDG to the GGSN through the LAN switch. The placement of the PDG is the same regardless of whether it is an IV&D PDG, HPD PDG or Conv PDG.

See the *Dynamic System Resilience Feature Guide* for additional configurations.

3.4.1.3 Charging Gateway Interface (L Zone Core)

The Charging Gateway provides a mechanism for the GGSN to collect usage statistics for data calls and forward them to your organization's billing interface, which exists outside the ASTRO® 25 system Radio Network Infrastructure (RNI) in the Customer Enterprise Network (CEN). This is achieved by switching on the charging function in the GGSN. The GGSN generates Call Detail Records (CDR), which it then forwards to the Charging Gateway Function (CGF) located in the DMZ, which in turn forwards the data to an external billing system in the CEN for further processing. The external billing system is considered to be part of your system, and is not provided as part of Motorola Solutions Radio Network Infrastructure (RNI).

3.4.1.4 GGSN Functions (L Zone Core)

The GGSN performs the following specific functions:

- Forwards outbound traffic to the appropriate home HPD or IV&D PDRs
- Sends inbound traffic through Virtual Private Network (VPN) tunnels to the appropriate CEN
- Originates/terminates the GTP tunnels to the Conventional HPD or IV&D PDRs, and the IP-IP tunnels to the CENs
- Sends dynamic updates to the Dynamic Domain Name Service (DDNS) server on the CEN for MSUs after context activation, if configured
- Queries the RADIUS or DHCP server on the CEN for authentication or dynamic addressing, if configured
- Provides local dynamic addressing for MSUs, if configured
- Collects usage statistics for data calls through the Charging Gateway and forwards them to your organization's billing interface

The GGSN originates IP-IP tunneling to the CENs. The IP-IP tunnels provide secure data delivery traffic to the CENs over the peripheral network. The IP-IP tunneling also provides IP isolation between the system and the CENs to prevent IP address conflicts.

The GGSN is configured with an Access Point Number (APN) for each CEN. The APN is mapped to the physical or virtual ports assigned for each of the CEN border routers. Each MSU is assigned to a particular CEN or APN through the Provisioning Manager application. When the GGSN receives inbound traffic, it forwards the traffic to the appropriate CEN, depending on the APN.

The GGSN is provisioned to interact with RADIUS, DHCP, and DDNS servers on each CEN. The GGSN queries the RADIUS server on the CEN with authentication credentials received from the context-activating MSU. It permits mobile users to authenticate with the CEN during the context activation process.

Depending on the MSU and system configuration, the GGSN also queries the DHCP server on the CEN to receive dynamic addresses for context-activating MSUs. When a RADIUS server is used at the CEN, it operates as both an authentication server and a DHCP server. Otherwise, the GGSN is configured with its own pool of IP addresses to locally provide dynamic addresses to context-activating MSUs.

The GGSN is configured to supply dynamic updates to a DDNS on the CEN. These dynamic updates provide Fully Qualified Domain Name (FQDN) bindings for each context-activating MSU. This FQDN consists of a host name plus the domain name for the MSU (such as: c620100000e0df659f.hpd.cen20). It allows CEN hosts to access the MSUs by using the FQDN associated with an MSU instead of its IP address.

3.4.1.5 GGSN Functional Requirements (L Zone Core)

Motorola Solutions GGSN functionality requires the following:

- GGM 8000 Gateway with an IP path to each HPD, IV&D PDG, or Conv PDG and your organization’s border router
- EOS software certified for this system release, that supports GGSN (GS or GW package)
- EOS software configuration for GGSN service:
  - Virtual ports configured to connect to the CEN domain
  - APN profiles created to configure IP address allocation
  - GGSN control enabled

The PDG consists of the PDR and the Radio Network Gateway (RNG). It performs the functions of a Serving General Packet Radio Service Support Node (SGSN) and mobility. The GGSN software configuration is contained in the `XGSN.cfg` configuration file.

NOTICE: The `XGSN.cfg` file is also known as the `xgsn.cfg` file.

3.4.2 GGSN Gateway (L Zone Core) – Installation

When and where to use: Follow this process to install the GGSN Gateway(s).

Process:

1. Install the GGSN Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the GGSN Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the GGSN Gateway(s). See Connecting a Chassis Ground on page 68.
4. Connect the master site equipment to the GGSN Gateway(s). See the following table in section GGSN Gateway (L Zone Core) – Site-Specific Cabling on page 181.
5. Configure the GGSN Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

3.4.2.1 GGSN Gateway (L Zone Core) – Site-Specific Cabling

The following table lists GGSN Gateway port assignments when used in an L Zone Core configuration.

Table 42: GGSN Gateways Cabling – L Zone Core Configuration

GGSN Gateway	Port	Device/Function
GGSN Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 1
	RS-232	Terminal Server or Local Serial Access

Table 43: GGSN Gateways Cabling – L2 Zone Core Configuration

GGSN Gateway	Port	Device/Function
GGSN Gateway 1	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access
GGSN Gateway 2	LAN 1	Core LAN Switch 1
	LAN 2	Core LAN Switch 2
	RS-232	Terminal Server or Local Serial Access

3.4.3 GGSN Gateway (L Zone Core) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply. For comprehensive information on configuring charging parameters, see the “GGSN Router Management” section in the *Unified Network Configurator User Guide*.

3.4.3.1 GGSN Configuration (xgsn.cfg) File Management (L Zone Core)

When the GGSN gateway is enabled, the gateway supports a GGSN configuration (`xgsn.cfg`) file in addition to the `boot.cfg` and `acl.cfg` configuration files. The `xgsn.cfg` file includes GGSN, virtual port, and APN configurations. The TNCT file, supplied by Motorola Solutions, creates the `xgsn.cfg` file and contains the GGSN configuration parameters and the APN configuration commands for the APNs. When there is no `boot.cfg` file in the GGSN gateway, the `xgsn.cfg` file does not execute. The `boot.cfg` file executes first, then the `xgsn.cfg` file.

NOTICE:
The `xgsn.cfg` file provides GGSN configuration manageability. When booting a gateway running a software package that supports the GGSN, the `xgsn.cfg` file is used for GGSN configuration commands. It includes GGSN configuration commands in the `boot.cfg` file. A `boot.cfg` file with GGSN configuration commands causes logging errors when used on a gateway running a software package that does not support the GGSN.

3.4.3.2 IP Address Allocation for Mobile Subscribers (L Zone Core)

IP addresses for mobile subscribers can be allocated in one of four ways:

Static subscriber IP address allocation

The IP assigner is set to the local DHCP, but no address pools are configured. All requesting subscribers are assigned statically; the User Configuration Server application (UCS) assigns proposed IP addresses before the Packet Data Protocol (PDP) context create reaches the GGSN.

Dynamic subscriber IP address allocation through a local server

The IP Assigner is set to the local DHCP with address pools configured. The Border gateway assigns the IP addresses from this pool to a requesting mobile subscriber during PDP context establishment. The GGSN gateway allocates one or more sets of IP addresses dynamically from a block of available addresses configured per APN from the CEN’s address space. The GGSN requests an IP address from the Border gateway configured IP pool on behalf of the mobile subscribers. The IP addresses can be assigned dynamically from a configured pool. They can also be reserved and specifically matched to the International Mobile Subscriber Identity (IMSI) numbers.

Dynamic subscriber IP address allocation through a DHCP server

The IP Assigner is set to Remote DHCP. A DHCP server, located within the address space of the CEN, assigns the subscriber addresses dynamically. The GGSN requests IP addresses from the DHCP server on behalf of mobile subscribers.

Dynamic subscriber IP address allocation through a RADIUS server

A RADIUS server, located within the address space of the CEN, assigns the subscriber addresses dynamically. Authentication is performed by the same RADIUS server. Authentication is required when IP addresses are allocated through a RADIUS server. The GGSN requests IP addresses and authentication from the RADIUS server on behalf of mobile subscribers.

3.4.3.3 New APN Configuration Parameters (L Zone Core)

The DDNS feature allows for the retrieval of the IP address of a specific mobile subscriber from the DNS server on the CEN.

In the data flow process, the GGSN performs the following functions:

- Receives a PDP context create message from the PDR during the context activation
- Opens the context when the optional RADIUS authentication process passes
- Stores the IP address of the mobile subscriber in the following ways:
  - Proposes in the context create message
  - Allocates from the Border gateway internal IP address pool
  - Allocates from the external DHCP service
  - Allocates from the external RADIUS services
- Sends out UDP-based dynamic DNS update messages to the DNS server located in the CEN
- Starts a retransmission timer after sending out a dynamic DNS update request

When the dynamic DNS response is not received, the GGSN retransmits the update request three times at five second intervals. It does not deactivate the PDP context. Dynamic DNS update messages sent by the GGSN include:

- A resource record that specifies the IP address of the mobile subscriber for DNS forward lookup.
- A PTR resource record that specifies the FQDN of the mobile subscriber for DNS reverse lookup.

The information about the mobile subscriber is registered by the Fully Qualified Domain Name (FQDN) and the assigned mobile IP address. The formatting for the FQDN is **MSISDN.DDName**.

NOTICE: When the GGSN receives a dynamic DNS update response in the middle of a retransmission, it stops the retransmission and frees up the retransmission timer.

To configure a GGSN gateway for dynamic DNS functionality, you need to specify the IP address of the DNS server and the DDNS server for the APN on the GGSN. Refer to the *Enterprise OS Software User Guide* for instructions.

3.4.3.4 Overload Protection Management (OPM) (L Zone Core)

The gateway software applications are designed for memory usage and CPU utilization within the acceptable margins, based on the required messages-per-hour rate.

For example: The GGSN application performs adequately by limiting the number of simultaneous contexts open at all times. When a packet or a data storm occurs, the packet rate increases above the stated required maximum. In such cases, limited data loss occurs in arbitrary places in the data pipeline of the router.

The purpose of the Overload Protection Management (OPM) feature is to monitor the following parameters and to inform registered applications (OPM clients) when any of the parameters meet or exceed the configured threshold.

- CPU utilizations
- Memory utilization
- Queue drop

The registered applications limit their activity during overload conditions, thereby preventing potential data loss.

NOTICE: In the initial release of the OPM, queue drops are accumulated for Ethernet ports only.

The initial release of the OPM supports the following two clients: GGSN and SNMP.

The OPM thresholds for each of the monitored parameters can be set to high, medium, or low. Each threshold level (high, medium, or low) is associated with internally configured high-water and low-water marks. OPM clients are called when either of the following events occurs:

- Overload – The parameter meets or exceeds the high-water mark associated with the specified threshold level (high, medium, or low).
- Normal – The parameter falls below the low-water mark associated with the specified threshold level (high, medium, or low).

NOTICE: The EOS implementation of overload protection management incorporates a 30-second Holddown timer, which prevents the gateway from entering or leaving Overload within that time period. For example, if a gateway enters Overload state at 3:30:15, the Holddown timer starts and the gateway cannot exit Overload state until the 30-second Holddown period expires (in this example, at 3:30:45).

The registered GGSN application takes the following appropriate actions when it discovers an overload:

- Reads the number of active PDP contexts (GTP tunnels)
- Freezes the number of active contexts at that value
- Rejects any new context creates until one of the following scenarios occurs:
  - An existing context is dropped when one new context is created for every existing context create.

    NOTICE: The maximum configurations of contexts created is 65,535. When no limit is configured, the default limit is 20,000.

  - A received normal event indicates that the monitored parameter falls below the low-water mark associated with the configured threshold.
- Sends a trap when it receives an Overload or a Normal event

Overload Protection Configuration

To activate the overload protection using Unified Network Configurator (UNC), see the “Managing GGSN Router Statistics” section in the *Unified Network Configurator User Guide*.

Overload Protection Statistics Retrieval

You can retrieve the following overload protection statistics:

- CPU Utilization – The current value for CPU utilization.
- Memory Usage – The current value for memory usage.
- Queue Drops – The current value for queue drops.

- The number of times the router has gone into Overload state.
- A log of the last five times the router went into Overload state, including the following information:
  - Start Time – The time at which the router went into Overload state.
  - End Time – The time at which the router exited the Overload state.
  - Duration – The amount of time the router was in the Overload state.
  - Cause In – The reason why the router went into the Overload state (CPU utilization, memory usage, or queue drops).
  - Cause Out – The reason why the router exited the Overload state (CPU utilization, memory usage, or queue drops).

For information on how to manage the overload protection statistics in the Unified Network Configurator (UNC), see the “Managing GGSN Router Statistics” section in the *Unified Network Configurator User Guide*.

3.4.4 GGSN Gateway (L Zone Core) – Operation

This topic provides user operation procedures for working with Access Point Number (APN) information and viewing statistics for the GGSN.

View and Edit Existing APNs

To view and edit existing GGSN parameters, see the “GGSN Router Configuration File Management” section in the *Unified Network Configurator User Guide*.

View Statistics

You can gather and display the following GGSN GTP statistics:

GTP Peer IP Address
The IP address of the GTP tunnel peer.

State
The operational status of the GTP tunnel (UP or DOWN).

Number of PDP Contexts
The currently configured maximum number of PDP contexts supported on the GGSN gateway.

Received Control Packets
The total number of control packets received from all IV&D, HPD, or Conv PDGs (Packet Data Gateways).

Sent Control Packets
The total number of control packets sent to any CEN.

Received Data Packets
The total number of data packets received from all IV&D, HPD, or Conv PDGs

Received Data Bytes
The total number of data bytes received from all IV&D, HPD, or Conv PDGs

Sent Data Packets
The total number of data packets sent to any CEN.

Sent Data Bytes
The total number of data bytes sent to any CEN.

Mobile IP Services
The total number of mobile node registrations sent from all Conv PDGs and received by any CEN.

APN Statistics

You can gather and display statistics for APN. To view APN statistics, see “Showing APN and RADIUS Statistics” in the *Unified Network Configurator User Guide*.

CEN Statistics for User Data

Sent Packets
The total number of packets sent to CEN through this APN

Rcvd Packets
The total number of packets received from CEN through this APN

Sent Bytes
The total number of bytes sent to CEN through this APN

Rcvd Bytes
The total number of bytes received from CEN through this APN

CEN Statistics for DHCP

Sent DHCP Discover
The number of DHCP discover messages sent to the DHCP server in CEN

Rcvd DHCP Offer
The number of DHCP offer messages received from the DHCP server in CEN.

Sent DHCP Req
The number of DHCP request messages sent to the DHCP server in CEN

Rcvd DHCP Ack
The number of DHCP Ack messages received from the DHCP server in CEN

Sent DHCP Release
The number of DHCP release messages sent to the DHCP server in CEN

Rcvd DHCP Rsp Err
The number of received DHCP response messages indicating an error

DHCP Discover Timeout
The number of DHCP discover messages that were retransmitted and eventually timed out

DHCP Req Timeout
The number of DHCP request messages that were retransmitted and eventually timed out

DHCP Switchover
The number of switchovers from primary to secondary or secondary to primary DHCP servers

DHCP
The IP address of the current external DHCP server

RADIUS Auth.
The IP address of the current RADIUS authentication server

RADIUS Acct.
The IP address of the current RADIUS accounting server

Authentication Statistics

Switchovers
The number of switchovers from primary to secondary or secondary to primary RADIUS authentication servers

Accepts
The number of authentication accept messages received from the RADIUS server

Rejects
The number of authentication reject messages received from the RADIUS server

Timeout
The number of context creation failures caused by authentication timeout

Retries
The number of authentication message retransmissions

Max RoundTrip
The maximum response time from the first authentication request message to the time when the response is received. It may include retransmissions.

Accounting Statistics

Switchovers
The number of switchovers from primary to secondary or secondary to primary RADIUS accounting servers

Success
The number of accounting start response messages received from the RADIUS server

Failure
The number of failures on the accounting start response messages received from the RADIUS server

Timeout
The number of timeouts on accounting start response messages

Duplicated IP
The number of RADIUS-allocated IP addresses, which are duplicated in the GGSN gateway

Max RoundTrip
The maximum response time from the first accounting start response message to the time when the start response is received. It may include retransmissions.

High Availability Statistics

Real Time Contexts Sent to Standby
The number of contexts that the Master GGSN sends to the StandBy GGSN

Number of Times Peer Came Up
A counter that increments after port 1 of the peer GGSN comes back **UP** after being disabled

Number of Times Peer Went Down
A counter that increments after port 1 of the peer GGSN goes **DOWN**

Number of HA Switchovers
This counter increments every time the HA vrrp Mastership gets switched from the Master GGSN to StandBy GGSN and reverse

3.4.5 GGSN Gateway (L Zone Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

3.4.5.1 General Troubleshooting for the GGSN (L Zone Core)

If there is a failure on the GPRS Gateway Support Node (GGSN) gateway, the system loses the ability to provide data messaging from your data network to the mobile data devices in your system, all IP services are dropped. When a GGSN router fails, the Packet Data Router (which this gateway interfaces to) sends “link down” status information to the Unified Event Manger (UEM) server in that zone. The GGSN Link object in the UEM displays the reported status of the logical link between the PDR and the GGSN gateway.

If Dynamic System Resilience (DSR) is implemented on your system, the gateways support multiple IPIP tunnels per APN for redundancy. This feature supports the GGSN Dynamic System Resilience feature. APN to multiple IPIP binding allows the system to support DSR to multiple Customer Enterprise Networks (CENs). When the link for one of the tunnels fails, the gateways switches over to the other IPIP tunnel, thereby preserving connectivity between the GGSN and the CEN.

NOTICE: Multiple IPIP tunnels are supported only for redundancy, and only one tunnel is active at a time.

To bind an APN to multiple IPIP tunnels, a bidirectional forwarding detection (BFD) gateway IP address (the IP address of the border router) and a priority value for each tunnel is specified when the APN is configured in the UNC. BFD maintains the link status for each tunnel and informs the GGSN software when a link comes up or goes down. When the GGSN receives a status change notification, the GGSN transparently uses the active IPIP tunnel with the highest priority value to connect to the CEN. If that tunnel fails, the GGSN switches over to the other IPIP tunnel until the higher priority link is re-established.

The GGSN sends an alarm to the UEM both when the GGSN connection to the CEN has been established and when the GGSN connection to the CEN goes down.

The data port (V1) on the GGSN has a static IP address and does not send any SNMP traps to the UEM.

For more information on the operation of the UEM, a list of devices managed by the UEM, and alarms managed by the UEM, see the *Unified Event Manager User Guide*.

If High Availability (HA) Data is configured in your system, GGSNs are deployed as a redundant pair. If the active GGSN experiences a failure which makes it unable to provide data service, the redundant GGSN becomes active. Data service is restored within 90 seconds of the failure. In this configuration, the gateways support multiple paths (two for HA Data, four for HA Data with DSR) to the Customer Enterprise Networks (CENs). When the active path to the CEN fails, the gateways switch over to the next highest priority path. For more information about the HA Data feature and for a failure and recovery scenario of GGSN HA Data subsystem gateways, see the *Trunked Data Services Feature Guide*.

Chapter 4

ASTRO 25 Repeater Site

This chapter provides information about the GGM 8000 transport gateway at an ASTRO® 25 Repeater Site.

At an ASTRO® 25 Repeater Site, GGM 8000 operates as a Repeater Site Gateway. It can be used as a replacement for the following S2500 routers:

- Site Router
- Repeater Site Router
- Remote Site Router

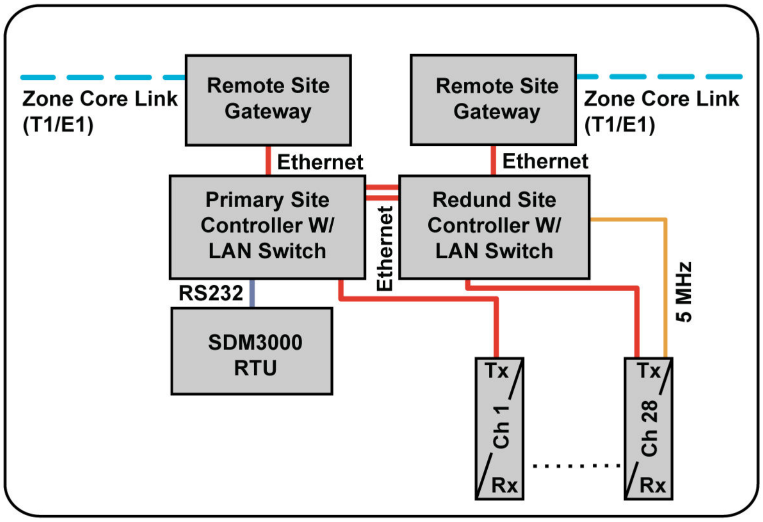
NOTICE: The ASTRO® 25 Repeater Site supports trunking and conventional channel operation. For details regarding the GGM 8000 Conventional Channel Gateway devices that support conventional channels, see ASTRO 25 Conventional Subsystem Architectures on page 234.

4.1 Repeater Site Gateway – Functional Description

The Repeater Site Gateway is used to provide connectivity from the LAN to the master site zone controller, zone manager, Network Management servers, and MOSCAD equipment. Depending on the configuration, one or two Repeater Site Gateways can be used (with one or two site links).

The following figure shows the Repeater Site Gateway.

Figure 90: Repeater Site Gateway



S_ASTRO_25_Repeater_Site_Gateway_D

4.1.1 Hybrid Site Link Overview

The Hybrid Site Links configuration is a flexible way of connecting a redundant zone core to redundant remote sites in ASTRO® 25 systems.

The Hybrid Site Links configuration allows redundant connections between the zone core and a remote site by using different connection types. Before the introduction of this configuration, the primary and redundant site links had to be of the same type, either E1/T1 or Ethernet links. This configuration enables mixing of E1/T1 and Ethernet site links, where the primary could be an E1/T1 and the secondary could be an Ethernet link, or an Ethernet link as the primary or E1/T1 as the secondary link.

Hybrid site links are available in the M2 and M3 system configurations with Dynamic System Resilience (DSR), and M3 system configuration without DSR. The Hybrid Site Links configuration connects redundant zone cores to the following remote sites:

- ASTRO® 25 Repeater Site (ISR)
- IP Simulcast Prime Site
- Network Manager/Dispatch Console Site (MCC 7100/MCC 7500E/MCC 7500 VPM Dispatch Consoles only)
- Conventional-only Site (Centralized Conventional Architecture)

The hybrid links support flexible transport types by employing transport devices such as redundant GGM 8000 site gateways and S6000 core routers. The transport between a primary core router and primary site gateway, or a secondary core router and secondary site gateway within the same site must be either of the T1/E1-to-T1/E1 or Ethernet-to-Ethernet transport type. For sites that require more than one T1/E bandwidth, the Hybrid Site Links configuration supports up to two T1/E1 links bundled together.

A site gateway supports one connection type, either redundant Ethernet or T1/E1 WAN terminations. A core router can support T1/E1 terminations for some sites and Ethernet terminations for other sites.

NOTICE: The GGM 8000 replaces the MNR S6000 for all Ethernet configurations; all T1/E1 configurations require an MNR S6000.

For more information regarding S6000 core routers, see the *S6000 and S2500 Routers Feature Guide*.

For more information about GGM 8000 site gateway transport devices, see the *RF Site Technician Reference Guide* webhelp.

4.1.2 Repeater Site Gateway – Modules Used

The Repeater Site Gateway can be used as an alternative to the S2500 Remote Site Router with ST 2511 FlexWAN module installed typically at a Circuit Simulcast Remote Site or a Trunked Repeater Site where colocated mutual aid channels reside. In such configurations, the Repeater Site Gateway is equipped with a FlexWAN module which provides a single 60-pin serial port which provides V.35 connectivity.

NOTICE: The S2500 Remote Site Router with the ST 2511 FlexWAN (V.35 serial interface) module supporting ASTRO® 25 Trunked Repeater Sites or Circuit Simulcast Remote Sites with mutual aid channels is replaced with the Site Gateway (FlexWAN) device.

For more information about the FlexWAN module, refer to Expansion Module on page 33.

4.2 Repeater Site Gateway – Installation

When and where to use: Follow this process to install the Repeater Site Gateway.

Process:

1. Install the Repeater Site Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Repeater Site Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Repeater Site Gateway(s). See Connecting a Chassis Ground on page 68.

4 Connect the repeater site equipment to the Repeater Site Gateway(s). See one of the following tables in section Repeater Site Gateway – Site-Specific Cabling on page 191:

- For single Repeater Site Gateway configuration, see Table 44: Repeater Site Gateway Cabling on page 191.
- For dual Repeater Site Gateway configuration, see Table 45: Dual Repeater Site Gateway Cabling on page 191.

5 Configure the Repeater Site Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

4.2.1 Repeater Site Gateway – Site-Specific Cabling

The following table lists cabling for a single Repeater Site Gateway configuration.

Table 44: Repeater Site Gateway Cabling

Site Gateway	Port	Device/Function
Repeater Site Gateway 1	LAN 1	Site LAN Switch
	T1/E1 5A	This T1/E1 link connects the repeater site through the Repeater Site Gateway to the master site.
	RS-232	Terminal Server or Local Serial Access

The following table lists cabling for a dual Repeater Site Gateway configuration.

Table 45: Dual Repeater Site Gateway Cabling

Site Gateway	Port	Device/Function
Repeater Site Gateway 1	LAN 1	Site LAN Switch
	T1/E1 5A	This T1/E1 link connects the repeater site through the Repeater Site Gateway to the master site.
	RS-232	Terminal Server or Local Serial Access
Repeater Site Gateway 2	LAN 1	Site LAN Switch (redundant link)
	T1/E1 5A	This redundant T1/E1 link connects the repeater site through the Repeater Site Gateway to the master site.
	RS-232	Terminal Server or Local Serial Access

NOTICE: For Expandable Site Subsystem, see the GGM 8000 Gateway cabling in the *RF Site Technician Reference Guide*.

If the Dynamic System Resilience feature is implemented on your system, there are two options for the Repeater Site Gateway setup. The site can be set up to benefit from the zone core redundancy afforded by DSR, or designed to connect to one zone core only as in systems without DSR.

- If the site is set up not to use DSR, the connections are made from the Repeater Site Gateway(s) to one zone core only.
- If the site is set up to use DSR, the connections are made to both primary and backup zone cores – additional T1/E1 connection needs to be established from the repeater site to the backup core.

4.3 Repeater Site Gateway – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

4.4 Repeater Site Gateway – Operation

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

4.5 Repeater Site Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

4.5.1 Repeater Site Gateway – Failures

Depending on the configuration, a Repeater Site Gateway failure can have different connotations:

- Single Repeater Site Gateway configuration – a failure of a single gateway causes failure of both zone controller and RF site controller paths and, in turn, forces the site into Site Trunking mode.
- Dual Repeater Site Gateway configuration – the site remains in wide area trunking mode if one of the two gateways fails or one of the links to the master site through any of these gateways fails.

Chapter 5

ASTRO 25 HPD Site

This chapter provides information about the GGM 8000 transport gateway in an ASTRO® 25 system HPD Site.

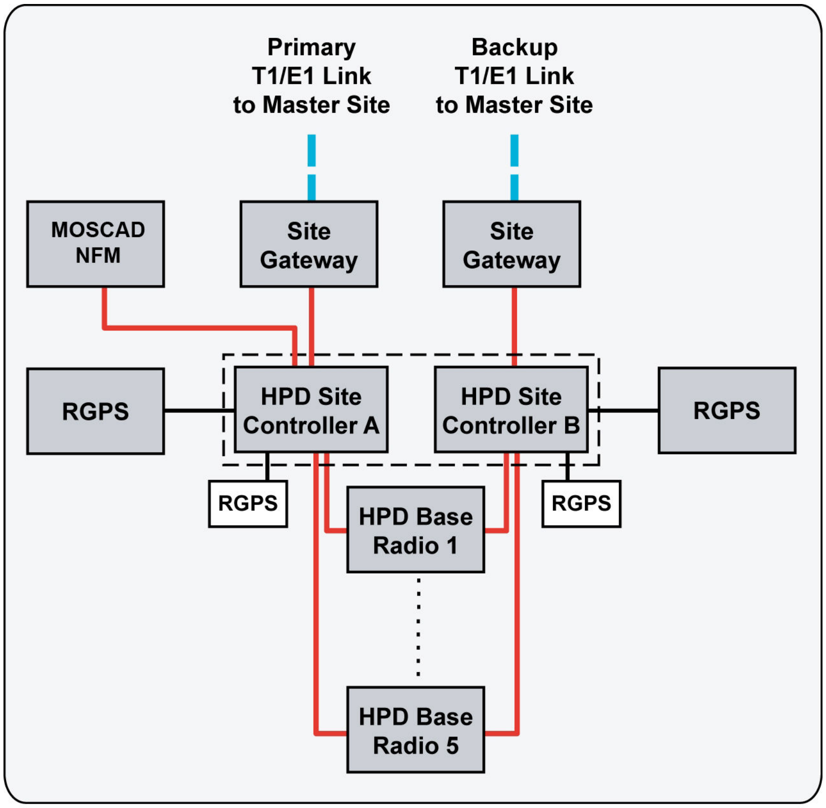
5.1 Site Gateway (HPD) – Functional Description

At an ASTRO® 25 system High Performance Data (HPD) site, the GGM 8000 operates as a Site Gateway.

The Site Gateway (HPD) is used to route all traffic between the equipment at the HPD remote site and the Cooperative WAN Routing (CWR) system at the master site. Depending on the configuration, an additional redundant HPD Site Gateway can be installed, but only a single path is active at all times.

The following diagram shows the Site Gateways at the HPD Remote Site.

Figure 91: Site Gateways (HPD)



S_HPD_Remote_site_gateway_A

5.2 Site Gateway (HPD) – Modules Used

The following table lists the modules that the GGM 8000 can be equipped with when used as a Site Gateway (HPD).

Table 46: Site Gateway (HPD) Modules Used

Module	Function
E&M daughterboard (part of the analog/V.24 interface kit)	Necessary if IP-based analog conventional mutual aid stations are colocated at the site.
FlexWAN daughterboard	Necessary if the GGM 8000 is used for mutual aid configurations.

5.3 Site Gateway (HPD) – Installation

When and where to use: Follow this process to install the HPD Site Gateway(s).

Process:

1. Install the Site Gateway(s) (HPD) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Site Gateway(s) (HPD) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Site Gateway(s) (HPD). See Connecting a Chassis Ground on page 68.
4. Connect the repeater site equipment to the Site Gateway(s) (HPD). See Site Gateway (HPD) – Site-Specific Cabling on page 194.
5. Configure the Site Gateway(s) (HPD). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

5.3.1 Site Gateway (HPD) – Site-Specific Cabling

The following table shows generic Site Gateway (HPD) cabling.

Table 47: HPD Site Gateway Connections

Site Gateway	Port	Device/Function	Description
Primary Site Gateway	LAN 1	HPD Site Controller A	If a standalone site controller is at the site, then the connection is made to the router port on the Site Controller A module on its internal switch. If a GTR 8000 Site Subsystem or GTR 8000 Expandable Site Subsystem is being used at the site, then this connection is to the router A port on the junction panel.
	T1/E1 5A	Primary Site Link	Connection to the site link (or CSU/DSU).

Site Gateway	Port	Device/Function	Description
	4W ports (8A-8D)	Conventional base station (optional)	If IP-based analog conventional mutual aid stations are colocated at the site, up to four stations may be connected to an optional analog 4-wire E&M module.
	FlexWAN	Channel bank (optional)	If circuit-based mutual aid equipment is located at the site, then a V.35 FlexWAN connection can be made to a channel bank to support the circuit-based equipment.
Secondary Site Gateway (optional)	LAN 1	HPD Site Controller B	The secondary site gateway and its connections are only required if redundant site links are installed at the site. • If a standalone site controller is at the site, then the connection is made to the Router port on the Site Controller B module on its internal switch. • If a GTR 8000 Site Subsystem or GTR 8000 Expandable Site Subsystem is being used at the site, then this connection is to the Router B port on the junction panel.
	T1/E1 5A	Backup Site Link	Connection to the secondary/backup site link (or CSU/DSU).
	4W ports (8A-8D)	Conventional base station	If IP-based analog conventional mutual aid stations are colocated at the site, up to four stations may be connected to an optional analog 4-wire E&M module.

If the Dynamic System Resilience (DSR) feature is implemented on your system, there are two options for the Site Gateway setup. The site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience, or designed to connect to one zone core only as in systems without Dynamic System Resilience:

- If the site is set up not to use DSR, the connections are made from the Site Gateway(s) to one zone core only.
- If the site is set up to use DSR, the connections are made to both primary and backup zone cores — additional T1/E1 connection needs to be established from the HPD site to the backup core.

For details about the Dynamic System Resilience feature, see the *Dynamic System Resilience Feature Guide* manual.

5.4 Site Gateway (HPD) – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

5.5

Site Gateway (HPD) – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

5.6

Site Gateway (HPD) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

5.6.1

Site Gateway (HPD) – Failures

Depending on the configuration, a Site Gateway (HPD) failure can have different connotations:

- Single Site Gateway (HPD) configuration – a failure of a single gateway causes failure of both zone controller and RF site controller paths and, in turn, forces the site into Site Trunking mode.
- Dual Site Gateways (HPD) configuration – thanks to the redundant gateway, if a failure occurs on the active path (or the primary site controller fails), then the system can revert to the standby path.

Chapter 6

ASTRO 25 Dispatch Console Subsystem

This chapter provides information about the GGM 8000 transport gateway in an ASTRO® 25 system Dispatch Console subsystem.

6.1

Site Gateway (Console Site) – Functional Description

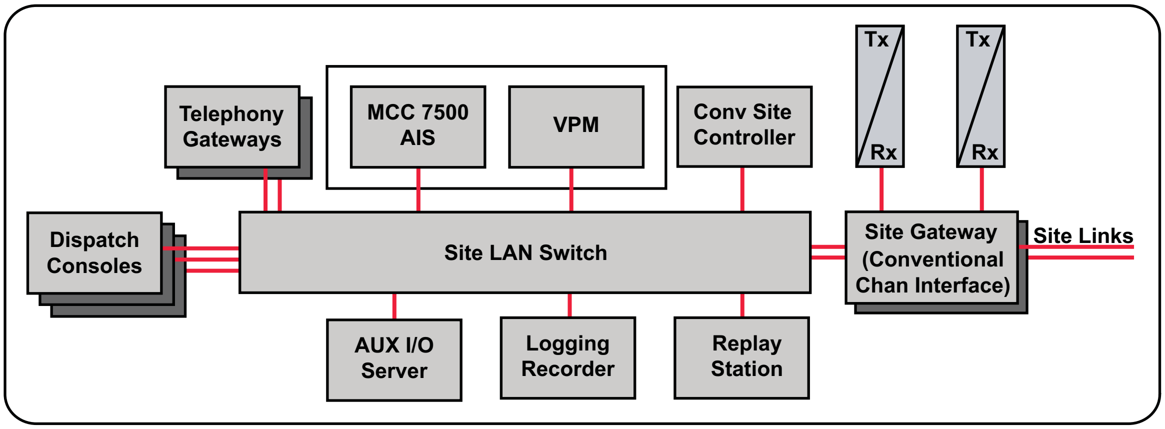
At ASTRO® 25 system console sites, the GGM 8000 operates as the Site Gateway (Console Site). It can be used as a replacement for the following S2500 routers:

- Dispatch Site Router
- Dispatch Console Site Router
- Console Site Router
- NM/Dispatch Site Router

The Dispatch Site Gateway provides a network interface for the flow of voice, control, data, and Network Management traffic. It also serves as the Ethernet transport interface to the Ethernet backbone on systems that implement the Flexible Ethernet Links feature.

The following diagram shows the Site Gateway at a Console Site.

Figure 92: Site Gateway (Console Site)



DispatchConsole_Sub_wConvCh_AuxIO_B

NOTICE: If the Console Site implements hybrid redundant site links, T1/E1 can be employed for one site link while Ethernet can be employed for the other site link. See Hybrid Site Link Overview on page 189.

6.1.1

ACIM Interface

For information aboutACIM interface and ACIM conventional channels, see ACIM Interface on GGM 8000 on page 48.

6.1.2 GGM 8000 Conventional Channel Interface (CCGW)

For a console site supporting conventional channels, the GGM 8000 is available as a Conventional Channel Gateway (CCGW) interface in a variety of different hardware configurations. GGM 8000 CCGW supports various types of conventional channels in your system.

For more information about GGM 8000 CCGW, see Physical Description on page 30.

6.2 Site Gateway (Console Site) – Installation

When and where to use: Follow the process to install the Site Gateway (Console Site).

Process:

1. Install the Site Gateway (Console Site) in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Site Gateway (Console Site) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Site Gateway (Console Site). See Connecting a Chassis Ground on page 68.
4. Connect the console site equipment to the Site Gateway (Console Site). See Site Gateway (Console Site) – Site-Specific Cabling on page 198.

   NOTICE: For A3.1 Coexistence feature, see A3.1 Coexistence on page 266.
5. Configure the Site Gateway(s) (Console Site). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

6.2.1 Site Gateway (Console Site) – Site-Specific Cabling

The following table presents Site Gateway (Console Site) cabling.

Table 48: Site Gateway (Console Site) Cabling

Gateway	Port	Device/Function
Site Gateway (Console Site)	LAN 1–3	Console Site LAN Switch, Ethernet Site Links, Colocated Base Radios
	T1/E1 5A	T1/E1 Relay Panel(s) — site links to the zone core
	T1/E1 5B (optional)	T1/E1 Relay Panel(s) — optional redundant site links to the backup core in DSR systems
	RS-232	Terminal Server or Local Serial Access

If your system implements the Dynamic System Resilience (DSR) feature, the dispatch console subsystem is designed to continue to function despite a failure of its primary zone core. In the event of a primary core failure, the dispatch console switches over to use the services provided by the backup zone core.

6.2.1.1 A3.1 Coexistence

For A3.1 Coexistence feature information, see A3.1 Coexistence on page 266.

6.3 Site Gateway (Console Site) – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

6.4 Site Gateway (Console Site) – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

6.5 Site Gateway (Console Site) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

6.5.1 Dispatch Core Gateway – Failures

A failure of the Site Gateway (Console Site) means the connectivity of the console site with the zone core is lost.

Chapter 7

ASTRO 25 IP Simulcast Subsystem

This chapter provides information about the GGM 8000 transport gateway in an ASTRO® 25 IP Simulcast subsystem.

The GGM 8000 Gateway can be used as a Site Gateway replacing the following S2500 and S6000 routers:

- IP Simulcast Prime Site Router
- IP Simulcast Remote Site Router
- IP Simulcast Remote Site Access Router (Ethernet link only)

NOTICE: The ASTRO® 25 IP Simulcast Subsystem can support Trunked Simulcast or Conventional Voting/Multicast/Simulcast or Conventional only Voting/Multicast/Simulcast subsystems for trunking and conventional channel operation. The GGM 8000 is available as a Conventional Channel Gateway (CCGW) interface device in a variety of different hardware configurations to support various types of conventional channels in your system. See Conventional Channel Gateway – Supported Channels and Sites on page 46.

7.1 IP Simulcast Subsystem – Site Gateway General Installation

When and where to use: Follow this process to install any Site Gateway in an IP Simulcast subsystem.

Process:

1. If needed, install the analog/V.24 interface kit to the GGM 8000. See Replacing Daughterboards on the GGM 8000 on page 129 for installation details.

   NOTICE: By default, if the GGM 8000 Gateway is ordered with the analog/V.24 interface kit, the kit will be mounted at the factory.

2. Install the Site Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
3. Connect the Site Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
4. If necessary, ground the Site Gateway. See Connecting a Chassis Ground on page 68.
5. Connect the site equipment to the Site Gateway. See one of the following:
   - Site Gateway (IP Simulcast Prime Site) – Installation on page 202
   - IP Simulcast Remote Site Gateway – Installation on page 205
   - Remote Site Access Gateway – Installation on page 208
6. Configure the Site Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

   IMPORTANT: The last 3 steps of Downloading a Stored Configuration File to the GGM 8000 on page 93 do not apply to configurations without the UNC application.

Postrequisites:
For details on specific information pertaining to each Site Gateway, refer to the individual sections:

- Site Gateway (IP Simulcast Prime Site) on page 201

- IP Simulcast Remote Site Gateway on page 204
- Remote Site Access Gateway on page 206

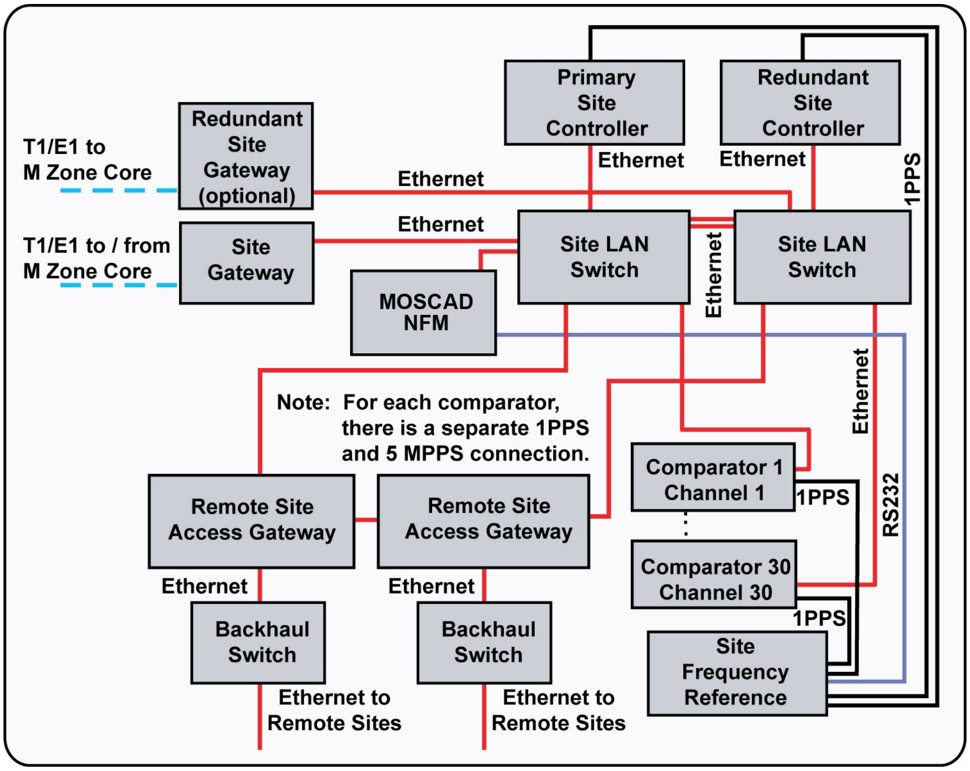
7.2

Site Gateway (IP Simulcast Prime Site)

The Site Gateway (IP Simulcast Prime Site) handles the traffic between the prime site network and the master site. It distributes voice, control, and Network Management traffic to the appropriate devices on the prime site network.

The following diagram shows the Site Gateway at the IP Simulcast Prime Site.

Figure 93: GGM 8000 Gateway in the IP Simulcast Prime Site

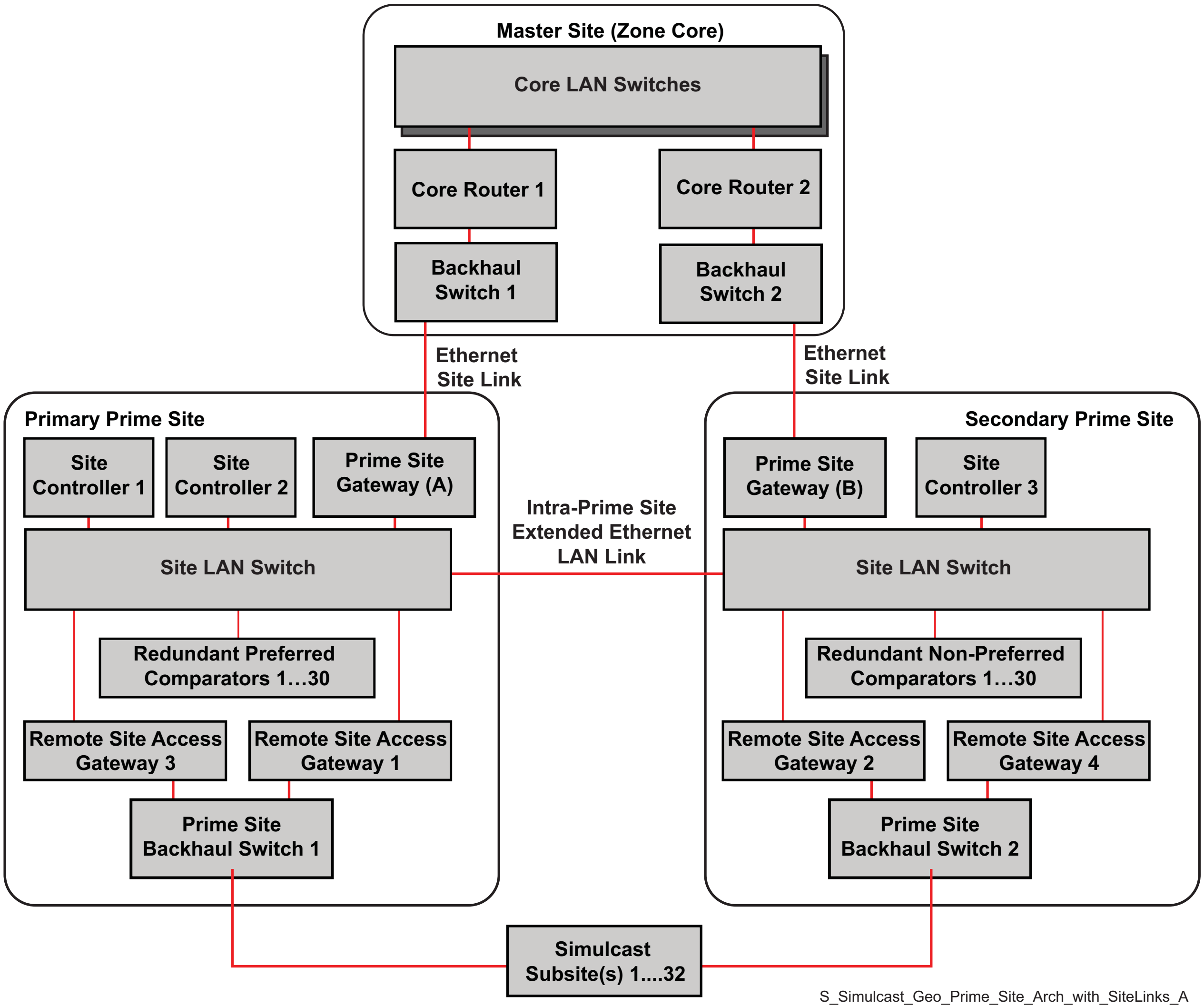


S_IP_Prime_Site_Ethernet_Remote_Site_Link_A

NOTICE:

- The Site Gateway supports T1/E1 or Ethernet links between the prime site and the zone core.
- The Site Gateway supports a T1 link from the prime site to the zone core for two or less T1 connections. For three or more T1 connections, the S6000 router must be used instead.

Figure 94: GGM 8000 Gateway in an IP Simulcast Geographically Redundant Prime Site


Master Site (Zone Core)
Core LAN Switches
Core Router 1
Core Router 2
Backhaul Switch 1
Backhaul Switch 2
Ethernet Site Link
Ethernet Site Link
Primary Prime Site
Site Controller 1
Site Controller 2
Prime Site Gateway (A)
Site LAN Switch
Intra-Prime Site Extended Ethernet LAN Link
Secondary Prime Site
Prime Site Gateway (B)
Site Controller 3
Site LAN Switch
Redundant Preferred Comparators 1…30
Redundant Non-Preferred Comparators 1…30
Remote Site Access Gateway 3
Remote Site Access Gateway 1
Remote Site Access Gateway 2
Remote Site Access Gateway 4
Prime Site Backhaul Switch 1
Prime Site Backhaul Switch 2
Simulcast Subsite(s) 1....32

S_Simulcast_Geo_Prime_Site_Arch_with_SiteLinks_A

NOTICE:

- The Site Gateway supports Ethernet links only in a Geographically Redundant Prime Site.
- The Site Gateway is configured to support Ethernet site link statistics for the Intra-Prime Site link between the Primary Prime Site and the Secondary Prime Site when a Geographically Redundant Prime Site is implemented. See the *Flexible Site and InterZone Links Feature Guide* for “Ethernet Site Link Statistics – Transport Devices” and the *RF Site Technician Reference Guide* for information regarding the Geographically Redundant Prime Site architecture.

7.2.1 Site Gateway (IP Simulcast Prime Site) – Installation

NOTICE: For a general installation process, refer to IP Simulcast Subsystem – Site Gateway General Installation on page 200.

The following table lists the cable connections from the IP simulcast prime site gateway.

Table 49: Site Gateway (IP Simulcast Prime Site) Cabling Gateway Port Device/Function

Gateway	Port	Device/Function
Prime Site Gateway 1	LAN 1	Prime Site LAN Switch 1
	LAN 2	Not used
	LAN 3	Ethernet Site Links
	LAN 4	Not used
	T1/E1 5A	T1/E1 connection to the zone core (primary zone core if DSR)
	T1/E1 5B	T1/E1 connection to the zone core (Multi-link Frame Relay) (primary zone core if DSR)
	RS-232	Terminal Server or Local Serial Access
Prime Site Gateway 2 (load sharing, multi-case traffic)	LAN 1	Prime Site LAN Switch 2
	LAN 2	Not used
	LAN 3	Ethernet Site Links
	LAN 4	Not used
	T1/E1 5A	T1/E1 connection to the zone core (backup zone core if DSR)
	T1/E1 5B	T1/E1 connection to the zone core (Multi-Link Frame Relay) (backup zone core if DSR)
	RS-232	Terminal Server or Local Serial Access

NOTICE: At a prime site with two prime site gateways, both gateways are in service to support load sharing of multicast traffic.

The prime site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR, or designed to connect to one zone core only as in systems without DSR.

- If the prime site is set up not to use DSR, the connections are made from the site gateway(s) to one zone core only.
- If the prime site is set up to use DSR, the connections are made to both primary and backup zone cores.

NOTICE: Contact your system administrator or refer to your customized system configuration plan for prime site gateway port connections in a DSR scenario. For details about the Dynamic System Resilience feature, see also the *Dynamic System Resilience Feature Guide* manual.

If the Geographically Redundant Prime Site feature is present in the system, two prime site gateways are required: the Primary and Secondary Prime Site Gateway.

7.2.2 Site Gateway (IP Simulcast Prime Site) – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

7.2.3 Site Gateway (IP Simulcast Prime Site) – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

7.2.4 Site Gateway (IP Simulcast Prime Site) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

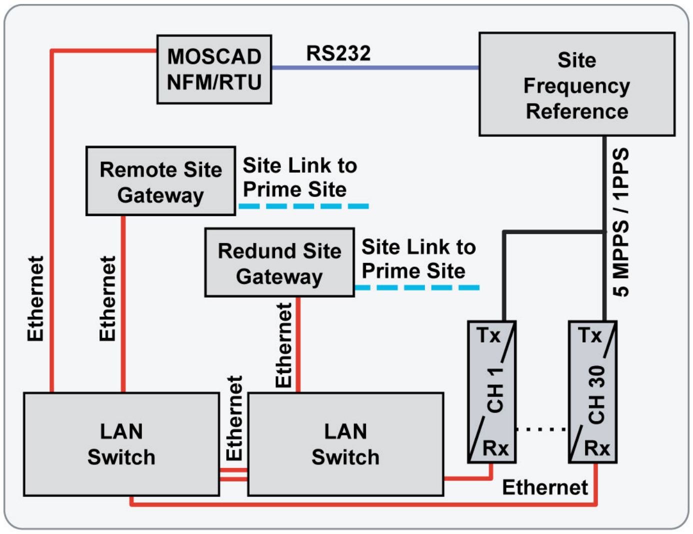
7.3 IP Simulcast Remote Site Gateway

The Site Gateway located at the IP Simulcast Remote Site provides the IP network routing interface between the remote site and the prime site.

In a simulcast remote site, the remote site gateway transports the site Network Management information to and from the Unified Network Configurator (UNC), Provisioning Manager, and MOSCAD Network Management servers. The Local Area Network (LAN) port is connected to the Ethernet switch where the base radio and MOSCAD RTU are also connected.

The following diagram shows the IP Simulcast Remote Site Gateway.

Figure 95: Remote Site Gateway



S_IP_Simul_Remote_Site_GGM8000

NOTICE: Ethernet site links are used for connecting to Geographically Redundant Prime Sites.

7.3.1
IP Simulcast Remote Site Gateway – Modules Used

The following table lists the modules that the GGM 8000 can be equipped with when used as an IP Simulcast Remote Site Gateway.

Table 50: IP Simulcast Remote Site Gateway – Modules Used

Module	Function
V.24 daughterboard (part of the analog/V.24 interface kit)	Necessary if the GGM 8000 is used as a Site Gateway (Digital Conventional Channel Interface)
Low Density Enhanced Conventional Channel Gateway module	Necessary if the GGM 8000 supports the Enhanced Conventional Gateway module
High Density Enhanced Conventional Channel Gateway module	
E&M daughterboard (part of the analog/V.24 interface kit)	Necessary if the GGM 8000 is used as a Site Gateway (Analog Conventional Channel Interface)
FlexWAN daughterboard	Necessary if the GGM 8000 is used for mutual aid configurations

7.3.2
IP Simulcast Remote Site Gateway – Installation

NOTICE: For a general installation process, go to IP Simulcast Subsystem – Site Gateway General Installation on page 200.

The following table shows cabling connections from the IP simulcast remote site gateway.

Table 51: IP Simulcast Remote Site Gateway Cabling

Gateway		Port	Device
IP Simulcast Remote Site Gateway Primary	Base module	LAN 1	Remote Site LAN Switch 1
		LAN 2	Not used
		T1/E1 5A	Remote Site Access Router
		LAN 3	Remote Site Access Router
		LAN 4	Not used
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire ports (8A-8D)	Analog Conventional Base Radios – used when the GGM 8000 operates as a Site Gateway (Analog Conventional Channel Interface)
		ASTRO (V.24 digital) ports (6A, 6B, 7A, 7B)	ASTRO Digital Conventional Base Radios – used when the GGM 8000 operates as a Site Gateway (Digital Conventional Channel Interface)

Gateway		Port	Device
IP Simulcast Remote Site Gateway Backup	Base module	LAN 1	Remote Site LAN Switch 2
		LAN 2	Not used
		T1/E1 5A	Remote Site Access Router
		LAN 3	Remote Site Access Router
		LAN 4	Not used
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire ports (8A-8D)	Analog Conventional Base Radios – used when the GGM 8000 operates as a Site Gateway (Analog Conventional Channel Interface)
		ASTRO (V.24 digital) ports (6A, 6B, 7A, 7B)	ASTRO Digital Conventional Base Radios – used when the GGM 8000 operates as a Site Gateway (Digital Conventional Channel Interface)
	FlexWAN module	FlexWAN	Channel Bank (remote site)

7.3.3 IP Simulcast Remote Site Gateway – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

7.3.4 IP Simulcast Remote Site Gateway – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

7.3.5 IP Simulcast Remote Site Gateway – Maintenance and Troubleshooting

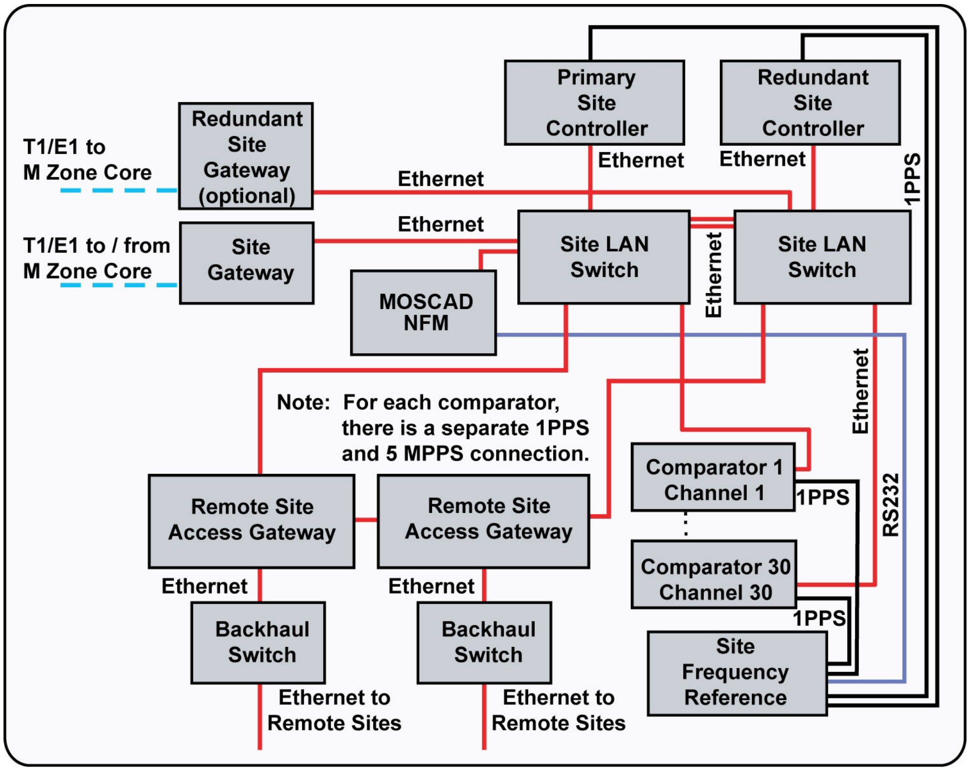
For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

7.4 Remote Site Access Gateway

The Remote Site Access Gateway located at the IP Simulcast Prime Site provides the IP network routing interface between the prime site and the remote site.

The following diagram shows the IP Simulcast Remote Site Access Gateway.

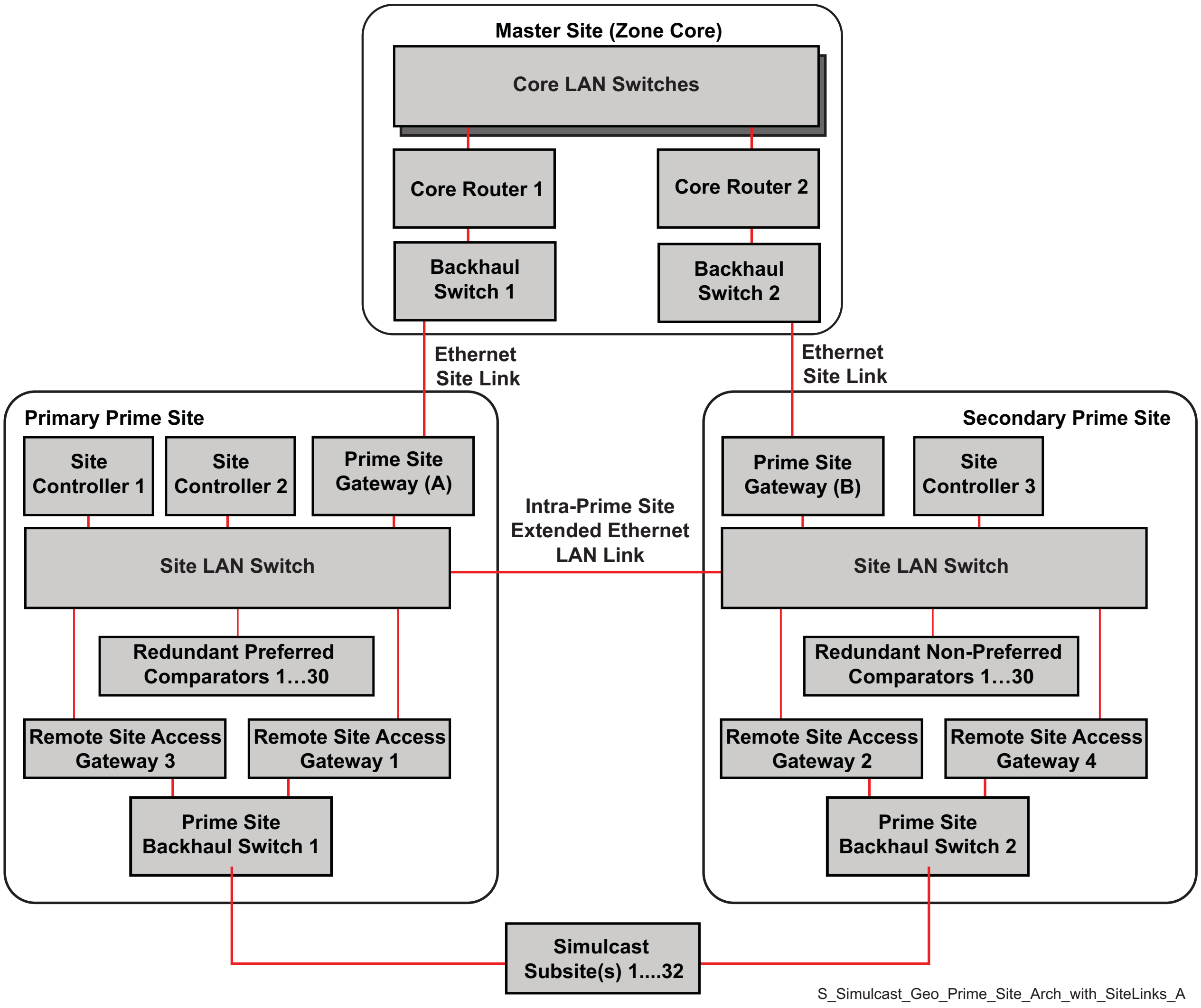
Figure 96: Remote Site Access Gateway



S_IP_Prime_Site_Ethernet_Remote_Site_Link_A

]

Figure 97: Remote Site Access Gateway (to Geographically Redundant Prime Sites)


Master Site (Zone Core)
Core LAN Switches
Core Router 1
Core Router 2
Backhaul Switch 1
Backhaul Switch 2
Ethernet Site Link
Ethernet Site Link
Primary Prime Site
Site Controller 1
Site Controller 2
Prime Site Gateway (A)
Intra-Prime Site Extended Ethernet LAN Link
Secondary Prime Site
Prime Site Gateway (B)
Site Controller 3
Site LAN Switch
Site LAN Switch
Redundant Preferred Comparators 1…30
Redundant Non-Preferred Comparators 1…30
Remote Site Access Gateway 3
Remote Site Access Gateway 1
Remote Site Access Gateway 2
Remote Site Access Gateway 4
Prime Site Backhaul Switch 1
Prime Site Backhaul Switch 2
Simulcast Subsite(s) 1....32
S_Simulcast_Geo_Prime_Site_Arch_with_SiteLinks_A

IMPORTANT: The Remote Site Access Gateway can be used with Ethernet links from the Prime Site to Remote Site only. The Remote Site Access Gateway cannot be used with T1/E1 links.

Increased Capacity

A standard configuration prime site with a 32 subsite capacity is the same as a standard configuration prime with a 15 subsite capacity, except there are three Ethernet LAN switches and an additional subsite access gateway pair at the prime site. Switches #1 and #2 are paired between the two subsite access gateway pairs and switch #3 is connected to both subsite access gateway pairs.

When using Ethernet links, each subsite access gateway is connected to a backhaul switch.

For more information regarding the IP Simulcast Prime Site, see the *RF Site Technician Reference Guide*.

7.4.1
Remote Site Access Gateway – Installation

NOTICE: For a general installation process, go to IP Simulcast Subsystem – Site Gateway General Installation on page 200.

The following table lists the remote site access gateway port connections for a single site link configuration for 15 subsites or less for a simulcast subsystem where the geographically redundant prime site feature is not implemented.

Table 52: Remote Site Access Gateway Port Connections for 15 Subsites or Less (Non-Geographically Redundant Prime Site)

Gateway	Port	Device/Function
Remote Site Access Gateway 1	LAN 1	Prime Site Switch 1
	LAN 2	Remote Site Access Gateway 2
	LAN 3	Backhaul Switch 1
	RS-232	Terminal Server or Local Serial Access
Remote Site Access Gateway 2	LAN 1	Prime Site Switch 2
	LAN 2	Remote Site Access Gateway 1
	LAN 3	Backhaul Switch 2
	RS-232	Terminal Server or Local Serial Access

The following table lists the remote site access gateway port connections for a prime site configured with more than 15 subsites where the geographically redundant prime site feature is not implemented.

Table 53: Remote Site Access Gateway Port Connections for Greater than 15 Subsites (Non-Geographically Redundant Prime Site)

Port	Destination
Remote Site Access Gateway 1	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 1
Remote Site Access Gateway 2	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 2
Remote Site Access Gateway 3	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 1
Remote Site Access Gateway 4	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 2

The following table lists the remote site access gateway port connections for the Primary Prime Site and Secondary Prime Site where the geographically redundant prime site feature is implemented.

Table 54: Remote Site Access Gateway Ports Connections (Geographically Redundant Prime Sites)

Port	Destination
	Remote Site Access Gateway 1
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
	Remote Site Access Gateway 2
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2
	Remote Site Access Gateway 3
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
	Remote Site Access Gateway 4
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

NOTICE: For implementation of a Geographically Redundant Prime Site, only Remote Site Access Gateways 1 and 2 are required to support 15 subsites or less. To support subsites greater than 15, additional Remote Site Access Gateways 3 and 4 are required.

7.4.2

Remote Site Access Gateway – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

7.4.3

Remote Site Access Gateway – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

7.4.4

Remote Site Access Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

Chapter 8

ASTRO 25 Trunking Subsystem

This chapter provides information about the GGM 8000 transport gateway in an ASTRO® 25 trunking subsystem.

The GGM 8000 Gateway can be used as a Site Gateway replacing the S6000 router:

- Prime Site Router
- Remote Site Access Router

NOTICE: The ASTRO® 25 trunking subsystem supports ASTRO 25® repeater sites and/or simulcast/voting subsystems, dispatch sites, and centralized conventional sites for trunking and conventional channel operation. The GGM 8000 is available as a Conventional Channel Gateway (CCGW) interface device in a variety of different hardware configurations to support various types of conventional channels in your system. See Conventional Channel Gateway – Supported Channels and Sites on page 46.

8.1

Trunking Subsystem - Site Gateway General Installation

When and where to use: Follow this process to install any Site Gateway in a trunking subsystem.

Procedure:

1. If needed, install the analog/V.24 interface kit to the GGM 8000. See Replacing Daughterboards on the GGM 8000 on page 129 for installation details.

   NOTICE: By default, if the GGM 8000 Gateway is ordered with the analog/V.24 interface kit, the kit will be mounted at the factory.

2. Install the Site Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
3. Connect the Site Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
4. If necessary, ground the Site Gateway. See Connecting a Chassis Ground on page 68.
5. Connect the site equipment to the Site Gateway. See one of the following:
   - Site Gateway (Trunking Subsystem Prime Site) – Installation on page 213
   - Remote Site Access Gateway (Trunking Subsystem Prime Site) – Installation on page 218
6. Configure the Site Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

   IMPORTANT: The last 3 steps of Downloading a Stored Configuration File to the GGM 8000 on page 93 do not apply to configurations without the UNC application.

Postrequisites:
For details on specific information pertaining to each Site Gateway, see the individual sections:

- Site Gateway (Trunking Subsystem Prime Site) on page 212
- Remote Site Access Gateway (Trunking Subsystem Prime Site) on page 215

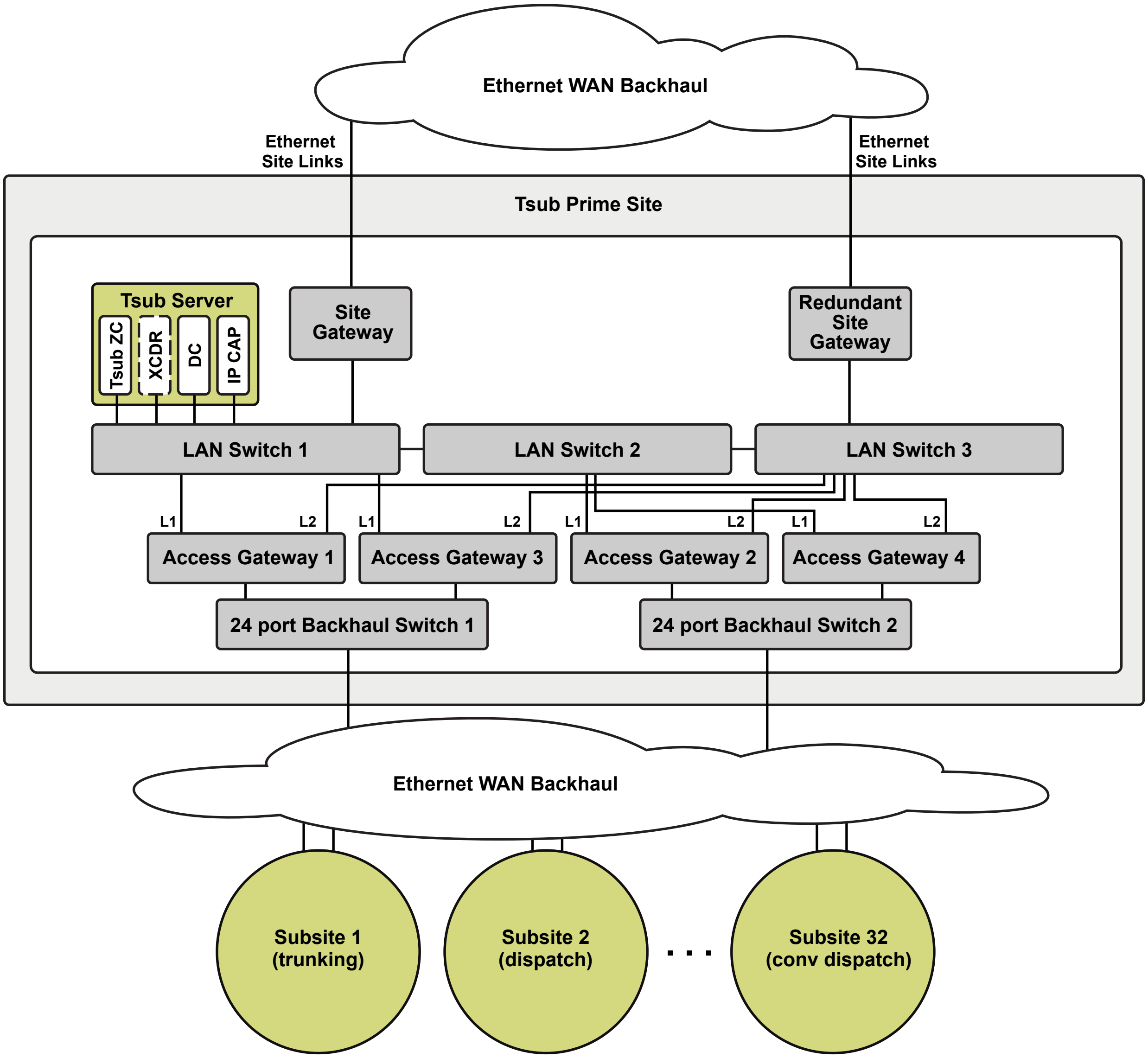
8.2
Site Gateway (Trunking Subsystem Prime Site)

The Site Gateway in a trunking subsystem prime site handles the traffic between the prime site network and the zone core using Ethernet links. The Site Gateway distributes voice, control, and Network Management traffic to the appropriate devices on the prime site network.

NOTICE: The Site Gateway does not support T1/E1 links in a trunking subsystem.

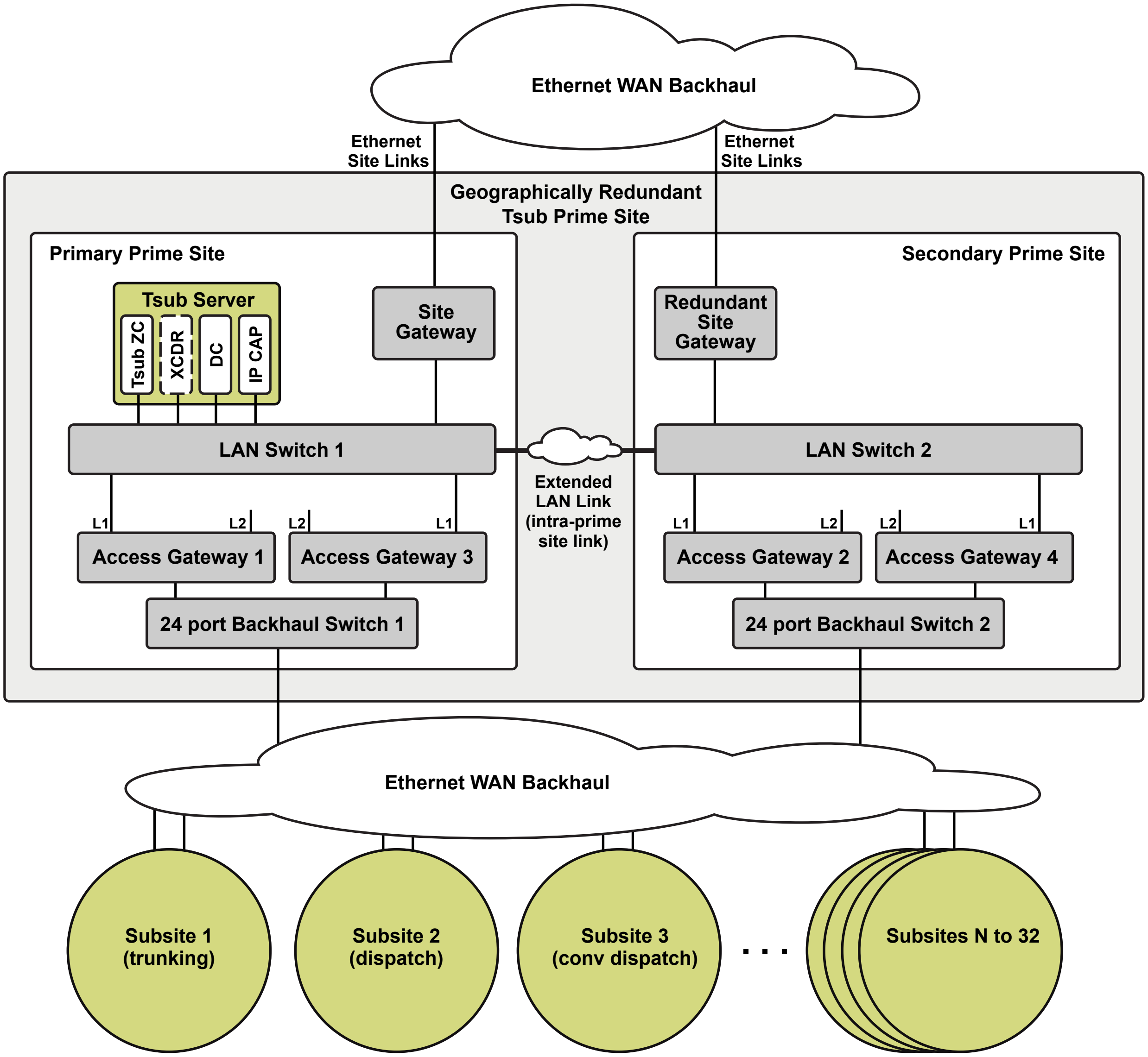
The following diagram shows the Site Gateway at a trunking subsystem prime site.

Figure 98: Site Gateway in a Trunking Subsystem Prime Site



S_Trunking_subsystem_prime_site_no_simulcast_E

Figure 99: Site Gateway in a Trunking Subsystem with Geographically Redundant Prime Site



S_Trunking_subsystem_redundancy_no_simulcast_E

NOTICE:

- See the *Flexible Site and InterZone Links Feature Guide* for “Ethernet Site Link Statistics – Transport Devices” and the *Edge Availability Feature Guide* for information regarding the Geographically Redundant Prime Site architecture.

8.2.1

Site Gateway (Trunking Subsystem Prime Site) – Installation

This section provides cabling information and the port connections.

NOTICE: For a general installation process, see Trunking Subsystem - Site Gateway General Installation on page 211.

The following table lists the cable connections from the trunking subsystem prime site gateway.

Table 55: Site Gateway (Trunking Subsystem Prime Site) Cabling Gateway Port Device/Function

Gateway	Port	Device/Function
Prime Site Gateway 1	LAN 1	Prime Site LAN Switch 1
	LAN 2	Not used
	LAN 3	Ethernet Site Links
	LAN 4	Not used
	RS-232	Terminal Server or Local Serial Access
Prime Site Gateway 2 (load sharing, multi-cast traffic)	LAN 1	Prime Site LAN Switch 2
	LAN 2	Not used
	LAN 3	Ethernet Site Links
	LAN 4	Not used
	RS-232	Terminal Server or Local Serial Access

NOTICE: At a prime site with two prime site gateways, both gateways are in service to support load sharing of multicast traffic.

There are two options for the prime site gateway setup. The prime site can be set up to benefit from the zone core redundancy afforded by Dynamic System Resilience (DSR), or designed to connect to one zone core only as in systems without DSR.

- If the prime site is set up not to use DSR, the connections are made from the site gateway(s) to one zone core only.
- If the prime site is set up to use DSR, the connections are made to both primary and backup zone cores.

NOTICE: Contact your system administrator or refer to your customized system configuration plan for prime site gateway port connections in a DSR scenario. For details about the Dynamic System Resilience feature, see also the *Dynamic System Resilience Feature Guide* manual.

If the Geographically Redundant Prime Site feature is present in the system, two prime site gateways are required: the Primary and Secondary Prime Site Gateway.

8.2.2 Site Gateway (Trunking Subsystem Prime Site) – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

8.2.3 Site Gateway (Trunking Subsystem Prime Site) – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

8.2.4 Site Gateway (Trunking Subsystem Prime Site) - Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

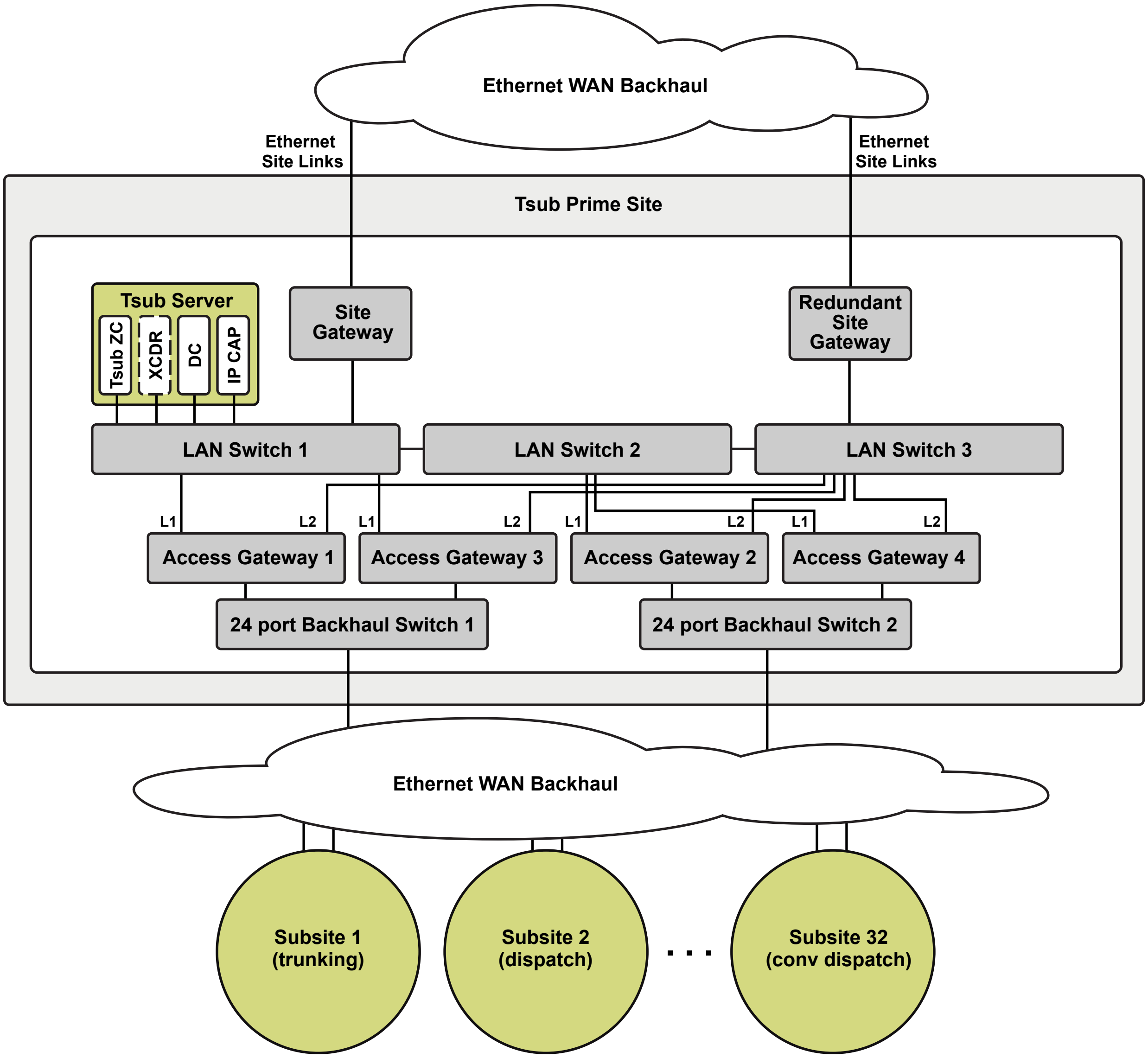
8.3 Remote Site Access Gateway (Trunking Subsystem Prime Site)

The Remote Site Access Gateway located at the trunking subsystem prime site provides the IP network routing interface between the prime site and the subsites using Ethernet links.

The following diagram shows the Trunking Subsystem Remote Site Access Gateway.

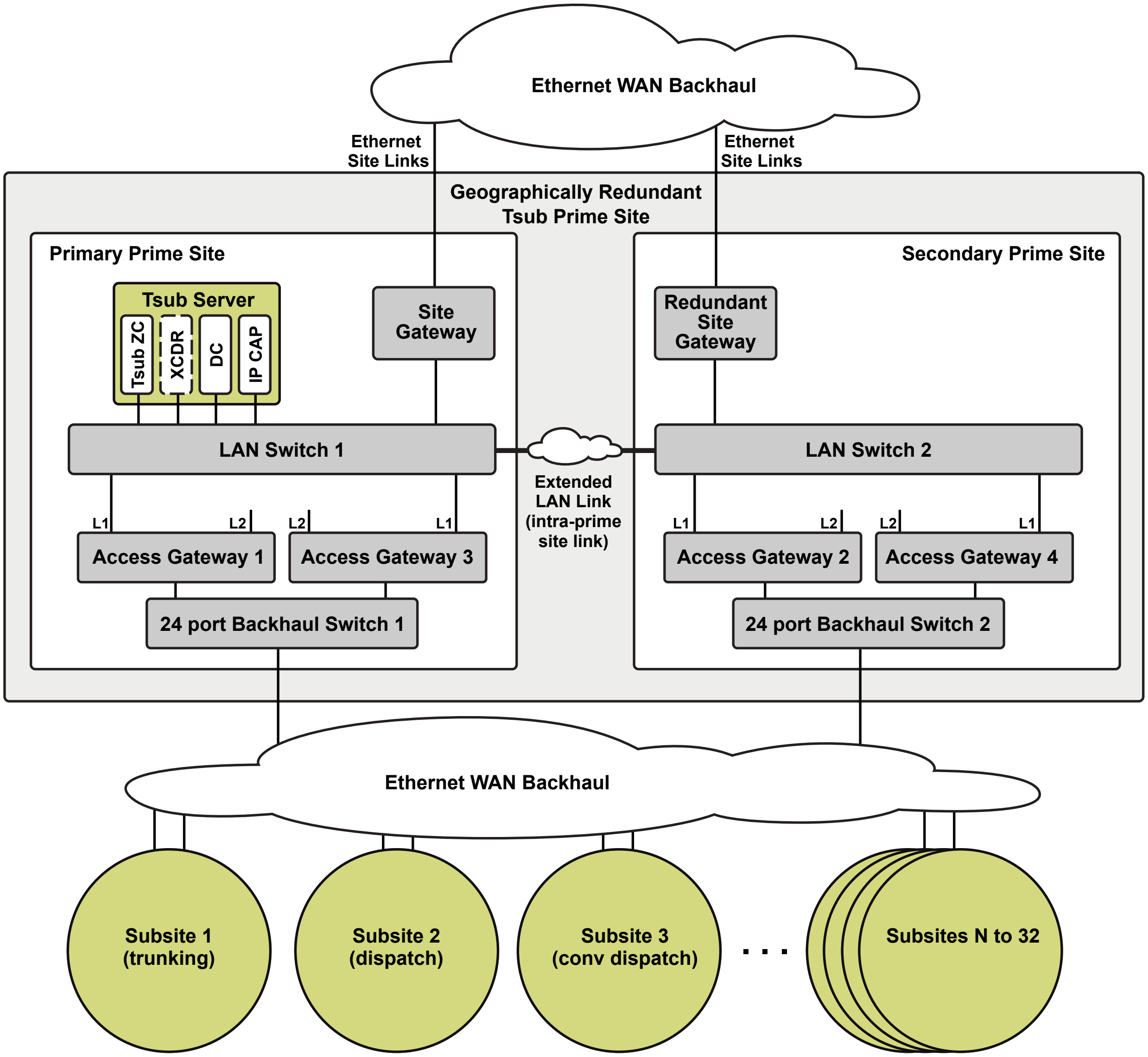
NOTICE: The remote site access site routers in the diagrams serve as the remote site access gateways.

Figure 100: Remote Site Access Gateway in a Trunking Subsystem Prime Site



S_Trunking_subsystem_prime_site_no_simulcast_E

Figure 101: Remote Site Access Gateway in a Trunking Subsystem with Geographically Redundant Prime Site



S_Trunking_subsystem_redundancy_no_simulcast_E

Increased Capacity

A standard configuration prime site with a 32 subsite capacity is the same as a standard configuration prime site with a 15 subsite capacity, except there are three Ethernet LAN switches and an additional subsite access gateway pair at the prime site. Switches #1 and #2 are paired between the two subsite access gateway pairs and switch #3 is connected to both subsite access gateway pairs.

When using Ethernet links, each subsite access gateway is connected to a backhaul switch.

For more information regarding the trunking subsystem prime site, see the *Edge Availability Feature Guide*.

8.3.1 Remote Site Access Gateway (Trunking Subsystem Prime Site) – Installation

This section provides cabling information and the port connections.

NOTICE: For a general installation process, go to Trunking Subsystem - Site Gateway General Installation on page 211.

The following table lists the remote site access gateway port connections for a single site link configuration for 15 subsites or less for a trunking subsystem where the geographically redundant prime site feature is not implemented.

Table 56: Remote Site Access Gateway Port Connections for 15 Subsites or Less (Non-Geographically Redundant Prime Site)

Gateway	Port	Device/Function
Remote Site Access Gateway 1	LAN 1	Prime Site Switch 1
	LAN 2	Remote Site Access Gateway 2
	LAN 3	Backhaul Switch 1
	RS-232	Terminal Server or Local Serial Access
Remote Site Access Gateway 2	LAN 1	Prime Site Switch 2
	LAN 2	Remote Site Access Gateway 1
	LAN 3	Backhaul Switch 2
	RS-232	Terminal Server or Local Serial Access

The following table lists the remote site access gateway port connections for a prime site configured with more than 15 subsites where the geographically redundant prime site feature is not implemented.

Table 57: Remote Site Access Gateway Port Connections for Greater than 15 Subsites (Non-Geographically Redundant Prime Site)

Port	Destination
Remote Site Access Router 1	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 1
Remote Site Access Router 2	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 2
Remote Site Access Router 3	
LAN 1	Prime Site Switch 1
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 1

Remote Site Access Router 4	
LAN 1	Prime Site Switch 2
LAN 2	Prime Site Switch 3
LAN 3	Backhaul Switch 2

The following table lists the remote site access gateway port connections for the Primary Prime Site and Secondary Prime Site where the geographically redundant prime site feature is implemented.

Table 58: Remote Site Access Gateway Ports Connections (Geographically Redundant Prime Sites)

Port	Destination
Remote Site Access Gateway 1	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Gateway 2	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2
Remote Site Access Gateway 3	
LAN 1	Prime Site Switch 1
LAN 3	Backhaul Switch 1
Remote Site Access Gateway 4	
LAN 1	Prime Site Switch 2
LAN 3	Backhaul Switch 2

NOTICE: For implementation of a Geographically Redundant Prime Site, only Remote Site Access Gateways 1 and 2 are required to support 15 subsites or less. To support subsites greater than 15, additional Remote Site Access Gateways 3 and 4 are required.

8.3.2 Remote Site Access Gateway (Trunking Subsystem Prime Site) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

8.3.3 Remote Site Access Gateway (Trunking Subsystem Prime Site) – Operation

For operation information,see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

8.3.4

Remote Site Access Gateway (Trunking Subsystem Prime Site) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

Chapter 9

ASTRO 25 K Core and Sites

This chapter provides information about the GGM 8000 transport gateway in an ASTRO® 25 system Small Conventional Configurations (K core). The ASTRO® 25 system Conventional Integrated Voice & Data architecture includes the K core, Conventional Hub Sites, and Conventional Base Radio Sites.

9.1 Conventional Master Site – K Core

The K core identifies the equipment located at the Conventional Master Site to support the conventional sites in the conventional system architecture. The K core is available in a Non-Redundant (K1) or Redundant (K2) master site configuration.

At an ASTRO® 25 system K core Small Conventional Configurations, the GGM 8000 Gateway operates as a Site Gateway.

9.1.1 Site Gateway (K Core) – Functional Description

At a K1 core, GGM 8000 can function as both Site Gateway and Conventional Channel Gateway. The single Site Gateway can also be used as a Site and Conventional Channel Gateway device supporting conventional base radios (conventional channels) colocated at the core.

At a K2 core, GGM 8000 can function as:

- Site Gateway – combining the function of core and gateway routers, handling traffic within the master site and providing an interface between the zone core and the customer network via a backhaul switch.
- Conventional Channel Gateway – supporting conventional base radios (conventional channels) colocated at the core.

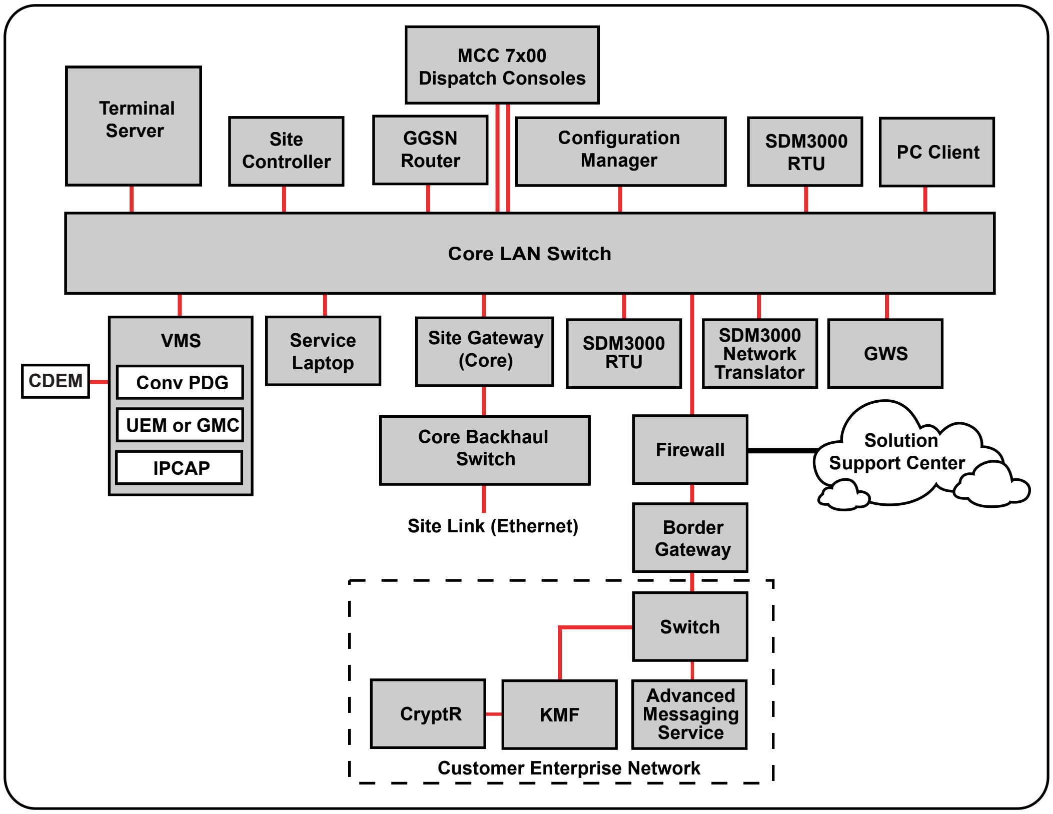
However, at the K2 core, redundant GGM 8000 Site Gateways only support a single-functional role as a Site Gateway device. GGM 8000 does not support the dual-role Site Gateway and CCGW functionality at the K2 core.

NOTICE: To support conventional channel base radios at a K2 core, a separate, dedicated Conventional Channel Gateway (CCGW) is required. Such a CCGW is available as a Conventional Channel Gateway device in a variety of different hardware configurations to support various types of conventional channels in your system. For more information, see Physical Description on page 30.

NOTICE: The GGM 8000 devices ordered from the factory do not require an encryption module in order for encryption to be enabled.

The following diagram shows the Site Gateway in K1 Small Conventional Configuration.

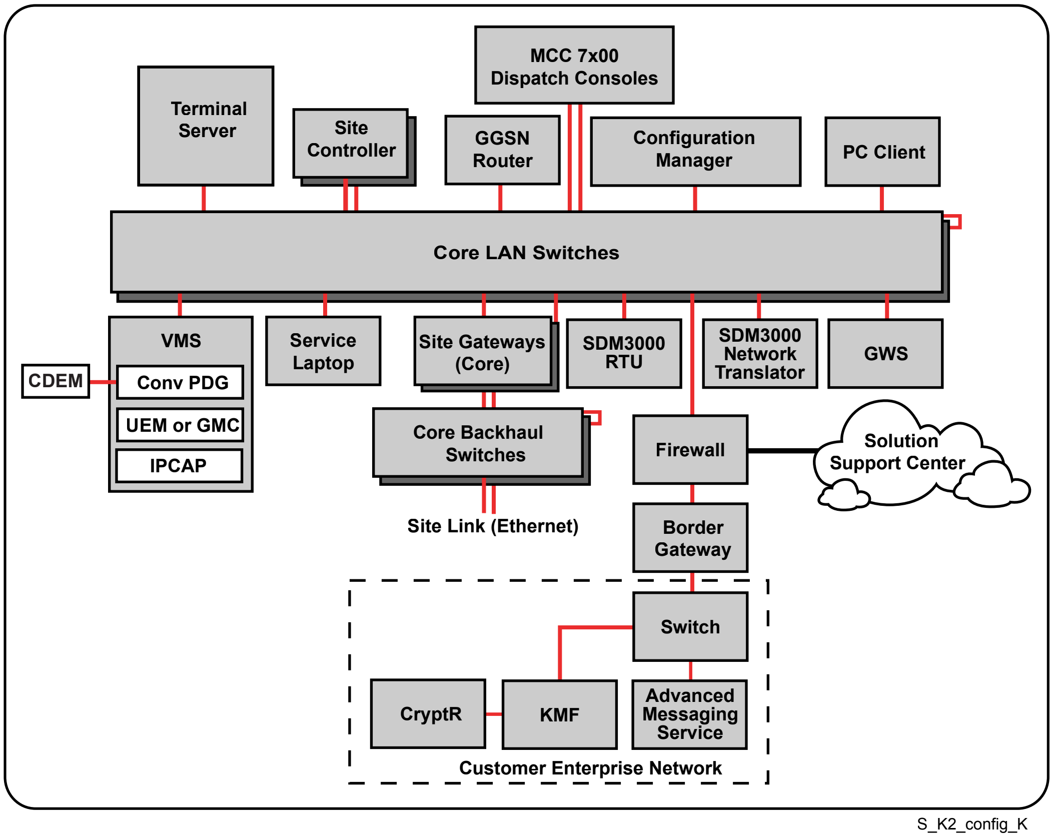
Figure 102: Core Gateway – K1 Configuration



S_K1_config_K

The following diagram shows the Site Gateways in K2 Small Conventional Configuration.

Figure 103: Core Gateways – K2 Configuration



9.1.1.1
Site Gateway (K Core) – Modules Used

The Site Gateway used in K core configuration can be installed with the analog/V.24 interface kit and serve as a Conventional Channel Interface to colocated Base Radio sites.

NOTICE: For more information about the GGM 8000 modules, see Expansion Module on page 33.

9.1.2
Site Gateway (K Core) – Installation

When and where to use: Follow this process to install the Site Gateway(s) in a K core.

Process:

1. If needed, install the analog/V.24 interface kit to the GGM 8000. See Replacing Daughterboards on the GGM 8000 on page 129 for installation details.

   NOTICE: By default, if the GGM 8000 Gateway was ordered with the analog/V.24 interface kit, the kit will be mounted at the factory.

2. Install the Site Gateway(s) in a rack. See Rack-Mounting the GGM 8000 on page 58.
3. Connect the Site Gateway(s) to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
4. If necessary, ground the Site Gateway(s). See Connecting a Chassis Ground on page 68.

5 Install the OS and configure the Site Gateway(s). See Downloading a Stored Configuration File to the GGM 8000 on page 93.

> **IMPORTANT:** The last three steps of Downloading a Stored Configuration File to the GGM 8000 on page 93 do not apply to configurations without the UNC application.

6 Connect the K core equipment to the Site Gateway(s). See Site Gateway (Console Site) – Site-Specific Cabling on page 198.

9.1.2.1

Site Gateway (K Core) – Site-Specific Cabling

The following table presents the cabling for the GGM 8000 if it used as a Site Gateway cabling in a K1 configuration.

Table 59: Site Gateway (K1)

Gateway		Port	Device/Function
Site Gateway	Base module	LAN 1–4	Core LAN Switch, Backhaul Switch
		DB-9	RS-232 link to the Terminal Server or Local Serial Access

The following table presents the cabling for the GGM 8000 if it is used as a Site and Conventional Channel Gateway in a K1 configuration.

Table 60: Site and Conventional Channel Gateway (K1)

Gateway		Port	Device/Function
Site and Conventional Channel Gateway	Base module	LAN 1-4	Core LAN Switch, Backhaul Switch
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit (optional)	4-wire ports (8A to 8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		ASTRO V.24 digital ports (6A, 6B, 6C, 6D)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D +8D to 9A+8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).

Gateway		Port	Device/Function
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A and 13D+12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

The following table presents the redundant Site Gateways cabling in K2 Small Conventional Configuration.

Table 61: Site Gateways (K2)

Gateway		Port	Device/Function
Site Gateway 1	Base module	LAN 1-4	Core LAN Switch(es), Backhaul Switch(es)
		RS-232	Terminal Server or Local Serial Access
Site Gateway 2	Base module	LAN 1–4	Core LAN Switch(es), Backhaul Switch(es)
		RS-232	Terminal Server or Local Serial Access

The following table presents the cabling for the GGM 8000 if it is used as a dedicated Conventional Channel Gateway.

Table 62: Conventional Channel Gateway (K Core)

Gateway		Port	Device/Function
Conventional Channel Gateway	Base module	LAN 1-4	Core LAN Switch(es), Backhaul Switch(es)
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire ports (8A-8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		ASTRO V.24 digital ports (6A, 6B, 6C, 6D)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations

Gateway		Port	Device/Function
			to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A and 13D+12D to 13A +12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

9.1.2.1.1 Site Gateway (K Core) – Site Links

Site links from the K core to a Conventional Hub Site must be an Ethernet site link. T1/E1 site links are not supported. The GGM 8000 Gateway device supports the site link from the K core to the Conventional Hub Site.

Site links between two Conventional Hub Sites or site links between a Conventional Hub Sites and Conventional Base Radio Sites employ Flexible Site and InterZone Links (Ethernet) only.

9.1.3 Site Gateway (K Core) – Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

9.1.4 Site Gateway (K Core) – Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

9.1.5 Site Gateway (K Core) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

9.2 K Core Conventional System Sites

In addition to the K core Conventional Master Site, the ASTRO® 25 Conventional System architecture includes the following conventional system sites:

- Conventional Hub Site
- Conventional Base Radio Site

At the system sites, GGM 8000 can operate as a Site Gateway and Conventional Channel Gateway.

9.2.1 K Core Conventional System Sites – General Installation

When and where to use: Follow this process to install GGM 8000 at any K core conventional system site.

Process:

1. Install the Analog/V.24 interface kit to GGM 8000. See Replacing Daughterboards on the GGM 8000 on page 129 for installation details.

   NOTICE: By default, if the GGM 8000 Gateway is ordered with the analog/V.24 interface kit, the kit will be mounted at the factory.

2. Install the Site Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
3. Connect the Site Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
4. If necessary, ground the Site Gateway. See Connecting a Chassis Ground on page 68.
5. Configure the Site Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

   IMPORTANT: Last 3 steps of Downloading a Stored Configuration File to the GGM 8000 on page 93 do not apply to configurations without the UNC application.

6. Connect the zone core equipment to the Site Gateway. Depending on the site type, refer to one of the following:
   - Conventional Hub Site – see Conventional Hub Site – GGM 8000 Installation on page 238.
   - Conventional Base Radio Site – see Conventional Base Radio Site – GGM 8000 Installation on page 244.

9.2.2 K Core Conventional Hub Site

The Conventional Hub Site is one of the conventional sites in the Integrated Voice & Data architecture supported by the K core. The Conventional Hub Site contains equipment other than, or in addition to, conventional base radio equipment to support conventional channel operation.

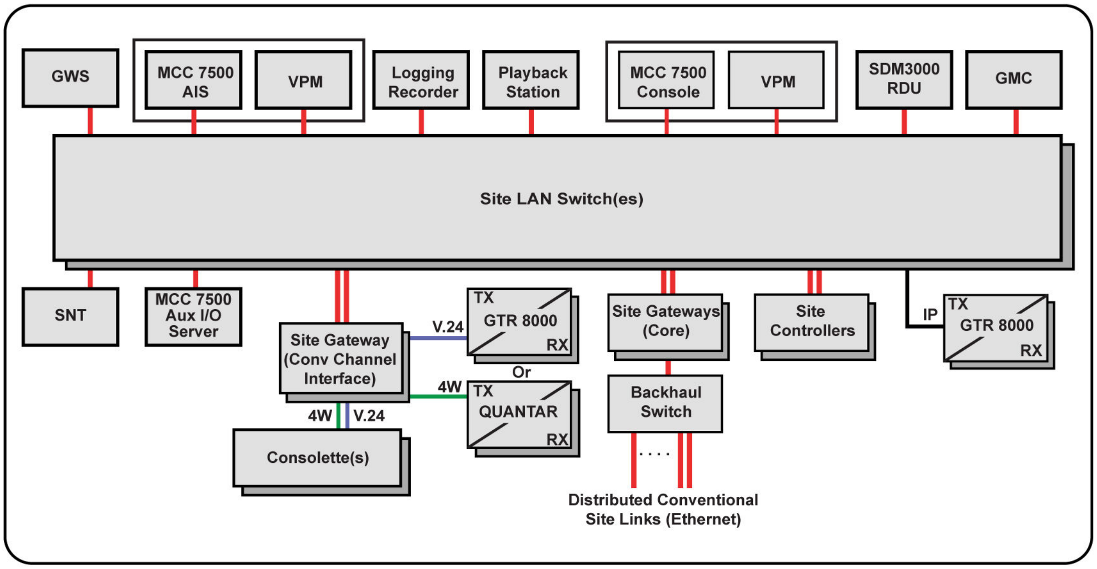
GGM 8000 at the Conventional Hub Site can fulfill three roles:

- Site Gateway – supporting site transport by providing an interface between the K core and the equipment at the Conventional Hub Site.
- Conventional Channel Gateway – supporting conventional base radios (conventional channels) colocated at the Conventional Hub Site.
- Site and Conventional Channel Gateway – supporting site transport and conventional base radios (conventional channels) colocated at the site.

NOTICE: GGM 8000 can operate as a Site and Conventional Channel Gateway only if it is the single Site Gateway used at a Conventional Hub Site. If the Conventional Hub Site has redundant Site Gateways, an additional, dedicated Conventional Channel Gateway device needs to be used in order to support conventional base radios (conventional channels) colocated at the site.

The following diagram shows the GGM 8000 Gateway at the Conventional Hub Site.

Figure 104: Conventional Hub Site



Distrib_Conv_Hub_Site_Redund_ColocatedBR_G

NOTICE: For more detailed information and diagrams of various Conventional Hub Site configurations, see the *L and M Core Conventional Architectures Engineer Guide* and *K Core Conventional Architecture Engineer Guide* manuals.

9.2.2.1
K Core Conventional Hub Site – GGM 8000 Functional Description

The GGM 8000 Gateway at the Conventional Hub Site, serves as an interface between the K core and the equipment at the Conventional Hub Site, connected to the Conventional Hub Site switch.

9.2.2.1.1
K Core Conventional Hub Site – Site Transport

The Conventional Hub Site Interfaces with other Conventional Hub Sites and Conventional Base Radio Sites. A GGM 8000 Gateway at a Conventional Hub Site designated to interface with the K core is configured specifically to support the site link for core-to-site transport.

9.2.2.1.2
Conventional Channel Interface (Colocated BR at a Conventional Hub Site)

To interface with conventional base radios, the Conventional Hub Site uses a Conventional Channel Gateway. For more details, refer to the Conventional Base Radio Site – Conventional Subsystem on page 239.

9.2.2.2 K Core Conventional Hub Site Gateway – Modules Used

In order to use the Site Gateway in conventional configurations, the analog/V.24 interface kit needs to be installed. It consists of the following modules:

- One four-wire E&M module
- One DSP SIMM (installed in the analog slot)
- Two V.24 modules (installed in the I/O slots)

9.2.2.3 K Core Conventional Hub Site – GGM 8000 Installation

NOTICE: For a general installation process, refer to K Core Conventional System Sites – General Installation on page 227.

The following table presents cabling for GGM 8000 used as a Site Gateway.

Table 63: Conventional Hub Site – Site Gateway

Gateway		Port	Device/Function
Site Gateway	Base module	LAN 1-4	Site LAN Switch, Ethernet Site Links to the K core
		RS-232	RS-232 link to the Terminal Server or Local Serial Access

The following table presents cabling for GGM 8000 used as a Site and Conventional Channel Gateway.

Table 64: Conventional Hub Site – GGM 8000 Cabling

Gateway		Port	Device/Function
Site and Conventional Channel Gateway	Analog/V.24 interface kit	4-wire ports (8A-8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		ASTRO V.24 digital ports (6A, 6B, 7A, 7D)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A +8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).

Gateway		Port	Device/Function
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A +8A and 13D+12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).
	Base module	LAN 1-4	Site LAN Switch, Ethernet Site Links to the K core
		RS-232	RS-232 link to the Terminal Server or Local Serial Access

The following table presents cabling for GGM 8000 used as a dedicated Conventional Channel Gateway.

Table 65: Conventional Hub Site – GGM 8000 Cabling

Gateway		Port	Device/Function
Conventional Channel Gateway	Analog/V.24 interface kit	4-wire ports (8A-8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		ASTRO V.24 digital ports (6A, 6B, 7A, 7D)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A +8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A +8A and 13D+12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

Gateway	Port	Device/Function
Base module	LAN 1-4	Site LAN Switch, connections to up to 3 conventional IP base stations
	RS-232	RS-232 link to the Terminal Server or Local Serial Access

9.2.2.4 K Core Conventional Hub Site – GGM 8000 Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

9.2.2.5 K Core Conventional Hub Site – GGM 8000 Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

9.2.2.6 K Core Conventional Hub Site – GGM 8000 Maintenance and Troubleshooting

For maintenance and troubleshooting information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

9.2.3 K Core Conventional Base Radio Site

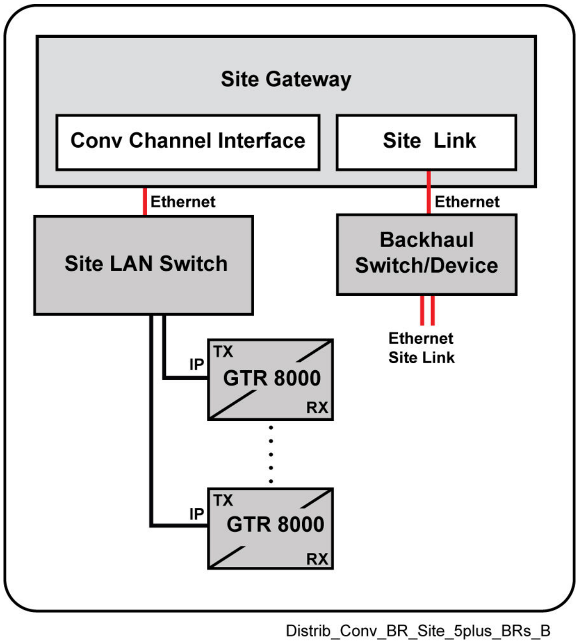
The Conventional Base Radio Site is one of the conventional sites in the Integrated Voice & Data architecture supported by the K core. This site is designed to support conventional base radios and a GGM 8000 Gateway to support site transport.

9.2.3.1 K Core Conventional Base Radio Site – GGM 8000 Functional Description

Analog and Digital conventional requires a separate cable connection between the base radio and the GGM 8000 Gateway. IP conventional uses Ethernet/IP and therefore a dedicated port for each base radio is not necessarily needed. Depending on the system software release, the GGM 8000 Gateway base unit supports up to 10 or 16 IP conventional channels.

The following diagram is an example of the GGM 8000 Gateway at the Conventional Base Radio Site.

Figure 105: Conventional Base Radio Site (1-10 or 1-16 base radios based on the software release)



NOTICE: For more detailed information and diagrams of various Conventional Base Radio Site configurations, see the *L and M Core Conventional Architectures Engineer Guide* and *K Core Conventional Architecture Engineer Guide* manuals.

9.2.3.2

K Core Conventional Base Radio Site – GGM 8000 Installation

NOTICE: For a general installation process, refer to K Core Conventional System Sites – General Installation on page 227.

The following table presents cabling for GGM 8000 used at the Conventional Base Radio Site with up to four base radios.

Table 66: Conventional Base Radio (up to Four BRs) – GGM 8000 Cabling

Gateway		Port	Device/Function
Site Gateway	Base module	LAN 1	Distributed Conventional LAN Switch
		LAN 2	Distributed Conventional Hub Site Link
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire ports (8A-8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		ASTRO V.24 digital ports (6A, 6B, 7A, 7D)	Connections to up to 4 colocated base stations (digital conventional channel interface). For de-

Gateway		Port	Device/Function
			tails, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A and 13D+12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

The following table presents cabling for GGM 8000 used at the Conventional Base Radio Site with five or more base radios.

Table 67: Conventional Base Radio (Five or More BRs) – GGM 8000 Cabling

Gateway		Port	Device/Function
Site Gateway	Base module	LAN 1-4	Site LAN Switch, Backhaul Switch
		RS-232	Terminal Server or Local Serial Access

9.2.3.3 K Core Conventional Base Radio Site – GGM 8000 Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

9.2.3.4 K Core Conventional Base Radio Site – GGM 8000 Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

9.2.3.5 K Core Conventional Base Radio Site – GGM 8000 Maintenance and Troubleshooting

For troubleshooting and maintenance information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic troubleshooting and maintenance procedures apply.

Chapter 10

ASTRO 25 Conventional Subsystem Architectures

The GGM 8000 gateway is used in ASTRO® 25 system conventional subsystem architectures. It can be used as a replacement for the MNR S2500 router and operate as the Conventional Channel Gateway in the following three site configurations:

- Conventional conduit hub site
- Conventional hub site
- Conventional base radio site

The GGM 8000 Conventional Channel Gateway also supports additional channel types not supported by the MNR S2500 Conventional Channel Gateway and can be used in any of the site types that may contain conventional channels.

NOTICE: Since sites can support up to 3 or 10 Conventional Channel Gateways, additional GGM 8000s may be necessary to support the conventional channel gateway (CCGW) application. Each Conventional Channel Gateway located at a physical site is considered a separate logical conventional site, and the site devices with which it communicates are the conventional channels.

10.1 GGM 8000 – Super Hub Site

The Super Hub architecture is a variant of the Distributed Conventional architecture which can be employed with the Enhanced Console Telephony feature to support Console Telephony for more than 50 dispatch console operator positions. This architecture is used to ensure that appropriate bandwidth is available to accommodate the Enhanced Console Telephony feature and the ability to collocate up to 100 consoles within a single Conventional Hub site. A Super Hub site is a group of 2 to 5 Conventional Hub sites at a single location.

A Super Hub site is a collocation of 2-5 hub sites at a single location. Where conventional hub sites are members of a Super Hub site, the IP tunnels that traverse the backhaul between those hub sites are no longer needed.

To support the Super Hub Site, port 4 on the GGM 8000 Conventional Hub site router needs to be configured to support and enable the OSPF / MOSPF protocol.

NOTICE: QoS will not be enabled on port 4 of the GGM 8000 Conventional Hub site router that supports the Super Hub Site architecture.

Each Conventional Hub Site router (GGM 8000) as a member of the Super Hub Site has OSPF and MOSPF enabled by default on Port 4.

Review the following information:

- It is highly recommended that all Conventional Hub Sites employ dual routers to maximize the probability of success for Console Telephony traffic sent over the WAN.
- Each router in a Conventional Hub Site as a member of a Super Hub Site will allocate a port (WAN port 4) for the Super Hub site link.
- The backhaul switch(es) supporting the Super Hub site at a Conventional Hub site (as a member of a Super Hub Site) will allocate a port for the Conventional Hub Site router’s local connections.

- Each Conventional Hub Site router (GGM 8000) as a member of the Super Hub Site will have OSPF and MOSPF enabled by default on Port 4 with the port speed and duplex settings set at the default (auto/auto).

10.2 Conventional Conduit Hub Site – Conventional Subsystem

This section contains information concerning the Conventional Conduit Hub Site – Conventional subsystem.

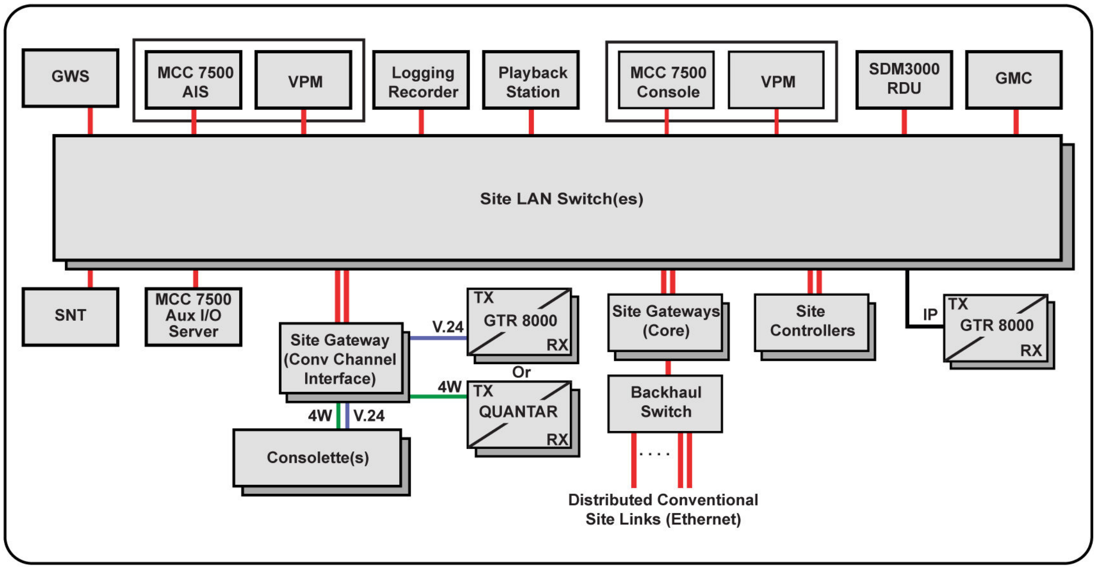
The Conventional Conduit Hub Site is the conventional site in the Conventional Subsystem that interfaces to the ASTRO® 25 system.

10.2.1 Conventional Conduit Hub Site – GGM 8000 Functional Description

At the Conventional Conduit Hub Site, the GGM 8000 gateway operates as an interface between an ASTRO® 25 system zone core and the customer backhaul network.

The following diagram shows the GGM 8000 gateway in the Conventional Hub Site.

Figure 106: Conventional Conduit Hub Site



Distrib_Conv_Hub_Site_Redund_ColocatedBR_G

NOTICE: For information about hub site topologies using MLC 8000 Comparators, refer to the *MLC 8000 Setup Guide*.

10.2.2 Conventional Conduit Hub Site – GGM 8000 Installation

NOTICE: For a general installation process, refer to Conventional Channel Gateway – Installation on page 73.

The following table presents GGM 8000 cabling for the Conventional Conduit Hub Site.

Table 68: Conventional Conduit Hub Site – GGM 8000 Cabling

Gateway		Port	Device/Function
Site Gateway	Base module	LAN 1	Connection to the M1/M2, M3 zone core
		LAN 2	Connection to the Backhaul Switch
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire analog ports (8A to 8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D +8D to 9A+8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D +8D to 9A+8A and 13D +12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

For more information about the Enhanced Conventional Gateway modules, see GGM 8000 Enhanced Conventional Channel Gateway Modules on page 34.

10.2.3 Conventional Conduit Hub Site – GGM 8000 Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

NOTICE: GGM 8000 used as a Site Gateway in a Conventional Conduit Hub Site uses a different configuration file.

10.2.4 Conventional Conduit Hub Site – GGM 8000 Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

10.2.5 Conventional Conduit Hub Site – GGM 8000 Maintenance and Troubleshooting

For troubleshooting and maintenance information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic troubleshooting and maintenance procedures apply.

10.3 Conventional Hub Site – Conventional Subsystem

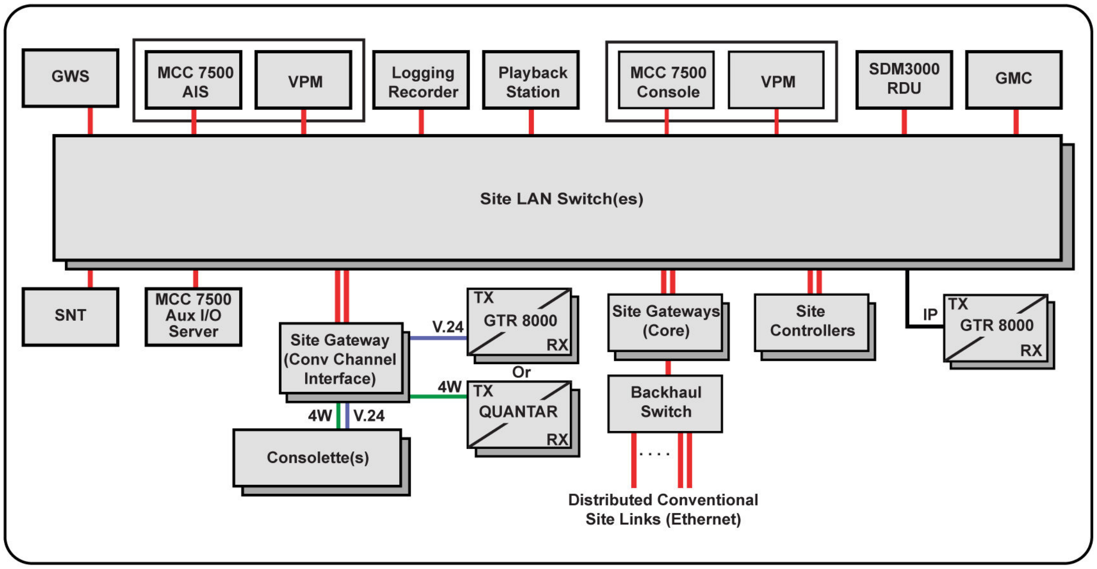
The Conventional Hub Site is the conventional site in the Conventional Subsystem that interfaces with other sites in the subsystem and the Base Radio sites. It does not interface with ASTRO® 25 system M1/M2/M3 zone core.

10.3.1 Conventional Hub Site – GGM 8000 Functional Description

At the Conventional Hub Site, GGM 8000 operates as an interface between the equipment at the Conventional Hub Site and the backhaul network.

The following diagram shows the GGM 8000 gateway at the Conventional Hub Site.

Figure 107: Conventional Hub Site



Distrib_Conv_Hub_Site_Redund_ColocatedBR_G

10.3.2 Conventional Hub Site – GGM 8000 Installation

NOTICE: For a general installation process, see K Core Conventional System Sites – General Installation on page 227.

The following table shows the cabling for GGM 8000 used at the Conventional Hub Site.

Table 69: Conventional Hub Site – GGM 8000 Cabling

Gateway		Port	Device/Function
Conventional Channel Gateway	Base module	LAN 1-4	Site LAN switch, connection to up to 3 colocated conventional IP base radios
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire ports (8A to 8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
		ASTRO V.24 digital ports (7A, 7B, 6A, 6B)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A +8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A +8A and 13D+12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).
Site Gateway (Core)	Base module	LAN 1-4	Ethernet Site Links to other Conventional Hub Sites
		RS-232	Terminal Server or Local Serial Access

For more information about the Enhanced Conventional Gateway modules, see GGM 8000 Enhanced Conventional Channel Gateway Modules on page 34.

10.3.3 Conventional Hub Site – GGM 8000 Configuration

For configuration information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

NOTICE: GGM 8000 used as a Site Gateway in a Conventional Hub Site, uses the same configuration file as when used in an IV&D system.

10.3.4 Conventional Hub Site – GGM 8000 Operation

For operation information, see the GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

10.3.5 Conventional Hub Site – GGM 8000 Maintenance and Troubleshooting

For maintenance and troubleshooting information, see the GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

10.4 Conventional Base Radio Site – Conventional Subsystem

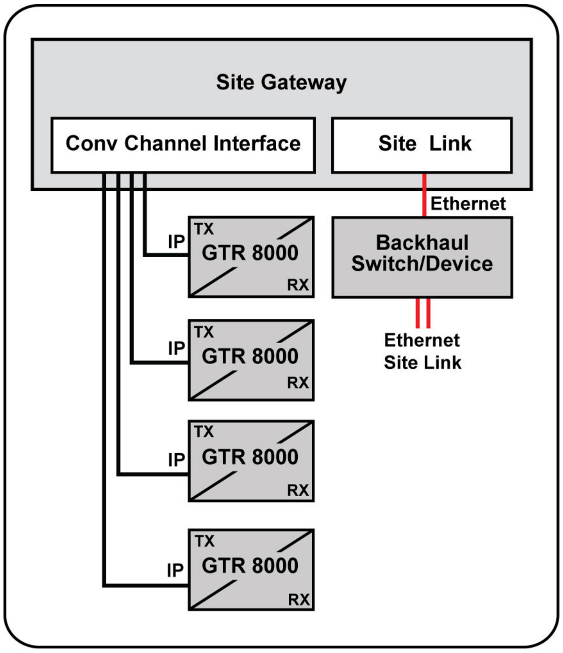
The Conventional Base Radio Gateway functions to provide network transport support for the Conventional Base Radio Site.

10.4.1 Conventional Base Radio Site – GGM 8000 Functional Description

GGM 8000 at a Conventional Base Radio Site interfaces with other Conventional Hub Sites and Conventional Base Radio Sites.

The following diagram shows GGM 8000 at the Conventional Base Radio site with four or less Base Radios.

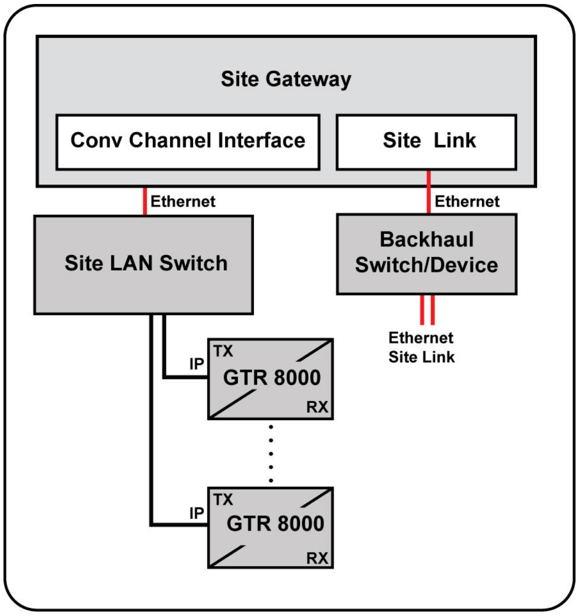
Figure 108: Site Gateway at the Conventional Base Radio Site (Four or Less BRs)



Distrib_Conv_BR_Site_4less_BRs_A

The following diagram shows GGM 8000 at the Conventional Base Radio site configuration with five or more Base Radios.

Figure 109: Site Gateway at the Conventional Base Radio Site (Five or More BRs)



Distrib_Conv_BR_Site_5plus_BRs_B

10.4.1.1
Conventional Base Radio Site – Conventional Channel Interface

The Conventional Channel Gateway interfaces with conventional base radios or Motorola Solutions consolettes using the following interfaces:

- Analog

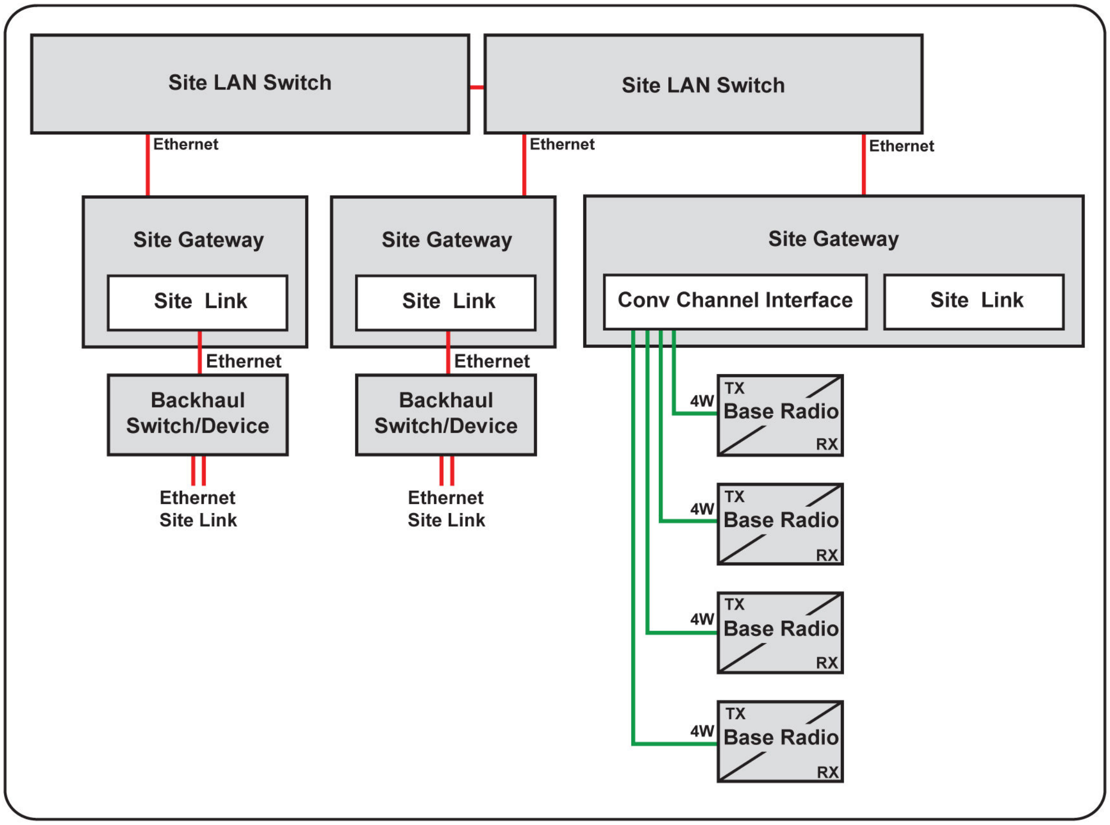
- Digital (V.24)
- IP conventional
- Mixed mode
- MDC 1200
- ACIM

10.4.1.1.1 Analog Interface

The analog interfaces uses 4-wire or 2-wire (supported on the Enhanced Conventional Gateway module only) connections with certain types of Motorola Solutions public safety network equipment that support digital audio connections. GGM 8000 configured with an analog/V.24 interface kit or the Low Density Enhanced Conventional Gateway module supports four analog ports and up to four analog conventional channels. GGM 8000 configured with the High Density Enhanced Conventional Gateway module supports eight analog ports and up to eight analog conventional channels.

The following diagram shows the Conventional Channel Gateway (Analog Conventional Channel Interface) at a Conventional Base Radio Site.

Figure 110: Site Gateway (Analog Conventional Channel Interface)



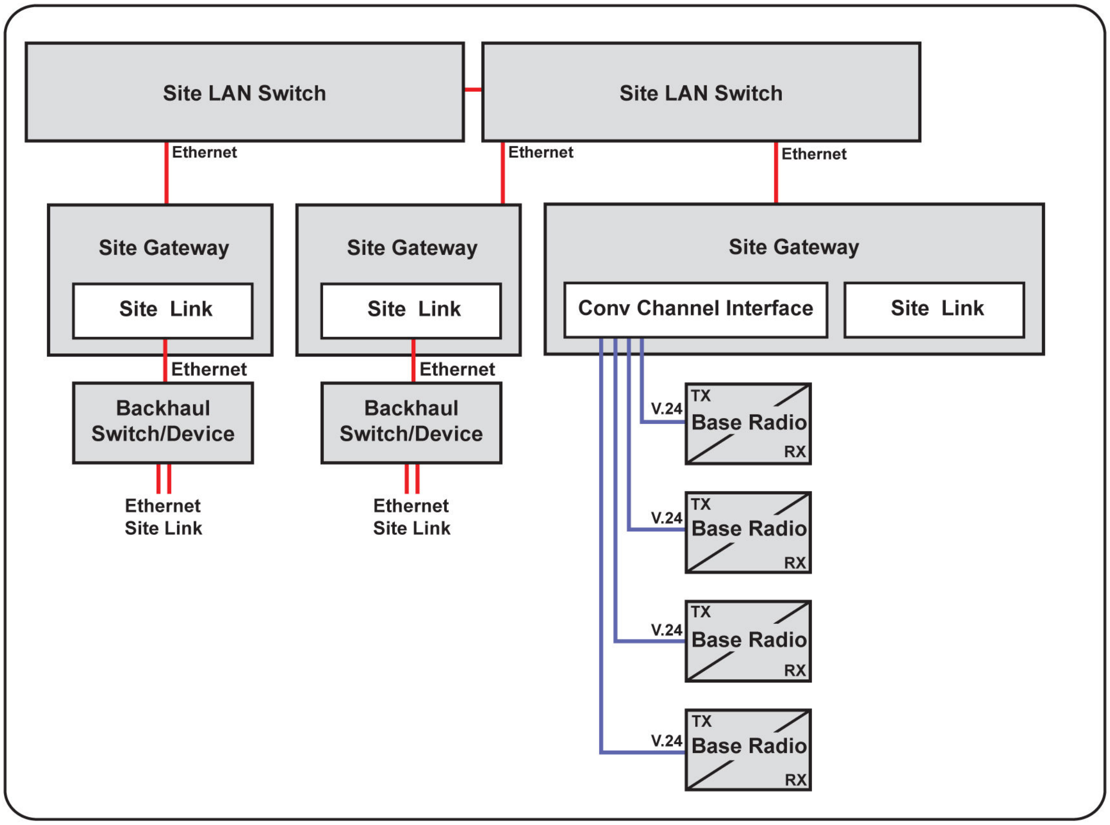
Distrib_Conv_BR_Site_Analog_D

10.4.1.1.2 Digital (V.24) Interface

The digital interface uses V.24 digital ports carrying digital audio with certain types of Motorola Solutions public safety network equipment that support digital audio connections. GGM 8000 configured with the analog/V.24 interface kit or the Low Density Enhanced Conventional Gateway module supports four V.24 ports and up to four digital conventional channels. GGM 8000 configured with the High Density Enhanced Conventional Gateway module supports eight V.24 ports and up to eight digital conventional channels.

The following diagram shows the Site Gateway (Digital Conventional Channel Interface) at a Conventional Base Radio Site.

Figure 111: Site Gateway (Digital Conventional Channel Interface)



Distrib_Conv_BR_Site_Digital_D

10.4.1.1.3 Conventional IP Interface

The IP conventional feature supports IP connectivity between the Conventional Channel Gateway and conventional IP base stations and comparators (in IP simulcast systems). conventional channels function as an IP interface between the base station and the console, creating an IP link between the conventional gateway and the base station using Motorola Solutions proprietary link management protocol. Typically, IP conventional channels run over the Ethernet interface.

10.4.1.1.4 Mixed Mode Interface

The Conventional Channel Gateway supports mixed mode channels over V.24 and IP digital interfaces.

V.24 mixed mode

Binds an analog interface and a V.24 digital interface The Conventional Channel Gateway associates the signaling information processed over the digital V.24 interface with the voice processed over the corresponding analog E&M interface.

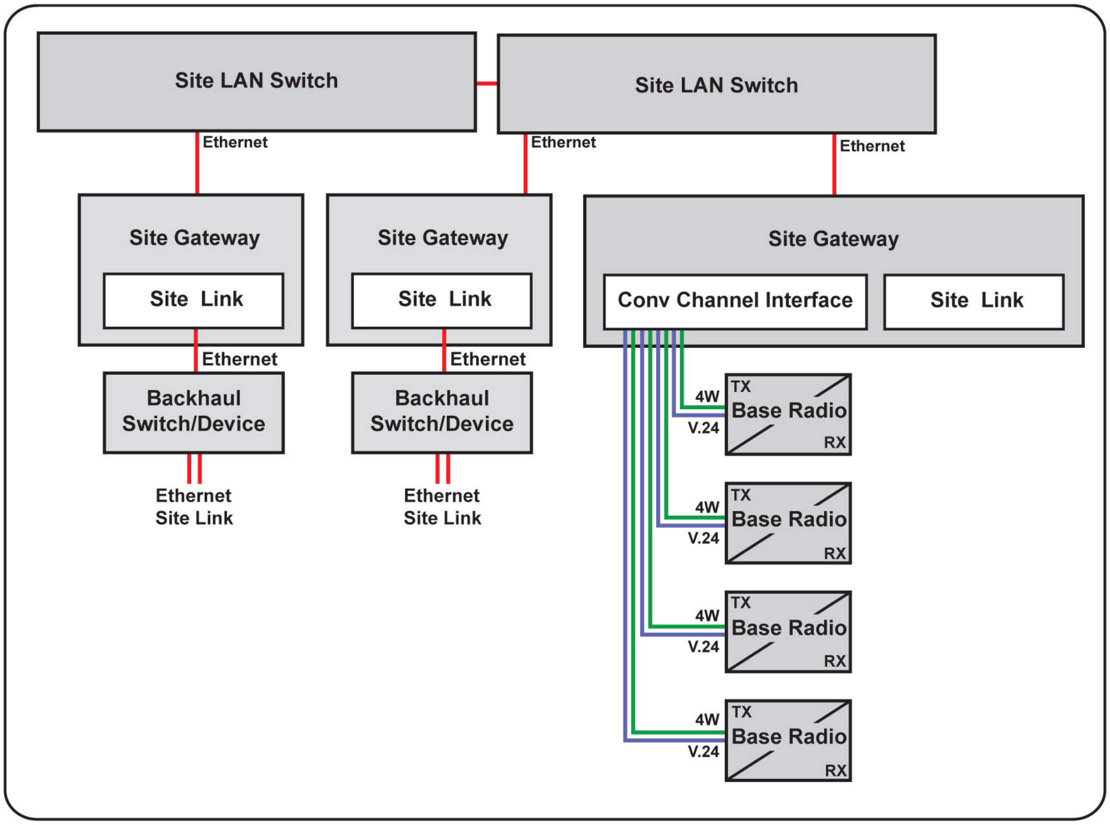
IP mixed mode

Binds an analog interface and an IP digital interface as a single channel. The IP interface is used for call signaling and control and digital audio for digital calls, while the analog interface is used for call signaling and control and analog audio for analog calls. Each direction is independent of the other

V.24 mixed mode and IP mixed mode channels use the same channel type (mixed mode); the difference being that for V.24 mixed mode channels the digital interface type is V.24, while for IP mixed mode channels the digital interface type is Ethernet (IP).

The following diagram shows the Site Gateway (Mixed Mode Conventional Channel Interface) at a Conventional Base Radio Site.

Figure 112: Site Gateway (Mixed Mode Conventional Channel Interface)



Distrib_Conv_BR_Site_Mixed_Mode_D

For information about conventional topologies that use MLC 8000s along with GGM 8000s for the analog, digital or mixed mode interface, see the *Quick MLC 8000 Setup Guide* manual.

10.4.1.1.5 Mixed Mode Support

The Conventional Channel Gateway supports two kinds of mixed mode channels.

V.24 Mixed Mode Support

A conventional mixed mode channel can run either in pure digital mode (audio and signaling is processed over the V.24 digital interface) or in mixed mode. In mixed mode, audio is processed over the analog E&M interface and the signaling related to this call is processed over the digital V.24 interface. The Conventional Channel Gateway associates the signaling information processed over the digital V.24 interface with the voice processed over the corresponding analog E&M interface.

IP Mixed Mode Support

The IP mixed mode feature (digital and analog on the same channel) supports the mixed mode comparator introduced for the ASTRO® 25 7.12 system release. This feature allows you to consolidate digital channels with existing analog channels without purchasing additional channels.

The Conventional Channel Gateway supports IP mixed mode channels, which bind an analog interface and an IP interface as a single channel. The IP interface is used for call signaling and control and digital audio for digital calls, while the analog interface is used for call signaling and control and analog audio for analog calls. Each direction is independent of the other. IP mixed mode functionality allows the Conventional Channel Gateway to multiplex a variety of analog/digital air interface devices through a combined channel and resolve channel contention in both data and voice traffic. Unlike a V.24 mixed mode channel, an IP mixed mode channel does not have to buffer audio packets while a data session is ongoing.

10.4.1.1.6 MDC 1200 Interface

MDC signaling integrates MDC 1200 and analog conventional signaling and makes digital calls with the zone controller. An MDC channel is a channel where audio and call control is processed over the analog E&M interface; however, the call control messages between the gateway and the zone controller are in digital conventional format.

10.4.2 Conventional Base Radio Site – GGM 8000 Installation

NOTICE: For a general installation process, refer to Conventional Channel Gateway – Installation on page 73.

The following table shows cabling for GGM 8000 used at the Conventional Base Radio Site (Analog).

Table 70: Conventional Base Radio Site (Analog) – Site-Specific Cabling

Gateway		Port	Device/Function
Site and Conventional Channel Gateway (Analog)	Base module	LAN 1	Distributed Conventional Site LAN Switch
		LAN 2	Distributed Conventional Hub Site Link
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire analog ports (8A to 8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details, see E&M (Analog) Connections on page 74.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D +8D to 9A+8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
	High Density Enhanced Conventional	4-wire or 2-wire analog ports (paired ports 9D +8D to 9A+8A and 13D +12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).

Gateway		Port	Device/Function
	Gateway module		

The following table shows cabling for GGM 8000 used at the Conventional Base Radio Site (Digital/ V.24).

Table 71: Conventional Base Radio Site (Digital/V.24) – Site-Specific Cabling

Gateway		Port	Device/Function
Site and Conventional Channel Gateway	Base module	LAN 1	Distributed Conventional Site LAN Switch
		LAN 2	Distributed Conventional Hub Site Link
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	V.24 digital ports (7A, 7B, 6A, 6B)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

The following table shows cabling for GGM 8000 used at the Conventional Base Radio Site (Mixed Mode).

Table 72: Conventional Base Radio Site (Mixed Mode) – Site-Specific Cabling

Gateway		Connection	Device/Function
Site and Conventional Channel Gateway	Base module	LAN 1	Distributed Conventional Site LAN Switch
		LAN 2	Distributed Conventional Hub Site Link
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire analog ports (8A-8D)	Connections to up to 4 colocated base stations (analog conventional channel interface). For details,

Gateway		Connection	Device/Function
			see E&M (Analog) Connections on page 74.
		V.24 digital ports (7A, 7B, 6A, 6B)	Connections to up to 4 colocated base stations (digital conventional channel interface). For details, see Digital Base Stations to Conventional Channel Gateway on page 83.
	Low Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A)	Connections to up to 4 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A)	Connections to up to 4 colocated base stations (digital conventional channel interface).
	High Density Enhanced Conventional Gateway module	4-wire or 2-wire analog ports (paired ports 9D+8D to 9A+8A and 13D+12D to 13A+12A)	Connections to up to 8 colocated base stations (analog conventional channel interface).
		V.24 digital ports (7B, 7A, 6B, 6A, 11B, 11A, 10B, and 10A)	Connections to up to 8 colocated base stations (digital conventional channel interface).

For more information about the Enhanced Conventional Gateway modules, see GGM 8000 Enhanced Conventional Channel Gateway Modules on page 34.

The following table shows cabling for GGM 8000 used at the Conventional Base Radio Site with 5 or more BRs.

Table 73: Conventional Base Radio Site with 5 or more BRs – Cabling

Gateway	Port	Device/Function
Site and Conventional Channel Gateway	LAN 1-4	Site LAN Switch(es), Backhaul Switch(es)
	RS-232	Terminal Server or Local Serial Access

10.4.3 Conventional Base Radio Site – GGM 8000 Configuration

For configuration information, see the GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

10.4.4 Conventional Base Radio Site – GGM 8000 Operation

For operation information, refer to GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

10.4.5 Conventional Base Radio Site – GGM 8000 Maintenance and Troubleshooting

For troubleshooting and maintenance information, see the GGM 8000 Introduction and Common Procedures on page 28. Generic troubleshooting and maintenance procedures apply.

Chapter 11

ASTRO 25 Standalone Conventional Voting System

This chapter provides information about the GGM 8000 transport gateway in the ASTRO® 25 system Standalone Conventional Voting System.

The Standalone Conventional Voting System architecture can be divided into two types:

- Standalone Conventional Voting System (Centralized Conventional)
- Standalone Conventional Voting System (Distributed Conventional)

The Standalone Conventional Voting System supports voting operation for conventional channels where GGM 8000 is available as a Conventional Channel Gateway (CCGW) interface device in a variety of different hardware configurations to support various types of conventional channels. See Physical Description on page 30.

11.1 Standalone Conventional Voting System – GGM 8000 Installation

When and where to use: Follow this process to install the GGM 8000 gateway in a Standalone Conventional Voting System.

Process:

1. Install the Site Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Site Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Site Gateway. See Connecting a Chassis Ground on page 68.
4. Configure the Site Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.
5. Connect the site equipment to the Site Gateway.
   - For Standalone Conventional Voting System (Centralized Conventional), see the following:
     - Conventional Comparator Site Gateway – Installation on page 250
     - Conventional Base Radio Subsite Gateway – Installation on page 250
   - For Standalone Conventional Voting System (Distributed Conventional), see the following:
     - Conventional Comparator Hub Site Gateway – Installation on page 252
     - Conventional Base Radio Site Gateway – Installation on page 253

11.2 Standalone Conventional Voting System (Centralized Conventional)

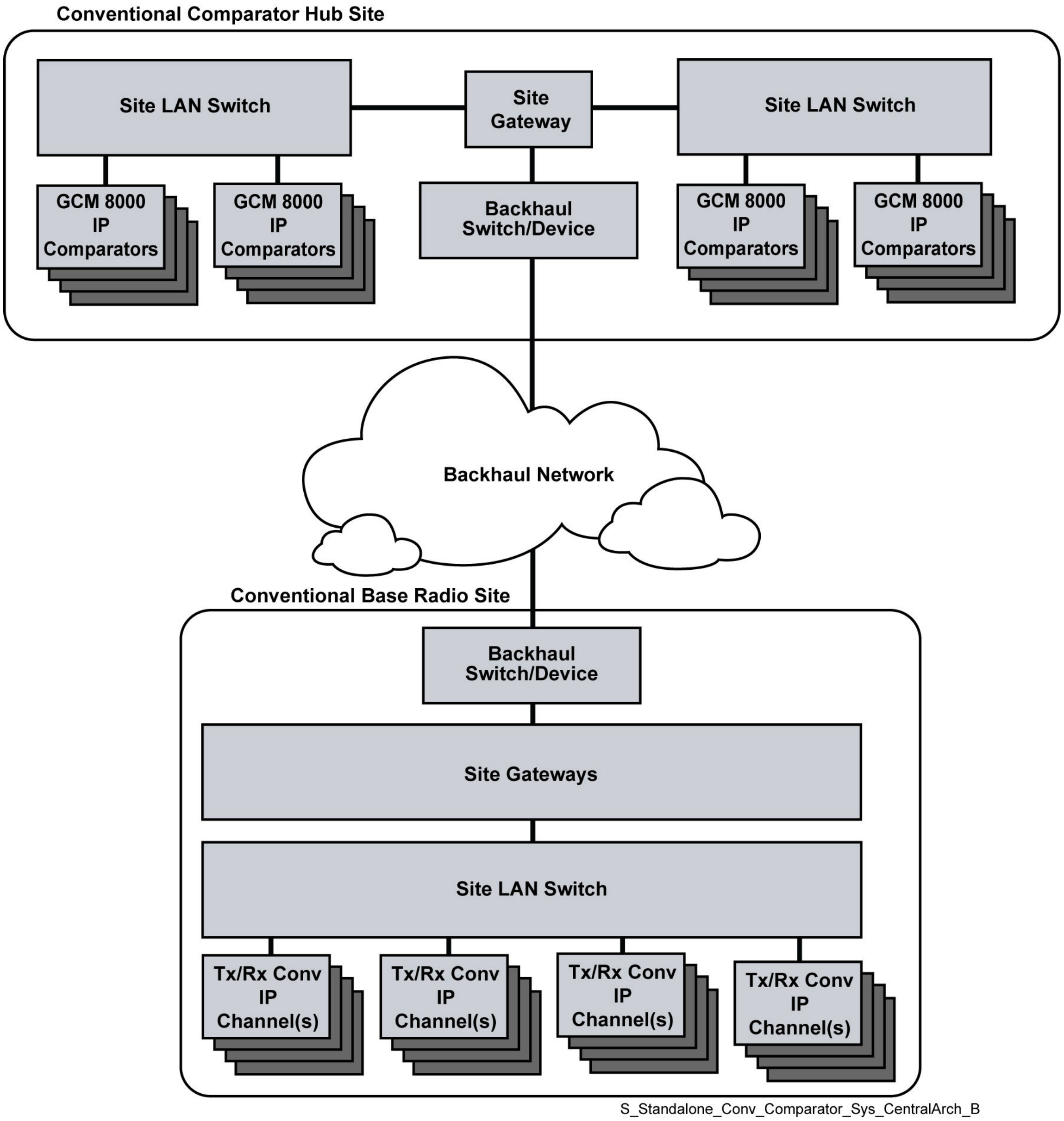
The Standalone Conventional Voting System (Centralized Conventional) system utilizes the following site types:

- Conventional Comparator Site
- Conventional Base Radio Site

As defined by the Centralized Conventional, the Standalone Conventional Voting System does NOT interface with other sites.

The following diagram shows the Site Gateways used in Standalone Conventional Voting System (Centralized Conventional).

Figure 113: Standalone Conventional Voting System (Centralized Conventional)



S_Standalone_Conv_Comparator_Sys_CentralArch_B

11.2.1 Conventional Comparator Site Gateway

At the Conventional Comparator Site (Centralized Conventional), GGM 8000 operates as a Site Gateway. It provides the interface between the Site LAN Switches and the Backhaul Switch.

11.2.1.1
Conventional Comparator Site Gateway – Installation

NOTICE: For a general installation process, see Standalone Conventional Voting System – GGM 8000 Installation on page 248.

The following table shows the site-specific cabling for GGM 8000 used at the Conventional Comparator Site (Centralized Conventional).

Table 74: Conventional Comparator Site (Centralized Conventional) – Cabling

Gateway	Port	Device/Function
Site Gateway	LAN 1– 4	Site LAN Switch(es), Backhaul Switch(es)
	RS-232	Terminal Server or Local Serial Access

11.2.1.2
Conventional Comparator Site Gateway – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

11.2.1.3
Conventional Comparator Site Gateway – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

11.2.1.4
Conventional Comparator Site Gateway – Maintenance

For troubleshooting and maintenance information, see GGM 8000 Introduction and Common Procedures on page 28. Generic troubleshooting and maintenance apply.

11.2.2
Conventional Base Radio Subsite Gateway

At the Conventional Base Radio Subsite (Centralized Conventional), GGM 8000 operates as a Site Gateway. The Site Gateway is used for transport between the site and the Conventional Base Radio sub-sites.

11.2.2.1
Conventional Base Radio Subsite Gateway – Installation

NOTICE: For a general installation process, refer to Standalone Conventional Voting System – GGM 8000 Installation on page 248.

The following table shows the site-specific cabling for GGM 8000 used at the Conventional Base Radio Subsite (Centralized Conventional).

Table 75: Conventional Base Radio Subsite (Centralized Conventional) – Cabling

Gateway	Port	Device/Function
Site Gateway	LAN 1-4	Site LAN Switch(es), Backhaul Switch(es)
	RS-232	Terminal Server or Local Serial Access

11.2.2.2 Conventional Base Radio Subsite Gateway – Configuration

For configuration procedures, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

11.2.2.3 Conventional Base Radio Subsite Gateway – Operation

For operation procedures, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

11.2.2.4 Conventional Base Radio Subsite Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see Conventional Base Radio Site – Conventional Subsystem on page 239.

11.3 Standalone Conventional Voting System (Distributed Conventional)

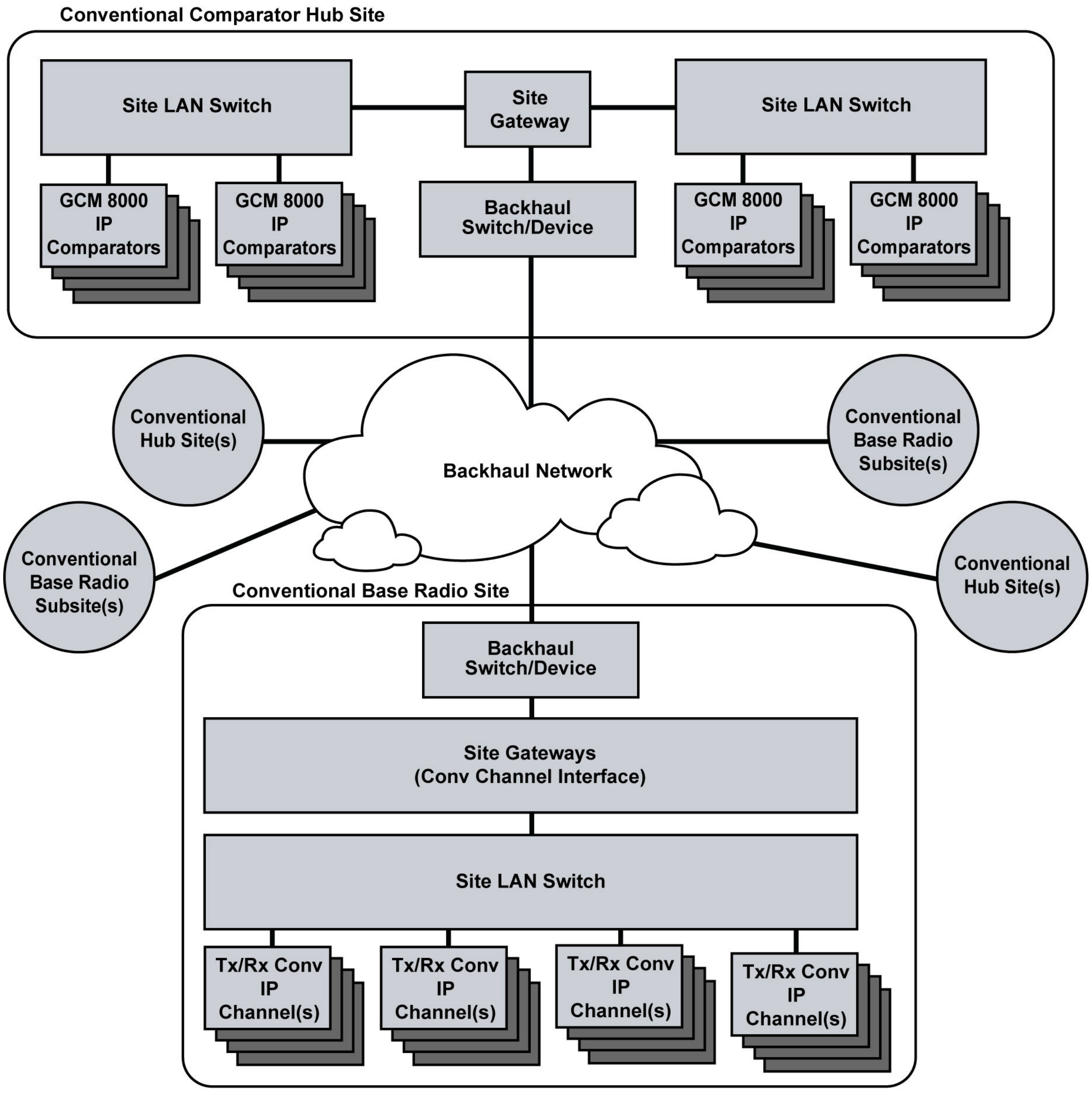
The Standalone Conventional Voting System (Distributed Conventional) system utilizes the following site types:

- Conventional Comparator Hub Site
- Conventional Base Radio Site

As defined by the Distributed Conventional, the Standalone Conventional Voting System DOES actually interface with other sites in a mesh (distributed) architecture.

The following diagram shows the Site Gateways used in Standalone Conventional Voting System (Distributed Conventional).

Figure 114: Standalone Conventional Voting System (Distributed Conventional)



S_Standalone_Conv_Comparator_Sys_DistribArch_B

11.3.1 Conventional Comparator Hub Site Gateway

GGM 8000 in a Conventional Comparator Hub Site is used as a Site Gateway. It provides interface between the Site LAN Switches and the Backhaul Switch.

11.3.1.1 Conventional Comparator Hub Site Gateway – Installation

NOTICE: For a general installation process, refer to Standalone Conventional Voting System – GGM 8000 Installation on page 248.

The following table lists the Site Gateway cabling in the Conventional Comparator Hub Site (Distributed Conventional).

Table 76: Conventional Comparator Hub Site (Distributed Conventional) – Cabling

Gateway	Port	Device/Function
Site Gateway	LAN 1-4	Site LAN Switch(es), Backhaul Switch(es)
	RS-232	Terminal Server or Local Serial Access

11.3.1.2 Conventional Comparator Hub Site Gateway – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

11.3.1.3 Conventional Comparator Hub Site Gateway – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

11.3.1.4 Conventional Comparator Hub Site Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

11.3.2 Conventional Base Radio Site Gateway

GGM 8000 in a Conventional Base Radio Site is used as a Site Gateway. It provides interface between the Site LAN Switch and the Backhaul Switch.

11.3.2.1 Conventional Base Radio Site Gateway – Installation

NOTICE: For a general installation process, refer to Standalone Conventional Voting System – GGM 8000 Installation on page 248.

The following table lists the Site Gateway cabling in the Conventional Base Radio Site (Distributed Conventional).

Table 77: Conventional Base Radio Site (Distributed Conventional) — Cabling

Gateway	Port	Device
Site Gateway	LAN 1-4	Site LAN Switch(es), Backhaul Switch(es)
	RS-232	Terminal Server or Local Serial Access

11.3.2.2 Conventional Base Radio Site Gateway – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

11.3.2.3 Conventional Base Radio Site Gateway – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

11.3.2.4 Conventional Base Radio Site Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

Chapter 12

ASTRO 25 Customer Enterprise Network

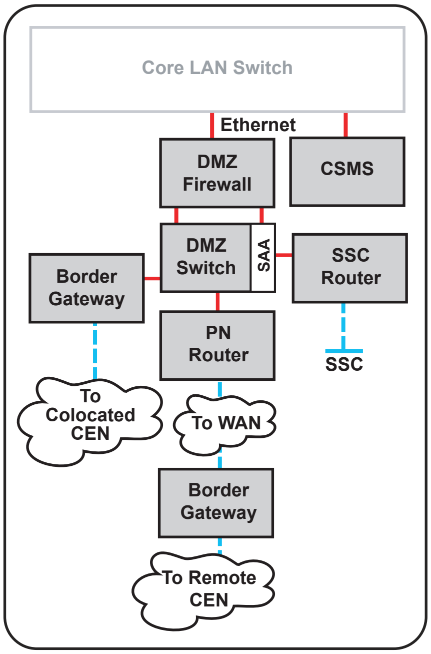
This chapter provides information about the GGM 8000 transport gateway in the Customer Enterprise Network.

12.1 Border Gateway – Functional Description

At the Customer Enterprise Network (CEN), the GGM 8000 Gateway operates as a Border Gateway.

The Border Gateway serves as the demarcation between a peripheral network and the Motorola Solutions Radio Network Infrastructure (RNI). One side of the border gateway provides an interface with the CEN. The other side of the border gateway attaches to a peripheral network to interface with devices included as part of the Motorola Solutions radio network infrastructure (RNI). The border gateway uses a Dynamic Host Configuration Protocol (DHCP).

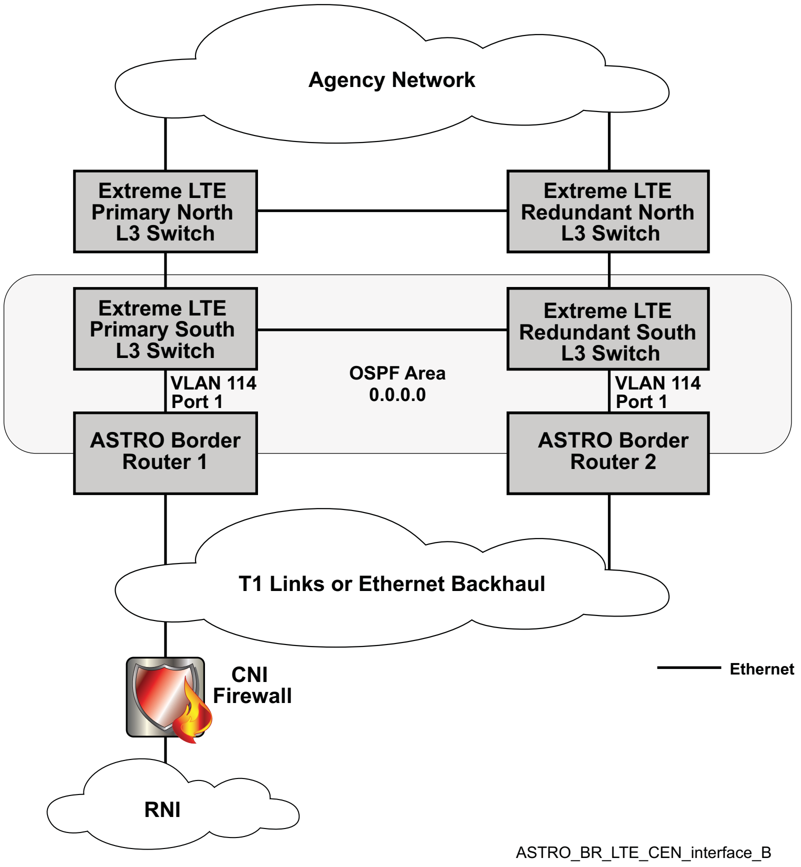
Figure 115: Border Gateway



S_Border_Gateway_C

In the ASTRO/LTE CEN configuration, if present in the system, the ASTRO Border Gateway(s) interface to LTE switching and routing equipment. Both single and dual Border Gateway configurations are supported. In case of dual Border Gateway configuration, one VLAN is provided on both Border Gateway connections. The OSPF protocol is used between the Border Gateway(s) and the LTE Primary South Router and Primary North Router.

Figure 116: ASTRO/LTE CEN Interface


Agency Network
Extreme LTE Primary North L3 Switch
Extreme LTE Redundant North L3 Switch
Extreme LTE Primary South L3 Switch
Extreme LTE Redundant South L3 Switch
OSPF Area 0.0.0.0
VLAN 114 Port 1
VLAN 114 Port 1
ASTRO Border Router 1
ASTRO Border Router 2
T1 Links or Ethernet Backhaul
CNI Firewall
Ethernet
RNI
ASTRO_BR_LTE_CEN_interface_B

12.2
Border Gateway – Installation

Process:

1 Install the Border Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.

2 Connect the Border Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.

3 If necessary, ground the Border Gateway. See Connecting a Chassis Ground on page 68.

4 Configure the Border Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.

> **NOTICE:** This step does not apply to Border Gateways in ASTRO/LTE CEN configuration. In this case the Border Gateways should be configured manually using a configuration document. For details concerning Border Gateways in ASTRO/LTE CEN configuration see Border Gateway – Functional Description on page 255.

5 Connect the CEN equipment to the Border Gateway. See one of the following tables in Border Gateway – Site-Specific Cabling on page 257:

- For CEN geographically separated from RNI, see Table 78: Border Gateway Cabling – CEN Separated from RNI on page 257.
- For colocated CEN, see Table 79: Border Gateway Cabling – Colocated CEN on page 257.

12.2.1 Border Gateway – Site-Specific Cabling

If a CEN is geographically separated from the RNI, the Border Gateway backhaul LAN/WAN connection is terminated on a peripheral network router that is colocated with the RNI. See the following table.

Table 78: Border Gateway Cabling – CEN Separated from RNI

Gateway	Port	Device/Function
Border Gateway	LAN 1	Backhaul Router
	T1/E1 5A	Connection to the Peripheral Router
	RS-232	Terminal Server or Local Serial Access

If a CEN is geographically colocated with the RNI, the Border Gateway backhaul LAN connection is directly terminated at the DMZ provided by the RNI-DMZ firewall. No peripheral network router is required for this scenario. See the following table.

Table 79: Border Gateway Cabling – Colocated CEN

Gateway	Port	Device/Function
Border Gateway	LAN 1	DMZ Switch
	T1/E1 5A	Connection to the customer enterprise network LAN Switch
	RS-232	Terminal Server or Local Serial Access

If Dynamic System Resilience is implemented on your system, there are two Border Gateways that provide paths to a DSR zone core pair. There are no changes in physical connections.

12.3 Border Gateway – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

12.4 Border Gateway – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

12.4.1 CEN Network Elements Operations

In Unified Event Manager (UEM), network elements in the Customer Enterprise Network (CEN) subsystem must have the IP address of the Network Address Translation (NAT) protocol configured.

The NAT IP address configuration is needed for UEM to be able to discover and manage network elements that are in the CEN subsystem.

For network elements in the CEN subsystem, a device managed resource (DMR) is created with the UEM NAT IP address instead of the UEM Radio Network Infrastructure (RNI) IP address. For network elements with subsystem different from CEN, a DMR is created with UEM RNI IP address.

You can configure single CEN network elements manually or you can configure multiple CEN network elements by loading an external NAT IP configuration file to UEM. The NAT IP configuration file is generated by Motorola Solutions Support Center (SSC) per request.

12.4.1.1 Configuring NAT IP for Multiple Network Elements in the CEN

Follow this procedure for expansion purposes only. In this procedure, you configure the IP address of the Network Address Translation (NAT) protocol of Customer Enterprise Network (CEN) network elements that are not managed by Unified Event Manager (UEM). Configure the NAT IP address in UEM to enable UEM to discover CEN network elements that use the NAT protocol. If the NAT IP address is not configured in UEM, UEM discovers the network elements but they do not communicate with UEM.

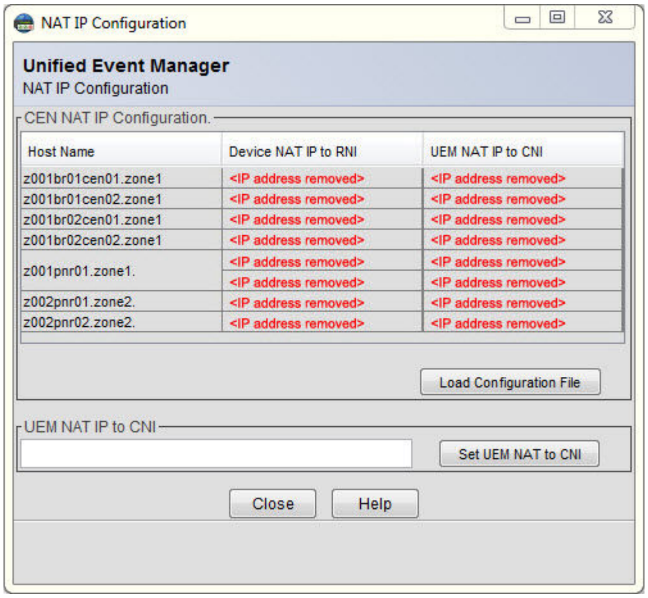
Prerequisites: Contact Solution Support Center (SSC) and request the creation of a NAT IP configuration `.xml` file.

Procedure:

1. Save the NAT IP configuration `.xml` file on a PC with network access to UEM and log on to UEM from the PC.
2. In UEM, from the main menu, select **Tools** → **Configure NAT IP**.
3. In the **NAT IP Configuration** window, click **Load Configuration file**.
4. Navigate to the NAT IP configuration`.xml` file you want to load. Click **Open**.

IP addresses necessary for UEM and CEN network elements to communicate are loaded to UEM and appear in the **NAT IP Configuration** window.

Figure 117: NAT IP Configuration Window



Unified Event Manager
NAT IP Configuration

CEN NAT IP Configuration.

Host Name	Device NAT IP to RNI	UEM NAT IP to CNI
z001br01cen01.zone1	<IP address removed>	<IP address removed>
z001br01cen02.zone1	<IP address removed>	<IP address removed>
z001br02cen01.zone1	<IP address removed>	<IP address removed>
z001br02cen02.zone1	<IP address removed>	<IP address removed>
z001pnr01.zone1.	<IP address removed>	<IP address removed>
	<IP address removed>	<IP address removed>
z002pnr01.zone2.	<IP address removed>	<IP address removed>
z002pnr02.zone2.	<IP address removed>	<IP address removed>

UEM NAT IP to CNI

Postrequisites: Discover reconfigured network elements to ensure correct communication with UEM.

1 If the reconfigured network elements are already discovered, delete them from UEM.

2 Discover the reconfigured network elements. See Discovering a Gateway in UEM on page 289.

12.4.1.2
Configuring NAT IP for a Single Network Element in the CEN

Follow this procedure to configure the IP address of the Network Address Translation (NAT) protocol of single Customer Enterprise Network (CEN) network elements that Unified Event Manager (UEM) manages. Configure the NAT IP address in UEM to enable UEM to discover CEN network elements that use the NAT protocol. If the NAT IP address is not configured in UEM, UEM discovers the network elements but they do not communicate with UEM.

Procedure:

1 From the main menu, select **Tools** → **Configure NAT IP**.

2 In the **UEM NAT IP to CNI** field, type the IP address of the network element you want to configure. Click **Set UEM NAT to CNI**.

IP addresses necessary for UEM and CEN network elements to communicate are loaded to UEM and appear in the **NAT IP Configuration** window.

Postrequisites: Discover reconfigured network elements to ensure correct communication with UEM.

1 If the reconfigured network elements are already discovered, delete them from UEM.

2 Discover the reconfigured network elements. See Discovering a Gateway in UEM on page 289.

12.5
Border Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting apply.

12.5.1
Border Gateway – Failures

In case of a Border Gateway failure, link between the CEN and the RNI is lost. If a redundant Border Gateway is present in the system, losing one link does not cause the connection to the RNI to be lost.

If the Border Gateway in the Unified Event Manager (UEM) displays a CommFailure message, the potential reason is that the gateway was re-configured and the maximum number of registered UEM managers was reached. To re-manage the Border Gateway, clear the registered SNMP managers. For information about clearing the registered SNMP managers, see “Resetting SNMPv3 Data on MNR Routers and GGM 8000 Gateways” in the *SNMPv3 Feature Guide*.

Chapter 13

ASTRO 25 Interoperability

This chapter provides information about the GGM 8000 used at the ISSI.1 and the SmartX sites.

13.1 Interoperability Site Gateway – Installation

When and where to use: Follow this process to install the Site Gateway (ISSI.1) and the SmartX Gateway.

Process:

1. Install the Site Gateway in a rack. See Rack-Mounting the GGM 8000 on page 58.
2. Connect the Site Gateway to a power source. See Connecting the GGM 8000 to a Power Source on page 67.
3. If necessary, ground the Site Gateway. See Connecting a Chassis Ground on page 68.
4. Configure the Site Gateway. See Downloading a Stored Configuration File to the GGM 8000 on page 93.
5. Connect the site equipment to the Site Gateway.
   - For the Site Gateway (ISSI.1), see Site Gateway (ISSI.1) – Installation on page 261.
   - For the SmartX Gateway, see SmartX Gateway – Installation on page 264.

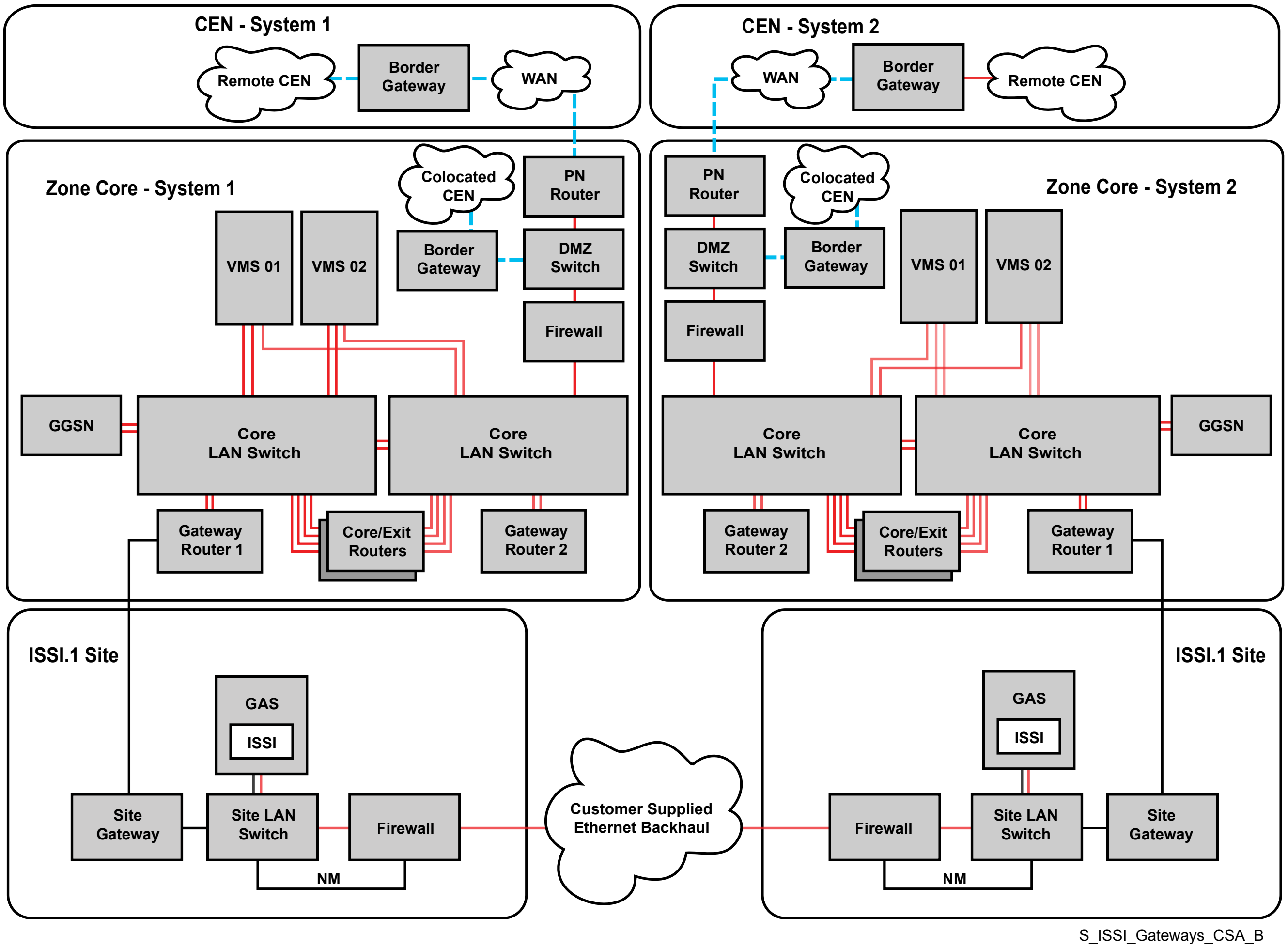
13.2 Site Gateway (ISSI.1) – Functional Description

GGM 8000 can operate as a Site Gateway to an ISSI.1 site. The Site Gateway (ISSI.1) provides an interface between the ISSI.1 site and an ASTRO® 25 system master site.

If more than one ISSI.1 Gateway application is installed on the Generic Application Server at the site, each of the applications requires its own dedicated Site Gateway (ISSI.1) link.

The following diagram shows the Site Gateway used at an ISSI.1 site.

Figure 118: ISSI.1 Gateway



13.2.1

Site Gateway (ISSI.1) – Installation

NOTICE: For a general installation process, refer to Interoperability Site Gateway – Installation on page 260.

The following table presents the cabling of a Site Gateway at an ISSI.1 site.

Table 80: Site Gateway (ISSI.1) – Cabling

Gateway	Port	Device/Function
Site Gateway	LAN 1	ISSI.1 Site LAN Switch
	T1/E1 5A	Connection to the customer-supplied Backhaul
	RS-232	Terminal Server or Local Serial Access

13.2.2 Site Gateway (ISSI.1) – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

13.2.3 Site Gateway (ISSI.1) – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

13.2.4 Site Gateway (ISSI.1) – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic maintenance and troubleshooting procedures apply.

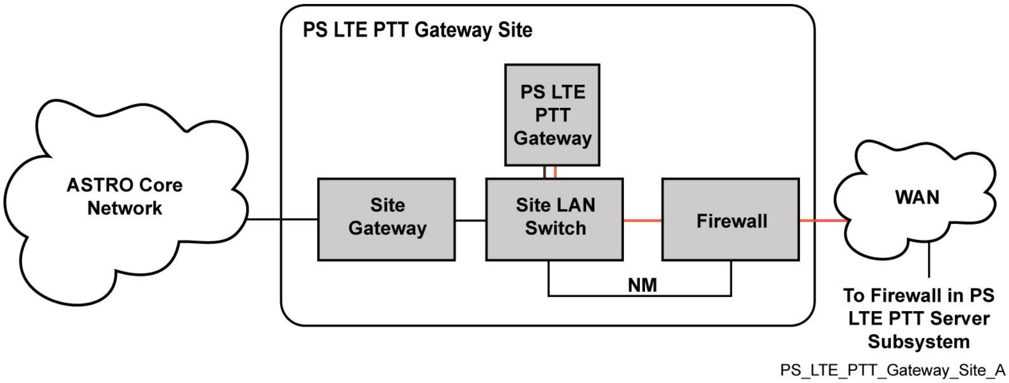
13.3 Site Gateway (PS LTE PTT Gateway) – Functional Description

GGM 8000 can operate as a Site Gateway to a PS LTE PTT Gateway site. The Site Gateway (PS LTE PTT Gateway) provides an interface between the PS LTE PTT Gateway site and an ASTRO® 25 system master site.

If more than one PS LTE PTT Gateway is installed at the site, each requires its own dedicated Site Gateway. The PS LTE PTT gateway to site gateway connection is through the site LAN switch.

The following diagram shows the Site Gateway that is used at a PS LTE PTT Gateway site.

Figure 119: PS LTE PTT Gateway Subsystem



13.3.1 Site Gateway (PS LTE PTT Gateway) – Installation

For a general installation process, see Interoperability Site Gateway – Installation on page 260. The following table presents the cabling of a Site Gateway at a PS LTE PTT Gateway site.

Table 81: Site Gateway (PS LTE PTT Gateway) – Cabling

Gateway	Port	Device/Function
Site Gateway	LAN 1	PS LTE PTT Gateway Site LAN Switch

Gateway	Port	Device/Function
	T1/E1 5A	Connection to the customer-supplied Backhaul
	RS-232	Terminal Server or Local Serial Access

13.3.2 Site Gateway (PS LTE PTT Gateway) – Configuration

For configuration information, see GGM 8000 Configuration on page 93. Generic configuration procedures apply.

13.3.3 Site Gateway (PS LTE PTT Gateway) – Operation

For operation information, see GGM 8000 Operation on page 103. Generic operation procedures apply.

13.3.4 Site Gateway (PS LTE PTT Gateway) – Maintenance and Troubleshooting

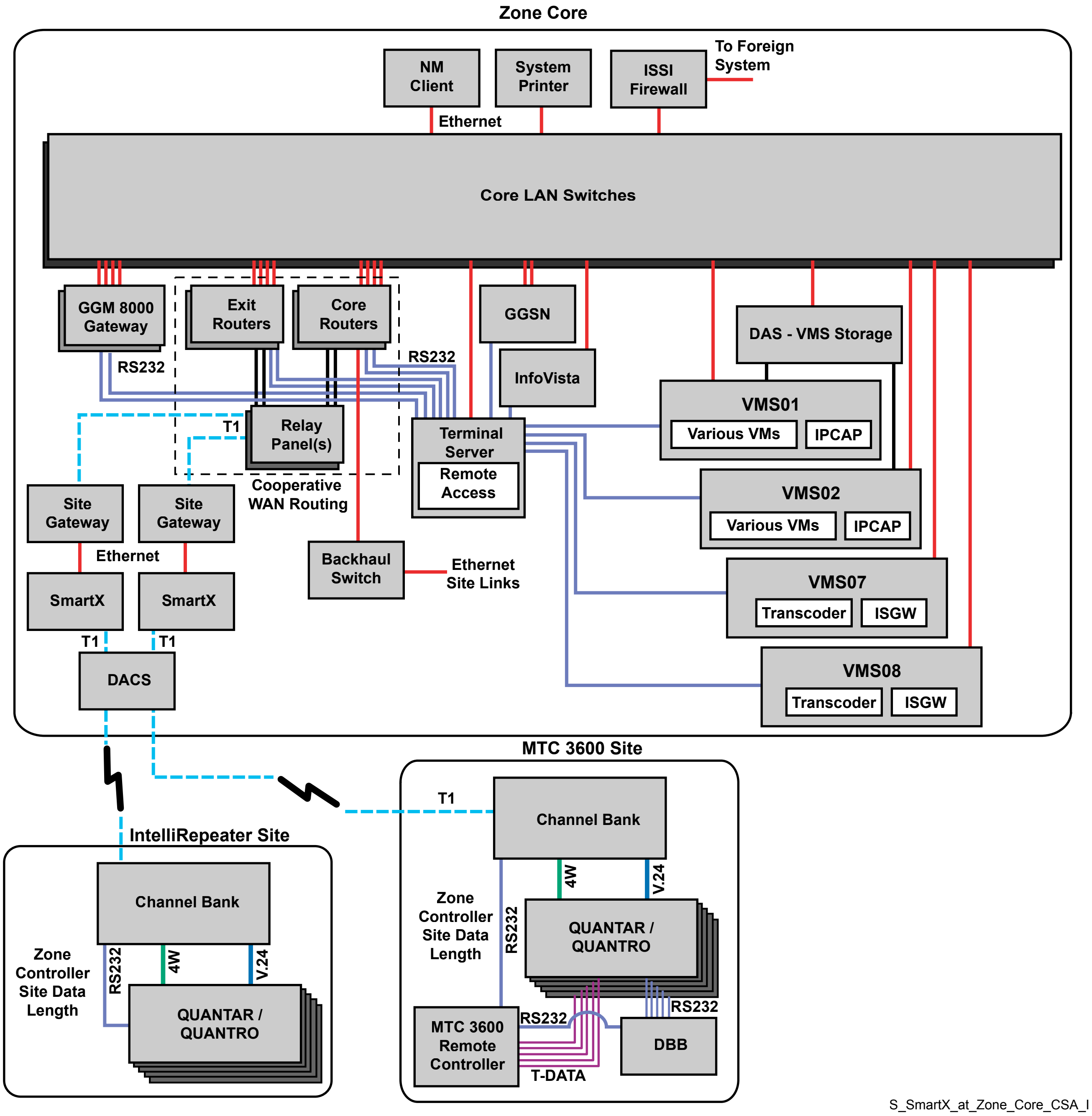
For maintenance and troubleshooting information, refer to GGM 8000 Maintenance on page 114 and Troubleshooting on page 114. Generic maintenance and troubleshooting procedures apply.

13.4 SmartX Gateway – Functional Description

GGM 8000 can operate as a Site Gateway to a SmartX Site Converter. The SmartX Gateway is placed with a SmartX Site Converter either at a 3600 RF Site or a master site. Its role is providing an interface between the SmartX Site Converter and the ASTRO® 25 system master site.

The following diagram shows the SmartX Gateway at an ASTRO® 25 master site.

Figure 120: SmartX Gateway



13.4.1
SmartX Gateway – Installation

NOTICE: For a general installation process, see Interoperability Site Gateway – Installation on page 260.

The following table presents the cabling of the SmartX Gateway at an RF repeater site.

Table 82: SmartX Gateway Cabling at an RF Repeater Site

Gateway	Port	Device/Function
SmartX Gateway	LAN 1	SmartX Site Converter
	LAN 3	Ethernet site link connection to the ASTRO® 25 system master site.
	T1/E1 5A	Connection to the ASTRO 25® system master site
	RS-232	Terminal Server or Local Serial Access

The following table presents the cabling of the SmartX Gateway at a master site.

Table 83: SmartX Gateway Cabling at a Master Site

Gateway	Port	Device/Function
SmartX Gateway	LAN 1	SmartX Site Converter
	LAN 3	Ethernet site link connection to the ASTRO® 25 Core Backhaul Switch
	T1/E1 5A	Connection to the relay panel at the ASTRO® 25 system master site
	RS-232	Terminal Server or Local Serial Access

The following table presents the cabling of the SmartX Gateway at an MTC3600 site.

Table 84: SmartX Gateway Cabling at MTC3600 Site

Gateway	Port	Device/Function
SmartX Gateway	LAN 1	SmartX Site Converter
	T1/E1 5A	Digital Access Cross-connect Switch (DACS)
	RS-232	Terminal Server or Local Serial Access

13.4.2 SmartX Gateway – Configuration

For configuration information, see GGM 8000 Introduction and Common Procedures on page 28. Generic configuration procedures apply.

13.4.3 SmartX Gateway – Operation

For operation information, see GGM 8000 Introduction and Common Procedures on page 28. Generic operation procedures apply.

13.4.4
SmartX Gateway – Maintenance and Troubleshooting

For maintenance and troubleshooting information, see GGM 8000 Introduction and Common Procedures on page 28. Generic troubleshooting and maintenance procedures apply.

13.5
A3.1 Coexistence

The A3.1 Coexistence feature provides connectivity between one or more ASTRO 3.1 Conventional systems and an ASTRO® 25 7.x system. To support the A3.1 Coexist feature, a GGM 8000 equipped with an expansion module can be used at an ASTRO® 25 system 7.x sites to provide the interface for comparator equipment and/or base radio equipment located at ASTRO 3.1 conventional sites in order to support conventional channel operation.

The Analog/V.24 interface kit, which consists of a four-wire E&M module and a DSP SIMM installed in the analog slot and two V.24 modules installed in the I/O slots, supports both analog conventional and digital conventional operation. For more information, see Expansion Module on page 33.

Table 85: Site Gateway (Console Site) Cabling – A3.1 Coexistence

Gateway		Port	Device/Function
Site Gateway (Console Site)	Base module	LAN 1	Console Site LAN Switch
		T1/E1 5A	T1/E1 Relay Panel(s) – site links to the zone core.
		T1/E1 5B	T1/E1 Relay Panel(s) – optional redundant site links to the backup zone core in DSR systems.
		RS-232	Terminal Server or Local Serial Access
	Analog/V.24 interface kit	4-wire ports / ASTRO (V.24 digital) ports	Colocated Base Radio and/or Comparator Interface ports (4 Analog, 4 Digital)

When both MCC dispatch consoles and non-MCC dispatch consoles are connected to the same conventional station (parallel console audio operation), dispatchers on both types of console must know when a dispatcher on the other type of console is transmitting on the station and to hear the transmitted audio. For analog and MDC-capable channels, Line Operated Busy Lights (LOBLs) and summing amplifiers support parallel console operation. See the *RF Site Technician Reference Guide* for details.

For more information about Conventional Channel Interface 4W and V.24 connections, refer to the following sections:

- GGM 8000 Analog Interfaces to a QUANTAR or GTR 8000 Base Station Connections on page 76
- Digital Base Stations to Conventional Channel Gateway on page 83

Chapter 14

System Gateways Disaster Recovery

This chapter provides references and information that will enable you to recover a GGM 8000 gateway in the event of a failure.

NOTICE: For disaster recovery procedures for the GGM 8000 with IPLC functionality, see "Replacing a GGM 8000 with IPLC Functionality" in the *GGM 8000 with IP Link Converter (IPLC) Functionality User Guide*.

14.1 Recovering Site/Core Gateways – Non-Hardened Systems

Prerequisites: If necessary, contact your system administrator to obtain the following items:

- IP address
- Account logins and passwords

Before beginning the replacement procedure, ensure that the replacement GGM 8000 has the same hardware installed in the left-hand slot. Possible hardware includes:

- Blank filler panel
- Enhanced Conventional Gateway module (High Density (8 analog ports and 8 V.24 ports) or Low Density (four analog ports and four V.24 ports))
- Expansion module equipped with one of the following:
  - analog/V.24 interface kit (E&M daughterboard and two V.24 daughterboards)
  - FlexWAN daughterboards

NOTICE: One way to test that the hardware configurations match is to make sure that there is a connector on the replacement unit for each of the cables connected to the existing unit.

When and where to use: Use this procedure when replacing a gateway device in a non-hardended system.

Process:

1. Physically replace the gateway hardware. See Replacing a GGM 8000 on page 126.
2. Execute the `Clear USM Cache` saved command in the VoyenceControl component of the Unified Network Configurator (UNC). `Clear USM Cache` is in the list of saved commands under **System** → **Motorola** → **SNMPv3**.

   For information about accessing and executing saved commands for a device, see the "Accessing and Executing Existing Saved Commands" section in the *Unified Network Configurator User Guide*.

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
3. If you do not have the correct EOS version on Unified Network Configurator (UNC), load the EOS onto UNC. See Loading the EOS Image to the UNC Server on page 272.
4. Check the version of the firmware if performing a downgrade. If the version is 16.8.0.19 or higher for an NMR, additional steps are necessary. See Performing a Firmware Downgrade on page 273.

5. Extract the configuration files from the UNC. See Extracting Configuration Files from UNC on page 274.
6. Install an EOS image and manage SSH keys. See Installing an EOS Image and Managing SSH Keys on page 275.
7. Only if link encryption is required, add link encryption. See Adding Link Encryption on page 277.
8. Assign passwords. See Assigning Passwords on page 281.
9. Push the configuration to the gateway. See Pushing the Configuration to the Gateway on page 284.
10. Set up Information Assurance. See Setting Up Information Assurance on page 285.
11. Test SNMPv3 Credentials. See Testing SNMPv3 Credentials on page 286.
12. Push the configurations from VoyenceControl to the secondary directory of the gateway. See Pushing Configurations to the Secondary Directory of a Gateway on page 287.

    NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

13. Pull the configuration to UNC. See Pulling the Configuration to Unified Network Configurator on page 288.
14. Delete the router from Unified Event Manager. See Deleting a Gateway from UEM on page 288.
15. Discover the router in Unified Event Manager. See Discovering a Gateway in UEM on page 289.

14.2 Recovering Site/Core Gateways – Hardened Systems

Prerequisites: If necessary, contact your system administrator to obtain the following items:

- IP address
- Account logins and passwords
- *Unified Network Configurator User Guide*
- *Unified Event Manager User Guide*
- Gateway root password (Reference System Password List)
- Gateway configuration file, `boot.cfg` (see instructions in the following process)
- Access Control List (ACL) file, `acl.cfg` (see instructions in the following process)
- StaticRP file, `staticRP.cfg` (see instructions in the following process)
- PSK file, `psk.cfg` located in the Customer Documentation Media section 13 Equipment Programming and Password>Equipment Programming> Network> “Customer files specific files”>routers **or** PSK file, `psk.cfg` located in Final System Documentation Section 07 Programming Information>7.2 ASTRO System Programming>7.21. Radio Network Configuration>USCG R21 AK_RRCS Configs_2014.06.25-14.19.01>routers
- The correct EOS Enterprise Operating System file, `boot.ppc` loaded in the UNC application
- RADIUS Secret (Reference System Password List)
- FipsPreShrdKey for link encryption (Reference System Password List)
- TFTP server (3COM, SolarWinds)
- Console cables for the GGM 8000 Gateway and the HP Switch that it connects to
- Laptop with terminal emulation program (PuTTY). Laptop or PC must have an RS-232 serial port. (If the laptop or PC does not have an RS-232 port, use a USB-to-RS-232 adapter).

- Ethernet cable
- ESP strap

Before beginning the replacement procedure, ensure that the replacement gateway has the same hardware installed in the left-hand slot. Possible hardware includes:

- Blank filler panel
- Enhanced Conventional Gateway module (High Density (eight analog ports and eight V.24 ports) or Low Density (four analog ports and four V.24 ports))
- Expansion module equipped with one of the following:
  - analog/V.24 interface kit (E&M daughterboard and two V.24 daughterboards)
  - FlexWAN daughterboard

NOTICE: One way to test that the hardware configurations match is to make sure that there is a connector on the replacement unit for each of the cables connected to the existing unit.

When and where to use: Use this procedure when replacing a gateway device in a hardened system.

Procedure:

1. Physically replace the gateway hardware. See Replacing a GGM 8000 on page 126 and perform steps 1 through 6.
2. Extract the configuration files from the UNC. See Extracting Configuration Files from UNC on page 274.

   NOTICE: Use Notepad over other text processing applications to ensure that the file is saved as ASCII text without control characters.
   When saving files in Notepad, change “Save As Type” to “All Files” to prevent the addition of `.txt` extension to the saved files.

   Verify that the correct files are saved and move them to the service laptop (reference security local policy to remove files from the NM client).
3. Delete files to a clean state, as follows: (Skip this step if the device is set with Factory default settings).
   - **a** Connect the PC to the Console port on the gateway and open a console session with PuTTY or other suitable terminal software.
   - **b** Log on to the gateway (need root password for the device).
   - **c** Enter: `cd a:/primary`
   - **d** Enter: `remove<filename.extension>` for each of the following files: `acl.cfg`, `boot.cfg`, `staticRP.cfg`, `override.cfg`, `system` (no file ext), and `ccgwdb` (no file ext) files from the primary directory.
   - **e** Enter: `zeroize`
   - **f** Enter: `kekgenerate`
   - **g** Enter: `Reboot`
4. Verify the EOS version and generate new SSH keys. See Installing an EOS Image and Managing SSH Keys on page 275.
   - **a** Verify if the EOS is current and is the same version as the system:
     1. Enter: `show version`
     2. Note the EOS version.
     3. If the EOS version does not match the current system EOS version, push the EOS from Voyence. See step 11.

b **For RSA and DSA algorithms (GenSshKey RSA 2048 and GenSshKey DSA 2048:** Generate the SSH keys on the gateway. Enter: `GenSshKey <algorithm><bite>`

c Delete the SSH keys from UNC by performing steps 1 through 4 of Deleting SSH keys on UNC on page 276.

If the admin menu does not appear when you log on to UNC, at the prompt enter: `admin_menu`

5 **For devices with link encryption:** Add the link encryption secret. See Adding Link Encryption on page 277 and perform the steps for IPV4 links only.

> **NOTICE:** This step is not applicable to standalone CCGWs.
> CCSI generates the `psk.cfg` file in the Customer Documentation media. This file contains the correct commands for each device with link encryption. This file can be found under “13 Equipment Programming and Password>Equipment Programming> Network> “Customer files specific files”>routers”.
>
> The `psk.cfg` file can also be on the Final System Documentation Disk, Section 07 Programming Information>7.2 ASTRO System Programming>7.21. Radio Network Configuration>USCG R21 AK_RRCS Configs_2014.06.25-14.19.01>routers.

6 Add the RADIUS secret and root passwords. See Assigning Passwords on page 281.

- For RADIUS secret, perform step 1b.
- For root password, perform step 2.

7 Display and obtain the MAC address of the router port connected to the switch, as follows:

a At the prompt, enter: `Show-IP Addr`

b Record the MAC address for Port 1, Type Local interface.

8 Push the configuration to the gateway using TFTP. See Pushing the Configuration to the Gateway on page 284.

> **NOTICE:** If you cannot connect to the gateway through Ethernet port 1, ensure that the PC or laptop Ethernet port speed and duplex settings are set to auto-negotiate.

a At the prompt, enter: `reboot`

9 Disable MAC port lockdown, cable the new gateway, and enable MAC port lockdown. See Setting Up Information Assurance on page 285 and perform steps 3 through 9.

> **NOTICE:** For sites with dual site links, both gateways must be rebooted after placing both switches in Learn mode for the port that is connected to the gateways. Step 7 of Setting Up Information Assurance on page 285 details the procedure for assuring that the switch Learns both MAC addresses.

10 Setup SNMPv3, as follows:

a Update the device credential to SNMPv3 “MotoMaster Clear” and test its credentials.

1 See “Updating the EMC Smarts Network Configuration Manager Credentials for a Device” in the *Unified Network Configurator User Guide* and perform steps 1 through 5, 7, and 9 for SNMPv3 credentials only.

2 See “Testing Credentials for Devices” in the *Unified Network Configurator User Guide*.

b If the device credential passes in substep a, execute the `Change SNMPv3 Users From Clear to AuthPriv` saved command in the VoyenceControl component of the Unified Network Configurator (UNC). `SNMPv3 AuthPriv` is in the list of saved commands under: **System** → **Motorola** → **SNMPv3**. See “Accessing and Executing Existing Saved Commands” in the *Unified Network Configurator User Guide*.

> **NOTICE:** The NewAuthPass and NewPrivPass are set to the system password. Check with your systems administrator to verify. The AdminAuthPass and AdminPrivPass are the MotoAdmin credentials and can be found in the system password list.
>
> The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

c Update the device credential to SNMPv3 "MotoMaster Secure" and test its credentials.

1 See "Updating the EMC Smarts Network Configuration Manager Credentials for a Device" in the *Unified Network Configurator User Guide* and perform steps 1 through 5, 7, and 9 for SNMPv3 credentials only.

2 See "Testing Credentials for Devices" in the *Unified Network Configurator User Guide*.

d If the credential fails, execute the `Clear USM Cache` saved command in the VoyenceControl component of the Unified Network Configurator (UNC). `Clear USM Cache` is in the list of saved commands under **System** → **Motorola** → **SNMPv3**. See "Accessing and Executing Existing Saved Commands" in the *Unified Network Configurator User Guide*.

e Test the device credential and verify SNMPv3 credentials are successful with "MotoMaster Secure". See "Testing Credentials for Devices" in the *Unified Network Configurator User Guide*.

11 Optional: Push the EOS from VoyenceControl. See "Updating OS and Configuration Files on MNRs and Switches in UNC" in the *Unified Network Configurator User Guide*.

> **NOTICE:** A manual reboot after the update is required and causes the resources served by this gateway to become unavailable causing a resource outage. This reboot can be delayed to a later time.

a Reboot the device after successfully updating the EOS. See "Rebooting Routers, Gateways, Site Controllers, Comparators, Base Radios, SmartX Site Converters, and MCC 7500 VPMs" in the *Unified Network Configurator User Guide*.

12 Test SNMPv3 in UEM. See "Testing the Outbound SNMPv3 configuration for a Managed Resource" in the *Unified Event Manager User Guide*.

13 If the SNMPv3 test fails in UEM, perform the following:

a In **Database View**, select the **GGM8000 Node**.

b Right-click and select **Re-Discover**.

c At the confirmation window, click **Yes**.

d Verify that the Re-Discovery was successful.

e If Re-Discovery was unsuccessful, right-click the **GGM8000 Node** and select **Delete object and traces**.

f Discover the device. See "Discovering Network Elements" in the *Unified Event Manager User Guide*.

14 If the GGM8000 has CCGW capabilities, at the prompt perform the following:

a Enter: `show -ccgw conf` to verify that the CCGW configuration is setup.

b Enter: `df a:/primary` and verify that the CCGWDB file was downloaded with a time stamp when the gateway was reloaded.

c If the CCGWDB file is not present, then reboot the GGM8000 and repeat steps a and b.

15 Create a backup of the Primary directory by copying the Primary to the Secondary directory, as follows:

a Access the gateway using the Cut-Through Method. See "Accessing Devices Using the Cut-Through Method" in the *Unified Network Configurator User Guide*.

b Enter: `copy a:/primary/*.* a:/secondar`

16 Perform a “Pull all” for the device in VoyenceControl. See “Scheduling the Pull of a Device Configurations” in the *Unified Network Configurator User Guide*.

17 If required, schedule a reboot of the gateway to activate the update EOS. See “Rebooting Routers or Gateways at a Scheduled Time” in the *Unified Network Configurator User Guide*.

18 Add the PIM-SM Authentication Feature. See “Adding the PIM-SM Authentication Feature” in the *Link Encryption and Authentication Feature Guide*.

NOTICE: If the gateway is in a Conventional subsystem, apply PIM and OSPF authentication to the conduit gateway. Apply only OSPF authentication to the other Conventional subsystem gateways.

a Run each of the four commands. Navigate to Authentication > Enable. After each command, navigate back to the folder to choose the next step.

1 Configure Router Key.

2 Activate Transit Mode Authentication.

3 Verify Transit Mode Authentication.

4 Activate Secure Mode Authentication.

NOTICE: VoyenceControl retains the PIM state for a device; clear_state, transit, and secured. If a gateway was replaced that had been secured and you attempt to perform substeps 1 or 2 on a new gateway, it might fail with an error that has some reference to the state. Follow step b to force the operation to clear_state.

b Go to the gateway saved commands and navigate to Authentication > Utils > Repair and select Override_Operation_State.

14.3 Loading the EOS Image to the UNC Server

When and where to use: This procedure is used by the Motorola Solutions Support Center (SSC) to load the EOS image (`boot.ppc`) on to the UNC server. Load the EOS image (`boot.ppc`) from the media device if you do not have the correct version of EOS on the UNC server. It is not necessary to perform this procedure if the correct version of the EOS already exists on the UNC server.

Procedure:

1 Perform the appropriate steps:

If…	Then…
You use PuTTY to log on to the UNC server,	perform the following tasks. a Using proper credentials for the UNC administrator, log on to UNC. b In the Host Name (or IP address) field, enter: ***`<username>`***`@`***`<IP address of the server>`*** **NOTICE:** Refer to the *Securing Protocols with SSH Feature Guide* for details. c At the prompt, enter: `su -` and the password for account with root privileges. d Press ENTER.
If you use VMware	perform the following tasks:

If…	Then…
VSphere Client to access UNC,	**a** Start the **VMware VSphere Client** client from the **NM** client. **b** Select the following VMserver address: **10.<*z*>.233.122**, where **<*z*>** is the zone number. **c** Enter a username and password. **d** Select **UNC** from the list on the left pane. **e** Select **Console**. **f** Enter a username and password.

2 At the root prompt, enter `admin_menu`

The **Main Menu** displays.

3 Enter the number corresponding to the **Application Administration** option. Press ENTER.

4 In the **Application Administration** menu that displays, enter the number that corresponds to the **OS Images Administration** option. Press ENTER.

5 In the **OS Images Administration** menu that displays, enter the number that corresponds to the **Load new OS images** option. Press ENTER.

Messages display, indicating that the OS image files referenced in the Voyence database are deleted and describing the two methods for loading an OS image. You are prompted to insert media now, if needed.

6 Insert the media device that contains the EOS `.tar` file to your PC's CD/DVD drive. Press ENTER.

Messages appear with descriptions of the status of the image processing, followed by the **OS Images Administration** menu.

7 Enter the number corresponding to the **Eject CD/DVD** option. Press ENTER.

The **CD/DVD ejected** message appears below the **OS Images Administration** menu.

8 Enter `q`. Press ENTER.

The **User Quit** message appears, followed by the root prompt.

Postrequisites: Proceed to Extracting Configuration Files from UNC on page 274.

14.4 Performing a Firmware Downgrade

Starting with the 16.8.0.19 firmware, the digital signature algorithm is enhanced on the GGM 8000 Gateway software. The enhancement prohibits the gateway from running an unsigned version of the EOS, or running a version of EOS that is signed with a prior pre-enhanced digital signature. If the EOS must be downgraded to a firmware version earlier than 16.8.0.19 but no older than 15.0.0.0, before applying the older firmware, a command must be run that allows the EOS and Boot Monitor to revert to using the older digital signature method for validating the firmware. After running the command, the downgrade can be executed.

If the gateway EOS version 16.8.0.19 or newer must be downgraded to a version older than 15.0.0.0, then a two-step process is required. Downgrade the EOS to 15.0.0.0 by performing the following procedure. Once the gateway is at 15.0.0.0, then downgrade to the older targeted EOS firmware version using normal procedures.

When and where to use: Use this procedure when downgrading the gateway.

Process:

1 To check the version of firmware on the gateway, enter: `sh ver`

2 Depending on the software version, choose one of the following:

- Version 16.8.0.18 or lower means that the downgrade can use the older signature algorithm. Go to step 4.
- Version 16.8.0.19 or higher, go to step 3.

3 To change the SW Signing Algorithm, enter: `setd -sys ssa = SHA1withRSA1024`

NOTICE: If this command is not performed before loading the older firmware, an error message appears. After bootup, the gateway may not have firmware to run if the gateway is configured with only one boot source (a:/primary or a:/secondary) as the firmware location. The gateway can be recovered from the Boot Monitor by performing the following substep:

a Enter: `SA SHA1withRSA1024`

4 Depending on the final target version, choose one of the following:

- Version 15.0.0.0 or higher, can be directly downgraded from the current version. No further steps are necessary. Proceed as normal with the downgrade process.
- Version lower than 15.0.0.0, go to step 5.

NOTICE: If step 5 is not performed before loading the older firmware, an error message appears informing about the incorrect firmware authentication signature.

5 Downgrade the firmware to any version with the numbers from the pool: 16.7.X.X. After the gateway bootup with the new temporary firmware, enter: `SETDefault -SYS FIPS = OFF`

6 Proceed as normal with the downgrade process.

14.5 Extracting Configuration Files from UNC

Prerequisites: Obtain access to Unified Network Configurator (UNC).

Procedure:

1 On the PNM Client, open the VoyenceControl (10.0.0.2) application.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

2 For the username and password, enter `Admin`.

3 Select **Tools** → **Networks Navigation**.

4 In the **Networks Navigation** window, select **Astro 25 Radio Network** → **Views**. Double-click **Motorola Network Resource**.

5 In the right pane, double-click the appropriate gateway.

The **Configs** window opens listing all the config files for the gateway, for example acl.cfg, boot.cfg, override.cfg, and staticRP.cfg.

6 In the left pane, double-click **A:/primary/acl.cfg** to open the acl.cfg file in the right pane.

NOTICE: If no acl.cfg file exists, for example no file is displayed in the right pane when you double-click the corresponding path in the left pane, continue with step 8.

7 Copy the acl.cfg file from the right pane, paste the file to a Notepad file. Save the file as acl.cfg.

8 Perform the following actions:

   a Repeat steps 6 and 7 for the boot.cfg file:

   - Double-click `A:/primary/boot.cfg` in step 6.
   - Save the file as boot.cfg in step 7.

   b Repeat steps 6 and 7 for the override.cfg file:

   - Double-click `A:/primary/override.cfg` in step 6.
   - Save the file as override.cfg in step 7.

   c Repeat steps 6 and 7 for the staticRP.cfg file:

   - Double-click `A:/primary/staticRP.cfg` in step 6.
   - Save the file as staticRP.cfg in step 7.

   d (GGSN gateways only) Repeat steps 6 and 7 for the xgsn.cfg file:

   - Double-click `A:/primary/xgsn.cfg` in step 6.
   - Save the file as xgsn.cfg in step 7.

NOTICE: If the gateways does not have a particular type of configuration file skip the step corresponding to that configuration file. For example, if the gateways does not have an override.cfg configuration file, skip step b.

Postrequisites: Proceed to Installing an EOS Image and Managing SSH Keys on page 275.

14.6 Installing an EOS Image and Managing SSH Keys

Prerequisites: Ensure you have the required cabling and connectors.

When and where to use: Perform this procedure to install EOS, generate SSH keys on the device, and delete SSH keys on Unified Network Configurator (UNC).

Process:

1 Connect the new gateway to the laptop by using the console and Ethernet cables.

IMPORTANT: Do not connect the gateway to the WAN or LAN yet.

2 From the laptop, push the new EOS locally by using TFTP. See Pushing EOS Locally on page 276.

3 If SSH is enabled, perform the following actions:

   a Generate SSH keys on the gateway by entering:

   `GenSshKey` ***`<algorithm><bits>`***
   Where RSA is the default ***`<algorithm>`*** and 2048 is the default ***`<bits>`*** value.

   b Delete SSH keys on UNC. See Deleting SSH keys on UNC on page 276.

4 Continue with one of the following procedures:

- If you add link encryption, perform Adding Link Encryption on page 277.
- If you do not add link encryption, perform Assigning Passwords on page 281.

14.6.1
Pushing EOS Locally

Push new EOS locally from a laptop by using TFTP.

Procedure:

1. Log on to the gateway by using the console connection. Enter the username (root) and appropriate password (usually no password on a new gateway).
2. Point the TFTP server to the boot.ppc file.
3. Assign an IP address to the laptop with the appropriate subnet mask.

   For example, assign 10.0.0.1 with 255.255.255.0.

   NOTICE: This IP address has to be in the same subnet as the gateway interface that is connected to the laptop Ethernet card.
4. Connect the laptop Ethernet card to port 1 of the device (!1) by using a crossover cable.
5. On the gateway (with the 10.0.0.2 IP address in this example), perform the following actions:
   - a Enter: `setd !1 -ip netaddr= 10.0.0.2 255.255.255.0`
   - b Enter: `setd !1 -po cont=e`
   - c Enter: `setd !1 -pa cont=e`
6. To check if Port 1 status is up, enter: `show -ip neta`
7. Ping the laptop IP address to check connectivity.
8. Enter: `copy 10.0.0.1:/boot.ppc a:/primary/boot.ppc`

   NOTICE: The boot.ppc file is copied from the TFTP directory into the gateway primary directory. The file transfer takes about 1 to 3 minutes.
9. Reboot the gateway .
10. After the reboot, verify EOS by entering: `show -sys soi a:/primary/boot.ppc`

    This command displays the EOS software package and version number for the specified boot file in the gateway primary directory. Verify that the correct package and version are listed.

Postrequisites: Return to step 3 in Installing an EOS Image and Managing SSH Keys on page 275.

14.6.2
Deleting SSH keys on UNC

Procedure:

1. Access the Unified Network Configurator (UNC) server by using its IP address.
2. In the login prompt that displays, enter the UNC administrator account credentials.
3. In the **UNC Administration Menu** that appears, perform the following actions:
   - a Enter the corresponding number for **OS Administration**. Press ENTER.
   - b Enter the corresponding number for **Security Provisioning**. Press ENTER.
   - c Enter the corresponding number for **Delete Device's Public SSH Key**. Press ENTER.
4. Enter the IP address for the device.

   The key is deleted.

5 Right-click the device in the VoyenceControl component of the UNC, select **Quick Commands Test Credentials** to establish an SSH connection.

The connection automatically adds the device's SSH host key to the UNC known hosts list.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.
Before you use Test Credentials, ensure that SSH/SCP are selected as the protocols that UNC will use for communication with the device.

Postrequisites: Return to step 4 in Installing an EOS Image and Managing SSH Keys on page 275.

14.7
Adding Link Encryption

Process:

Perform one of the following actions:

- To add link encryption on the site gateway, perform Adding Link Encryption on Site Gateway on page 277.
- To add link encryption on the core or exit routercore gateway, perform Adding Link Encryption on Core Gateway on page 280.

14.7.1
Adding Link Encryption on Site Gateway

Prerequisites: Obtain the location of the required pre-shared keys from your system administrator. The ***<pre-shared key>*** value is the customer-specific secret passphrase.

When and where to use:

NOTICE: Perform this procedure only if Link Encryption is required.

IMPORTANT: This procedure adds crypto keys on the site gateway. The keys **must** match the ones on the core routers or gateways for each site link.

Procedure:

1 Log on to the appropriate site gateway by using the console connection and a null modem serial cable. Enter the username (root) and the appropriate password (usually no password on a new device).

2 Connect a crossover Ethernet cable between the laptop and the gateway.

3 Assign an IP address to the laptop with the appropriate subnet mask.

For example, assign 10.0.0.1 with 255.255.255.0. This IP address has to be in the same subnet as the gateway’s interface that will be connected to the laptop’s Ethernet card.

4 On the gateway (in this example the IP address 10.0.0.2.), enter:

```
setd !1 -ip netaddr= 10.0.0.2 255.255.255.0
```

```
setd !1 -po cont=e
```

```
setd !1 -pa cont=e
```

5 Add crypto keys for the associated core routers or gateways:

If…	Then…
If you add crypto keys for IPv4 links,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey` ***<SysIP_Core1> “<pre-shared key>” “<pre-shared key>”*** where: ***<SysIP_Core1>*** is the system IP address of core router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey` ***<SysIP_Core2> “<pre-shared key>” “<pre-shared key>”*** where: ***<SysIP_Core2>*** is the system IP address of core router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for IPv6 links,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core1_IPv6_backhaul address> “<pre-shared key>” “<pre-shared key>”*** where: ***<Core1_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core2_IPv6_backhaul address> “<pre-shared key>” “<pre-shared key>”*** where: ***<Core2_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for IPv4 links and for architectures where the subsites are connected to the Prime Site through a backhaul switch,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey` ***<SysIP_AccessRouter1> “<pre-shared key>” “<pre-shared key>”*** where: ***<SysIP_AccessRouter1>*** is the system IP address of access router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter:

If…	Then…
	`add -crypto fipspreshrdkey` ***<SysIP_AccessRouter2>*** ***“<pre-shared key>”*** ***“<pre-shared key>”*** where: ***<SysIP_AccessRouter2>*** is the system IP address of access router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for IPv6 links and for architectures where the subsites are connected to the Prime Site through a backhaul switch,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey ikev2` ***<AccessRouter1_IPv6_backhaul address>*** ***“<pre-shared key>”*** ***“<pre-shared key>”*** where: ***<AccessRouter1_IPv6_backhaul address>*** is the IPv6 backhaul address of access router 1 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey ikev2` ***<AccessRouter2_IPv6_backhaul address>*** ***“<pre-shared key>”*** ***“<pre-shared key>”*** where: ***<AccessRouter2_IPv6_backhaul address>*** is the IPv6 backhaul address of access router 2 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)
If you add crypto keys for systems with the Dynamic System Resilience feature implemented,	perform the following actions: **a** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core9_IPv6_backhaul address>*** ***“<pre-shared key>”*** ***“<pre-shared key>”*** where: ***<Core9_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 9 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks) **b** Enter: `add -crypto fipspreshrdkey ikev2` ***<Core10_IPv6_backhaul address>*** ***“<pre-shared key>”*** ***“<pre-shared key>”*** where: ***<Core10_IPv6_backhaul address>*** is the IPv6 backhaul address of core router 10 ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks)

6 Enter `sh -crypto fipspreshrdkey` on the site gateway and on the router or gateway on the other end of the site link. Verify that the key strings match.

7 Connect the LAN cable to the new gateway and connect it to the switch on the other end.

8 Connect the T1 cable or the Ethernet WAN cable to the appropriate ports.

9 Observe that both the link and activity LEDs for the T1 or Ethernet WAN port illuminate (the site transitions to site trunking).

10 To monitor link status, open a command prompt and run a continuous ping to the master site.

CAUTION: This procedure adds crypto keys on site gateways. The keys on the site gateways must match the keys on the core routers or gateways on the other end of the site link(s).

11 When instructed by the master site, enter:

```
setd !v<port#> —crypto cont = e
```

on the site gateway, where ***<port#>*** is the port on which you activate link encryption.

12 If the link does not come back up, enter:

```
setd !v<port#> —crypto cont = d
```

on the site gateway and on the core router or gateway on the other end of the site link, to disable the encryption on both ends.

13 Verify that the FIPS pre-shared keys match. Type `sh -crypto fipspreshrdkey` on both devices and compare the results.

14.7.2 Adding Link Encryption on Core Gateway

Prerequisites: Obtain the location of the required pre-shared keys from your system administrator. The ***<pre-shared key>*** value is the customer-specific secret passphrase.

When and where to use: Perform this procedure only if link encryption is required; otherwise proceed to Assigning Passwords on page 281.

IMPORTANT: This procedure adds crypto keys on core gateways or core/exit gateways. The keys **must** match the keys on the site gateway(s) for each site link.

Procedure:

1 Log on to the appropriate core or core/exit gateway by using the console connection and a null modem serial cable. Enter the username (root) and the appropriate password (usually no password on a new device).

2 To add crypto keys on the core or core/exitgateway for the associated site gateway(s) (for site gateways 1 and 2 in the following examples), perform the following actions:

- For IPv4 links, perform the following actions:
  - For a single-site link, enter:

    ```
    add -crypto fipspreshrdkey <SysIP_Site_Gateway1> “<pre-shared key>” “<pre-shared key>”
    ```

  - For a dual-site link, enter:

    ```
    add -crypto fipspreshrdkey <SysIP_Site_Gateway1> “<pre-shared key>” “<pre-shared key>”
    add -crypto fipspreshrdkey <SysIP_Site_Gateway2> “<pre-shared key>” “<pre-shared key>”
    ```

Where ***<SysIP_Site_Gateway1>*** is the system IP address of site gateway 1, ***<SysIP_Site_Gateway2>*** is the system IP address of site gateway 2, and ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks).

- For IPv6 links, perform the following actions:
  - For a single-site link, enter:
    `add -crypto fipspreshrdkey ikev2` ***<Site_Gateway1_IPv6_backhaul address> "<pre-shared key>" "<pre-shared key>"***
  - For a dual-site link, enter:
    `add -crypto fipspreshrdkey ikev2` ***<Site_Gateway1_IPv6_backhaul address> "<pre-shared key>" "<pre-shared key>"***
    `add -crypto fipspreshrdkey ikev2` ***<Site_Gateway2_IPv6_backhaul address> "<pre-shared key>" "<pre-shared key>"***

  Where ***<Site_Gateway1_IPv6_backhaul address>*** is the IPv6 backhaul IP address of site gateway 1, ***<Site_Gateway2_IPv6_backhaul address>*** is the IPv6 backhaul IP address of site gateway 2, and ***<pre-shared key>*** is the pre-shared key (which must be enclosed in quotation marks).

3. Enter `sh -crypto fipspreshrdkey` on the site gateway and on the router or gateway on the other end of the site link. Verify that the key strings match.
4. Connect the LAN cable to the new gateway and connect it to the switch on the other end.
5. Connect the T1 cable or the Ethernet WAN cable to the appropriate ports.
6. Observe that both the link and activity LEDs for the T1 or Ethernet WAN port illuminate (the site transitions to site trunking).
7. To monitor link status, open a command prompt and run a continuous ping to the remote site.

   ⚠ **CAUTION:** Do not press ENTER after the following steps until you contact the remote site. This is a coordinated effort between personnel at the master site and the remote sites.

8. As coordinated with the remote site, enter:

   `setd !v`***<port#>*** `—crypto cont = e`
   on each core or core/exit gateway, where ***<port#>*** is the port on which you activate link encryption.

9. If the link does not come back up, enter:

   `setd !v`***<port#>*** `—crypto cont = d`
   on the core or core/exit gateway and on the site gateway(s) at the other end of the site link(s) to disable encryption, where ***<port#>*** is the port on which you disable link encryption. Then, verify that the FIPS pre-shared keys match by comparing the results after you enter: `sh –crypto fipspreshrdkey` on the gateways at both ends of the link.

14.8 Assigning Passwords

Procedure:

1. If RADIUS is not enabled, go to step 2. If RADIUS is enabled, add a RADIUS secret key:
   a. Log on to the gateway by using the console connection. Enter the username (root) and the appropriate password (usually no password on a new gateway).
   b. Enter: `setd –ac secret =` ***"<secret>"***

      Where ***<secret>*** is the RADIUS secret (up to 32 characters).

The RADIUS secret which must be enclosed in quotation marks and must match the RADIUS secret on the RADIUS server.

- **c** To set the security server type to RADIUS, enter `setd -ras st=radius`.

2 Assign a root password to the gateway.

- **a** Enter: `Setd NMpassword =` “***<old_password>***” “***<new_password>***” “***<new_password>***”

  Where ***<old_password>*** is the existing password (generally "" (blank string) on a new gateway) and ***<new_password>*** is the new password. The old and new passwords must be enclosed in quotation marks.

  NOTICE: ***<new password>*** is case-sensitive and must be at least 7 but no more than 15 characters in length. Valid characters are limited to ASCII codes 32 through 126.
  The string of six asterisks (******) is not allowed as a Network Manager password. This string is reserved for use as a nonoperational value when passwords are captured using the ASCII capture feature.

3 If PIM authentication is enabled, add the keys, and transition the device from **Transit** to **Secure** state. See Manually Enabling PIM Authentication on page 282.

NOTICE: Ensure that the right keys are used.

4 If OSPF authentication is enabled, refer to the “Enabling Transport Devices for OSPF MD5 Authentication for CNI Transport Devices” section in the *Link Encryption and Authentication Feature Guide* for instructions on how to manually configure the OSPF authentication features.

5 If BGP authentication is enabled, refer to the “Enabling Transport Devices for BGP MD5 Authentication on CNI Transport Devices” section in the *Link Encryption and Authentication Feature Guide* for instructions on how to manually configure the BGP authentication features.

6 Reboot the gateway once.

7 Continue with Pushing the Configuration to the Gateway on page 284.

14.8.1 Manually Enabling PIM Authentication

Prerequisites: This procedure assumes that a global security association has been configured and enabled for all PIM-enabled devices across the domain. Before beginning this procedure, obtain the policy name for the global security association used for PIM authentication as well as the authentication key used for all PIM-enabled devices across the domain.

When and where to use: Perform this procedure to configure and manually enable PIM authentication on all PIM-enabled devices across the domain.

Procedure:

1 Define a keyset for PIM authentication on the device by entering the following command:

```
ADD -crypto ManKeySet <keyset_name> AuthKey “<auth-key>” “<auth-key>”
```

Where ***<keyset_name>*** is a unique 1-15 character name and ***<auth_key>*** is the authentication key (enclosed in quotation marks). You can include standard alphanumeric characters and special characters (other than quotation marks) in the authentication key.

Step example: For example, to configure keyset “mks1” with authentication key “secret”, enter:

```
ADD -crypto ManKeySet mks1 AuthKey “secret” “secret”
```

IMPORTANT: The ***<keyset_name>*** must match the ***<keyset_name>*** that is configured on the device’s PIM authentication peers. In addition, the authentication key should be the same for all PIM-enabled routers and gateways across the domain. To view the authentication key configured on a PIM authentication peer, enter the following command on the peer:

```
SHow -crypto ManKeySet
```

2 Create a global security association (SA) on the device by entering the following command:

```
ADD -crypto GblManKeyInfo <policy_name><keyset_name> SpiAh
<spi_in><spi_out>
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication; ***<keyset_name>*** is the keyset name defined with the `ManKeySet` parameter; and ***<spi_in>*** and ***<spi_out>*** are the incoming and outgoing authentication SPI values (256-512).

NOTICE: ***<spi_in>*** and ***<spi_out>*** must be the same value.

Step example: For example to create a global manual security association that binds policy “pim1” with keyset “mks1” and an incoming and outgoing authentication SPI value of 300, enter:

```
ADD -crypto GblManKeyInfo pim1 mks1 SpiAh 300 300
```

3 Specify that the global SA you created in step 2 is the transmit SA (the SA which will be used to authenticate outgoing packets using the specified SPI value) by entering the following command:

```
ADD -crypto GblManXmitSA <policy_name><spi_out>
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication and ***<spi_out>*** is the outgoing authentication SPI value.

Step example: For example to specify policy “pim1” (with outgoing authentication SPI value 300) as the transmit SA, enter:

```
ADD -crypto GblManXmitSA pim1 300
```

NOTICE: If you do not specify an active transmit SA, the device uses the SA with the lowest ***<spi_out>*** value as the transmit SA.

4 Set the PIM authentication state to “Transit” on the device you are configuring for PIM authentication, as well as its PIM authentication peers, by entering:

```
ADD -crypto GblManPolState <policy_name> Transit
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

Step example: For example to set the PIM authentication state for policy “pim1” to “Transit”, enter:

```
ADD -crypto GblManPolState pim1 Transit
```

IMPORTANT: Put all PIM-enabled routers and gateways configured for PIM authentication in “Transit” state at the same time to avoid losing communication between the PIM devices. If some devices are placed in “Transit” state and others are left in “Clear” state, a communication failure will occur.

NOTICE: The device remains in PIM authentication “Transit” state until you explicitly move it to any other state using the `ADD -crypto GblManPolState` command.

5 Enter the following command to display the PIM authentication state and verify that it is set to “Transit”:

```
SHow -crypto GblManPolState <policy_name>
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

Step example: For example to display the PIM authentication state for policy “pim1”, enter:

```
SHow -crypto GblManPolState pim1
```

6 Reboot the device and connect it to the LAN.

7 Display the PIM authentication status on the device you are configuring for PIM authentication, as well its PIM authentication peers, by entering:

```
SHow -crypto ManPeerReport
```

IMPORTANT: Verify that the **Authentication Result** is PASS for all peers. If the **Authentication Result** column lists FAIL for any peer, verify that the SAs on that peer are configured correctly.

8 Set the PIM authentication state to “Secure” on the device you are configuring for PIM authentication, as well as its PIM authentication peers, by entering:

```
ADD -crypto GblManPolState <policy_name> Secure
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

Step example: For example to set the PIM authentication state for policy “pim1” to “Secure”, enter:

```
ADD -crypto GblManPolState pim1 Secure
```

IMPORTANT: Put all PIM-enabled routers and gateways configured for PIM authentication in “Secure” state at the same time to avoid losing communication between the PIM devices. If some devices are placed in “Secure” state and others are left in “Transit” state, a communication failure will occur.

9 Enter the following command to display the PIM authentication state and verify that it is set to “Secure”:

```
SHow -crypto GblManPolState <policy_name>
```

Where ***<policy_name>*** is the policy name defined for the global manual security policy used for PIM authentication.

Step example: For example to display the PIM authentication state for policy “pim1”, enter:

```
SHow -crypto GblManPolState pim1
```

14.9 Pushing the Configuration to the Gateway

Prerequisites: Install Trivial File Transfer Protocol (TFTP) server software.

When and where to use: Use this procedure to copy the configuration files from the TFTP directory into the device’s primary directory.

Procedure:

1 To log on, point the TFTP server to the appropriate location, assign an IP address to the laptop, and connect to the Ethernet card:

   a Log in to the router (Console connection) using the username (root) and the appropriate password (usually no password on a new gateway).

   b Point the TFTP server on the laptop to the boot.cfg file and other cfg files (acl.cfg, staticRP, override.cfg, if applicable).

   c Assign an IP address (for example, 10.0.0.1) to the laptop with the appropriate subnet mask (for example, 255.255.255.0). This IP address has to be in the same subnet as the IP address of the gateway interface that is connected to the laptop's Ethernet card.

   d Connect the laptop's Ethernet card to port 1 of the gateway (!1) using a crossover cable.

2 Perform the following actions on the gateway (this example uses IP address 10.0.0.2):

   a Enter: `setd !1 -ip netaddr= 10.0.0.2 255.255.255.0`

   b Enter: `setd !1 -po cont=e`

   c Enter: `setd !1 -pa cont=e`

3 To check if Port 1 status is Up, enter: `show -ip neta`

4 Ping the laptop IP address to check connectivity.

5 To copy the configuration files from the TFTP directory into the gateway's primary directory, perform the following actions:

   NOTICE: If the gateway does not have a particular type of configuration file skip the command line corresponding to that configuration file. For example, if the gateway does not have an override.cfg configuration file, skip the `copy 10.0.0.1:/override.cfg a:/primary/override.cfg` command.

   a Enter: `copy 10.0.0.1:/boot.cfg a:/primary/boot.cfg`

   b Enter: `copy 10.0.0.1:/acl.cfg a:/primary/acl.cfg`

   c If applicable, enter: `copy 10.0.0.1:/override.cfg a:/primary/override.cfg`

   d Enter: `copy 10.0.0.1:/staticRP.cfg a:/primary/staticRP.cfg`

   e For a GGSN gateway only, enter:
   `copy 10.0.0.1:/xgsn.cfg a:/primary/xgsn.cfg`

6 To view the boot.cfg file and ensure it matches what was deployed, perform the following actions:

   a Enter: `cd`

   b Enter: `cat boot.cfg`

7 For all other configuration files loaded on the gateway (acl.cfg, override.cfg, staticRP.cfg), repeat step 6.

14.10
Setting Up Information Assurance

Prerequisites: Contact your system administrator for IP addresses.

When and where to use: Perform this procedure to set up Information Assurance (IA) on the devices.

Procedure:

1 When IA is in use, enable SNMPv3 auth/priv with correct passphrases. See “Adding an SNMPv3 USM User for MNR Routers and GGM 8000 Gateways” in the *Network Technician Guide*.

2 Reboot the router/gateway.

3 Disable MAC Port Lockdown:

   a Log on to the switch by using the console connection. Enter the username and the appropriate password.

   b Enter the following commands:

```
config
no port-security <port#>
```

   Where ***<port#>*** is the switch port on which you are disabling MAC Port Lockdown.

4 Connect the new router/gateway (port 1) to port 1 of the switch for the LAN connection.

5 Turn on the router/gateway.

The LAN and WAN link come up.

6 Connect to the site LAN switch ***<port#>***, where ***<port#>*** is the switch port on which you are enabling MAC Port Lockdown. Perform the following actions:

a Enter: `interface` ***<port#>*** `enable`

b Enter: `port-security` ***<port#>*** `clear-intrusion-flag`

c Enter: `port-security` ***<port#>*** `learn-mode static address-limit 31`

NOTICE: This command is given to learn the MAC addresses on the particular port specified. The switch does not learn the MAC address of the connected device dynamically. You may have to ping the device for the switch to learn its MAC address. Contact your system administrator for the IP addresses.

7 In case of dual devices, reboot the primary device. This will cause the second device to take over through the VRRP session. This will also cause the VRRP MAC to appear on the switch port enabled for learn mode.

8 Enter `show port-security` ***<port#>***

The MAC addresses associated with the port appear. This number of MAC addresses should be used for ***<numberMacAllowed>***.

9 To lock the port, perform the following actions:

a Enter:
`port-security` ***<port#>*** `learn-mode static address-limit`
<numberMacAllowed> `action send-Disable`

b Enter: `show interfaces brief`

NOTICE: This command is used to show the status of the port to which MAC Port Lockdown is applied.

14.11
Testing SNMPv3 Credentials

Procedure:

1 Log on to VoyenceControl.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

2 From **Networks** in the navigation pane, select **Astro 25 Radio Network** → **Views**.

3 In the navigation pane, double-click **Devices**.

4 Hold down the CTRL key. Click the device for which you want to check credentials.

5 Right-click one of the selected devices.

6 Select **Quick Commands** → **Test Credentials**.

NOTICE: Troubleshoot if the credentials are not correct.

14.12 Pushing Configurations to the Secondary Directory of a Gateway

When and where to use: Perform this procedure to push configurations from VoyenceControl to the gateway's secondary directory.

NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

Procedure:

1. Log on to the VoyenceControl application.
2. In the navigation pane, select **Networks** → **Astro 25 Radio Network**.
3. Double-click **Motorola Network Resource**.
4. In the navigation pane, select **Workspaces** and double-click **TNCT** ***<Date>***.

   <Date> is the date associated with the appropriate TNCT configuration files.
5. Start the push for the configuration files. See Starting a Configuration File Push on page 287.

14.12.1 Starting a Configuration File Push

Procedure:

1. In the **Selected Device** list, select the gateways to which you want to load the configuration files.
2. Right-click the selected gateways. Select **Schedule** → **Select All** → **Schedule**.
3. In the **Job Name** field, type a name for the job.
4. Select the **Tasks** tab.
5. Click the gateway in the **Post Operation** column.
6. Click **OK**.
7. Click **Approve & Submit**.
8. Reboot the gateway:
   a. Return to the terminal program.
   b. At the `EnterpriseOS#` prompt, enter: `rb` (ReBoot). Press ENTER.

   The router reboots and processes the configuration files. Once complete, `System Initialized and Running` is displayed.
9. Press F7.

   The Schedule Manager dialog box appears. The configuration push to the device takes approximately 1 minute to complete. The state for the device appears as **Completed** and a green dot appears next to the device when the push is complete. A red dot appears next to the device if the push fails and the state shows **Failed**.

14.13 Pulling the Configuration to Unified Network Configurator

When and where to use: Pull the configuration from the gateway to Unified Network Configurator (UNC).

Procedure:

1. Log on to the VoyenceControl application.

   NOTICE: The names EMC Smarts™ Network Configuration Manager and VoyenceControl are used interchangeably for this product.

2. In the navigation pane, select **Networks** → **Astro 25 Radio Network**.
3. Double-click **Devices**.
4. Navigate to the device. Right-click the name of the view from which you want to pull device configurations.
5. Select **Pull** → **Pull Config**.

   The configuration for the selected device is pulled back into UNC and the device and UNC are now synchronized.

6. After the pull is complete, verify the configuration.

14.14 Deleting a Gateway from UEM

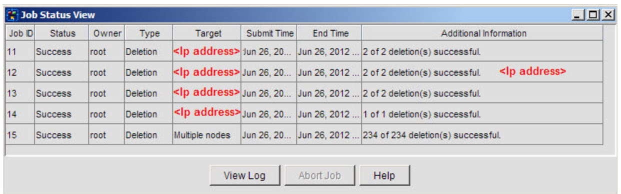
Procedure:

1. Log on to Unified Event Manager (UEM).
2. From the **Network Database** view, select a row.
3. Right-click selected row and select **Delete Object and Traces**.
4. In the confirmation dialog box, click **Yes**.
5. In the **Deletion Status** dialog box, click **View Job Status**.

   A separate job is initiated for each deletion request. The status of the request appears in the **Job Status View** window.

6. In the **Job Status View** window, verify the deletion status.

   Figure 121: Job Status View for Deletion Jobs Window

Job ID	Status	Owner	Type	Target	Submit Time	End Time	Additional Information
11	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	2 of 2 deletion(s) successful.
12	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	2 of 2 deletion(s) successful. <Ip address>
13	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	2 of 2 deletion(s) successful.
14	Success	root	Deletion	<Ip address>	Jun 26, 20...	Jun 26, 2012 ...	1 of 1 deletion(s) successful.
15	Success	root	Deletion	Multiple nodes	Jun 26, 20...	Jun 26, 2012 ...	234 of 234 deletion(s) successful.

   If the job status is **Success** or **Completed** the device or node and the alarms associated with it are also deleted. Events are not deleted, as events are part of the history and they are deleted only when the database is reinitialized.

7. If the **Warning Discovery in progress** dialog box appears, to the view active jobs that are related to the object being deleted, click **Open Job View**.

NOTICE: Once a device is deleted, you cannot restore its alarms.

Job View with the first job highlighted appears.

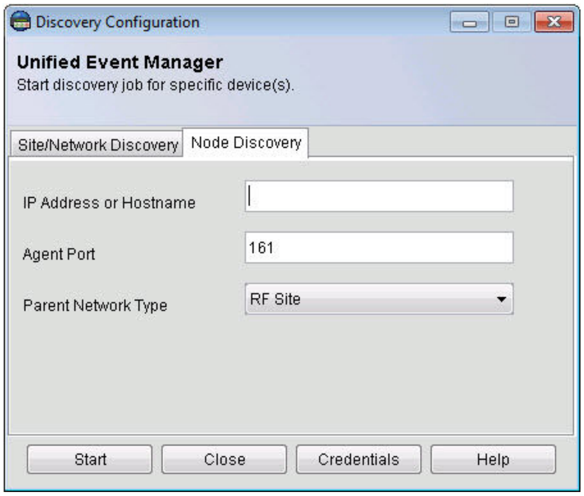
14.15

Discovering a Gateway in UEM

Procedure:

1. Log on to Unified Event Manager (UEM).
2. From the menu, select **Tools** → **Discovery**.
3. In the **Discovery Configuration** window, click the **Node Discovery** tab.

   Figure 122: Discovery Configuration – Node Discovery



Discovery Configuration

Unified Event Manager

Start discovery job for specific device(s).

IP Address or Hostname:

Agent Port: 161

Parent Network Type: RF Site

4. In the **Node Discovery** tab, provide discovery credentials:
   a. In the **IP Address or Hostname** field, enter an IP address or hostname of the device you want to discover.
   b. In the **Agent Port** field, enter an SNMP agent port.

      You can leave the default value unchanged as it applies to most of devices.
   c. From the **Parent Network Type** list, select the parent network type. Click **Start**.

NOTICE: The Parent Network Type value is used to create the appropriate Network managed resource. It applies when the IP address being discovered is the first node added to UEM in this subnet. The network type that the device belongs to can be different from the physical location of the device.
For example, choose **RF Site** when discovering a device at a site that is physically located at the Primary Zone Core.

5. In the **IP Address or Hostname** field, enter an IP address or hostname of the device you want to discover.
6. In the **Agent Port** field, enter an SNMP agent port.

   You can leave the default value unchanged as it applies to most devices.
7. Click **Start**.
8. In the **Node Discovery Status** window, click **View Job Status**.

For each discovery request, a separate job is initiated. You can view jobs statuses in the **Job Status View** window.

In the**Job Status View** window, the status of the discovery is displayed. If the discovery is based on hostname, the **TARGET** column shows the hostname with the IP address appended.