System Release 7.17
ASTRO® 25
INTEGRATED VOICE AND DATA

GCP 8000 Site Controller

NOVEMBER 2016

MN003278A01-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.

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 particular system, or may be dependent upon the characteristics of a particular 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.

This page intentionally left blank.

Contact Us

Motorola Solutions Support Center

The Solutions Support Center (SSC) is the primary Motorola Solutions support contact. Call:

- Before any software reload.
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) and Field Replaceable Entity (FRE) to repair the system.

For...	Phone
United States Calls	**800-221-7144**
International Calls	**302-444-9800**

North America Parts Organization

For assistance in ordering replacement parts or identifying a part number, contact the Motorola Solutions Parts organization. Your first response when troubleshooting your system is to call the Motorola Solutions SSC.

For...	Phone
Phone Orders	**800-422-4210** (US and Canada Orders) For help identifying an item or part number, select choice 3 from the menu.
	302-444-9842 (International Orders) Includes help for identifying an item or part number and for translation as needed.
Fax Orders	**800-622-6210** (US and Canada Orders)

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 with the error
- A description of the error

We welcome your feedback on this and other Motorola Solutions manuals. To take a short, confidential survey on Motorola Solutions Customer Documentation, go to docsurvey.motorolasolutions.com or scan the following QR code with your mobile device to access the survey.

This page intentionally left blank.

Document History

Version	Description	Date
MN003278A01-A	Original release of *GCP 8000 Site Controller* manual.	November 2016
MN003278A01-B	Updated the following sections: • CSS Configuration Parameters for the GCP 8000 Site Controller (Trunked Repeater) on page 109 • CSS Configuration Parameters for the GCP 8000 Site Controller (Trunked Simulcast) on page 111 • GCP 8000 Site Controller General Troubleshooting on page 123	November 2016

This page intentionally left blank.

Contents

List of Figures

List of Tables

This page intentionally left blank.

List of Processes

This page intentionally left blank.

List of Procedures

This page intentionally left blank.

About GCP 8000 Site Controller

This manual provides descriptive and procedural information on the GCP 8000 Site Controller. Included in this manual is the description of the GCP 8000 Site Controller and the following hardware configurations: Standalone GCP 8000 Site Controller, HPD – GTR 8000 Site Subsystem, and GTR 8000 Expandable Site Subsystem. Additional information is provided for procedures on installation, configuration, operation, troubleshooting, and FRU/FRE replacement. Finally, a reference section provides information on the GCP 8000 Site Controller LED indicators.

This manual is intended to be used by technicians and system operators as a resource for understanding and installing the GCP 8000 Site Controller after they have attended the Motorola Solutions formal training. The manual should be used in conjunction with the ASTRO® 25 system documentation and *Standards and Guidelines for Communication Sites*.

What Is Covered In This Manual?

This manual contains the following chapters:

- GCP 8000 Site Controller Description on page 25 provides an overview of the GCP 8000 Site Controller.
- GCP 8000 Site Controller Theory of Operation on page 35 provides additional explanation of the functions and connectors of the GCP 8000 Site Controller.
- GCP 8000 Site Controller Installation on page 47 provides installation information for the different hardware configurations of the GCP 8000 Site Controller.
- GCP 8000 Site Controller Configuration on page 93 provides configuration information for the GCP 8000 Site Controller using the Configuration/Service Software and Unified Network Configurator.
- GCP 8000 Site Controller Optimization on page 115 provides optimization information for the GCP 8000 Site Controller.
- GCP 8000 Site Controller Operation on page 117 provides operations information for the GCP 8000 Site Controller.
- GCP 8000 Site Controller Maintenance on page 121 provides maintenance information for the GCP 8000 Site Controller.
- GCP 8000 Site Controller Troubleshooting on page 123 provides troubleshooting information for the GCP 8000 Site Controller and the different systems supported by its hardware configurations.
- GCP 8000 Site Controller FRU/FRE Procedures on page 135 provides information and procedures for replacing Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) for the GCP 8000 Site Controller. Part numbers are also listed.
- GCP 8000 Site Controller Reference on page 149. This chapter provides information on the LED indicators for the GCP 8000 Site Controller.
- GCP 8000 Site Controller Disaster Recovery on page 155 provides references and information that will enable you to recover a GCP 8000 Site Controller in the event of failure.

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

See the following documents for associated information about the radio system.

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. This may be purchased on CD 9880384V83, by calling the North America Parts Organization at 800–422–4210 or the international number at 302–444–9842.
System Overview and Documentation	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.
Dynamic System Resilience Feature Guide	Provides all the information required to understand, operate, maintain, and troubleshoot the Dynamic System Resilience feature.
Conventional Operations	Provides all the information required to understand and operate the conventional GCP 8000 Site Controller in a Centralized or Distributed Conventional Architecture.
Trunked IP Simulcast Subsystem Prime Site Repeater Site Infrastructure Reference Guide	Provides the information required to understand and operate the GCP 8000 Site Controller in an ASTRO® 25 trunked system.

Chapter 1

GCP 8000 Site Controller Description

This chapter provides a high-level description of GCP 8000 Site Controller and the function it serves on your system.

1.1 Trunked GCP 8000 Site Controller Overview

The GCP 8000 Site Controller is the control interface between a trunked system and the zone controller. The site controller manages and controls the site and channels, administers broadcasts, provides a time and frequency reference signals to the base radios, monitors the base radios and RFDS equipment, along with providing redundant site control support to the site.

1.2 Conventional GCP 8000 Site Controller Overview

The Conventional GCP 8000 Site Controller is used to provide zone controller functionality for site conventional operation when the control path to the zone controller is lost. The conventional site controller supports conventional operation as an interface between base radios and consoles.

1.3 Supported System Configurations

The GCP 8000 Site Controller is available in the following system configurations:

- Trunked Systems
  - IP Simulcast Subsystem
  - Circuit Simulcast Subsystem
  - ASTRO® 25 Repeater Site
  - High Performance Data (HPD) Subsystem
- Centralized Conventional Architectures
  - Dispatch Console Site with Colocated Conventional Channels
- Distributed Conventional (Subsystem) Architectures
  - Conventional Hub Sites
- Conventional Master Sites
  - K1 Core
  - K2 Core

1.4 GCP 8000 Site Controller Hardware Configurations

The GCP 8000 Site Controller is used for any one of the following hardware configurations:

- Standalone GCP 8000 Site Controller configuration
- GTR 8000 Site Subsystem configuration

- GTR 8000 Expandable Site Subsystem configuration

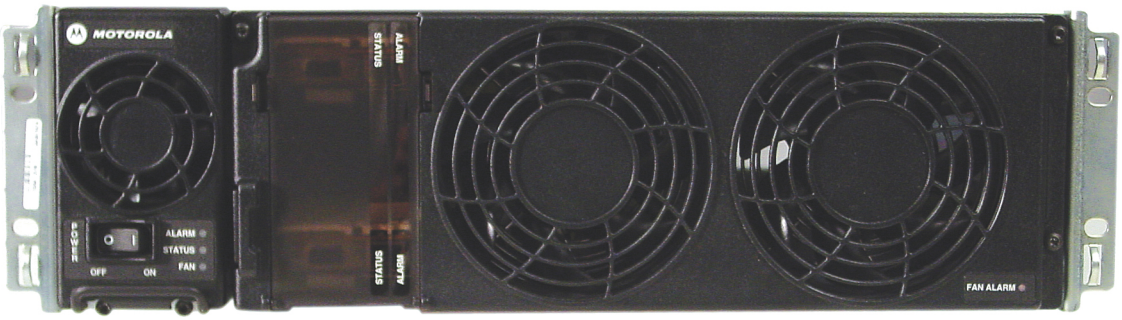
Table 1: GCP 8000 Site Controller Hardware Configurations and the Systems Supported

GCP 8000 Site Controller Hardware Configuration	Systems Supported
Standalone GCP 8000 Site Controller	• High Performance Data (HPD) subsystem • Circuit simulcast subsystem • Trunked IP simulcast subsystem • ASTRO® 25 repeater site • Centralized conventional architectures • Distributed conventional (subsystem) architectures • Conventional master site
GTR 8000 Site Subsystem	• HPD subsystem
GTR 8000 Expandable Site Subsystem	• HPD subsystem • ASTRO® 25 repeater site • ASTRO® 25 Express site

1.4.1
GCP 8000 Site Controller Standalone Configuration

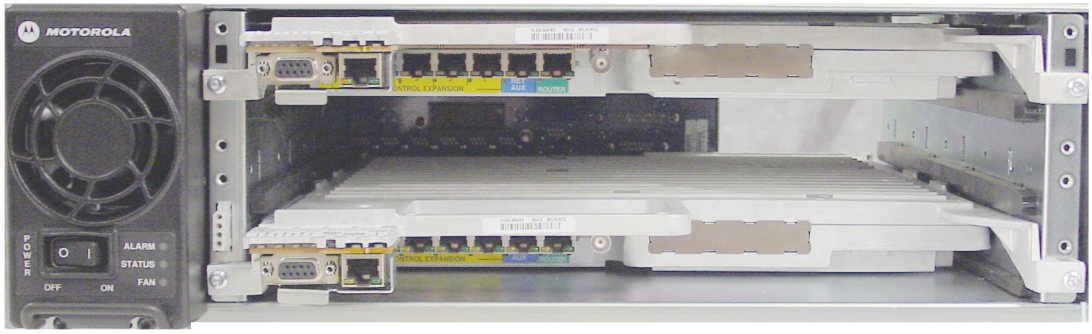
The standalone configuration of the GCP 8000 Site Controller can be used in a multitude of different types of subsystems. The configuration of the site controller modules within the chassis differs slightly depending on the type of subsystem it supports. All standalone configurations contain a power supply, and a fan assembly.

Figure 1: GCP 8000 Site Controller – Standalone Configuration



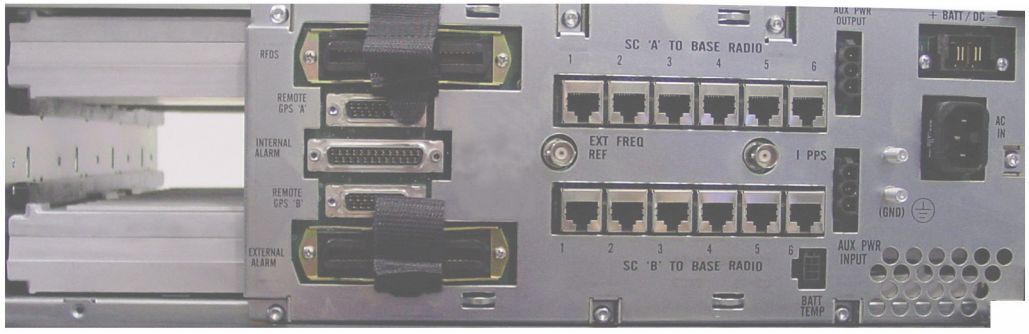
HPD_GCP_site_controller_front.jpg

Figure 2: GCP 8000 Site Controller (standalone HPD configuration shown) Front – Inside



HPD_GCP8000_site_controller_front_wo_cover5

Figure 3: GCP 8000 Site Controller (standalone HPD configuration shown) – Rear View



HPD_GCP8000_site_controller_rear_2

High Performance Data (HPD) Subsystem

The standalone configuration of the GCP 8000 Site Controller for an HPD subsystem is comprised of one chassis that holds two site controller modules that have embedded LAN switches and two remote Global Navigation Satellite System (GNSS) connections.

Circuit Simulcast Subsystem

The standalone configuration of the GCP 8000 Site Controller for a circuit simulcast subsystem requires two chassis, with each chassis holding a single site controller module in the upper slot within the chassis.

Trunked IP Simulcast Subsystem

The standalone configuration of the GCP 8000 Site Controller for a trunked IP simulcast subsystem requires two chassis, with each chassis holding a single site controller module. The site controller that has been assigned as site controller 1 must have the site controller module in the upper slot within the chassis, and the site controller that has been assigned as site controller 2 must have the site controller module in the lower slot within the chassis.

The standalone configuration of the site controller for a Trunked IP Simulcast Prime Site Geographic Redundancy (TPSGR) subsystem requires three chassis. A TPSGR subsystem geographically separates a trunked IP simulcast prime site into two separate locations. Site controllers 1 and 2 reside at the primary prime site. The third site controller resides at the secondary prime site and activates on the failure of the primary prime site. The third site controller module may be in the upper or lower slot within the chassis.

ASTRO® 25 Repeater Site

The standalone configuration of the GCP 8000 Site Controller for an ASTRO® 25 repeater site supports a mix of the following equipment configurations:

- Standalone site controller and standalone GTR 8000 Base Radio with or without 10Base-T Ethernet Epic IV or Epic VI QUANTAR® stations.
- Standalone site controller and GTR 8000 Expandable Site Subsystem cabinets/racks with XHubs with or without QUANTAR® stations.
- Standalone site controller and QUANTAR® stations.

The site controller is comprised of one chassis that holds two site controller modules that have embedded LAN switches.

If a mix of GCP 8000 Site Controllers and QUANTAR® stations are at the site, SNMPv1 and clear SWDL transfer support is used at the site.

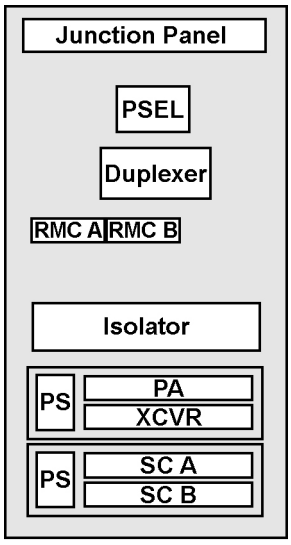
Conventional Architectures

The standalone configuration of the conventional GCP 8000 Site Controller is used to provide zone controller functionality for site conventional operation when the control path to the zone controller is lost. The conventional site controller in centralized and distributed conventional architectures along with a K1 core conventional master site consist of one chassis that holds one site controller module with no redundancy. The standalone conventional site controller in a K2 core conventional master site requires redundancy with two chassis, with each chassis holding a single site controller module in the upper slot within the chassis.

1.4.2
GTR 8000 Site Subsystem Configuration

The GTR 8000 Site Subsystem configuration consists of a standalone GTR 8000 Base Radio, a standalone GCP 8000 Site Controller, and RFDS equipment. This configuration is used only in a High Performance Data (HPD) Site Subsystem.

Figure 4: GTR 8000 Site Subsystem Configuration



HPD_site_subsystem_config

1.4.3

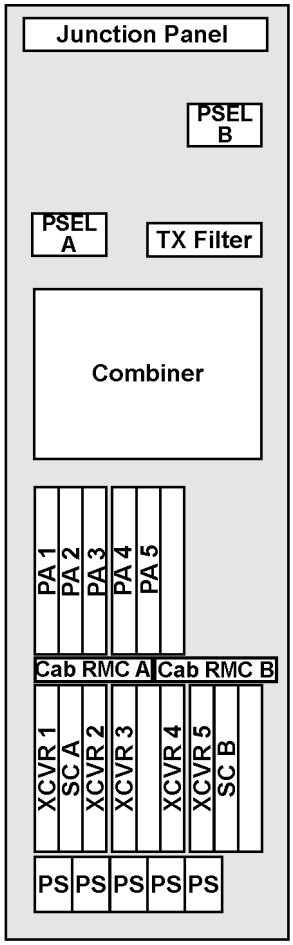
GTR 8000 Expandable Site Subsystem Configuration

The GTR 8000 Expandable Site Subsystem configuration is the most versatile of the hardware configurations for the GCP 8000 Site Controller and supports two different subsystems.

GTR 8000 Expandable Site Subsystem for HPD Subsystem

This configuration consists of one cabinet or rack. The cabinet or rack in the GTR 8000 Expandable Site Subsystem contains two GCP 8000 Site Controller modules, and a maximum of five GTR 8000 Base Radios, power supplies, power amplifiers, fan assemblies, and RFDS equipment per site.

Figure 5: GTR 8000 Expandable Site Subsystem Configuration – HPD Subsystem



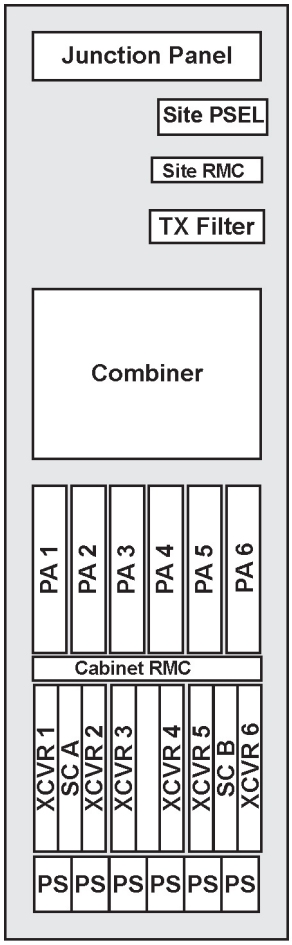
HPD_expandable_site_subsystem_config_1

GTR 8000 Expandable Site Subsystem for an ASTRO® 25 Repeater Site

The cabinet or rack in the GTR 8000 Expandable Site Subsystem contains two GCP 8000 Site Controller modules with a maximum of six GTR 8000 Base Radios, power supplies, power amplifiers, fan assemblies, and RFDS equipment.

When the number of base radios required for the system exceeds six, a second rack is added. This second rack is referred to as an expansion rack. It contains a pair of redundant Expansion Hubs (XHubs) instead of the site controllers. Each XHub is directly cabled to the site controller to provide the network and reference connections between the racks. Additional expansion racks are added up to a maximum of five racks, with a total of 28 base radios.

Figure 6: GTR 8000 Expandable Site Subsystem Configuration – ASTRO 25 Repeater Site



The ASTRO® 25 repeater site can also support a mix of GTR 8000 Expandable Site Subsystem cabinets/racks and standalone 10Base-T Ethernet Epic IV or Epic VI QUANTAR® stations. The site controllers can be either integrated into the rack/cabinet or in a standalone configuration outside the rack/cabinet. If the site controllers are in a standalone configuration outside the rack/cabinet, XHubs are included in the first cabinet/rack.

If a mix of GCP 8000 Site Controllers and QUANTAR® stations are at the site, SNMPv1 and clear SWDL transfer support is used at the site.

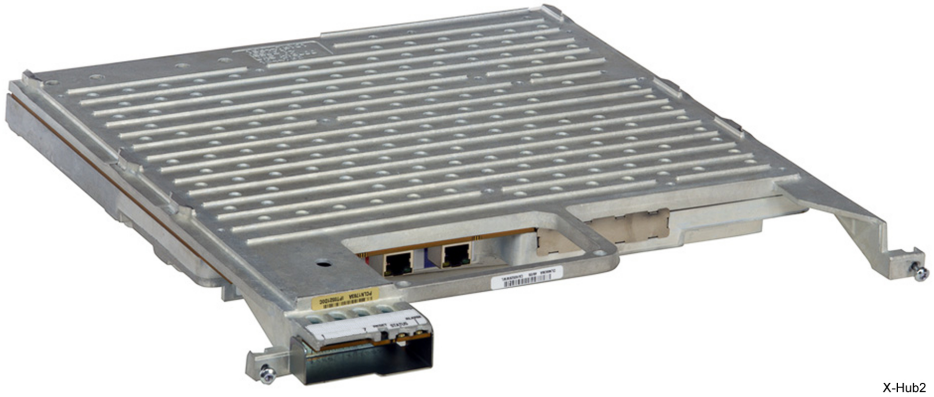
Expansion Hub Overview

The Expansion Hub (XHub) is a switching and interface module that connects to the GCP 8000 Site Controller. The XHub has the same clamshell type of housing as the site controller.

In an ASTRO® 25 repeater site, the XHub allows the GCP 8000 Site Controller to support additional GTR 8000 Base Radios beyond what the site controller supports on its own. One site controller supports up to five XHubs with each XHub supporting up to six base radios.

For further information on the XHub, see the *GTR 8000 Expandable Site Subsystem* and *Repeater Site Infrastructure Reference Guide* manuals.

Figure 7: Expansion Hub



1.5

GCP 8000 Site Controller Module Hardware Configurations

Table 2: GCP 8000 Site Controller Module Hardware Configurations

Where Used	Hardware Configuration	Hardware Configuration Type	Hardware Configuration Description
ASTRO® 25 Repeater Site	GTR 8000 Expandable Site Subsystem	Cabinet or Rack	Active SC module 1 Standby SC module 2
	Standalone GCP 8000 Site Controller	One Chassis	Active SC module, upper slot, chassis 1 Standby SC module, lower slot, chassis 1
Trunked IP Simulcast Subsystem	Standalone GCP 8000 Site Controller	Two Chassis	Active SC module 1, upper slot, chassis 1 Standby SC module 2, lower slot, chassis 2
Trunked IP Simulcast Prime Site Geographic Redundancy Subsystem	Standalone GCP 8000 Site Controller	Three Chassis	Primary prime active SC module 1, upper slot, chassis 1 Primary prime standby SC module 2, lower slot, chassis 2 Secondary prime SC module, upper slot, chassis 3
Circuit Simulcast Subsystem	Standalone GCP 8000 Site Controller	Two Chassis	Active SC module 1, upper slot, chassis 1 Standby SC module 2, upper slot, chassis 2
HPD Subsystem	GTR 8000 Expandable Site Subsystem	Cabinet or Rack	Active SC module 1 Standby SC module 2
	Standalone GCP 8000 Site Controller	One Chassis	Active SC module, upper slot, chassis 1

Table continued…

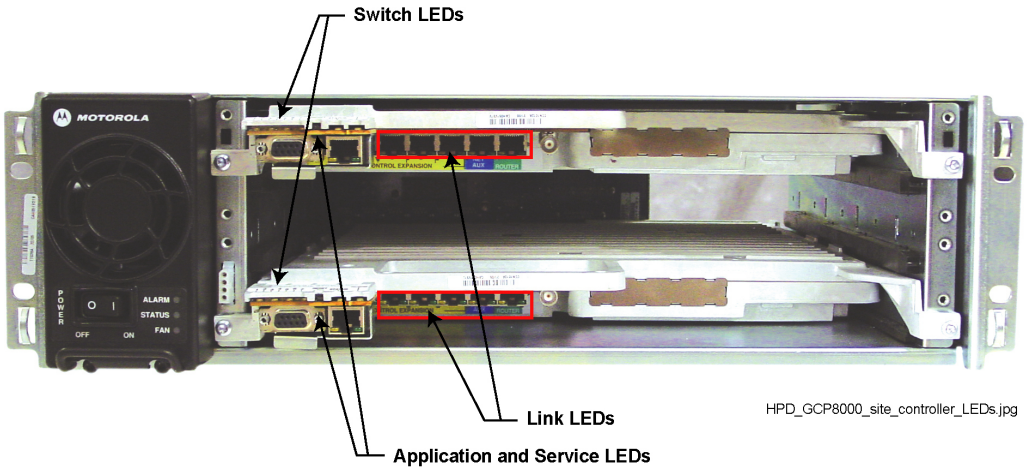
Where Used	Hardware Configuration	Hardware Configuration Type	Hardware Configuration Description
			Standby SC module, lower slot, chassis 1
	GTR 8000 Site Subsystem	One Chassis within cabinet or rack	Active SC module, upper slot, chassis 1 Standby SC module, lower slot, chassis 1
Dispatch Console Subsystem	Standalone GCP 8000 Site Controller	One Chassis	SC module, upper slot, chassis 1
Conventional Hub Site	Standalone GCP 8000 Site Controller	One Chassis	SC module, upper slot, chassis 1
Conventional Master Site (K1 Core)	Standalone GCP 8000 Site Controller	One Chassis	SC module, upper slot, chassis 1
Conventional Master Site (K2 Core)	Standalone GCP 8000 Site Controller	Two Chassis	Active SC module 1, upper slot, chassis 1 Standby SC module 2, upper slot, chassis 2

1.6

GCP 8000 Site Controller LED Descriptions

The GCP 8000 Site Controller LEDs are found at the extended part of the site controller module as well as in the chassis above the ports. See GCP 8000 Site Controller Reference on page 149 for information on specific LEDs.

Figure 8: GCP 8000 Site Controller Front LEDs



1.7

GCP 8000 Site Controller Specifications

All equipment at the site support operation from 90/264 VAC nominal single-phase power sources at 47/63 Hz or a 43.2-60 VDC power source or battery. The 60 VDC maximum input voltage limit includes consideration of the battery charging “float voltage” associated with the intended supply system, regardless of the marked power rating of the equipment.

CAUTION: Failure to follow the power supply guideline may result in an electric shock.

The Standalone GCP 8000 has automatic battery revert capabilities and can charge batteries from the AC power supply. The power supply includes an integrated charging system that eliminates the need for UPS. The power supply provides battery equalization.

The Standalone GCP 8000 has an internal power supply and is able to provide 29 VDC auxiliary power output as a backup power source. This allows, for example, a connected RMC with a power supply failure to maintain continued operation.

Table 3: GCP 8000 Site Controller Technical and Environmental Specifications

GCP 8000 Site Controller	Specifications
Physical Dimensions:	Height: 5.25 in. (133 mm) Width: 19 in. (483 mm) Depth: 18 in. (457 mm)
Weight:	40 lb (18 kg)
Temperature Operating Temperature: Storage Temperature:	 -30 °C to 60 °C (-22 °F to 140 °F) -40 °C to 85 °C (-40 °F to 185 °F)
Relative Humidity:	90% relative humidity at 50 °C non-condensing
Input Supply Voltage:	AC: 90–264 VAC, 4763 Hz DC: 43.2 to 60.0 VDC (+/-48 VDC nominal)
Auxiliary Power Outputs:	28.94 V +/- 3%
Power Consumption:	DC, 1 module: 60 W AC, 1 module: 130 W DC, 2 modules: 80 W AC, 2 modules: 160 W
Operating Altitude:	Up to 5,000 m (16,400 ft) above mean sea level

1.8 GCP 8000 Site Controller Port Default Speed/Duplex Settings

Table 4: GCP 8000 Site Controller Port Default Speed/Duplex Settings

Switch Port	Speed/Duplex
Net/Aux	Auto-Negotiate
Site Controller Expansion 1	100BaseT/Full Duplex*
Site Controller Expansion 2	100BaseT/Full Duplex*
Site Controller Expansion 3	100BaseT/Full Duplex*
Site Controller Expansion 4	100BaseT/Full Duplex*
Site Controller Expansion 5	100BaseT/Full Duplex*
Service Port	Auto-Negotiate

Table continued…

Switch Port	Speed/Duplex
Gateway Port	100BaseT/Full Duplex
SC to Base Radio 1	100BaseT/Full Duplex*
SC to Base Radio 2	100BaseT/Full Duplex*
SC to Base Radio 3	100BaseT/Full Duplex*
SC to Base Radio 4	100BaseT/Full Duplex*
SC to Base Radio 5	100BaseT/Full Duplex*
SC to Base Radio 6	100BaseT/Full Duplex*
Alarm	Auto-Negotiate

* = When QUANTAR® stations are connected, the ports must be set to 10BaseT/Half Duplex.

Chapter 2

GCP 8000 Site Controller Theory of Operation

This chapter explains how the GCP 8000 Site Controller works in the context of your system.

2.1 GCP 8000 Site Controller Functions

The following tables lists the functions of the GCP 8000 Site Controller for trunked and conventional systems.

Table 5: GCP 8000 Site Controller Functions and Applications

Function	HPD	Conven-tional	IP Simul-cast	Circuit Simul-cast	Repeater
Manages the site and the chan-nels	✓	✗	✓	✓	✓
Registration	✓	✗	✓	✓	✓
Network status	✓	✗	✓	✓	✓
Context activation	✓	✗	✓	✓	✓
Administers broadcasts	✓	✗	✓	✓	✓
Enhanced data channel	✓	✗	✓	✓	✓
Time synchronization and fre-quency reference	✓	✗	✗	✗	✓
Monitors GTR 8000 Base Ra-dios and RF distribution equip-ment	✓	✗	✓	✗	✓
Fault Management Reporting through the SDM RTU	✓	✓	✓	✓	✓
Integrated Ethernet LAN	✓	✗	✗	✗	✓
Provides redundant site control	✓	✗	✓	✓	✓
Provides zone controller func-tionality for site conventional and conventional talk group op-erations when the control path to the zone controller is lost	✗	✓	✗	✗	✗
Receives the 1PPS from the TRAK 9100 Simulcast Site Ref-erence and Global Positioning	✗	✗	✓	✗	✗

Table continued…

Function	HPD	Conven-tional	IP Simul-cast	Circuit Simul-cast	Repeater
Antenna and then provides a unique launch time reference for the GCM 8000 Comparators and GTR 8000 Base Radios.					
Standalone site controllers con-nected to external LAN switches, receive the 1PPS from the TRAK 9100 or TRAK 8835 Site Reference and then provide a unique launch time reference to the GTR 8000 Base Radios.	✗	✗	✗	✗	✓
Provides sub-band restriction for talkgroups	✗	✗	✓	✓	✓

2.1.1
Registration Function of a Trunked GCP 8000 Site Controller

For registration events, the site controller is responsible for forwarding requests and responses between the base radios and the comparators. The site controller maintains, in memory, a database of active Mobile Subscriber Units (MSUs) at the site. This database includes the channel assignment and registration status for each MSU operating at the site.

2.1.2
Network Status Function of a Trunked GCP 8000 Site Controller

Under the direction of the zone controller and depending on the network status, the site controller controls whether the site is in Wide Area mode or in Site Trunking mode. When the site is not in Wide Trunking mode, the channels at the site are under the direction of the site controller. The site controller dictates the selection and assignment of subscribers to the channels, including the control channels assignment and channel loading features. When the site is in Wide Trunking mode, the zone controller dictates the channel assignment.

2.1.3
Context Activation Function of a Trunked GCP 8000 Site Controller

The site controller plays a role in the context activation. For context activation events, the site controller is involved in forwarding the context activation requests and responses between base radios and the Radio Network Gateway (RNG) in the zone. In a similar fashion, the site controller is involved in forwarding user data between the base radios and the RNG in the zone.

2.1.4
Administering Broadcasts Function of a Trunked GCP 8000 Site Controller

The site controller administers a number of different broadcasts to the Mobile Subscriber Unit (MSU) population. These broadcasts indicate important information for MSUs in the region, such as the status and home channel frequencies for adjacent sites, time and date, channel access, system identification, base station identifier, and channel information updates.

For example, the Additional Channel Broadcast message is sent out as a background message from each control channel. Its purpose is to inform the MSU population of the presence and status of the backup control channels at the same site. The site controller provides the control channels at each site with the information needed for this broadcast.

Another example is the Time and Date Broadcast. This message informs the MSU population of the current date (day/month/year) and time (hours/minutes/seconds). The broadcast includes the local time offset and has flags that indicate whether the time and date values are valid. This allows the MSU population to support common real-time clocking for time stamping of logging messages. This service is provided by the Global Navigation Satellite System (GNSS)/NTP functionality within the site controller.

2.1.5
Enhanced Data Function of a Trunked GCP 8000 Site Controller

Enhanced data is a Global Navigation Satellite System (GNSS) option that adds data applications to APX subscriber units operating within a trunked integrated data system. Enhanced data allows a dispatcher to track the location of a subscriber unit, and allows text messaging to be sent between the subscriber unit and the dispatcher.

The site controller allocates an enhanced data channel at the site that enables support for enhanced data services. An enhanced data channel supports up to 375 subscriber units.

2.1.6
Time Synchronization and Frequency Reference Function of a Trunked GCP 8000 Site Controller

Table 6: Time Synchronization and Frequency Reference for Different Trunked Site Controller Configurations

	Hardware Configurations		
Subsystem Type	**Standalone**	**GTR 8000 Site Subsystem**	**GTR 8000 Expandable Site Subsystem**
HPD Subsystem	Remote Global Navigation Satellite System (GNSS) is the primary NTP source, providing time synchronization and frequency reference.	Remote GNSS is the primary NTP source, providing time synchronization and frequency reference.	Remote GNSS is the primary NTP source, providing time synchronization and frequency reference.
ASTRO® 25 repeater site	The internal reference oscillator may be used for frequency reference to the first six GTR 8000 Base Radios connected directly to the site controller, or a TRAK 9100 SSR or TRAK 8835 SSR provides the 1PPS time reference to the site controllers.	✗	The internal reference oscillator is used to provide frequency reference and time synchronization to the GTR 800 Base Radios.

Table continued…

	Hardware Configurations		
Subsystem Type	**Standalone**	**GTR 8000 Site Sub-system**	**GTR 8000 Expandable Site Subsystem**
Circuit simulcast subsystem	TRAK 9100 SSR at the prime site is the primary NTP source.	✗	✗
IP simulcast sub-system	TRAK 9100 SSR at the prime site is the primary NTP source and provides 1PPS time reference to the site controller.	✗	✗

In an HPD site subsystem:

- The active site controller acts as the Network Time Protocol (NTP) server for the site, providing the time to the GTR 8000 Base Radios and other devices at the site. The Remote GNSS connected to the site controller is the primary NTP source. The time and frequency reference is supplied to GTR 8000 Base Radios at the site through the Ethernet cable. The site controller keeps the time accurate to within +/- 1 microsecond per day across the valid temperature range of the site controller.
- The active site controller broadcasts time updates periodically. The standby site controller uses the NTP source time to verify correct time setting. If the internal time variance in a device is equal to, or greater than 500 milliseconds from the NTP source time, the device corrects the NTP Time of Day clock to match the received NTP time.
- The frequency reference and time reference are distributed on the LAN cables for the site controller to the base radio. The GNSS receivers provide the necessary references to the site controller. The time reference is used to synchronize the data transmissions from the radios, and the high stability frequency reference is used to provide a reference for both the transmit and receive frequency synthesizers in the radios.
- The site controller includes a high-stability ovenized crystal oscillator, which is trained by the input from a GNSS antenna. One GPS antenna must be connected to each site controller. The Configuration/Service Software (CSS) indicates whether the GNSS capability is configured. The site controller indicates the alarms for GNSS service to Unified Event Manager.

In an ASTRO® 25 repeater site:

- The active site controller broadcasts time updates periodically. The standby site controller uses the NTP source time to verify correct time setting. If the internal time variance in a device is equal to, or greater than 500 milliseconds from the NTP source time, the device corrects the NTP Time of Day clock to match the received NTP time.
- The site controller has an internal reference oscillator used for the frequency reference. This oscillator is aligned initially when the site controller is installed. See GCP 8000 Site Controller Reference Oscillator Alignment on page 115 in the Optimization chapter for the alignment intervals after initial installation.
- If a TRAK 9100 SSR or TRAK 8835 SSR is present at the site, the site controller uses the 1PPS time reference and as the primary Network Time Protocol (NTP) source for time synchronization.

In a circuit simulcast subsystem:

- The site controller uses the TRAK 9100 SSR for frequency reference and as the primary Network Time Protocol (NTP) source for time synchronization.

In an IP simulcast subsystem:

- The site controller uses the TRAK 9100 SSR for the 1PPS time reference and as the primary Network Time Protocol (NTP) source for time synchronization.

2.1.7
Base Radio Monitoring Function of a Trunked GCP 8000 Site Controller

The site controller monitors the status of base radios and RFDS equipment at the site. The site controller concludes that a base radio has failed if the radio is not acknowledging messages or is not responding to periodic pings. The site controller takes a failed radio out of service and creates an appropriate Additional Channel Broadcast to advertise other channels at the site. An MSU attempts to acquire another channel if the site controller gives it the Move channel command, or if the radio that the subscriber is on fails.

The active site controller module monitors and forwards the alarm information to the Unified Event Manager for fault management monitoring. If MOSCAD NFM or SDM3000 NFM is supported at the site, then the active site controller module also passes alarms as LAN messages to MOSCAD NFM or SDM3000 NFM for processing. The MOSCAD NFM or SDM3000 NFM processes the alarms and informs the affected base radios about the changes in alarm state to take the appropriate action (bring themselves in or out of service).

2.1.8
Integrated Ethernet LAN Function of a Trunked GCP 8000 Site Controller

The site controller modules provide integrated Ethernet LAN switching. An interface between the integrated Ethernet switch provides access to all the base radios or XHubs by either site controller. The interface also makes it possible for any base radio to route its traffic to a site router or gateway.

If six or more standalone QUANTAR® stations or standalone GTR 8000 Base Radios are at an ASTRO® 25 repeater site, external HP LAN switches must be used.

2.1.9
MOSCAD NFM Indicator Function with a Trunked GCP 8000 Site Controller

When the MOSCAD NFM (Network Fault Management) system is employed at the site, it can be used to monitor and respond to failures on the transmit or receive paths at the site. The site controller monitors the RF distribution equipment, including the power monitor and the multi-coupler receiver to determine the condition of the transmit and receive paths. Upon failure on either path, the site controller indicates the event to the MOSCAD NFM. The MOSCAD NFM responds to the base radio and indicates that a failure has occurred in the RFDS. The base radio de-keys and sends a status message to the site controller indicating that the base radio is no longer available.

See the *MOSCAD Network Fault Management* manual for additional information on the alarm function.

NOTICE: The Unified Event Manager (UEM) can be established as a more centralized fault management solution replacing the MOSCAD GMC. See the *Unified Event Manger* and the *UEM GMC MOSCAD Transition Guide* for details.

2.1.10
Redundancy Function of a Trunked GCP 8000 Site Controller

Two site controller modules are provided. One module acts as the active site controller and the second is the standby site controller. To provide maximum availability, the two site controllers actually take on some aspects of the active tasks at the same time. There are two RF control paths between the zone

controller and a trunked subsystem. Upon failure of the active site controller, the standby site controller takes over as the active site controller. Or, if the LAN connected to the active site controller fails, the standby site controller becomes active. The redundancy ensures that a single site controller failure at the trunked site does not reduce overall functionality.

The two site controllers operate in an active/standby configuration for protection against a single site controller failure at the site. The active site controller manages operations at the site while the standby site controller monitors the periodic status messages from the active site controller. A programmed set of rules determines which site controller assumes the role of a primary controller and when it is necessary for the other site controller to take over the operation of the subsystem.

During the rollover process, the newly active site controller transits through the initialization process. Rollover can take place also when the site is in the site trunking mode.

If redundancy of the site controllers is split within a Trunked IP Simulcast Prime Site Geographic Redundancy (TPSGR) subsystem, a third site controller (secondary prime site controller) is applied. The secondary prime site controller monitors the activity of both the primary prime site controllers. If no activity is detected within 10 seconds, the secondary prime site controller becomes active and starts the initialization process with the zone controller. When the secondary prime site controller detects the primary prime site controllers (recovery scenario), the secondary prime site controller executes the procedures necessary to return control to the primary prime site controllers.

NOTICE: To support a TPSRG subsystem, the Site Trunking Indication Holdoff (sec) field in the site controller Configuration/Service Software (CSS) can be set to a non-zero value to help prevent radio scatter upon recovering from a primary prime site failure.

The redundancy function of the site controller is configured through CSS and Unified Network Configuration (UNC). Status of the redundancy state or when a site controller fails is reported to the system manager through CSS, UNC, Unified Event Manager, SDM3000, or MOSCAD.

For configuration details for site controller geographic redundancy, see Site Controller Configuration & Service Help > Mutli-Site Controller > Configuration Window in the *CSS Online Help*.

2.1.11
Sub-band Restriction Function of a Trunked GCP 8000 Site Controller

To support talkgroup calls for sub-band restricted radios that operate in RF sites providing both 700 MHz and 800 MHz channel resources, a talkgroup can be configured as an S-SBR (static SBR) talkgroup. When an S-SBR talkgroup is used for a call, the system assigns an 800 MHz channel to the call even if all subscriber radios registered at a site may be non-SBR subscriber radios capable of operating in the 700 MHz and 800 MHz band. With this method, channel utilization is based on the SBR status of the talkgroup.

An alternative method for channel utilization is available where an RF site provides both 700 MHz and 800 MHz channel resources and the system employs SBR and non-SBR subscriber radios. A Dynamic Sub-Band Restriction (D-SBR) method can be enabled to determine channel utilization. This method is based on the capabilities of the subscriber radios and can improve utilization of 700 MHz channel resources at an RF site providing both 700 MHz and 800 MHz channels. The dynamic SBR method is used only by the zone controller in Wide Area trunking mode.

The site controller uses the static SBR method for channel utilization for calls initiated, while an RF site is in Site Trunking mode.

2.1.12
Tri-Band Control Channel Hosting

The GCP 8000 Site Controller can provide the ability for a site to simultaneously host control channels on the 800 MHz, UHF, and VHF frequency bands which extends a talkgroup across all three bands.

This capability is supported in ASTRO® 25 L and M zone core configurations for simulcast or non-simulcast trunking RF site configurations that use G-series equipment (only). This feature supports the APX8000 tri-band capable subscriber radio.

2.1.13
License Auditing

License auditing for ASTRO® 25 G-series devices at M and L core systems can be enabled through the License Manager to ensure that site licenses have been purchased and also to prevent the transfer of site licenses across systems.

The License Manager performs the following functions:

- Monitors the number of site devices in use within the system.
- Audits the number of active licenses.
- Displays a noncompliance notification on the Unified Event Manager (UEM) when the number of devices exceeds the licenses.

If a site license is not present, the following functions do not occur:

- Send or receive audio
- Vote audio
- Implement site control functions; such as assigning channels or calls.

Any issues with an existing site license are sent to the UEM without system functionality being restricted.

2.1.14
Conventional GCP 8000 Site Controller Functions

A conventional operation called site conventional is a feature, providing the console ability to use conventional channels when the control path is lost between the console site and master site zone controller. The conventional site controller supports site conventional operation where a Conventional Channel Gateway (CCGW) is located at an MCC 7500/7100 console site.

The conventional site controller can support analog conventional operation with a CCGW interface between analog base radios and the consoles as well as ASTRO® 25 Conventional operations with a digital CCGW interface between digital base radios and the consoles.

Wide to Site Mode Transition

Site conventional operation involves the transition of a conventional site:

- From wide conventional to site conventional mode of operation utilizing the zone controller
- From site conventional to wide conventional mode of operation utilizing the conventional site controller

Affiliation

The conventional site controller allows base radio and console operation to affiliate to conventional channels in site conventional mode. This is similar in wide conventional mode, except that the operation is required to re-affiliate whenever there is a transition from wide to site conventional mode.

The conventional site controller stores affiliation information throughout the period of site conventional operation. When the console site link goes down and then comes back up, the site controller uses the stored affiliation information to update console operations with the statuses of conventional channels they are affiliated to.

Association

Association is an attribute of affiliation. The conventional site controller supports association as a part of Cross Busy/Cross Mute feature. Console operation associated to a given conventional channel receives all call processing events related to that channel, but no audio.

2.1.15 Conventional Talkgroup GCP 8000 Site Controller Functions

A conventional operation called ASTRO® 25 Digital Conventional Talkgroup is a feature, providing conventional talkgroup capability for selected channels on subscriber units and consoles on ASTRO® 25 systems. Conventional talkgroups support the separation of calls from multiple groups on a single channel at the consoles, allowing separation of calls between the groups and console operators so they do not monitor and/or interfere with other groups.

Conventional talkgroups support the following features:

- Console Priority (same talkgroup)
- Queuing (different talkgroup)
- Channel Wide Talkgroup

2.2 GCP 8000 Site Controller Power Supply

NOTICE: The power supply is used only for the standalone GCP 8000 Site Controller.

Figure 9: GCP 8000 Site Controller Power Supply

The GCP 8000 Site Controller power supply operates from either an AC or DC input and provides the DC operating voltage for the site controller.

When operating from an AC source (90 to 264 VAC, 47-63 Hz), the supply generates 2 DC output voltages of 29 V with respect to output ground. The power supply automatically adjusts to AC input ranges and supplies a steady output.

In the AC mode, the power supply may provide a separate battery charger, which is used to maintain the charge on a 48 VDC nominal system, positive or negative ground, if installed. The supply

generates 2 DC output voltages of 29V with reference to the output ground, when operating from a DC source (43.2 VDC to 60 VDC maximum, positive or negative ground). This voltage limit includes consideration of the battery charging “float voltage” associated with the intended supply system, regardless of the marked power rating of the equipment.

The battery charger is not usable when operating from a DC input power source.

The power supply contains several switching-type power supply circuits as follows:

- Power factor correction circuitry
- Battery charging circuitry
- Diagnostics and monitoring circuitry

The battery charger outputs of the power supply can be bussed together so that up to six power supplies provide charging services to a single battery bank.

The power supply controls its own continuously running fan, changing its speed to fast or slow as needed.

2.2.1
AC/DC Power Distribution

Figure 10: AC and DC Power Distribution in the Standalone GCP 8000 Site Controller Chassis With One Module

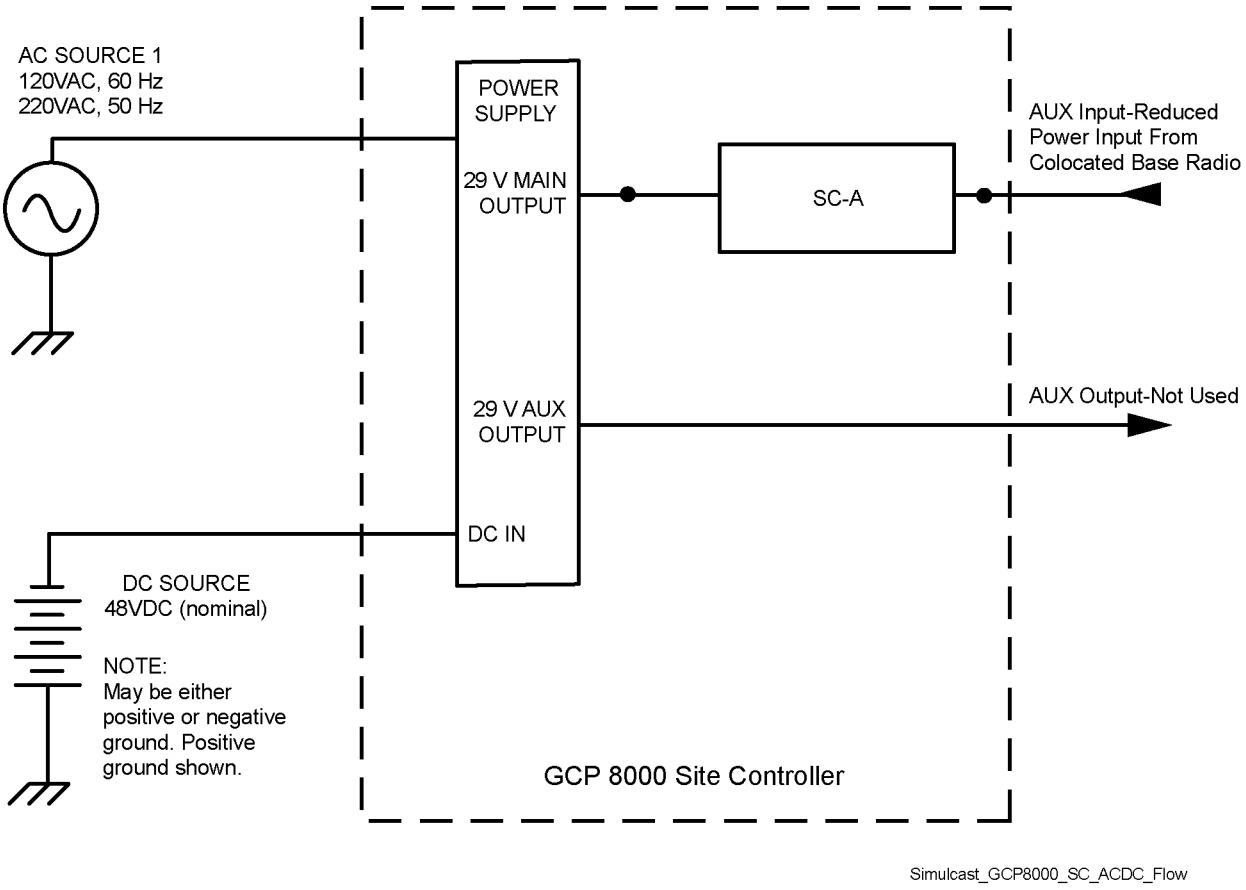
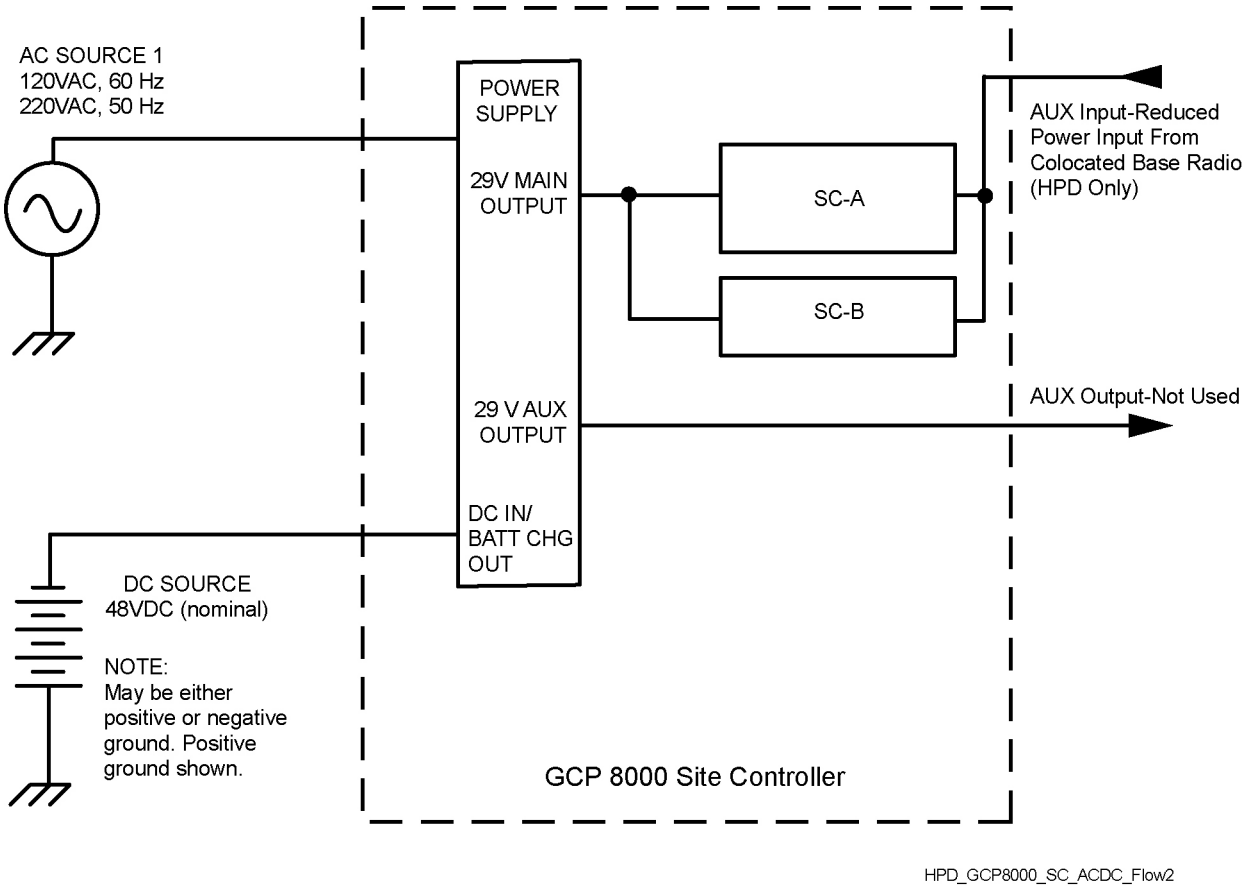


Figure 11: AC and DC Power Distribution in the Standalone GCP 8000 Site Controller Chassis With Two Modules



The GCP 8000 Site Controller operates from AC power as the preferred power source. When AC power is not available, the site controller switches to operate from the DC source. Operation returns to the AC source when the AC source is restored. Switch over from AC to DC and back again is fully automatic. No operator action is required.

The main DC output of the power supply is used to provide power to the site controller modules. The Auxiliary output of the power supply is reserved for use as a redundant power input.

2.2.2
Power Supply Battery Charger

The power supply may include an integrated battery charger. The battery charger is controlled through software residing on the associated device module. Software contains the information on supported battery types and obtains user-specific information pertaining to the particular site. The device software receives battery bus voltage and battery temperature information from the power supply, and uses these variables with supported battery charging profiles to return a signal which sets the charger output voltage appropriately. The battery charge and temperature conditions are viewed through Configuration/Service Software (CSS) and Unified Network Configurator (UNC), or through alarms to Unified Event Manager (UEM).

The maximum charging current available from the integrated charger is 3 A (48 VDC nominal system). A battery with capacity no larger than 60 Ah should be connected to a single charger to ensure that the charger maintains an adequate state-of-charge on the backup battery, and the backup battery is restored to full capacity within a reasonable amount of time following operation on battery backup power.

In addition to standard sealed lead-acid batteries (valve-regulated lead acid or gel cells), the power supply supports charging of vented lead-acid and NiCd batteries.

2.2.3
Battery Temperature Sensor Cable

The integrated charger in the power supply performs temperature compensated battery charging when a temperature sensor is connected. If the sensor is disconnected, the charger continues to operate as an uncompensated charger with the charging profile following the minimum charger voltage specified by the battery manufacturer.

Included is a 40 ft battery temperature sensor cable, which attaches to a battery pack, supplied by your organization, and to the backplane of the device. This three-wire cable carries a voltage signal to the power supply from the sensor element, which must be mounted close to the storage battery. Voltage is proportional to the battery temperature, and the diagnostic circuitry in the power supply module. This cable is extended to a total length of 190 ft using 50 ft extensions. See Battery Temperature Sensor Mounting on page 66.

IMPORTANT: Continuous operation with a disconnected sensor is not recommended.

2.2.4
ON/OFF Switch for Power Supply and Battery Charger

This table identifies the switch states for the power supply and battery charger.

Table 7: ON/OFF Switch - States for Power Supply and Battery Charger

Switch Position	Power Supply State	Battery Charger State
ON (1)	• Power Factor Correction (PFC) section is active (AC input only) • Main DC converter runs to create the MAIN and AUX DC outputs	DLN6781A can be started if desired (AC input only) DLN6805A Disabled
OFF (0)	• Main DC converter is turned OFF and the MAIN and AUX DC outputs become 0.0 VDC	Disabled (AC input only)

2.2.5
Power Supply Module Backplane Connections

NOTICE: Only the standalone GCP 8000 Site Controller uses the power supply module backplane connection.

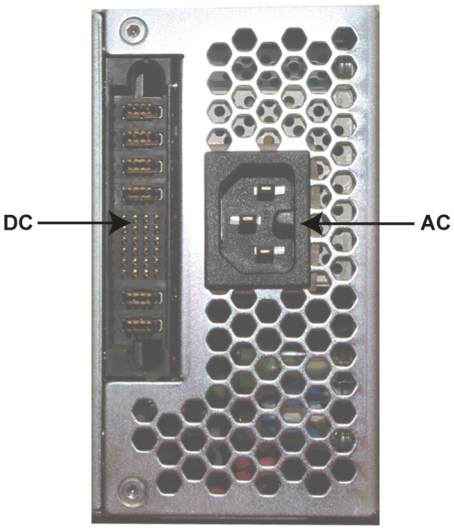
Table 8: GCP 8000 Power Supply Module Backplane Connections

Port/Type	Description
AC	Input only

Table continued…

Port/Type	Description
Battery / DC Power and Control Signal	**48 VDC:** • Provides the DC input to the power supply when operating from a DC source. • Connects the charger output to the standby battery when operating from an AC input with a standby DC battery. **29 VDC:** • Provides the Main and Aux DC outputs of the power supply for use by the power amplifier, transceiver, and site controller. Other signals handled by this connector include control interface and battery temperature interface.

Figure 12: GCP 8000 Power Supply Connections (Rear)



G_Series_PS_Rear1

2.3 GCP 8000 Site Controller Auxiliary Power

The GCP 8000 Site Controller receives auxiliary power from other devices as well as provides auxiliary power. For example, in a GTR 8000 Expandable Site Subsystem, it receives auxiliary power through the AUX PWR Input port, from the base radio, and benefits from the backup power source when needed.

The site controller also provides 29 VDC auxiliary power to other devices. For example, from the RFDS port of the GTR 8000 Expandable Site Subsystem backplane, the site controller provides auxiliary power to another device such as the Receiver Multi-coupler.

For a GTR 8000 Expandable Site Subsystem, a power supply can be removed without disabling the site controllers if the site controllers are cabled to auxiliary power. Auxiliary power is available from any base radio that is still connected to a power supply. An AUX DC bus is automatically set up to provide backup power to the site controllers.

Chapter 3

GCP 8000 Site Controller Installation

This chapter details installation procedures relating to the GCP 8000 Site Controller.

3.1 Pre-Installation Tasks

Follow this process to perform the installation tasks. Ensure that you have the following:

- Appropriate cables
- Access to Software Download Manager (SWDL), Configuration/Service Software (CSS), and the Unified Network Configurator (UNC)
- IP/DNS information
- Login and password information

3.1.1 Equipment Installation Process Overview

Process:

1. Prepare the site to comply with the Motorola Solutions requirements and specifications for the equipment, as listed in the *Standards and Guidelines for Communication Sites* manual. Other codes and guidelines that may apply to the location must also be met. See General Safety Precautions on page 48.
2. Inspect and inventory all racks, cabinets, cables, and other equipment with a Motorola Solutions representative to ensure that the order is complete. See General Installation Standards and Guidelines on page 50.
3. Various tools are used to install and service the equipment. If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solutions Support Center (SSC). See General Installation/Troubleshooting Tools on page 56 for a list of general recommended tools for installing and servicing the hardware.
4. Install all equipment using the site drawings and other documents provided by the Field Engineer. Use the installation standards and guidelines for placing and installing equipment.
5. Properly ground all the racks and cabinets to protect against ground faults, electrical surges, and lightning. See GCP 8000 Site Controller Hardware Installation on page 58.
6. Connect all necessary cables within a rack and between the racks for system interconnection. See either GCP 8000 Site Controller Ports (Front View) on page 68 or GCP 8000 Site Controller Ports for Standalone and GTR 8000 Site Subsystem Configurations (Rear View) on page 72 for cable connections.
7. Run a preliminary check of a site before applying power.
8. See Installing Device Software Prerequisites on page 81 for a list of items you need access to before installing the software.
9. See Installing Devices in the UNC on page 84 to discover the site controller and to load OS software images from the UNC.
10. See Device Configuration in CSS on page 95 to program the configurations into the site controller in CSS.

11 See Configuring Centralized Authentication on Devices in VoyenceControl on page 113 to program the site controller in UNC.

3.2 General Safety Precautions

WARNING: Compliance with FCC guidelines for human exposure to Electromagnetic Energy (EME) at Transmitter Antenna sites generally requires that personnel working at a site must be aware of the potential for exposure to EME, and can exercise control of exposure by appropriate means, such as adhering to warning sign instructions, using standard operating procedures (work practices), wearing personal protective equipment, or limiting the duration of exposure. For more details and specific guidelines, see “Appendix A” of the Motorola Solutions *Standards and Guidelines for Communications Sites* manual.

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 all equipment. See the appropriate section of the product service manual for additional pertinent safety information. Due to the danger of introducing additional hazards, do not install substitute parts or perform any unauthorized modifications of equipment.

NOTICE: The installation process requires preparation and knowledge of the site before installation begins. Review installation procedures and precautions in the Motorola Solutions *Standards and Guidelines for Communications Sites* manual before performing any site or component installation.

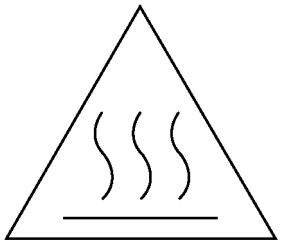
Always follow all applicable safety procedures, such as Occupational Safety and Health Administration (OSHA) requirements, National Electrical Code (NEC) requirements, local code requirements, and safe working practices. Also, all personnel must practice good judgment. General safety precautions include 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.
- If troubleshooting the equipment while power is on, be aware of the live circuits.
- Do not operate the radio transmitters unless all RF connectors are secure and all connectors are properly terminated.
- Ground all equipment properly in accordance with the Motorola Solutions *Standards and Guidelines for Communications Sites* manual and specified installation instructions for safe operation.
- Slots and openings in the cabinet are provided for ventilation. Do not block or cover openings that protect the devices from overheating.
- Only a qualified technician familiar with similar electronic equipment should service equipment.
- Some equipment components can become hot during operation. Turn off all power to the equipment and wait until sufficiently cool before touching.
- Maintain emergency first aid kits at the site.
- Direct personnel to call in with their travel routes to help ensure their safety while traveling between remote sites.
- Institute a communications routine during certain higher risk procedures where the on-site technician continually updates management or safety personnel of the progress so that help can be dispatched if needed.
- 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.
- Equipment installed at the site meeting the requirements of a "restricted access location," per UL60950-1, is defined as follows: "Access can only be gained by service persons or by a user who

has been warned about the possible burn hazard on equipment metal housing. Access to the equipment is by using a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location."

WARNING: Burn hazard. The metal housing of the product may become extremely hot. Use caution when working around the equipment.

Figure 13: Warning Label on Hot Modules



warning_hot

WARNING: DC input voltage must be no higher than 60 VDC. This maximum voltage includes consideration of the battery charging "float voltage" associated with the intended supply system, regardless of the marked power rating of the equipment. Failure to follow this guideline may result in electric shock.
RF energy burn hazard: disconnect power in the cabinet to prevent injury while disconnecting and connecting antennas.

CAUTION: All Tx and Rx RF cables outer shields must be grounded per Motorola Solutions *Standards and Guidelines for Communications Sites* manual requirements.
All Tx and Rx RF cables must be connected to a surge protection device according to the Motorola Solutions *Standards and Guidelines for Communications Sites* manual. Do not connect Tx and Rx RF cables directly to an outside antenna.

IMPORTANT: All equipment must be serviced by Motorola Solutions-trained personnel.

3.2.1
DC Mains Grounding Connections

CAUTION: This equipment is designed to permit the connection of the earthed conductor of the DC supply circuit to the earthing conductor at the equipment. If this connection is made, you must meet all following conditions:

- Connect this equipment directly to the DC supply system earthing electrode conductor or to a bonding jumper from an earthing terminal bar or bus in which the DC supply system earthing electrode conductor is connected.
- Locate this equipment in the same immediate area (such as adjacent cabinets) as any other equipment that has a connection between the earthed conductor of the same DC supply circuit and the earthing conductor (and also the point of earthing of the DC system). Do not earth the DC system elsewhere.
- Locate the DC supply source within the same premises as the equipment.
- Do not install switching or disconnecting devices in the earthed circuit conductor between the DC source and the point of connection of the earthing electrode conductor.

3.2.1.1
Disconnect Device Permanently Connected

Incorporate a readily accessible disconnect device (circuit breaker or switch) in the building installation wiring.

3.2.1.2
Multiple Power Source

This product has multiple power sources. If service requires the removal of a power source, disconnect all inputs (AC and DC powers) to remove power completely to the equipment before servicing.

3.2.1.3
Connection to Primary Power

For supply connections, use wires suitable for at least 75 °C.

3.2.1.4
Replaceable Batteries

WARNING: Risk of Explosion if you replace the battery with an incorrect type. Dispose of used batteries according to the instructions.

3.2.2
Maintenance Requiring Two People

Identify maintenance actions that require two people to perform the repair. Two people are required when:

- A repair has the risk of injury that would require one person to perform first aid or call for emergency support. An example is work around high-voltage sources. If an accident occurs to one person, another person may be required to remove power and call for emergency aid.
- Heavy lifting is involved. Use the National Institute of Occupational Safety and Health (NIOSH) lifting equation to determine whether one or two persons are required to lift a system component when it must be removed and replaced in its rack.

3.2.3
Equipment Racks

Lift equipment racks without the use of lifting equipment only when sufficient personnel are available to ensure that regulations covering health and safety are not breached. Use an appropriately powered mechanical lifting apparatus for moving and lifting the equipment racks. In addition to these points, comply with any local regulations that govern the use of lifting equipment.

WARNING: Crush Hazard could result in death, personal injury, or equipment damage. Equipment racks can weigh up to 360 kg (800 lb). See the following instructions for proper lifting procedures.

3.3
General Installation Standards and Guidelines

This section provides several guidelines to ensure a quality install. Review these guidelines before unpacking and installing the system. Additionally, review the installation information in the *Standards and Guidelines for Communication Sites* manual for more details, including:

- Equipment installation
- Antenna installation

You should also review installation information specifically for GCP 8000 Site Controllers and subsystems in GCP 8000 Site Controller Hardware Installation on page 58.

3.3.1
General Site Preparation Overview

Perform the activities listed in this table to ensure proper site preparation. The table references specific chapters in the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for more information.

Table 9: Activities for Site Preparation

Activity	Description of Activity	Chapter Reference
Review the site plan.	• Prevents potential on-site and off-site interference by local trunked systems. • Minimizes cable lengths. • Determines the location of telecom equipment.	• Chapter 2 "Site Design and Development"
Determine site access and security.	Outlines of site access and security measures.	• Chapter 2 "Site Design and Development"
Review safety considerations.	Outlines general, installation, and environmental safety guidelines and requirements and OSHA-related considerations.	• Chapter 3 "Communications Site Building Design and Installation"
Schedule installation of telephone service.	Ensures options and functions of on-site, two-way communications for personnel safety and maintenance.	• Chapter 3 "Communications Site Building Design and Installation"
Review grounding specifications.	Ensures that the site meets or exceeds the Quality Audit Checklist in Appendix F as well as the Power and Grounding Checklist in Appendix D.	• Appendix D. “Grounding (Earthing) Electrode System Testing/ Verification” • Appendix F. “R56 Compliance Checklist”
Schedule installation of site power.	Covers grounding, power sources, and surge protection.	• Chapter 4 "External Grounding (Earthing)" • Chapter 5 "Internal Grounding (Earthing)" • Chapter 6 "Power Sources" • Chapter 7 "Surge Protective Devices"

3.3.2
General Equipment Inspection and Inventory Recommendations

Take an inventory of all equipment with a Motorola Solutions representative to ensure that the order is complete. Carefully inspect all equipment and accessories to verify that they are in good condition. Promptly report any damaged or missing items to a Motorola Solutions representative.

CAUTION: Do not tamper with factory configuration settings for these devices. These settings include software configuration, firmware release, password, and physical connections. Motorola Solutions has configured and connected these devices to meet specific performance requirements. Tampering with these devices may result in unpredictable system performance or catastrophic failure.

3.3.3
General Placement and Spacing Recommendations

When placing equipment at a site, perform the following:

- Place each rack on a firm, level, and stable surface, and bolt the racks together.
- Use correct mounting hardware and shims to prevent rack movement.
- Use strain relief when installing and positioning cables and cords to help ensure that no interruption of service occurs.
- Provide an appropriate amount of space around all components to allow for proper air flow, cooling, and safe access to equipment.
- Locate the site racks and other equipment with enough spacing to allow access for service.

  NOTICE: Proper spacing of equipment is essential for ease of maintenance and safety of personnel. Spacing requirements have been established to meet the National Fire Protection Associations (NFPA) code, and the American Society of Heating, Refrigerating, and Air Conditioning Engineers (ASHRAE) standards. Adhere to any local regulations that apply to the installation.
- Locate the system in an area free of dust, smoke, and electrostatic discharge (ESD).
- See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for details on these space requirements.

3.3.4
General Cabinet Bracing Recommendations

Use all supplied bracing hardware when installing a rack or cabinet, and secure all equipment within a rack or cabinet.

If additional equipment is installed, see the system design document the field engineer provided, or consult the Motorola Solutions Field Representative.

Subsystem cabinets are self-supporting structures. In areas subject to seismic activity, additional bracing of the cabinet may be required to prevent it from tipping. However, the bracing hardware must be locally procured. No specific procedures are provided within this manual for bracing cabinets in active seismic areas. See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for details on seismic conditions.

3.3.5
Mounting Cabinets or Racks to a Floor

When and where to use: Perform the following steps to properly install a cabinet or open rack within a site building. Secure the cabinets and racks to the floor for optimum stability. This procedure is written so that the cabinet or rack is moved only once.

Procedure:

1. Carefully mark the mounting holes with a pencil, as indicated on the appropriate cabinet or rack footprint.
2. Drill the marked mounting holes to the appropriate depth of the mounting hardware with a hammer drill and bit.
3. Insert an anchor into the drilled hole. If necessary, tap the anchor into place using a hammer.
4. For cabinets, remove the four screws securing the bottom kick panel to the front and back of the cabinet. Remove the kick panel and set aside during installation.
5. Carefully move the cabinet or rack into the position indicated by the holes in the floor.

   WARNING: Equipment cabinets and racks are heavy and may tip. Use extreme caution when moving. Lift from top eyenuts with the appropriate apparatus, or secure the cabinet or rack from tipping if lifting from the bottom. Failure to do so could result in death or serious injury or equipment damage.
6. Adjust and level the cabinet or rack as necessary to position the cabinet mounting holes with the pre-drilled holes.
7. Secure the cabinet or rack to the site floor with the locally procured mounting hardware.

   IMPORTANT: If securing the cabinet or rack to a concrete floor, use 1/2-inch grade 8 bolts with anchors.

3.3.6
General Bonding and Grounding Requirements

Cabinets and racks include a Rack Grounding Bar (RGB) with the capacity to terminate numerous ground wires. Attach equipment added to the cabinet or rack to the ground bar using solid or stranded 6 AWG copper wire.

The RGB uses dual-hole lugs to terminate ground wires. The minimum number of dual-hole attachments is system-dependent and specified by the customer. This bar provides electrical continuity between all bonds and ground wire with a current-carrying capacity equal to or exceeding that of a 6 AWG copper wire.

See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for more information on proper bonding and ground at a site.

3.3.7
General Cabling Requirements

Diagrams for cabling are typically included in the system-specific configuration documentation Motorola Solutions provides. Also see the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for cabling standards.

IMPORTANT: System certification was completed using shielded cables. To prevent emission problems, use only shielded cables. Do not substitute other cable types.

- Position the equipment to avoid excessive tension on cables and connectors. Cables must be loose with absolutely no stress on the connectors. Careful cable routing and securing the cables with tie wraps (or other devices) is one way to provide this protection. Set up preventive maintenance loops .
- Dress the cables neatly using cable ties. Do not tighten the cable ties until you are sure that the required service length and bend radius requirements are met. Leave cable ties loose enough to allow adjustment.
- Verify that all cables are properly labeled to match System-specific configuration documentation Motorola Solutions provided.
- Ensure that cables do not exceed the minimum bend radius as outlined in the Motorola Solutions *Standards and Guidelines for Communication Sites* manual.

CAUTION: Use only Category 5 Shielded Twisted Pair (or higher) for cabling Ethernet connections. Motorola Solutions has engineered this system to meet specific performance requirements. Using other cabling and connectors may result in unpredictable system performance or catastrophic failure.

NOTICE: For more information on cabling guidelines, see the documentation supplied with components from each equipment manufacturer.

3.3.8
General Power Guidelines and Requirements

See the Motorola Solutions *Standards and Guidelines for Communication Sites* manual for information on providing electrical service, power budgeting, selecting batteries, and other topics for supplying power at the site.

Perform electrical installation work in accordance with the current edition of the NFPA 70 and local building codes. Where required, use a qualified and licensed electrician for all electrical installations.

3.3.8.1
General AC Power Guidelines and Requirements

The Motorola Solutions *Standards and Guidelines for Communication Sites* manual defines the guidelines and requirements for cabinets and racks which house equipment that requires AC power input. Some of the guidelines and requirements are as follows:

- The cabinet or rack is designed to accept 120/240 V, single-phase power with an amperage service size as required by the electronic equipment.
- Cabinets and racks powered by commercial power must be equipped with a Nationally Recognized Test Laboratory (NRTL) certified power distribution module that contains a main circuit breaker or individual circuit breakers of the correct size as required for the electronic equipment or as the customer specified.
- A decal showing an electrical schematic of the power wiring is affixed to the inside surface of the cabinet.
- All AC power equipment and electrical components must conform to National Electrical Manufacturers Association (NEMA) and National Electrical Code (NEC). The AC power equipment must also be listed by an NRTL.
- A surge arrestor, designed to protect equipment systems from a 120/240 V service and load center, is placed on the power feed ahead of all individual load center circuit breakers. This gapless arrestor must be listed by an NRTL for the purpose intended.

- Selection of a surge arrestor is based on the susceptibility of the equipment powered by the electrical service, with margin provided for locally generated disturbances. See ANSI/IEEE C62.41 (21) for more details.
- At least one 120 VAC, 15 A duplex convenience outlet equipped with Ground Fault Interrupter (GFI) protection must be provided in the electronic equipment compartment.

CAUTION: Do not use surge/transient suppressors without careful and expert power system analysis.

NOTICE: Redundant devices could be terminated on different AC main phases so that a single phase failure does not result in a power loss for both devices.

3.3.8.2
General Breaker Recommendations

Each power supply should have its own supply breaker to ensure that a fault which causes the breaker to open does not result in the loss of multiple transmit channels. The breaker recommendations for AC and DC supply breakers are as follows:

- For a 120 VAC, 60 Hz application, the AC supply breaker should be rated for a continuous current of 20 A. For a 220 VAC, 50 Hz application, the AC supply breaker should be rated for a continuous current of 10 A minimum, not to exceed 20 A.
- For a 48 VDC application, the DC supply breaker must be rated for a continuous current of at least 5 A but not to exceed 25 A.

3.3.8.3
General Battery Installation Recommendations

The batteries and charger should be as close as possible to the rectifier system using the cables. A very heavy gauge stranded cable is advised to minimize voltage drop. The resistance of some heavy gauge wire is:

Table 10: Heavy Gauge Wire Resistance Examples

Gauge	Resistance
#6 gauge	0.3951 /1000 ft
#4 gauge	0.2485 /1000 ft
#2 gauge	0.1563 /1000 ft

The maximum voltage drop can be calculated by knowing the peak current drawn by the radio system. Use the following formula:

Total Voltage drop = [/1000 ft] x [total loop length (ft)] x [Ipeak (A)] + [connector(s) voltage drop(s)]

3.3.9
General Electrostatic Discharge Recommendations

Electronic components, such as circuit boards and memory modules, can be sensitive to Electrostatic Discharge (ESD). Use an antistatic wrist strap and a conductive foam pad when installing or upgrading the system.

If an ESD station is not available, wear an antistatic wrist strap. Wrap the strap around the wrist and attach the ground end (usually a piece of copper foil or an alligator clip) to an electrical ground. An electrical ground can be a piece of metal that literally runs into the ground (such as an unpainted metal pipe), or the metal part of a grounded electrical appliance. An appliance is grounded if it has a three-prong plug and is plugged into a three-prong grounded outlet.

NOTICE: Do not use a computer as a ground, because it is not plugged in during installation.

3.3.10
FCC Requirements

Radio frequency (RF) transmitters installed at sites within the US must be in compliance with the following FCC regulations:

- The station licensee is responsible for the proper operation of the station at all times and is expected to provide observations, servicing, and maintenance as often as may be necessary to ensure proper operation.
- The transmitter ERP must not exceed the maximum power specified on the current station authorization.
- The frequency of the transmitter must be checked during initial installation of the transmitter, when replacing modules, or when making adjustments that affect the carrier frequency or modulation characteristics.

This equipment has been tested and found to comply with the limits for a Class A digital device, according to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference to radio communications when the equipment is operated in a commercial environment.

This equipment generates, uses, and can radiate radio frequency energy. If not installed properly and used in accordance with the instruction manuals, the equipment may cause harmful interference to radio communications. Operation of some compliant equipment in a residential area may cause harmful interference to radio communications, in which case the interference must be corrected.

3.3.11
Networking Tools

Use the following networking tools for installing and servicing the network:

- Fluke® OneTouch Assistant LAN tester
- NiMH rechargeable battery for Fluke
- T1/E1 or E1 test set (such as the Hewlett-Packard® HP37702A)
- Serialtest® software with the ComProbe® and SerialBERT option

3.3.12
General Installation/Troubleshooting Tools

If information is needed regarding where to obtain any of the equipment and tools listed, contact the Motorola Solutions Support Center (SSC). See Motorola Solutions Support Center on page 132.

3.3.12.1
General Tools

Use the following general tools to install, optimize, and service equipment in the system:

- 150 MHz 4 Channel Digital Storage Oscilloscope
- Transmission Test Set (TIMS Set)
- Aeroflex 3900 Series Service Monitor or equivalent
- 50 Ohm Terminated Load
- Digital Multimeter (DMM)
- Terminal Emulation Software
- DB-9 Straight through serial cable
- RS-232 Cables with Connectors
- Punch Block Impact Tool
- MODAPT – RJ-45 Breakout Box
- Remote RJ-11/ RJ-45 Cable Tester (1200 ft length maximum)
- PC Cable Tester (RG-58, 59, 62, BNC, RJ-45, RJ-11, DB-9, DB-15, DB-25, Centronics 36-pin connectors)
- ESD field service kit
- Amprobe Instruments GP-1 Earth Tester
- AEMC 3730 Clamp-on Ground Resistance Tester

3.3.12.2
Rack Tools

Use the following tools to install, optimize, and service the equipment:

- Service Monitor: Aeroflex 3900 Series Service Monitor with P25 Options installed (plus High Performance Data (HPD) and Time Division Multiple Access (TDMA) options as required)
- Personal Computer meeting the following specifications:
  - Operating Systems:
    + Windows 10 (Server 2012 R2)
- Hardware Requirements:
  - Processor:
    + 1 GHz or higher Pentium grade
  - Processor Memory:
    + 2 GB RAM recommended for Windows 10
  - Hard Disk Space:
    + 300 MB minimum free space (for a Typical Installation, including Help Text and Software Download Manager) or 100 MB minimum free space (for a Compact Installation)
  - Peripherals:
    + Microsoft Windows supported mouse or trackball
    + Microsoft Windows supported serial port for product communication
    + Microsoft Windows supported Ethernet port for product communication
    + Microsoft Windows supported printer port for report printing
    + CD-ROM for software installation
- Configuration/Service Software (CSS) DLN6455

- CSS serial programming cable
- Ethernet cable
- Antenna tester
- 50 Ohm terminated load
- Rohde & Schwarz NRT-Z14 Directional Power Sensor, 25-1000 GHz, 0.1-120 W. Recommended for all uses when a service monitor is not available.

3.3.13
Technical Support for Installation

Technical support is available from the site-specific documents the Field Engineer or Motorola Solutions Field Representative provided for the system, one of the Motorola Solutions Support Centers (SSC), or qualified subcontractors.

- SSC can help technicians and engineers resolve system problems and ensure that warranty requirements are met. Check your contract for specific warranty information. See Motorola Solutions Support Center on page 132.
- The Motorola Solutions System Service Subcontractor Assessment program ensures that service people contracted by Motorola Solutions meet strict minimum requirements before they can work on any system. For more information on this program, contact the Motorola Solutions representative.

3.3.13.1
Site-Specific Information

When the Motorola Solutions Center for Customer Solution Integration (CCSi) stages a system, the Field Engineer assigned to the system creates all site-specific system documentation to document how the system was staged. Site-specific information includes the following:

- Site design drawings showing the location of racks, cabinets, cable trays, and other components
- Rack drawings showing the location of the equipment in each rack
- Cable matrix in a table format that shows each cable and its connections
- Interconnect wiring diagrams to show the cable connections between devices
- Pre-programmed parameters of each site component
- Templates used to program each device
- All firmware and software revisions of each site component
- Test data from each device that requires operational verification
- Optimization requirements and settings of each electrical path
- Acceptance Test Plan for the site components

NOTICE: Maintain this site-specific information to reflect the current site configuration and layout for the system.

3.4
GCP 8000 Site Controller Hardware Installation

See the *Standards and Guidelines for Communication Sites* manual for guidelines on designing and installing equipment at an RF site. The following guidelines are covered:

- Safety guidelines
- Site selection, design, and development

- Site building design and installation
- External/internal grounding
- Power sources
- Transient voltage surge suppression
- Minimizing site interference
- Equipment installation
- Antenna installation

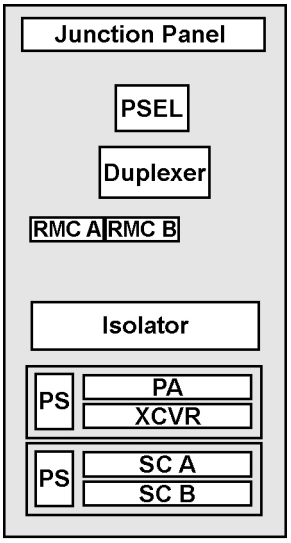
The GCP 8000 Site Controller is installed in one of three hardware configurations:

- **Standalone GCP 8000 Site Controller:** This is only available as a unit. Hardware is available to mount it to a rack. It comes with either one or two modules within the chassis. It does not ship with a rack or a cabinet. For detailed information, see GCP 8000 Site Controller in a Standalone Configuration on page 64.
- **GTR 8000 Site Subsystem:** This is a specific set of hardware modules in a special 52 inch rack. It includes a base radio, two redundant site controller modules with one chassis, and RFDS equipment. For detailed information, see GCP 8000 Site Controller in a GTR 8000 Site Subsystem Configuration on page 59.
- **GTR 8000 Expandable Site Subsystem:** This is available in a cabinet or an open rack with two redundant site controller modules, and RFDS equipment. For detailed information, see GCP 8000 Site Controller in a GTR 8000 Expandable Site Subsystem Configuration for HPD on page 60 and GCP 8000 Site Controller in a GTR 8000 Expandable Site Subsystem Configuration for Repeater Site on page 60.

3.4.1
GCP 8000 Site Controller in a GTR 8000 Site Subsystem Configuration

The GTR 8000 Site Subsystem configuration comes from the factory pre-wired and installed.

Figure 14: GTR 8000 Site Subsystem Configuration



HPD_site_subsystem_config

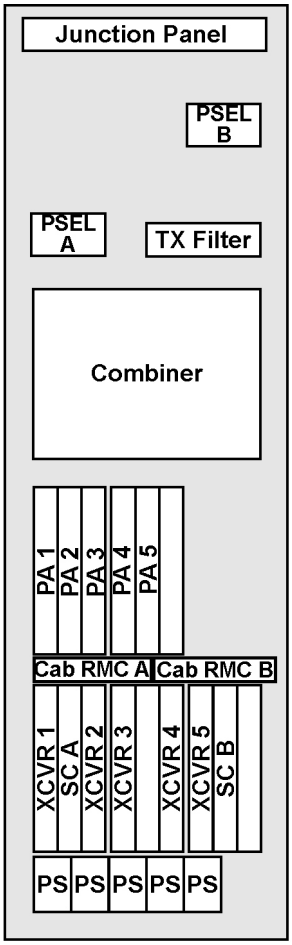
When the GCP 8000 Site Controller is part of the GTR 8000 Site Subsystem, the wiring is internal through the junction panel.

3.4.2

GCP 8000 Site Controller in a GTR 8000 Expandable Site Subsystem Configuration for HPD

The GTR 8000 Expandable Site Subsystem configuration comes from the factory pre-wired and installed with up to five base radios. The cabinet has two redundant GCP 8000 Site Controller modules.

Figure 15: GTR 8000 Expandable Site Subsystem Configuration – Example of an HPD Subsystem



HPD_expandable_site_subsystem_config_1

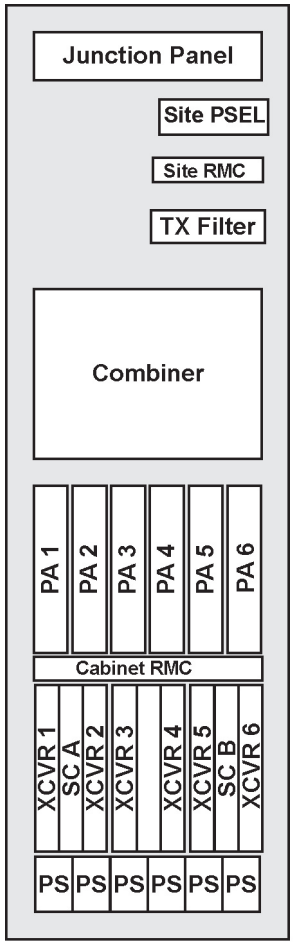
The wiring is internal through the junction panel and connected at the factory.

3.4.3

GCP 8000 Site Controller in a GTR 8000 Expandable Site Subsystem Configuration for Repeater Site

The GTR 8000 Expandable Site Subsystem configuration comes from the factory pre-wired and installed with up to six cabinets for a repeater site. The first cabinet has two redundant GCP 8000 Site Controllers. In the second through sixth expansion cabinets, XHubs are used to support additional expansion cabinets with channels beyond what the site controller can support on its own.

Figure 16: GTR 8000 Expandable Site Subsystem Configuration – Example of a Repeater Site



The wiring is internal through the junction panel and connected at the factory. Additional sub-panels are added for expansion cabinets.

3.4.4
Placement and Spacing

Cabinets and racks allow equipment to be added to a site. Always consider room for expansion when setting up a site. Cabinets or racks may be installed next to each other or to other equipment. However, provide all cabinets and racks with sufficient floor space to permit access for installation and service.

Clearance required for service and installation is at least 2 ft in the front and rear.

Front access:

- At least 2 ft floor access in front of the cabinet or rack.

Side and rear access:

- At least 2 ft floor access at the rear of the cabinet or rack, or
- At least 2 ft access on at least one side of the cabinet or rack, plus 6 inches at the rear of the cabinet or rack.

To maintain this clearance, the following is required:

- If there is less than 2 ft rear access, do not install more than two cabinets or racks side by side, and allow at least 2 ft access on at least one side of each cabinet or rack.
- For the cabinet version, if there is less than 2 ft rear access, do not install the optional rear door on the cabinet.

NOTICE: For the cabinet version, when an eyenut has to be replaced, provide at least 2 ft access to both sides of the cabinet so that both side panels can be removed.

3.4.5
Power Requirements

Follow the guidelines in the *Standards and Guidelines for Communication Sites* manual for information on providing electrical service, power budgeting, selecting batteries, and other topics for supplying power at the site.

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

Table 11: Standalone GCP 8000 Site Controller Input Power Wiring

If the GCP 8000 Site Controller uses	Then
AC power	Connect a power cord from the Input port on the rear of the unit to an AC outlet.
DC power	Input from a +/- 48 VDC nominal power supply. **IMPORTANT:** You must ground the battery system, either positive or negative, at the battery because the DC power system in the GCP 8000 Site Controller floats, it is not grounded.

GTR 8000 Expandable Site Subsystem: The power sources for the site controllers and XHubs are two shared sources. The even-numbered base radio power supplies are one source. The odd-numbered base radio power supplies are the other source.

3.4.6
GCP 8000 Site Controller Grounding

The GCP 8000 Site Controller has a double lug with two lock nuts on the rear panel where the ground wire connects to the site controller on one end, and to the rack grounding bar on the other. The rack grounding bar is connected to the internal ground system. To use the grounding lug, you need a length of #6 AWG wire with UL-listed ring lugs on both ends. This wire is shipped with the site controller.

Figure 17: GCP 8000 Site Controller Rear View with Grounding Lugs

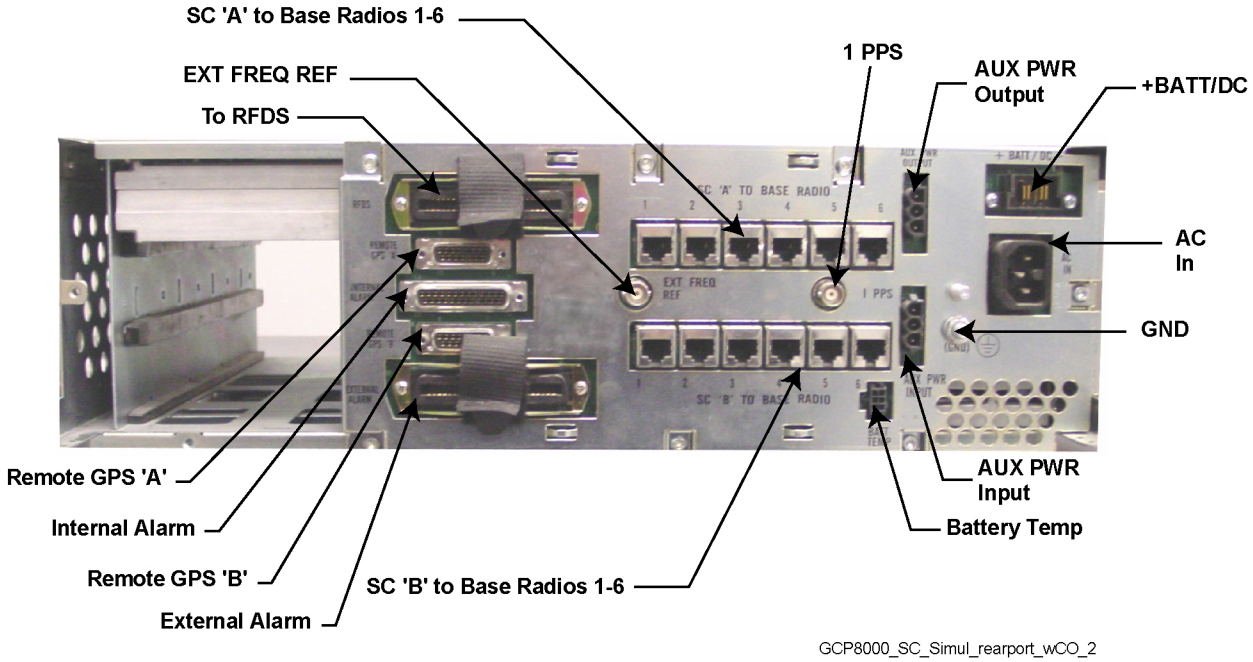
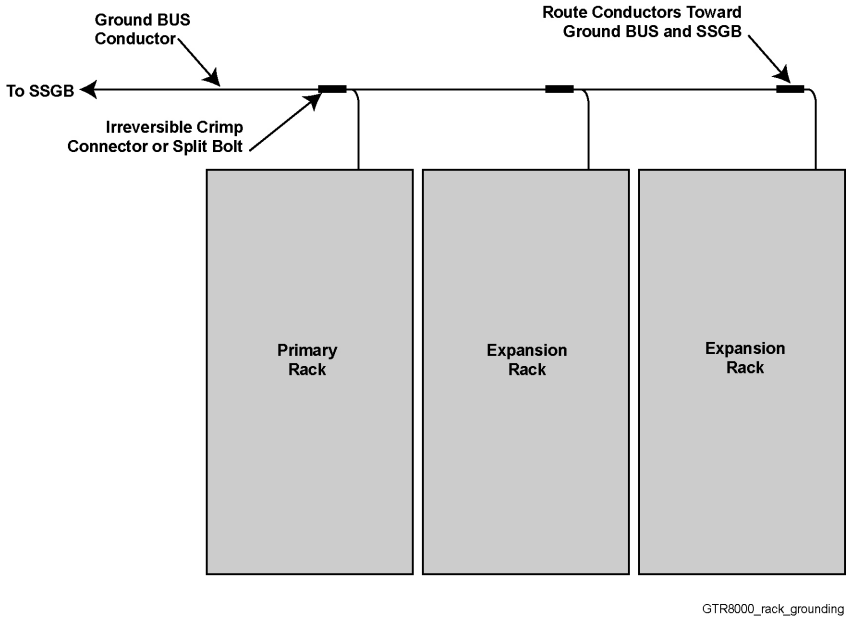


Figure 18: Rack Grounding



Detailed grounding information is beyond the scope of this manual. See the *Standards and Guidelines for Communication Sites* manual for detailed information about grounding and lightning protection.

3.4.6.1
Grounding the GCP 8000 Site Controller

Prerequisites: This procedure assumes that all telephone lines, antenna cables, and AC or DC power cables are properly grounded and lightning-protected.
GTR 8000 Expandable Site Subsystems: If rack installations have a primary rack and one or more expansion racks, then all these racks must be connected to the same Sub System Ground Bus Bar

(SSGB) (and no other rack connected to the SSGB). This is to ensure surge events do not produce ground potential differences that affect signals between the racks.

Procedure:

1. Take the ground wire already attached to the two grounding lugs at the rear of the site controller, and connect the other end to the rack grounding bar.
2. Tighten the ground lock nut to 60 inch-pounds (6.94 newton-meters).

3.4.7
GCP 8000 Site Controller in a Standalone Configuration

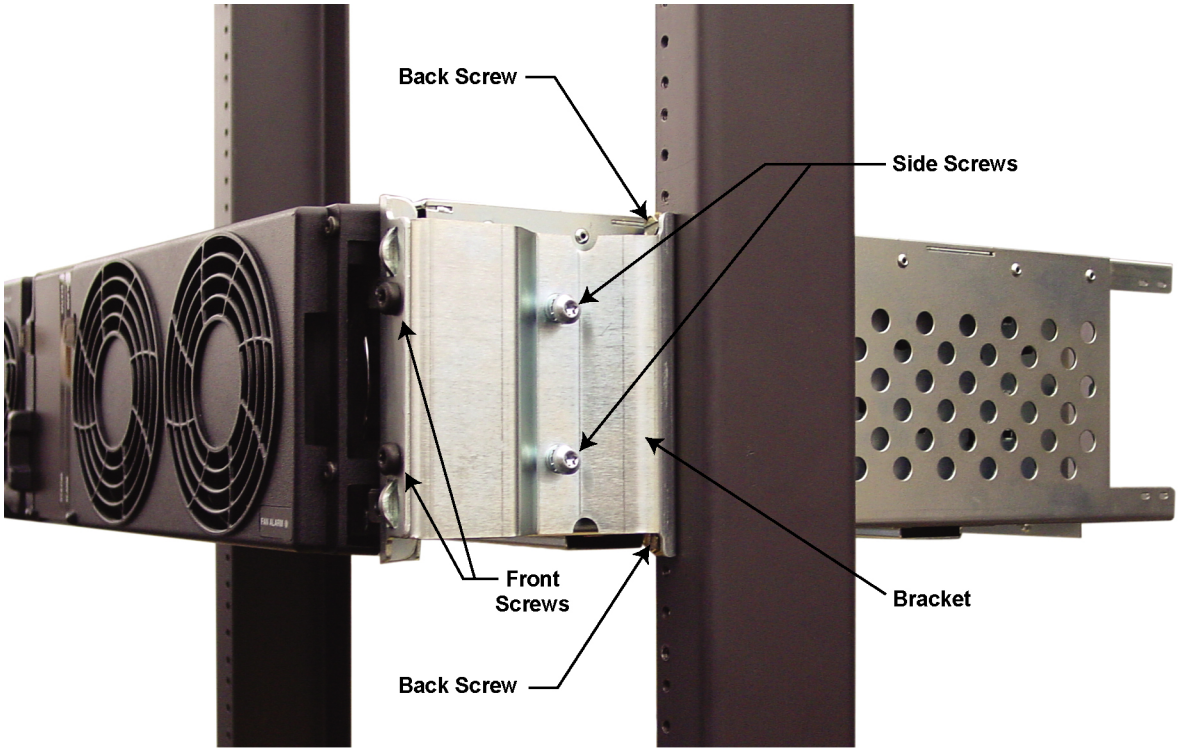
The GCP 8000 Site Controller is a standalone chassis. This is only available as a unit. Hardware is available to mount it to a rack. It does not ship with a rack or a cabinet.

- In an HPD subsystem or ASTRO® 25 repeater site, the two site controller modules are mounted in one chassis.
- In a circuit simulcast subsystem, the standalone configuration requires two chassis, with each chassis holding a single site controller module in the upper slot within the chassis.
- In an IP simulcast subsystem, the standalone configuration requires two chassis, with each chassis holding a single site controller module. The site controller that has been assigned as site controller 1 must have the site controller module in the upper slot within the chassis, and the site controller that has been assigned as site controller 2 must have the site controller module in the lower slot within the chassis.

3.4.7.1
Rack Mounting the Standalone GCP 8000 Site Controller

The Standalone GCP 8000 Site Controller mounts in a rack that is secured to the floor. For open racks, two brackets are required to distribute the weight. Without brackets, the center of gravity of the system shifts to the back, potentially causing structural issues with the rack. The brackets come with the required number of screws.

Figure 19: GCP 8000 Site Controller Mounted in Rack



NOTICE: Perform this installation with two people so that one person can hold the device in place while the other person attaches the brackets to the rack.

3.4.7.1.1

Mounting the GCP 8000 Site Controller

Procedure:

1. Determine where on the rack to mount the site controller and mark the location. The brackets are useful in making this determination, and the pin on the back of the bracket helps finding the exact location on the rack.
2. Attach the brackets to the sides of the site controller:
   a. Use M6x1x13 machine screws with a captivated washer (zinc plated).
   b. Screw one bracket into the clinch nuts on the side of the site controller chassis.
   c. Screw the second bracket into the clinch nuts on the other side of the site controller chassis.
3. Lift the site controller into place on the rack using the pins on the brackets to properly line up the device.
4. Attach the two brackets to the rack:
   a. For a Motorola Solutions modular rack, use M6x1x10 thread forming screws with a black finish.
   b. For a Motorola Solutions open rack, use 12-24x5/8 in. thread forming screws (zinc plated).
   c. For your own rack, use hardware appropriate for the rack.
   d. Attach the brackets to both sides of the rack through the upper back openings on the brackets.

e Attach the brackets to the rack on both sides through the lower back openings.

5 In the front, attach the chassis to the brackets:

a Screw two M6x1x10 thread forming screws (black finish) through the front holes on one side of the site controller chassis and into the bracket.

b Screw two M6x1x10 thread forming screws (black finish) through the front holes on the other side of the site controller chassis and into the bracket.

3.4.8
Battery Temperature Sensor Mounting

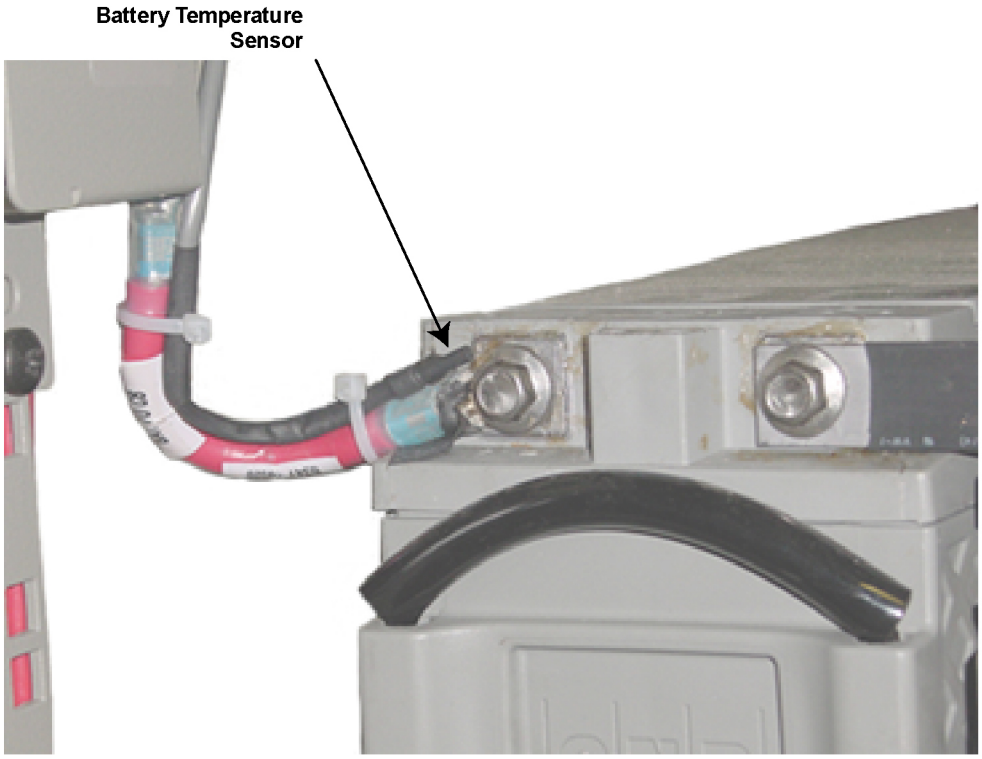
A 40 ft battery temperature sensor cable is shipped with your device. This three-wire cable carries a voltage signal to the power supply from a sensor element which must be mounted close to the storage battery. Voltage is proportional to the battery temperature and the diagnostic circuitry in the power supply module. The 40 ft cable can be extended to a total length of 190 ft using 50 ft extensions (Motorola Solutions part number 3084827Y04. See Motorola Solutions Support Center on page 132.

Mount the sensing element of the temperature sensor so that it detects the actual battery temperature (or the ambient temperature as close as possible to the batteries being charged). The two examples of mounting are as follows:

Example 1

Use cable ties to attach the sensing cable to the positive (or negative) power cable. A minimum of two cable ties should be used (spaced 6 inches apart), with one of the cable ties not more than 2 inches from the sensing element. Mount the sensing element not more than 2 inches from the battery post where the power cable connects. See Figure 20: Battery Temperature Sensor Example 1 on page 67.

Figure 20: Battery Temperature Sensor Example 1



GTR8000_Battery_Temperature_Sensor_1

Example 2

Attach the sensing cable to an existing battery tray support bracket using cable ties or nylon loop straps of the proper size. Mount the sensing element not more than 2 inches from the surface of the batteries being monitored. Use a minimum of two cable ties and/or loop straps to secure the sensing cable to the bracket. Place the cable ties/ loop straps no more than 6 inches apart with one placed no more than 2 inches from the sensing element. See Figure 21: Battery Temperature Sensor Example 2 on page 68.

Figure 21: Battery Temperature Sensor Example 2

3.4.9
GCP 8000 Site Controller Ports (Front View)

The ports on the front of the GCP 8000 Site Controller module are the same, whether the module is in a standalone configuration or GTR 8000 Expandable Site Subsystem configuration.

Figure 22: GCP 8000 Site Controller Ports for Standalone and GTR 8000 Site Subsystem Configurations (Front View)

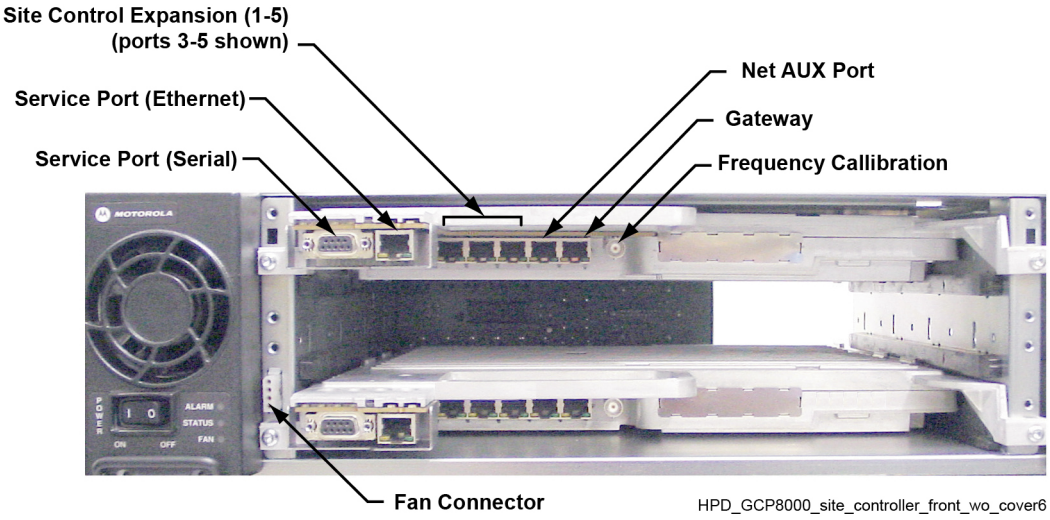
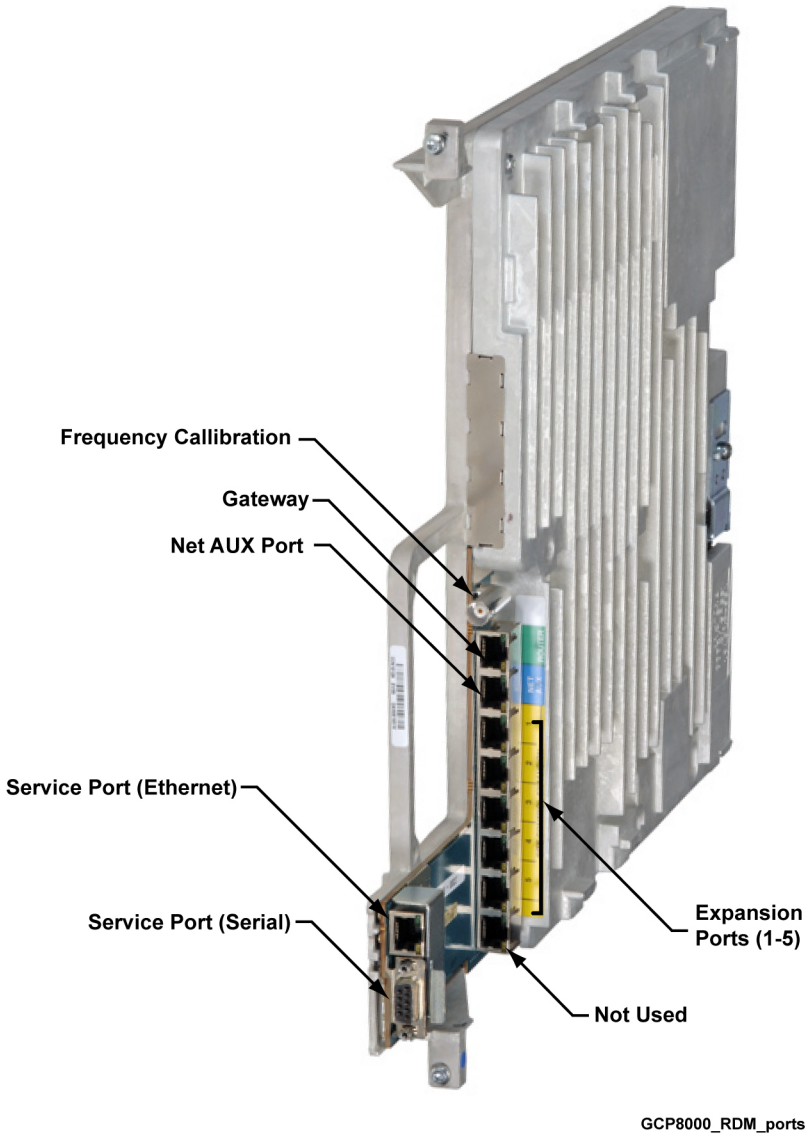


Figure 23: GCP 8000 Site Controller Ports for a GTR 8000 Expandable Site Subsystem



NOTICE: For the detailed junction panel connections for a GTR 8000 Expandable Site Subsystem or GTR 8000 Site Subsystem, see the Installation chapter in the *GTR 8000 Expandable Site Subsystem* and *HPD – GTR 8000 Site Subsystem* manuals.

Table 12: Description of Ports on the GCP 8000 Site Controller (Front View)

Port / Type	Device it connects to:	Port / Type	Description
Service Port, DB-9	Service PC	RS-232 port	Service port for initial configuration of the site controller IP address.
Service Port, RJ-45	Service PC	LAN port	Connects to service PC for local access using Configuration/

Table continued…

Port / Type	Device it connects to:	Port / Type	Description
			Service Software. Also may be used for localized software downloads.
Gateway port, RJ-45	Site router or site gateway	RJ-45	Connection to the site router or site gateway.
	External LAN Switch	RJ-45	Connection to a LAN switch at K core.
Net AUX, RJ-45 for Site Controller in a GTR 8000 Expandable Site Subsystem	External LAN Switch	LAN 1, RJ-45	LAN connection to the SDM RTU for local fault monitoring. Or, external switch connection. **ASTRO® 25 Repeater Site:** Connection between site controllers and external LAN switches with **More** than six QUANTAR® stations.
NET AUX, RJ-45 for Standalone Site Controller	External LAN Switch	LAN 1, RJ-45	LAN connection to the SDM RTU for local fault monitoring. Or, external switch connection. **ASTRO® 25 Repeater Site:** Connection between standalone site controllers and external LAN switches with **More** than six standalone GTR 8000 Base Radios and/or QUANTAR® stations.
Expansion Ports (1-5), RJ-45 for Site Controller in a GTR 8000 Expandable Site Subsystem	QUANTAR® station* and/or Junction panel	QUANTAR = Port 61, RJ-45 Junction panel = Cab #1-5 A and Cab#1-5 B ports, RJ-45	**ASTRO® 25 Repeater Site:** Connection between site controllers and six or **Less** QUANTAR® stations. The Expansion ports are also used in a combination of connecting to QUANTAR® stations and connecting to the junction panel Cab #1-5 A and B ports for a connection to one expansion cabinet.  **CAUTION:** Expansion to Net AUX conversion cables (part # CLN8731A) are required to prevent CP3 timing signaling and LAN corruption when the Expansion ports are connected to QUANTAR® stations.
Expansion Ports (1-5), RJ-45 for	Junction panel	Expansion Input A and B ports, RJ-45	**ASTRO 25 Repeater Site:** Connection between standalone site controllers and GTR

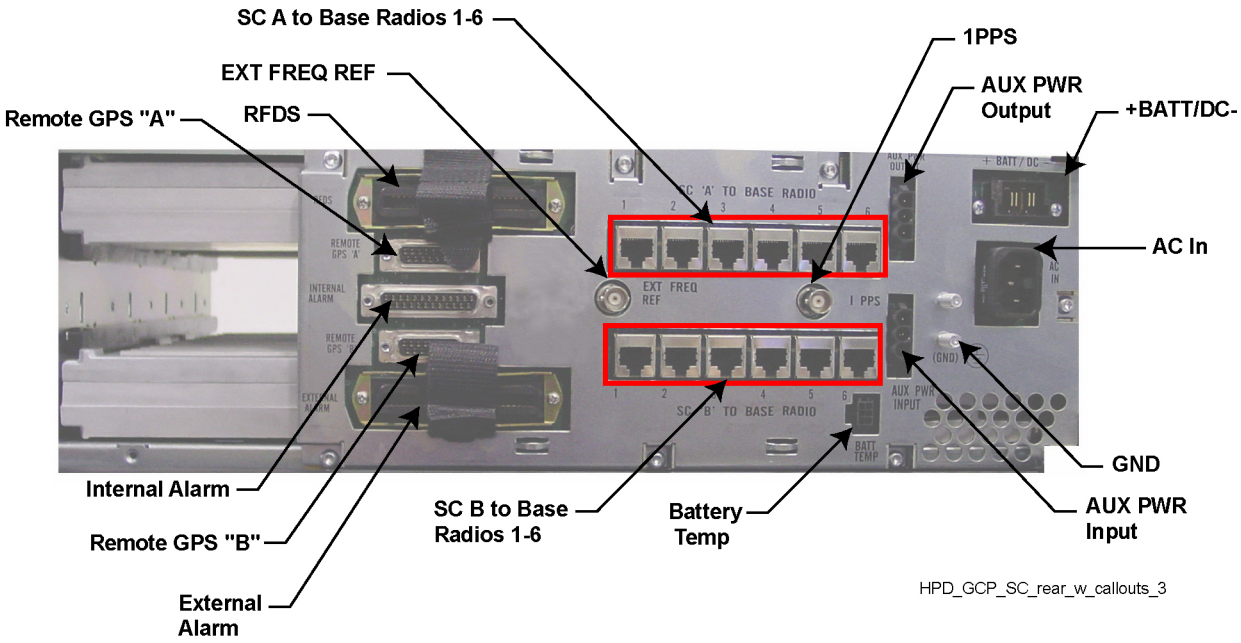
Table continued…

Port / Type	Device it connects to:	Port / Type	Description
Standalone Site Controller			8000 Expandable Site Subsystem junction panel.
Frequency Calibration	Service monitor	BNC	Port available on the site controller module for measuring and calibrating the frequency reference.
Fan Connector, 4-port	Fan assembly		Plug-in connection when the fan assembly is mounted.

* Each QUANTAR® station connects to one site controller. Distribute the QUANTAR® stations evenly among site controllers 1 and 2.

3.4.10
GCP 8000 Site Controller Ports for Standalone and GTR 8000 Site Subsystem Configurations (Rear View)

Figure 24: GCP 8000 Site Controller Ports for Standalone and GTR 8000 Site Subsystem Configurations (Rear View)



NOTICE: For the junction panel connections for a GCP 8000 Site Controller within a GTR 8000 Site Subsystem, see the Installation chapter in the *HPD – GTR 8000 Site Subsystem* manual.

Table 13: Description of Ports on the GCP 8000 Site Controller (Rear View)

Port / Type	Device it connects to:	Port / Type	Description
RFDS	PMU and receiver multicoupler		Monitors RFDS alarms from the power monitor and receiver

Table continued…

Port / Type	Device it connects to:	Port / Type	Description
			multi-coupler in an HPD system.
Remote GPS A	GPS antenna		Connection between the RGPS A and the site controller in an HPD system.
Internal Alarm			Not in use
Remote GPS B	GPS antenna		Connection between the RGPS B and the site controller in an HPD system.
External Alarm			Not in use
SC ‘A’ to Base Radio 1-6, RJ-45	GTR 8000 Base Radios or QUANTAR® stations*	GTR = SC-A port, RJ-45 QUANTAR = Port 61, RJ-45	**ASTRO 25 Repeater Site:** Connection between site controller A and up to six standalone GTR 8000 Base Radios and/or QUANTAR® stations. **HPD System:** Connection between the site controller A and GTR 8000 Base Radios at the site. For a GTR 8000 Site Subsystem, use only port 1.
SC ‘B’ to Base Radio 1-6, RJ-45	GTR 8000 Base Radios or QUANTAR® stations*	GTR = SC-A port, RJ-45 QUANTAR = Port 61, RJ-45	**ASTRO 25 Repeater Site:** Connection between site controller B and up to six standalone GTR 8000 Base Radios and/or QUANTAR® stations. **HPD System:** Connection between the site controller B and GTR 8000 Base Radios at the site. For a GTR 8000 Site Subsystem, use only port 1.
EXT FREQ REF			Not in use
1PPS, BNC	TRAK 9100 or 8835 SSR	Reference output, BNC Female	Connection between the site controllers and TRAK 9100 SSR for time reference in an IP simulcast subsystem and TRAK 9100 or 8835 in an ASTRO® 25 repeater site. The 1PPS input must have a BNC “T” connected to it. A 50 Ohm termination is on one leg of the “T” and the cable to the site controller is on the other side of “T”.
Battery Temp, 6-pin	Battery temperature sensor		Connection to temperature sensor, allowing for temperature compensated battery charging.

Table continued…

Port / Type	Device it connects to:	Port / Type	Description
AUX PWR OUPUT	GCP 8000 Site Controller	AUX PWR INPUT	For power supply redundancy.
AUX PWR INPUT	GTR 8000 Base Radio or GCP 8000 Site Controller	AUX PWR OUTPUT	The auxiliary input is connected with a GTR 8000 Base Radio as a secondary power source in an HPD system and ASTRO® 25 repeater site.
+ Batt/DC	DC power supply or battery		Input from and output to a 48 VDC power supply or backup battery. When AC power is not available, the device switches to operate from a DC source if the optional DC power (8 AWG; length 9 ft), CA01400AA is ordered and installed. One end connects into the Batt/DC port and the other end connects into the DC source. The contacts are 39-83503N02 (AMP #53880-2), the receptacle housings are 15-83502N01 (AMP #53884-1) and the mounting ears are 07-83504N01 (AMP #53887-1). 3084869Y06 cable is used for a positive ground system. 3084869Y02 cable is used for a negative ground system.
AC	120/240 VAC Power source		Input from 90/264 VAC nominal power source.
GND			Two grounding lugs and cable.

For ASTRO® 25 repeater sites with a mix of standalone GTR 8000 Base Radios and QUANTAR® stations, each GTR 8000 Base Radio connects to both site controllers. Each QUANTAR® station connects to one site controller. Distribute each QUANTAR® station evenly among site controllers 1 and 2.

3.4.11
GNSS Unit Installation

GCP 8000 Site Controllers (SCs) for High Performance Data (HPD) use Global Navigation Satellite System (GNSS) units that lock onto a satellite system. The site controllers use the signals from the GNSS unit to generate the time and frequency reference for the remote site. Alignment of timing is handled by each remote site independently locking to the satellite system.

IMPORTANT:

- Improper installation of the GNSS unit (mainly reflection issues) can lead to improper position information, and is reported by the GNSS unit.
- During initial startup, if the GNSS unit is not locked onto at least four satellites, the system may not operate properly. These satellites are used to establish a three-dimensional fix (latitude, longitude, and altitude) for the site. Once the three-dimensional fix has been determined, only one satellite is required to maintain proper operation.
- Wait until the GNSS units have locked onto the satellites before verifying proper operation.

The active site controller acts as the Network Time Protocol (NTP) server for the site, providing the time to the GTR 8000 Base Radios and other devices at the site. The GNSS unit connected to the site controller is the primary NTP source. The time and frequency reference is supplied to GTR 8000 Base Radios at the site through the Ethernet cable. The site controller keeps the time accurate to within +/- 1 microsecond per day across the valid temperature range of the site controller.

The active site controller broadcasts time updates periodically. The standby site controller uses the NTP source time to verify correct time setting. If the internal time variance in a device is equal to, or greater than 500 milliseconds from the NTP source time, the device corrects the NTP Time of Day clock to match the received NTP time.

The frequency reference and time reference are distributed on the LAN cables for the site controller to the base radio. The GNSS units provide the necessary references to the site controller. The time reference is used to synchronize the data transmissions from the radios, and the high stability frequency reference is used to provide a reference for both the transmit and receive frequency synthesizers in the radios.

The site controller includes a high-stability ovenized crystal oscillator, which is trained by the input from a GNSS antenna. One GNSS antenna must be connected to each site controller. The Configuration/ Service Software (CSS) indicates whether the GNSS capability is configured. The site controller indicates the alarms for GNSS service to Unified Event Manager.

3.4.11.1
GNSS Equipment

The Global Navigation Satellite System (GNSS) equipment is ordered in a quantity of one per site controller. Redundant site controllers are required, therefore each item must be ordered in a quantity of two.

The following lists the equipment to install the GNSS units:

- GNSS Antenna/Receiver: PMUG1017A
- Wall Mounting Brackets: DSWM4
- Mounting Pole: DSP04268
- GNSS Primary Surge Protector: DSIX2L1M1DC48IG
- GNSS Antenna/Receiver to Site Controller Cable (125 ft): DS30C87465CO1
- GNSS Antenna/Receiver to Site Controller Cable (350 ft): DS30C87465CO2

3.4.11.1.1
GNSS Unit

The Global Navigation Satellite System (GNSS) unit includes the antenna and the receiver/modem. Because the actual receiver is integrated with the antenna, the connection between the GNSS unit and the GCP 8000 Site Controller is digital using a 6-pair twisted pair cable.

3.4.11.1.2

Surge Suppression

This primary surge suppression is used at the point where the cable enters the site building. There should be one surge suppression for each GCP 8000 Site Controller. The surge suppression is installed by cutting the cable at the point where the cable enters the site building and connecting both ends to the surge suppressor.

3.4.11.1.3

GNSS Cables

Choose the cable length required for the site configuration. One cable is required for each GCP 8000 Site Controller. These cables have a Deutsch connector at one end that connects to the Global Navigation Satellite System (GNSS) unit and a DB15 connector that connects to the site controller.

In a typical installation using 6-pair twisted pair cable, the recommended cable length should be 106.7 m (350 ft) or less. This cable length is sufficient for most installations. For cable lengths greater than 106.7 m (350 ft), contact Motorola Solutions Support Center (SSC) for guidance on the installation and configuration.

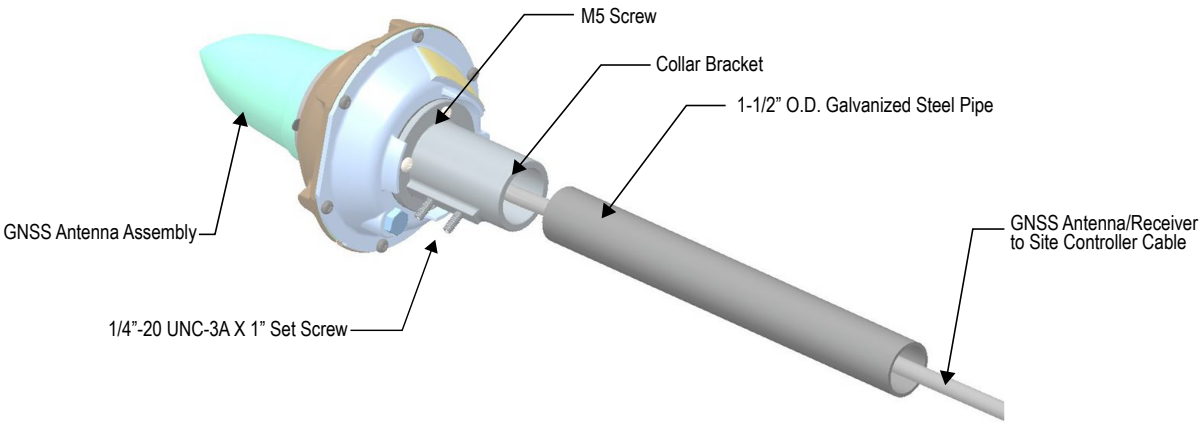
3.4.11.2

Assembling the GNSS Antenna

Perform this procedure to assemble a Global Navigation Satellite System (GNSS) antenna.

The following figure presents the exploded view of the GNSS antenna.

Figure 25: GNSS Antenna Assembly – Exploded View



The following part numbers are valid for the relevant elements:

GNSS Antenna Assembly
PMUG1017A

Mounting Pole (steel pipe)
DSP04268

GNSS Antenna/Receiver to RDM/SC Cable

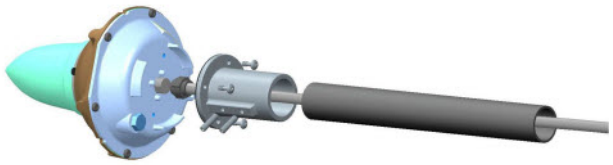
- DS30C87465C01 (125 ft)
- DS30C87465C02 (350 ft)

Prerequisites: Verify that you have the Allen wrench (included in the set), a T30 screwdriver, and a Phillips screwdriver.

Procedure:

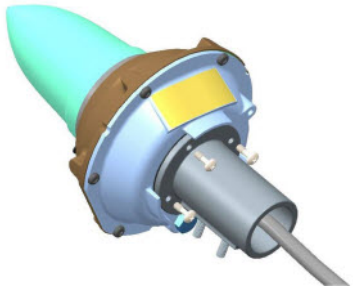
1 Run the digital cable through the steel pipe and collar bracket. Attach the digital cable connector to bottom of the antenna module (male to female Deutsch connector).

Figure 26: GNSS Antenna Assembly – Cable



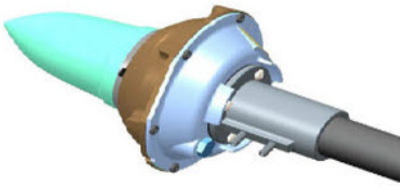
2 Align four bracket screw holes with the GNSS antenna bottom mounting holes and screw the collar bracket to the bottom of the antenna module using a Phillips screwdriver.

Figure 27: GNSS Antenna Assembly – Collar Bracket



3 Fix the mounting pipe to the mounting bracket by tightening the two set screws.

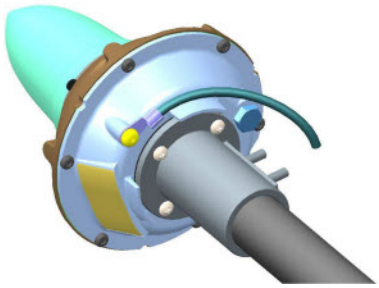
Figure 28: GNSS Antenna Assembly – Securing the Pipe



4 Attach the mounting pipe to the support structure.

5 Attach the grounding cable to the antenna module by tightening a T6 screw using a T30 screwdriver.

Figure 29: GNSS Antenna Assembly – Grounding Cable



3.4.11.3
Installing the GNSS Units

Follow this process to install the Global Navigation Satellite System (GNSS) units.

Procedure:

1. Mount the GNSS units with an unrestricted aerial down view to within ten degrees of the horizon in all directions.
2. Mount the GNSS units high enough so they have an un-obstructed view of the sky. Adjacent structures (such as trees, buildings, and antenna towers) are considered obstructions. If an un-obstructed view is not possible, install the GNSS units so they have a clear view of the appropriate sky region. Adjacent antenna towers at the RF site which protrude into the required region have a minimal effect on GNSS unit reception due to their narrow, largely open profiles and are not considered obstructions.
   - For northern hemisphere installations, ensure that an un-obstructed view of the southern sky is maintained.
   - For southern hemisphere installations, ensure that an un-obstructed view of the northern sky is maintained.
3. Isolate the GNSS units from RF interference by mounting the units at a distance of at least 3.66 m (12 ft) horizontally from the other units.
4. Validate the correctness of the position information (latitude, longitude, elevation) reported by the GNSS unit. Proper timing operation is dependent on proper position identification.
5. Validate that both GCP 8000 Site Controllers in the CSS Reference Service Screen are within 250 nsec of each other. If not, verify the position information (latitude, longitude, elevation) reported by the GNSS units on both site controllers.
6. Configure the Time Reference for both site controllers in Configuration/Service Software (CSS). For details, see **Site Controller Configuration & Service Help → High Performance Data (HPD) Site Controller → Service Screens → Reference Service Screen** in the *CSS Online Help*.

3.4.11.4
Alarm Indication (No Lock on GNSS Signal)

A system alarm indicates when the GNSS signal cannot be located and that the GNSS unit must be repositioned.

3.4.11.5
GNSS Lightning Arrestor

A lightning arrestor must be installed between the GCP 8000 Site Controller and the Global Navigation Satellite System (GNSS) antenna. One GNSS antenna is connected to each of the site controllers. Each antenna requires its own arrestor.

Figure 30: Lightning Arrestor System Connections on page 79 illustrates the connections between the lightning arrestor and the GCP 8000 Site Controller.

Figure 30: Lightning Arrestor System Connections

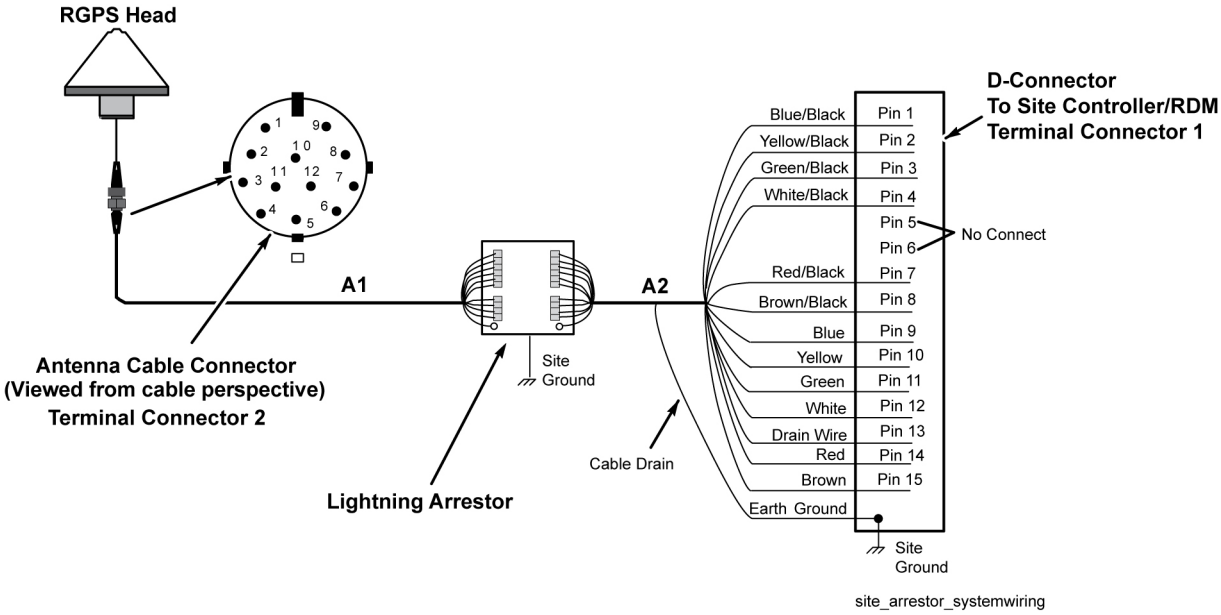


Figure 31: Lightning Arrestor DS109–0129H-A Model Wiring on page 80 shows one possible configuration of the connections and terminal assignments for installing the DS109–0129H-A model lightning arrestor.

Figure 31: Lightning Arrestor DS109–0129H-A Model Wiring

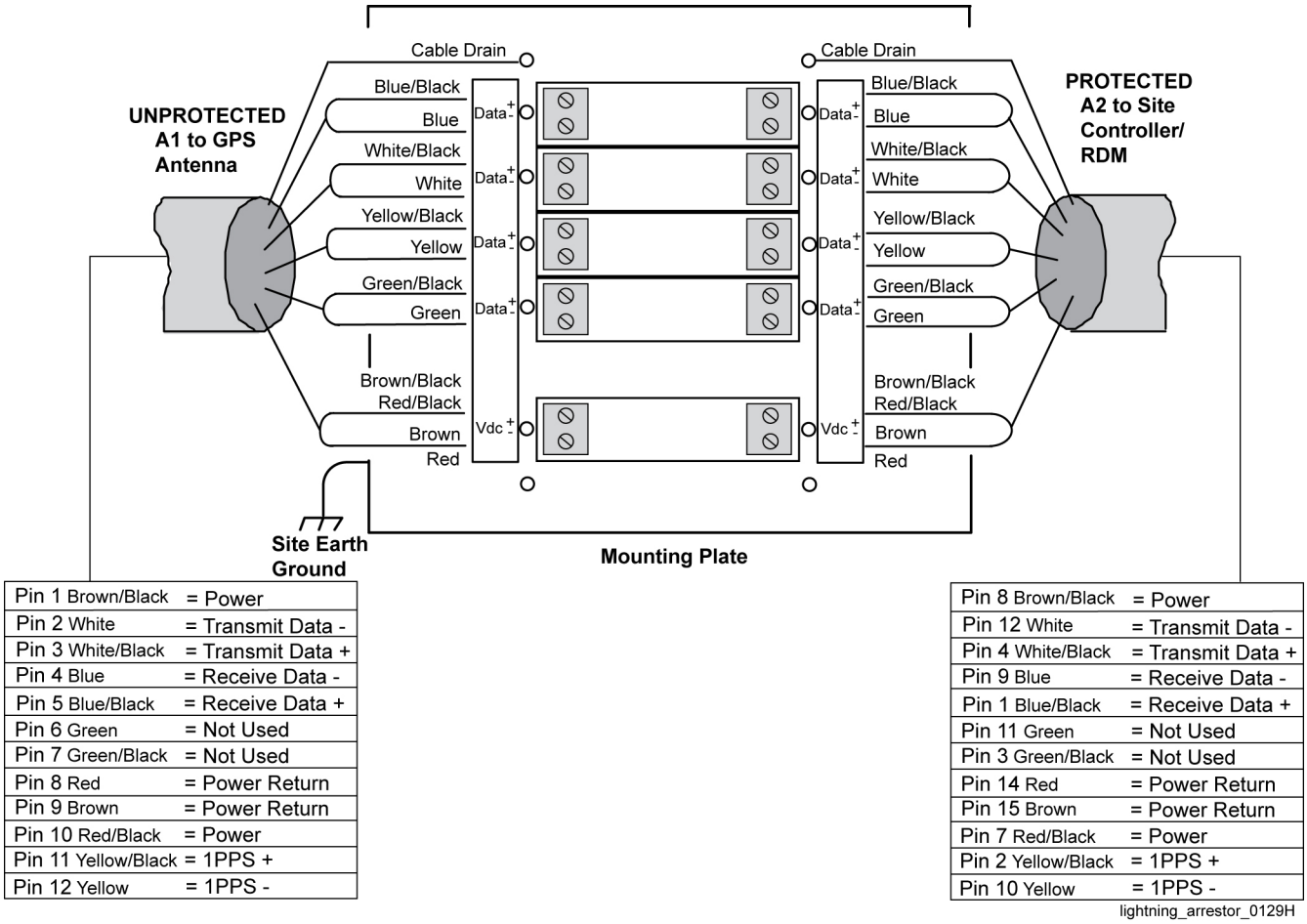
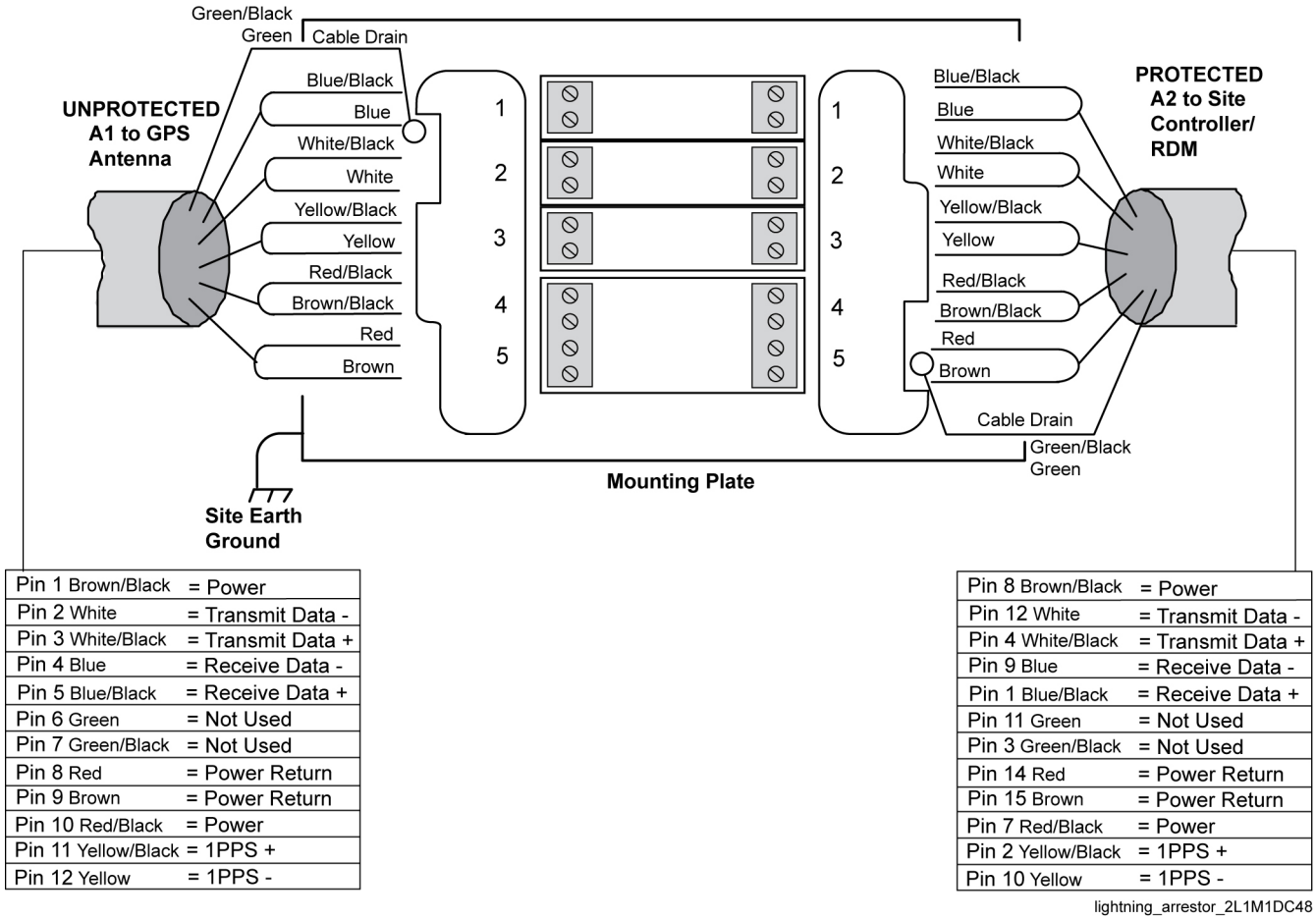


Figure 32: Lightning Arrestor DS-IX-2L1M1DC48–IG Model Wiring on page 81 shows one possible configuration of the connections and terminal assignments for installing the DS-IX-2L1M1DC48–IG model lightning arrestor.

Figure 32: Lightning Arrestor DS-IX-2L1M1DC48–IG Model Wiring



Pin 1 Brown/Black	= Power
Pin 2 White	= Transmit Data -
Pin 3 White/Black	= Transmit Data +
Pin 4 Blue	= Receive Data -
Pin 5 Blue/Black	= Receive Data +
Pin 6 Green	= Not Used
Pin 7 Green/Black	= Not Used
Pin 8 Red	= Power Return
Pin 9 Brown	= Power Return
Pin 10 Red/Black	= Power
Pin 11 Yellow/Black	= 1PPS +
Pin 12 Yellow	= 1PPS -

Pin 8 Brown/Black	= Power
Pin 12 White	= Transmit Data -
Pin 4 White/Black	= Transmit Data +
Pin 9 Blue	= Receive Data -
Pin 1 Blue/Black	= Receive Data +
Pin 11 Green	= Not Used
Pin 3 Green/Black	= Not Used
Pin 14 Red	= Power Return
Pin 15 Brown	= Power Return
Pin 7 Red/Black	= Power
Pin 2 Yellow/Black	= 1PPS +
Pin 10 Yellow	= 1PPS -

lightning_arrestor_2L1M1DC48

3.5 Installing Device Software Prerequisites

When and where to use: The following tasks are required before you can complete the device software installation and begin the configuration procedures in the “Configuration” chapter.

Process:

1. Transfer and install new software to a device using the Software Download Manager. See Software Download Manager on page 82.
2. Obtain the ASTRO® 25 media. Specifically, you need the Motorola Solutions Device OS Image media. See Loading Device OS Images to the UNC on page 86.
3. Obtain user names, passwords, and procedures required to access the devices on the network. For specific user names and passwords to access devices on the network, contact your system administrator.
4. Set up the users in the IT Admin group in Active Directory Users and Computers. See the *Authentication Services* manual.
5. Obtain the following values from the system administrator:
   - Line interface number
   - Zone Controller (ZC) site link path 1 IP address
   - ZC site link path 2 IP address

- Host name to access the Unified Network Configurator (UNC) server application using Secure SHell (SSH) (***<username>*** @IP address format)
- Site ID number
- IP address 1 and 2
- Primary and secondary NTP IP addresses

  NOTICE: The following are applicable to systems with Authentication, Authorization, and Accounting (AAA) Servers, Domain Controllers, or Syslog Servers.
- Primary, secondary, and tertiary Domain Name Services (DNS) IP addresses
- Requested DNS Domain Name
- Requested DNS Host Name
- System Name
- Primary SYSLOG Service Name Fully Qualified Domain Name (FQDN)
- Backup SYSLOG Service Name Fully Qualified Domain Name (FQDN)
- Remote Authentication Dial-In User Service (RADIUS) FQDN parameter value
- RADIUS Row Status parameter value
- RADIUS Service Time Out (seconds) parameter value
- RADIUS Service Retransmits Attempts parameter value
- RADIUS Service Dead Timer (min) parameter value
- RADIUS Specific Key parameter value
- RADIUS Service Global Key parameter value

6 Obtain the default credentials (local accounts, central authentication, and SNMPv3) for the device being installed, as well as the updated passwords for those types of accounts (so that you can change the password after you install the device). Contact your system administrator, if you do not have this information. See the *SNMPv3* manual or see Local Password and SNMPv3 Passphrase Troubleshooting on page 127 for more information.

7 Configure the device as a RADIUS client on the RADIUS server. When these devices are configured with a RADIUS key that matches a shared secret for that device in Microsoft Windows Internet Authentication Service (IAS), they become RADIUS clients. They do not join the Active Directory domain. See the *Authentication Services* manual for more information.

8 **NOTICE:** This step is applicable to systems with AAA Servers, Domain Controllers, or Syslog Servers.

To use the VoyenceControl component of the Motorola Solutions centralized configuration application for any of the site device procedures, set up the UNC. Depending on your organizational policies, you may also need to implement a secure protocol between the UNC and the site device. Before performing any procedures using VoyenceControl, the device must be discovered in VoyenceControl, and the device configurations must be recently pulled to the UNC database. See the following ASTRO® 25 system documentation: *Unified Network Configurator* manual and *Securing Protocols with SSH* manual.

3.6 Software Download Manager

The Software Download Manager (SWDL) is an application that can transfer only, install only, or transfer and install new software to devices. The new software can be installed either locally at a site or

on the Network Management subsystem. Individual devices not connected to the system can be downloaded using single device mode.

NOTICE: Throughout this manual, the name SWDL is used to refer to the Software Download Manager application.

Software Download Security Transfer Modes

A software download can be performed using the following security transfer modes:

Clear SWDL
Transfers the software without security, based on the File-Transfer Protocol (FTP)

Secure SWDL
Transfers the software as encrypted, based on the Secure File-Transfer Protocol (SFTP)

NOTICE: All secure sequential and simultaneous transfers use the Diffie-Hellman group exchange. The Diffie-Hellman group exchange is used for devices supporting Diffie-Hellman group exchange. The Diffie-Hellman group exchange enhances the security of Secure Shell (SSH) protocol initial key exchange. See the *Software Download Manager* manual for details.

Before initiating transfer, SWDL connects to the site in the zone to discover all devices. The transfer mode of all devices is displayed in the SWDL window. It is important that all devices have the same SWDL transfer mode. Otherwise, SWDL flags a mismatch of the SWDL transfer modes across site devices.

SWDL provisions the credentials for Secure SWDL as part of initiating the SWDL operation. No user intervention is required. For a single device, Secure or Clear SWDL is configured based on the SWDL Transfer Mode configuration within the Configuration/Service Software (CSS). The Unified Network Configurator (UNC) can be used to schedule and configure all devices in the system at once.

For information on how to configure the secure or clear SWDL transfer mode, see the *Unified Network Configurator* manual and “Configuring Devices for Security” in the *CSS Online Help*.

Software Download Transfer Methods

A software download can be accomplished in two ways:

Site Software Download
Allows you to transfer and install application software from any location within a network. The Software Download Manager resides on the Network Management Client computer and a service computer/laptop loaded with the CSS application. From either of the computers, you can select device types to download software. Site Software Download allows you to select the zone, site, device types, and software download operation to perform. When performing a site software download, the site controller coordinates the software transfer for all trunked base radios, receivers, comparators, and reference distribution modules installed at the site. A site software download can only be performed on a trunked ASTRO® 25 system.

NOTICE: Trunked GPW 8000 Receivers in a circuit simulcast configuration are not supported using a site software download.

Single Device Software Download
Allows you to transfer and install software to a single instance of a device (such as one base radio). This feature gives the technician the ability to install different versions of software. Single device software download is done from a service computer/laptop loaded with the CSS application either connected directly to the device or connected to the network.

NOTICE: Conventional devices and 3600 base radios are supported only in single device software download.

Site Software Download Functionality

When SWDL is connected from a central remote location, SWDL performs a site software download to the site controllers, then to the comparators and base radios or receivers installed at the site. Both active and standby site controller modules have two flash memory banks for storing software. The device application is run from RAM, and is loaded from the active flash memory bank after a reset. One bank is active while the other bank is inactive. The transfer of the software using SWDL is a background process, without interruption of services at the site, that loads the software into the inactive bank. The site controller executes the software from one bank, while software is simultaneously downloaded to the inactive bank. The transfer and install are done in the background. An install causes the site controller to reset and load the RAM from the bank that was installed with the new software.

NOTICE: For geographically redundant prime sites, a site software download should not be attempted while the third Site Controller (SC3) is in the active state.

SWDL communicates with the site controllers to determine the number of existing remote sites and the number of channels. SWDL considers a channel or remote site to be accessible if its status is “Not Unconfigured.” This term means that the site must be set up with a service computer/laptop with CSS or a network management client before software download is performed on the site.

The system downloads software to the site controllers, comparators, base radios, or receivers as a unit. Use SWDL to transfer software to each device type, then perform an install operation. During the transfer, the operation designates a proxy for each device type at each LAN. Site controllers proxy for comparators, and base radios or receivers proxy for each other. The proxy cross-transfers the software to other devices on the LAN. Using proxies minimizes system downtime. Transfers to the LAN are done simultaneously except for the site controller and comparators.

Software installation is done on a channel-by-channel basis, starting with the highest number channel. When a channel software download occurs, the base radio or receiver which incorporates that channel is processed along with the comparator for that channel. For example, if channel 3 was being downloaded, comparator 3 and the base radios or receivers for channel 3 at each of the remote sites would be installed simultaneously.

SWDL operation can be fault managed through Unified Event Manager (UEM), syslog, local SWDL log files, user messages, and device reports.

For further information on SWDL, see the *Software Download Manager* manual.

The operating software can also be loaded using the UNC. See the *Unified Network Configurator* manual to perform single device software downloads (ruthless download) to the devices.

See the *G-Series Equipment System Release User Guide* for SWDL instructions specific to the operating characteristics of your existing system release.

3.7
Installing Devices in the UNC

When and where to use: The Unified Network Configurator (UNC) is the Network Manager used to discover a device and load Operating System images. This process lists the basic steps involved using the UNC on a device.

NOTICE: The UNC is not applicable for K core or non-networked sites.

Process:

1. Discover the device in the UNC. See Discovering a Device in the UNC on page 85.
2. Log in to the UNC server application using PuTTY. See the *Securing Protocols with SSH* manual.

3 Load the operating system images to the UNC. See Loading Device OS Images to the UNC on page 86.

4 Enable FTP services on the UNC. See Enabling FTP Service on page 87.

5 Transfer and install the OS image to the device. See Transferring and Installing the OS Image on page 87.

6 Inspect the device properties for the transferred and installed software. See Inspecting Device Properties for Transferred and Installed Software on page 90.

7 Disable FTP services for the UNC. See Disabling FTP Service on page 91.

3.7.1
Discovering a Device in the UNC

When and where to use:
The discovery process allows the Unified Network Configurator (UNC) to manage the site devices. Once the device is installed, configured through the Configuration/Service Software (CSS), and security parameters are enabled, follow this procedure to discover the device. The configuration information can then be updated using this configuration management application.

The UNC network management solution consists of two applications. Both the UNC Wizard and the VoyenceControl applications are used in this procedure.

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

Once the device is discovered in the UNC, the OS images and CSS configuration files can be loaded to add a device to a site, which then connects the site to the current ASTRO® 25 zone core.

Procedure:

1 Ensure that Domain Name Services (DNS) is functional on your system. DNS is supplied by a specific server application, which must be operational before you can discover the device.

2 Log on to the UNC Wizard from the Network Management (NM) client, by double-clicking the **Internet Explorer** icon on the desktop.

The Internet Explorer browser opens.

3 In the **Address** field, enter: `http://ucs-unc0<Y>.ucs:9443/UNCW`

where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

The UNC Wizard launches and a login dialog box appears.

4 Type the administrative user name and password. Click **OK**.

The UNC Wizard appears.

5 From the list of available wizards on the left side, select **Subnet Discovery**.

The right side of the window is updated with the **Subnet Discovery** form.

6 Select **RF Site** by clicking the **Discovery Type** drop-down list.

7 Enter the **Zone ID** and the **Site ID**. Click **Submit**.

An auto-discovery job is created in the UNC Schedule Manager.

8 Log on to the UNC from the NM client by entering:

`http://ucs-unc0<Y>.ucs`

where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

The UNC client launches and a login dialog box appears.

9 Type the administrative user name and password. Click **OK**.

VoyenceControl launches.

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

10 Press F7 (Schedule Manager).

The **Schedule Manager** window appears in the UNC with the discovery jobs.

11 Verify that the **Zone** and **Site** containers include any devices discovered.

IMPORTANT: No site devices should be in the **Lost and Found** folder. If any devices are in the folder, see the *Unified Network Configurator* manual for troubleshooting guidance.

12 In the UNC Wizard, verify the devices by selecting **Channel** under **RF Site Level Configuration**. If multiple zones exist, choose **Zone**.

The device sites are listed, which means they are available for channel configuration.

3.7.2
Loading Device OS Images to the UNC

Prerequisites: This procedure requires the Motorola Solutions device Operating System (OS) Image media. Locate the Transport OS Image media packaged with the Network Management media.

When and where to use: This procedure loads the OS images for the devices for distribution through the Unified Network Configurator (UNC). Once OS images are distributed to the UNC, you can update the device Configuration/Service Software (CSS) configuration files to the UNC.

Procedure:

1 Launch a Secure SHell (SSH) terminal server session in PuTTY to access the UNC **Server Administration** menu. See the *Securing Protocols with SSH* manual.

2 From the UNC **Server Administration** menu, select **OS Images Administration**. Press ENTER.

3 From the OS **Images Administration** menu, select **Load new OS images**. Press ENTER.

A message appears indicating there are two methods for loading OS Images.

4 Insert the **Motorola Solutions Device OS Images** media into the CD/DVD-ROM drive of the server.

The drive light starts blinking on the server.

5 When the drive light stops blinking, press ENTER.

The OS images load on the UNC.

6 From the menu, select **View OS Images**. Press ENTER.

The device software image appears.

7 From the menu, select **Eject CD**. Press ENTER.

The media ejects from the drive on the server.

8 Remove the **Motorola Solutions Device OS Images** media from the CD/DVD-ROM drive of the server.

9 To log out of the server, press ENTER.

The **User Configuration Server Administration** menu appears.

10 Press ENTER again.

The prompt appears.

3.7.3
Loading Software to a Device

NOTICE: These procedures are for a single device download. For a site download, see Software Download Manager on page 82.

The following procedures describe how to load software images onto Unified Network Configurator (UNC) and download and install this software to the device. Secure protocols for software download is the preferred approach to transfer operations. However, as a backup option, FTP service can be enabled before installing the software.

3.7.3.1
Enabling FTP Service

When and where to use: Follow this procedure to enable FTP service before installing the OS software.

Procedure:

1 Launch a Secure Shell (SSH) terminal server session in PuTTY to access the Unified Network Configurator (UNC) **Server Administration** menu. See the *Securing Protocols with SSH* manual.

2 From the Server Administration menu, select **Unix Administration**. Press ENTER.

3 From the Unix Administration menu, select **FTP Services**. Press ENTER.

4 From the FTP Services menu, select **Enable FTP service**. Press ENTER.

The FTP Services are enabled and available for software transfer and install operations.

3.7.3.2
Transferring and Installing the OS Image

When and where to use: Use this procedure to download the OS from the Unified Network Configurator (UNC) to the device.

Procedure:

1 On the Private Network Management (PNM) client where you set up VoyenceControl, double-click the UNC shortcut on the desktop.

You can also paste the following address into an IE web browser: `http://ucs-unc0<Y>.ucs`, where <Y> is the number of the UNC server (01 for primary core UNC server, and 02 for backup core UNC server).

Internet Explorer opens to the URL of the application server, and a VoyenceControl client session launches with the welcome page.

Figure 33: VoyenceControl Welcome Page

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

2 Click the **launch VoyenceControl™** link.

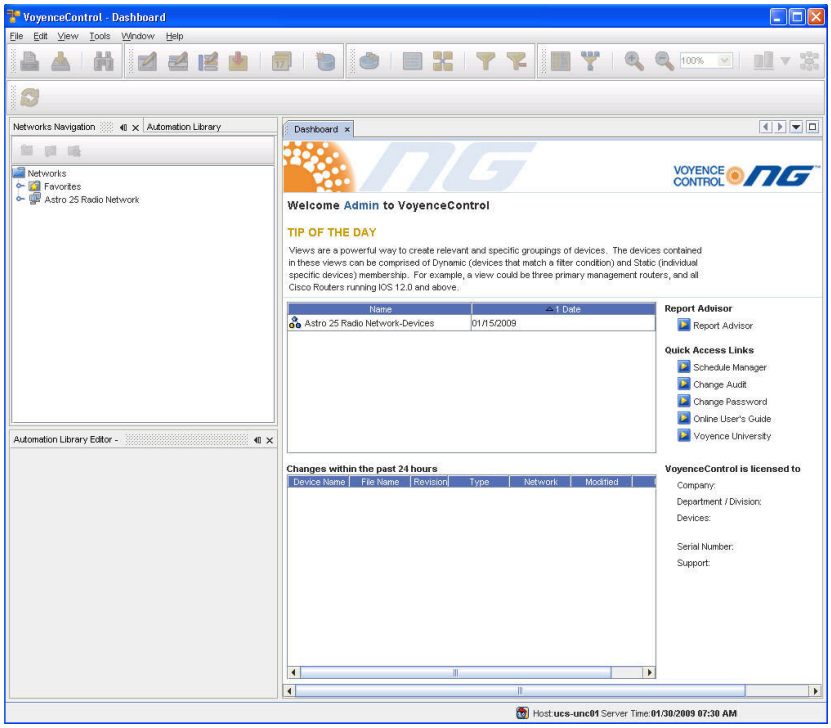
A VoyenceControl client session launches with the login window.

Figure 34: VoyenceControl Login Window

3 Enter the User ID and Password. Click **OK**.

The **VoyenceControl Dashboard** appears.

Figure 35: VoyenceControl Dashboard



4 In the left navigation pane, expand **Networks**, then select **ASTRO 25 Radio Network**, then **Views**.

The list of options expands.

5 From the navigation pane, double-click **Motorola <device>**.

The view opens and all currently discovered devices appear.

6 From the menu, select **Tools** → **OS Inventory**.

A list of the OS images appears.

7 Verify OS images loaded on the UNC server appear in the OS inventory.

NOTICE: These images were automatically created during the Loading Device OS Images to the UNC on page 86 procedure.

8 Under **Networks** in the navigation pane, select one or more devices from the same device class by right-clicking the selections.

9 From the menu, select **Update OS Image**.

10 From the **Select OS Image** window, select **Software Image**. Click **Next**.

11 From the **Update OS Image** window, select each device that appears in the **Selected Devices** section.

This action associates a version to a device instance.

NOTICE: In most cases, the “summary of device partitions” is already set up and the values in step 11 through step 14 must be verified.

12 Select **nvm partition** from the **Manage Partition for Device** section.

NOTICE: Selecting **nvm partition** defines where the OS image is transferred and is the only choice for the device.

13 From the **Selected Image** section, select the image for this device.

NOTICE: Ignore the **Install** and **Copy** check boxes.

The **Image Info** tab is populated and informs the application which image to use.

14 Click **Add**.

The **Summary of Device Partitions for Device** populates and confirms the proper setup.

15 Select the **Device Options** section, **Software Operations**, then choose **transfer**, **install**, or **both**.

These selections indicate which operations occur when the job is executed.

NOTICE: If **transfer** is chosen, select the install option later to complete the installation. If **both** is chosen, the software is transferred and installed. There are up to two resets of the device during installation.

16 Click **Schedule**.

17 From the **Schedule Push Job** window, configure the schedule information. Click **Approve and Submit**.

The job is approved and can be viewed in the **Schedule Manager** window.

NOTICE: If only **Submit** is chosen, the job must be approved later.

18 Verify the job status by pressing F7 (Schedule Manager).

The **Schedule Manager** window appears in the UNC with the discovery jobs.

3.7.3.3
Inspecting Device Properties for Transferred and Installed Software

When and where to use: When the software has been transferred and installed, follow this procedure to inspect the device properties before assuming the installation was a success and disabling FTP service

Procedure:

1 From the **Device** view, right-click the device, select **Pull**, and then **Pull Hardware Spec**.

The current software version information is updated in the Unified Network Configurator (UNC).

NOTICE: Skip this step if a Pull All or Pull Hardware Spec has already occurred.

2 From the **Device** view, right-click on the device, and then choose **Properties**.

The **Device Properties** window appears.

NOTICE: Select the **Properties** icon to view the device properties appear directly within the **Device** view.

3 Choose the **Configuration** tab, and then the **Hardware** tab.

4 Double-click the **Chassis** object from the **Physical Hardware** properties.

5 From the **Chassis** property tree, view the following properties and their values:

- **Bnk1:<*device*>**: Transferred software in bank 1.
- **Bnk2:<*device*>**: Transferred software in bank 2.
- **<*device*>**: Installed and Running Software.

NOTICE: The Table format can be used (instead of the Diagram format) to view the Installed and Running Software in the **Device** view.

3.7.3.4 Disabling FTP Service

When and where to use: Follow this procedure to disable the FTP service after the transfer and installation of the software is completed.

Procedure:

1 Launch a Secure SHell (SSH) terminal server session in PuTTY to access the Unified Network Configurator (UNC) **UNC Server Administration** menu. See the *Securing Protocols with SSH* manual.

2 From the **UNC Server Administration** menu, select **Unix Administration**. Press ENTER.

3 From the Unix Administration menu, select **FTP Services**. Press ENTER.

4 From the **FTP Services** menu, select **Disable FTP service**. Press ENTER.

The FTP services are disabled and unavailable for software transfer and install operations.

5 To back out of the menus, press Q three times.

6 At the prompt, enter: `exit` to return to the previous menu.

7 To log out of the application, enter: `exit`.

8 Close the PuTTY connection.

This page intentionally left blank.

Chapter 4

GCP 8000 Site Controller Configuration

This chapter details configuration procedures relating to the GCP 8000 Site Controller.

4.1 Configuration Software

Configuration of a device can be done on two software applications: Configuration/Service Software (CSS) and Unified Network Configurator (UNC).

CSS
is used to configure the parameters on the device. CSS can access devices remotely over the network, or locally through an Ethernet/serial connection to the service port on the device or through a LAN switch. CSS also can be used to view status information, equalize batteries, and check internal logs of the equipment at the site. See the *CSS Online Help* for configuration details.

UNC Wizard
is a component of UNC used to configure the parameters of a site, subsite, and channel. See the *UNC Wizard Online Help* for configuration details.

VoyenceControl
is a component of UNC used to pull and push configurations and configure the parameters of the device. See the *Unified Network Configurator* manual for general information about using VoyenceControl functions.

NOTICE: While it is possible to configure a conventional device using the UNC, it is preferable to use CSS because configuration dependencies are enforced.
The UNC is not applicable for K core or non-networked sites.

All parameters are programmed locally when the site is installed but not linked to a network. Test all parameters before making the site available. The ability to locally program provides the means to test the site before making it available for system operation.

4.2 Discovering a Device in the UNC

When and where to use: Use these high-level steps to discover the devices in the Unified Network Configurator (UNC). See the *Unified Network Configurator* manual for details on discovering devices.

Process:

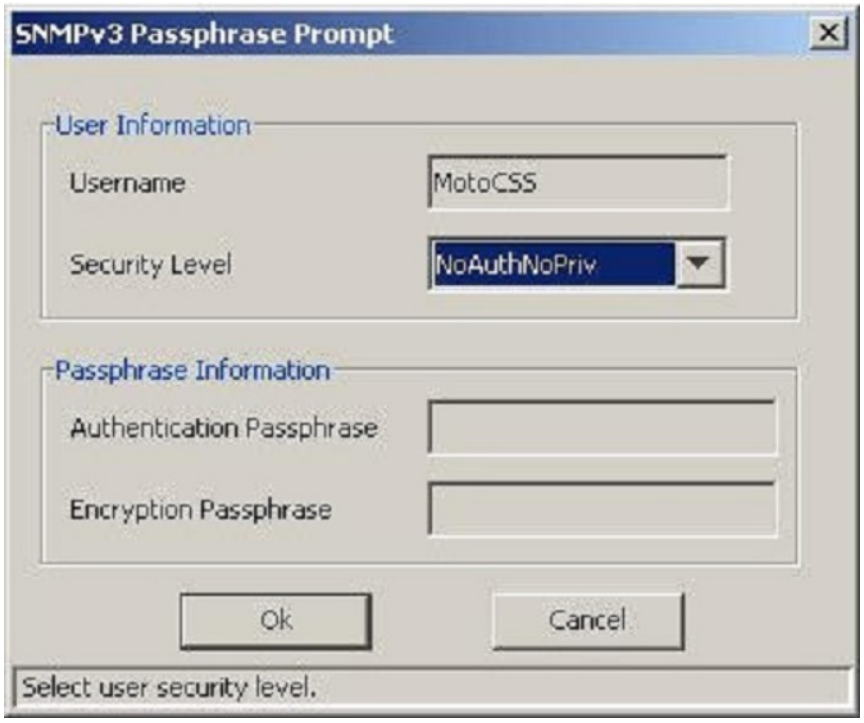
1. Use the UNC Discovery Wizard to:
   - Discover the devices.
   - Upload configurations for the devices.
   - Generate changes for non-compliant devices.
2. Approve jobs (if any).

4.3

Security/Authentication Services

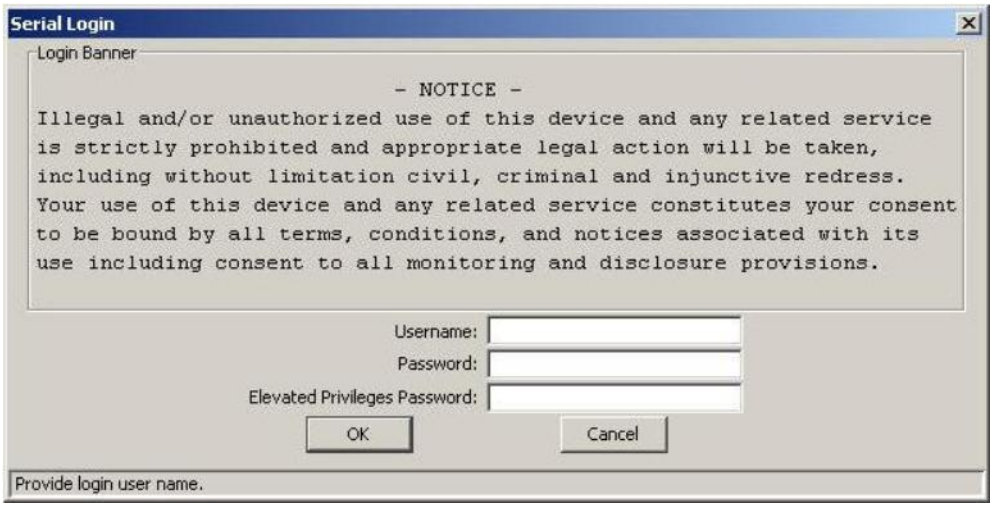
If the device supports SNMPv3 protocol, a pop-up dialog box appears displaying the SNMPv3 Password Prompt when logging in to a device through Configuration/Service Software (CSS) using an Ethernet connection. For configuration details, see the *Information Assurance Features Overview*, *Software Download Manager*, and *SNMPv3* manuals. See Figure 36: SNMPv3 Security Level Option Prompt on page 94.

Figure 36: SNMPv3 Security Level Option Prompt



A pop-up window appears displaying the File Transfer Access Services for CSS. Use this logon when communicating to a device through CSS using either an Ethernet or DB-9 Serial Port connection. See Figure 37: CSS Login Banner on page 94.

Figure 37: CSS Login Banner



4.4
Device Configuration in CSS

This section covers configuration of a device using the Configuration/Service Software (CSS).

NOTICE: The IP address for the device is available through a serial port connection in the **Tools** → **Set IP Address** from the CSS menu.

4.4.1
Initial Configuration of a Device in CSS

When and where to use: Use this process to initially configure the device in CSS.

Process:

1. Perform the following configuration steps that require a serial connection. See Connecting Through a Serial Port Link on page 96.
   - **a** Set the IP address of the device. See Setting the Device IP Address in CSS on page 97.
   - **b** Set the serial security services. See Setting the Serial Security Services in CSS on page 98.
2. Perform the following configuration steps that require an Ethernet connection. See Connecting Through an Ethernet Port Link on page 99.
   - **a** Set the current date and time. See Setting the Date and Time in CSS on page 102.
   - **b** Change the SNMPv3 configuration and user credentials on a selected device in the site. See Changing SNMPv3 Configuration and User Credentials in CSS on page 103.
   - **c** Create, update, or delete an SNMPv3 user. See Adding or Modifying an SNMPv3 User in CSS on page 105.
   - **d** Verify the SNMPv3 credentials. See Performing an SNMPv3 Connection Verification in CSS on page 106.
   - **e** Configure DNS. See “Configuring DNS in CSS” in the *Authentication Services* manual.
   - **f** Set the SWDL transfer mode. See Setting the SWDL Transfer Mode in CSS on page 107.
   - **g** Configure for SSH. See the *Securing Protocols with SSH* manual, “Configuring SSH for RF Site Devices and VPMs in CSS” section in Chapter 4.
   - **h** Enable RADIUS Authentication. See Chapter 7, “Configuring RADIUS Sources and Parameters in CSS” in the *Authentication Services* manual. Make sure that the site controllers have been added to the RADIUS servers on the domain controllers as RADIUS clients.
   - **i** Enable Centralized Authentication. See Chapter 7, “Enabling/Disabling Centralized Authentication in CSS” in the *Authentication Services* manual.
   - **j** Set the Local Cache Size for Centralized Authentication. See Chapter 7, “Setting the Local Cache Size for Central Authentication in CSS” in the *Authentication Services* manual.
   - **k** Customize the login banner text using CSS (optional). See Customizing the Login Banner in CSS on page 106.
   - **l** Enable Centralized Event Logging (if required by your organization). See Chapter 6, “Enabling/Disabling Centralized Event Logging on Devices in CSS” in the *Centralized Event Logging* manual.
   - **m** Configure the Reference Source. See Configuring the Reference Source in CSS on page 108.
   - **n** Set the NTP Server Settings. See NTP Server Settings on page 108.

3 Set up the local Password Configuration (optional). See Setting the Local Password Configuration in CSS on page 108.

4.4.2
Connecting Through a Serial Port Link

Prerequisites: This procedure assumes that the Configuration/Service Software (CSS) application is loaded on your service computer/laptop. See the *Private Network Management Client* manual.

When and where to use: This procedure describes the steps required to connect through a serial port link to set the IP address of the device and to set the serial security services. Perform all other device function and feature configurations through an Ethernet port connection in the CSS.

Procedure:

1 Connect a serial cable to a service computer/laptop running CSS, and the serial connector on the device module. The serial cable is an RS232, female DB-9 to male DB-9 straight through cable. If the service computer/laptop does not have a serial port, use a USB-to-serial converter external device.

2 Open the CSS application.

3 From the menu, select **Tools** → **Connection Configuration**.

The **Connection Screen** dialog box appears.

4 In the **Connection Type** area, select **Serial**.

The **Serial Settings** area on the dialog box becomes enabled.

5 In the **Serial Port** field, select the communication port that matches the one selected on the service computer/laptop.

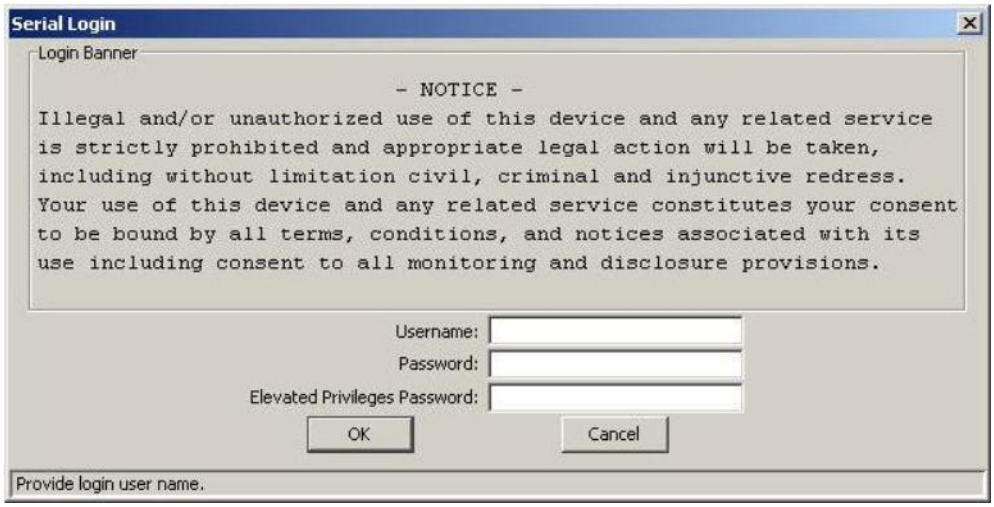
6 In the **Baud Rate** field, select the baud rate with which you want to communicate with the device.

- Baud Rate 19200

7 Click **Connect**.

A login/password prompt screen appears.

Figure 38: CSS Login Banner



8 Provide the required credentials. Perform one of the following actions:

- If a domain controller is available on the network, enter the **Username** and **Password** for the RADIUS service user account assigned to the netwadm group in the Active Directory. (The default service user is `serviceuser`.)
- If a domain controller is not available on the network, enter the **Username** and **Password** for the local bts_service account.
- If the **Elevated Privileges Password** field is active, enter the **Elevated Privileges Password** that was set up for this device.

When accessing the device, if the default passwords do not work, the passwords may have been set to default values by a different system release of software. See "Resetting Device Passwords" in the *CSS Online Help* to reset the passwords to the current software release defaults. If Authentication Services are not enabled on a device, type any alphanumeric characters to populate the [**Username**, **Password**, and **Elevated Privileges Password**] fields, as they cannot be left blank.

9 To access the device and close the dialog box, click **OK**.

The blank CSS main window appears.

NOTICE: The **Service** menu is not available until you read the configuration file from the device using an Ethernet connection.

4.4.3
Serial Connection Configurations

The following procedures set configuration parameters in the Configuration/Service Software (CSS) using a serial connection.

4.4.3.1
Setting the Device IP Address in CSS

Prerequisites: Ensure that you have the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. See Local Password and SNMPv3 Passphrase Troubleshooting on page 127.

NOTICE: Setting or changing the device IP Address causes the SNMPv3 configuration and user credentials to automatically reset.

Procedure:

1 Connect to the device using Configuration/Service Software (CSS) through a serial port link. See Connecting Through a Serial Port Link on page 96.

2 From the menu, select **Tools** → **Set IP Address/Box Number**.

The **Set IP Address and Box Number** dialog box appears.

3 Enter the device box number. Click **Set Box Number**.

4 Enter the device IP address in the **Device IP Address** field. Click **Set Device IP Address**.

5 To close the dialog box, click **OK**.

6 Initiate a hardware restart. Click **Reset**.

SNMPv3 user credentials reset to their factory default values.

7 To close the dialog box, click **Close**.

8 To reconfigure the SNMPv3 user credentials, go to Changing SNMPv3 Configuration and User Credentials in CSS on page 103.

4.4.3.2
Serial Security Services in CSS

The Serial Security Services in Configuration/Service Software (CSS) enables the secure services and changes the device password.

NOTICE: The Serial Security Services must be set before changing the SNMPv3 configuration and user credentials on a selected device in the site.

Before enabling this parameter, any login and password may be used on the File Transfer Access Services login window to access a device. After Authentication Services are enabled, the login and password provided is checked against the following authentication sources:

Stored password
RF site devices support a configurable password for the Local Service and Elevated Privileges accounts. The password is verified against the stored password for these accounts.

Built-in logins and passwords
RF site devices support built-in login/password combinations for a login by services such as the software downloads. Only certain software download login names are authenticated in this way.

Centralized Authentication
For authentication through centralized accounts instead of Local Service, Elevated Privileges, and built-in user accounts, use the **Configure the Centralized Authentication** parameter in CSS for the Challenge Handshake Authentication Protocol (CHAP). See “Enabling/Disabling Centralized Authentication with CSS” in the *Authentication Services* manual. This procedure requires an Ethernet connection to the device being configured.

4.4.3.2.1
Setting the Serial Security Services in CSS

Prerequisites: Obtain the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. See Local Password and SNMPv3 Passphrase Troubleshooting on page 127. Changing to the incorrect user credentials may lead to not being able to access the device through Configuration/Service Software (CSS) or Secure Shell (SSH).

Procedure:

1 Connect to the device using CSS through a serial port link. See Connecting Through a Serial Port Link on page 96.

2 From the menu, select **Security** → **Device Security Configuration** → **Security Services (Serial)**.

3 From the **Security Services Configuration** dialog box, set the **Test Application Configuration** field according to your organizational policies. The recommended secure configuration is **Disabled**.

4 Set the **Authentication Services** field to **Enabled**. Click **Apply**.

This field enables local authentication services and must be enabled as a prerequisite for centralized authentication.

5 Set the **Password Reset Mechanism** field.

This field allows a reset of the passwords for two built-in device accounts to their default values.

6 To update the password for the device, select either **Service Account** or **Elevated Privilege** from the drop-down list. Click **Update password**.

7 In the **Change Account Password** dialog box, enter the old password, then enter a new password, and confirm the new password before clicking **Change Password**.

8 To save the new password, click **OK**.

The **Change Account Password** dialog box closes.

4.4.3.3
Resetting SNMPv3 User Credentials to Factory Defaults in CSS

Prerequisites: Obtain the required credentials information (local service account password and elevated privileges password) to configure the site devices before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. To obtain the keys for resetting either password or SNMPv3 passphrases for the device, contact Motorola Solutions Support Center (SSC). Changing to the incorrect user credentials may lead to not being able to access the device through Configuration/Service Software (CSS) or Secure SHell (SSH).

Procedure:

1 Connect to the device using CSS through a serial port link. See Connecting Through a Serial Port Link on page 96.

2 From the menu, select **Security** → **SNMPv3 Configuration** → **Reset SNMPv3 Configuration (Serial)**.

The **Reset SNMPv3 Configuration** dialog box opens.

3 Click **Reset SMPv3 Configuration**.

The SNMPv3 configuration is reset to factory defaults in the device.

4 Click **Exit**.

The **Reset SNMPv3 Configuration** dialog box closes.

5 To reboot the device for the SNMPv3 user credentials to take effect, perform the following actions:

a From the menu, select **Tools** → **Set IP Address/Box Number** or **Set IP Address/BR_CM Pairing Number**.

b In the dialog box, click **Reset**.

The device reboots.

6 Proceed to Changing SNMPv3 Configuration and User Credentials in CSS on page 103.

4.4.4
Connecting Through an Ethernet Port Link

Prerequisites: Load Configuration/Service Software (CSS) on the service computer/laptop. See the *Private Network Management Client* manual if necessary or see the instructions in the CSS DVD jewel box for instructions on loading the CSS onto the service computer/laptop.

When and where to use: Use the Ethernet port link to configure all CSS parameters for the device.

Procedure:

1 Connect a service computer/laptop to a device using one of the following methods:

NOTICE: Normally the service computer/laptop is connected through the local site switch or remotely through the network. Do not connect directly to the Ethernet service port of the device unless downloading software or individually configuring the device.

a Remote Connection to Network or Local Site Switch:

1 Connect remotely to the network or to the local site switch using a straight-through an Ethernet straight-through Ethernet cable.

2 If connecting to the local site switch, configure the Ethernet interface of the service computer/laptop to a Speed/Duplex setting of **Auto-Negotiate**. Set the IP address of the service computer/laptop to an unused IP address on the subnet of the local site. The IP address on the subnet varies depending on the site and zone numbers.

b Direct Connection to Front Ethernet Service Port:

1 Connect directly to the front panel Ethernet service port with a straight-through Ethernet cable.

2 If connecting to a base radio or receiver, set the IP address of the service computer/laptop to 192.168.x, where x is any number between 2 and 253.

3 If connecting to a site controller or reference distribution module, set the IP address of the service computer/laptop to an unused IP address on the subnet of the local site. The IP address on the subnet varies depending on the site and zone numbers.

4 Configure the Ethernet interface of the service computer/laptop to a Speed/Duplex setting of **Auto-Negotiate**

NOTICE: The comparator does not support a direct connection to the front panel Ethernet service port. The connection must be done remotely through the network or through the local site switch.

2 Open the CSS application.

3 From the menu, select **Tools** → **Connection Configuration**.

4 From the **Connection Screen**, in the **Connection Type** area, select **Ethernet**.

5 If connected directly to the front panel Ethernet service port of a base radio or receiver, click **Front Panel Ethernet** and go to step 7.

6 Perform one of the following actions:

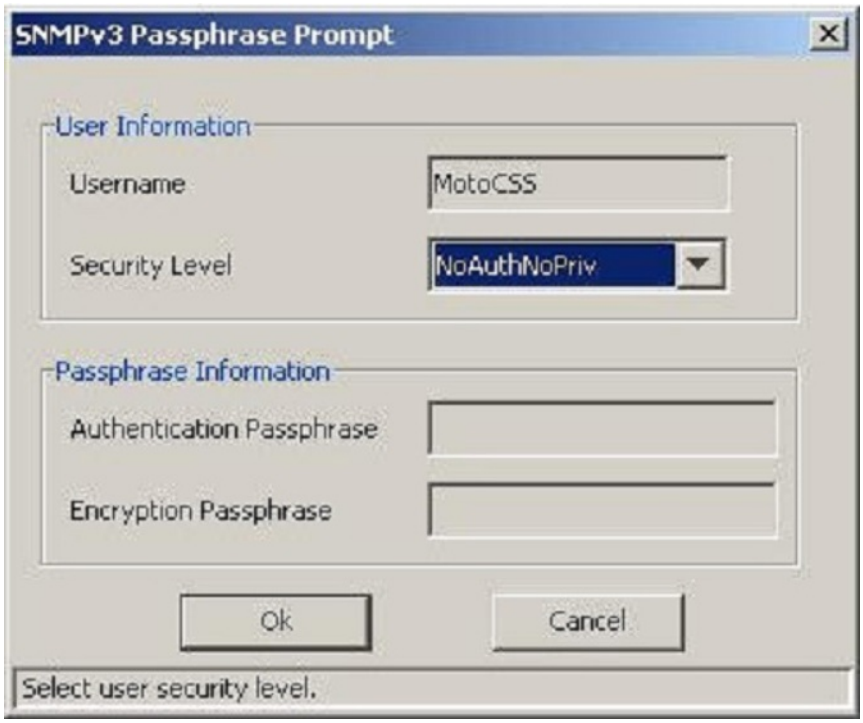
If…	Then…
If you know the IP address for the device,	perform the following actions: **a** In the **Device IP Address** field, enter the IP address for the device. **b** Click **Connect**. **c** Go to step 7.
Trunked Device: If you do not know the IP address, but know the system identification of the device (the zone,	perform the following actions: **a** Click **Device Name Wizard** to open the **Device Name Wizard** dialog box. **b** From the **Device** drop-down list, select the relevant device type.

If…	Then…
physical site, subsite, and device ID of the device),	**c** In the **Zone**, **Physical Site**, **Subsite**, and **Device ID** fields, enter the proper values. **NOTICE:** Some fields, such as **Subsite**, do not allow entries for some devices. Therefore, select the device first. **d** Click **OK**. The Domain Name Services (DNS) information of the device automatically appears in the **Device IP Address** field. **e** Click **Connect**. **f** Go to step 7.
Conventional Device: If you do not know the IP address,	perform the following actions: **a** Establish a serial connection to the device. See Connecting Through a Serial Port Link on page 96. **b** For a base radio, receiver, or comparator, from the menu, select **Tools** → **Set IP Address/BR_CM Pairing Number**. For a site controller or reference distribution module, select **Set IP Address/Box Number**. **c** In the **Device IP Address** field, record the IP address. **d** Re-establish an Ethernet connection and repeat steps 1 through 4. **e** In the **Device IP Address** field, enter the IP address for the device. **f** Go to step 7.

7 To make the connection, click **Connect**.

If this device is SNMPv3-capable, the **SNMPv3 Passphrase Prompt** dialog box appears.

Figure 39: SNMPv3 Passphrase Prompt



8 In the **SNMPv3 Passphrase Prompt** dialog box, enter the **User Information** and **Passphrase Information**. Click **OK**. If Authentication Services are not enabled on a device, click **OK** when the dialog box appears.

9 From the menu, select **File** → **Read Configuration From Device**.

The parameters download from the device to the service computer/laptop. When the download is complete, the CSS main window opens. Use the map on the left side of the screen to view configuration information for the device.

4.4.5
Ethernet Connection Configurations

The following procedures set configuration parameters in the Configuration/Service Software (CSS) using an Ethernet connection.

4.4.5.1
Setting the Date and Time in CSS

This procedure provides the date and time to the device.

When and where to use: During installation, the date and time is set through an Ethernet cable connected directly to the Ethernet port of the device. After installation, this procedure may be performed remotely.

NOTICE: If a power outage occurs, the device does not retain the date and time settings.

Procedure:

1 Connect to the device using CSS through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.

2 From the menu, select **Tools** → **Set Device Date and Time**.

3 Enter the current date and time. Click **OK**.

The date and time are set.

4.4.5.2

Changing SNMPv3 Configuration and User Credentials in CSS

Prerequisites: Obtain the required SNMPv3 credentials information (Authentication passphrase, Encryption passphrase, and Authoritative Engine ID) to configure the device before proceeding. The user credentials information includes both the current and new credentials. Without the current credentials, you cannot access the device and cannot change the user credentials. See Local Password and SNMPv3 Passphrase Troubleshooting on page 127. Changing to the incorrect user credentials may lead to not being able to access the device from the Unified Network Configurator (UNC), or for the device to be unable to send alarms to the Unified Event Manager (UEM) (for fault management).

When and where to use: This procedure changes the SNMPv3 configuration and user credentials from Configuration/Service Software (CSS) on a selected device in the site. For more information on this feature, see the *SNMPv3* manual.

NOTICE: During installation, perform this procedure through an Ethernet cable connected directly to the Ethernet port of the device. After installation, this procedure may be performed remotely from CSS.

Procedure:

1 Connect to the device using CSS through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.

2 From the menu, select **Security** → **SNMPv3 Configuration** → **Configure SNMPv3 Users (Ethernet)**.

The **SNMPv3 Passphrase Prompt** dialog box appears with **MotoAdmin** as the selected SNMPv3 user.

3 In the **SNMPv3 Passphrase Prompt**, enter the appropriate **Authentication** and **Encryption Passphrases** in the text fields.

NOTICE: When accessing the device for the first time, if the default passphrases do not work, the passphrases may have been set to default values by a different system release of software. See “Reset SNMPv3 Configuration (Serial)” in the *CSS Online Help* to reset the passphrases to the current software release defaults.

4 If connecting remotely through the network to a different device, perform one of the following actions. Otherwise, go to step 5.

If…	Then…
If you know the IP address for the device,	perform the following actions: **a** In the **Device IP Address** field, enter the IP address for the device. **b** Go to step 5.
If you do not know the IP address, but know the system identification of the	perform the following actions: **a** Click **Device Name Wizard**. **b** From the **Device** list box, select the desired device type.

If…	Then…
device (the zone, physical site, subsite, and device ID of the device),	**c** In the **Zone**, **Physical Site**, **Subsite**, and **Device ID** fields, enter the proper values. **NOTICE:** Some fields, such as **Subsite**, do not allow entries for some devices. Therefore, select the device first. **d** Click **OK**. The Domain Name Services (DNS) information of the device automatically appears in the **Device IP Address** field. **e** Click **Connect**. **f** Go to step 5.

5 Click **OK**.

If the passphrases are authenticated, the **Configure SNMPv3 Users** window appears. If the connection fails, a message appears.

6 To update the SNMPv3 credentials for a selected user, from the **User Information** section, select a Username in the **Username** drop-down list.

The CSS retrieves the current credentials from the device for a selected user.

NOTICE: Depending on the user selected, some fields on this dialog box become read-only or disabled. Click **Cancel** at any time to discard changes made to a selected user.

7 To change or update the SNMPv3 security level for a selected user, from the **User Information** section, select the security level in the **Security Level** drop-down list.

The security level options are:

NoAuthNoPriv
Neither the **Authentication Passphrase** nor **Encryption Passphrase** are needed for communicating with the device.

AuthNoPriv
Authentication Passphrase is needed; but no **Encryption Passphrase** is needed for communicating with the device.

AuthPriv
Both **Authentication Passphrase** and **Encryption Passphrase** are needed for communicating with the device.

The **User Status** field reflects the current operational status of the selected SNMPv3 User. The **Status Types** include:

Active
User configured on the device; the **Update** and **Delete** options are enabled.

Not in service
User configured on the device; the **Update** and **Delete** options are enabled.

Not ready
User configured on the device; the **Update** and **Delete** options are enabled.

Not present
Not present on the device; the **Create** option is enabled.

The security level of the selected user is set.

8 To change the Authentication Passphrase for the selected SNMPv3 user, if applicable to the selected security level, perform the following actions:

   a From the **Authentication Passphrase** section, enter the passphrase into the **Old Passphrase** field.

   NOTICE: If you do not know the passphrase, select the **I do not remember old passphrase** check box.

   b Enter the new passphrase into the **New Passphrase** field.

   NOTICE: The passphrase must be between 8 and 64 characters in length and consist of upper or lowercase alphanumeric characters (excluding the @ # $ ^ or _ characters).

   c Enter the same new passphrase into the **Confirm New Passphrase** field.

9 To change the encryption passphrase for the selected SNMPv3 user, if applicable to the selected security level, perform the following actions:

   a From the **Encryption Passphrase** section, enter the old passphrase into the **Old Passphrase** field.

   NOTICE: If you do not know the passphrase, select the **I do not remember old passphrase** check box.

   b Enter the new passphrase into the **New Passphrase** field.

   c Enter the same new passphrase into the **Confirm New Passphrase** field.

10 To change the Authoritative Engine Identifier, applicable to MotoInformA and MotorInformB users only, perform the following actions:

   a From the **Authoritative Engine ID** section, select the desired current engine ID from the **Current Engine ID** drop-down list.

   b In the **New Engine ID** field, enter the new engine ID.

   NOTICE: The new engine ID must be between 1 and 27 characters and comply with the Engine ID Domain Name Syntax.

11 To create, update, or delete SNMPv3 users, go to Adding or Modifying an SNMPv3 User in CSS on page 105.

4.4.5.2.1
Adding or Modifying an SNMPv3 User in CSS

When and where to use: Use this procedure to create, update, or delete an SNMPv3 user from the **Configure SNMPv3 Users** window.

Procedure:

1 From the **Configure SNMPv3 Users** window, to add or modify the selected SNMPv3 user, click one of the following:

- **Create:** Creates a user when the status is Not Present.
- **Update:** Updates an existing user.
- **Delete:** Removes an existing user.

NOTICE: The MotoZSS Username is used only in an ASTRO® 25 repeater site or Multisite subsystem.

A **Confirmation** dialog box appears and prompts if you want to continue.

2 Click **Yes**.

The **Processing Requests** dialog box appears and processes the request. A green square X indicates OK and a red square X indicates failure.

3 After reviewing the processing status, click **OK**.

NOTICE: If you encounter any errors, go back to the appropriate step and correct the information entered.

4 Repeat these steps for any SNMPv3 users you wish to create, update, or delete.

5 Click **Cancel** to exit the **Configure SNMPv3 Users** window.

The **Configure SNMPv3 Users** window closes, and the CSS main window returns.

4.4.5.2.2
Performing an SNMPv3 Connection Verification in CSS

When and where to use: When the SNMPv3 user credentials have been created, modified, or deleted, ensure that the device is properly configured for SNMPv3. Follow this procedure to verify the SNMPv3 connection.

Procedure:

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.

2 When the passphrase prompt screen opens, select the configured security level and enter the required passphrases.

3 If the connection was successful, click **OK**.

4.4.5.3
Customizing the Login Banner in CSS

This procedure describes how to edit the login banner security notice.

Procedure:

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.

2 From the menu, select **Security** → **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)**.

3 From the **Remote Access/Login Banner** screen, **Remote Access Configuration** tab, click the **Login Banner** tab.

4 Edit the text of the banner.

5 Click one of the following:

- **Refresh:** re-reads the original Login Banner text.
- **Apply:** saves the changes and keep the screen open.
- **OK:** saves the changes and close the screen.
- **Cancel:** closes the screen without saving the changes.

4.4.5.4

Setting the SWDL Transfer Mode in CSS

This procedure sets the Software Download Manager (SWDL) transfer mode.

When and where to use: Follow this procedure to set the SWDL transfer mode to Ftp (clear) or Sftp (secure) before performing a software download on the device.

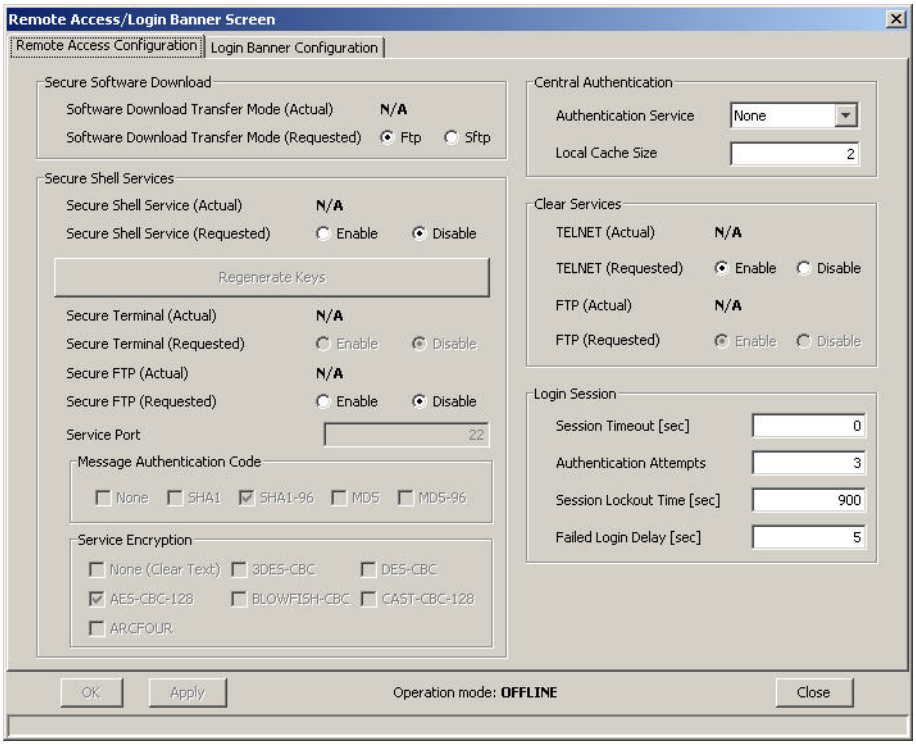
NOTICE: The SWDL transfer mode must be set to **Ftp** (clear) if any PSC 9600, STR 3000, QUANTAR®, or ASTRO-TAC® 9600 device is present at a site.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.
2. From the menu, select **Security** → **Device Security Configuration** → **Remote Access/Login Banner (Ethernet)**.

   The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.

   Figure 40: Remote Access Configuration Tab



3. In the **Software Download Transfer Mode (Requested)** field, choose either **Ftp** (clear) or **Sftp** (secure). Click **OK**.

   NOTICE: Secure Shell Service (Requested) and Secure FTP (Requested) are automatically set to **Enabled** and grayed out when you choose **Sftp**.

4.4.5.5
Configuring the Reference Source in CSS

When and where to use: This procedure identifies the 1PPS time reference source (GPS Receiver or TRAK) that is connected to the GCP 8000 Site Controller, whether a TRAK is present or not at a site.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.
2. From the menu, select **Service** → **Reference Service Screen**.

   The **Reference Service Screen** appears.
3. In the **Requested Primary/Secondary Sources** field, choose one of the following:
   - **External/None** – used when there is a TRAK device and no GPS Receivers.
   - **Redundant/None** – used when there is no TRAK and no GPS Receivers.

4.4.5.6
Manager IP Address Settings in CSS

When IP addresses exceed the allowed total, remove the IP addresses that are no longer used at the site. This removal allows the Unified Event Manager (UEM) to be identified as the current manager and handles traps for the device.

See “Clearing Manager IP Addresses in CSS” in the *CSS Online Help* for removing these IP addresses.

4.4.5.7
NTP Server Settings

Network Time Protocol (NTP) provides a clock synchronization mechanism for various Network devices and computers. To allow the NTP server to provide date and time synchronization for a particular device, the NTP servers IP address must be entered on the Manager / NTP Definition Screen.

See the NTP Server Settings in the *CSS Online Help* for defining, editing, and removing these settings.

NOTICE: When the IP addresses exceed the total, removing IP addresses allows the UEM to be identified as the current manager that can handle traps for the device.

4.4.5.8
Setting the Local Password Configuration in CSS

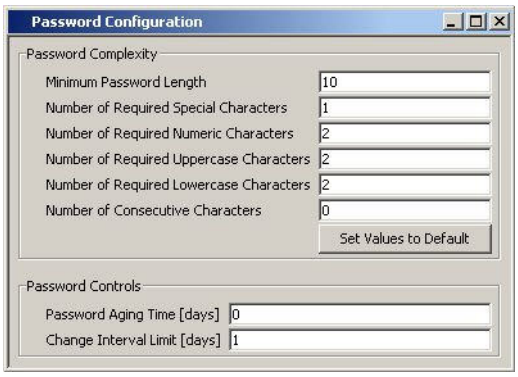
When and where to use: Use this procedure to set the complexity requirements and controls for the local service account password. The updated password criteria is enforced on the next password change for the device local service account. Password Configuration is an optional feature. For information, see “Password Configuration" in the *CSS Online Help*.

Procedure:

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See Connecting Through an Ethernet Port Link on page 99.
2. In the navigation pane, click the **Password Configuration** element.

   The **Password Configuration** window appears.

Figure 41: Password Configuration Window



3 Complete the following fields:

Minimum Password Length
This field allows you to enter a value as the minimum length for the password. The minimum can be between 8 and 255 characters, with a default of 10 characters.

Number of Required Special Characters
This field allows you to enter a value for the required number of special characters which must be included in the password. The value can be between 0 and 255, with a default of 1.

Number of Required Numeric Characters
This field allows you to enter a value for the required number of numeric characters which must be included in the password. The value can be between 0 and 255, with a default of 2.

Number of Required Uppercase Characters
This field allows you to enter a value for the required number of uppercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2.

Number of Required Lowercase Characters
This field allows you to enter a value for the required number of lowercase alphabetic characters which must be included in the password. The value can be between 0 and 255, with a default of 2.

Number of Consecutive Characters
This field allows you to enter the maximum number of consecutive repeated characters permitted in the password.

Set Values to Default
This field returns all fields to their system default values.

Password Aging Time [days]
This field allows you to enter a value between 0 and 65535 for the maximum number of days a local password is valid. After the **Password Aging Time** has elapsed, the password must be changed. The default value is 0.

Change Interval Limit [days]
This field allows you to enter a value between 0 and 65535 for the number of days which must elapse before a local password can be changed. The default value is 1.

4.4.6
CSS Configuration Parameters for the GCP 8000 Site Controller (Trunked Repeater)

When and where to use:
Before proceeding with this process, complete the initial configuration of the device in Initial Configuration of a Device in CSS on page 95.

For configuration details of the GCP 8000 Site Controller at a repeater site, see "Repeater Site Controller" in the Site Controller Configuration & Service Help in the *CSS On-line Help*.

Process:

1. In the System tree, click **System** and complete the fields.
2. In the System tree, click **Sub-Band** and complete the fields in the two tabs.
3. In the System tree, click **Band Plan Configuration** and complete the fields in the two tabs.
4. In the System tree, click **Zone** and complete the fields in the two tabs.
5. In the System tree, click **Site** and complete the fields in the three tabs.
6. In the System tree, click **Channel** and complete the fields.
7. In the System tree, click **Configuration** and complete the fields.
8. In the System tree, click **Network Services Configuration** and complete the fields on the three tabs.

   NOTICE: For configuration details for DNS and RADIUS Services, see the *Authentication Services* manual. For configuration details for SYSLOG Services, see the *Centralized Event Logging* manual.
9. In the System tree, click **Password Configuration** and complete the fields.

   NOTICE: Password Configuration is only required if you have passwords entered for local accounts. This sets the password complexity and controls. For details on password complexity and controls see “Password Configuration” in *CSS Online Help*.
10. In the System tree, click **Site Controller Switch** and complete the fields.
11. In the System tree, click **Data Configuration** and complete the fields in the four tabs.
12. From the menu, select **File** → **Save As** to save the configuration data to a new archive file, or select **File** → **Save** to overwrite the existing archive file.

    IMPORTANT: Save any configuration changes to a local or network drive so that if the device module fails, you can load your settings to a replacement device module. If the configuration file is not saved to a local or network drive, repeat the set-up steps after replacing a device module.
13. From the menu, select **File** → **Write Configuration to Device**.

4.4.7
CSS Configuration Parameters for the GCP 8000 Site Controller (HPD)

When and where to use:
Before proceeding with this process, complete the initial configuration of the device in Initial Configuration of a Device in CSS on page 95.

For configuration details of the GCP 8000 Site Controller at an HPD site, see "HPD Site Controller" in the Site Controller Configuration & Service Help in the *CSS On-line Help*.

Process:

1. In the System tree, click **System** and complete the fields.
2. In the System tree, click **Band Plan Configuration** and complete the fields in the two tabs.
3. In the System tree, click **Zone** and complete the fields in the two tabs.
4. In the System tree, click **Site** and complete the fields in the three tabs.
5. In the System tree, click **Channel** and complete the fields.

6 In the System tree, click **Site Controller** and complete the fields.

7 In the System tree, click **Network Services Configuration** and complete the fields on the three tabs.

NOTICE: For configuration details for DNS and RADIUS Services, see the *Authentication Services* manual. For configuration details for SYSLOG Services, see the *Centralized Event Logging* manual.

8 In the System tree, click **Password Configuration** and complete the fields.

NOTICE: Password Configuration is only required if you have passwords entered for local accounts. This sets the password complexity and controls. For details on password complexity and controls see “Password Configuration” in *CSS Online Help*.

9 In the System tree, click **Site Controller Switch** and complete the fields.

10 In the System tree, click **Data Configuration** and complete the fields in the two tabs.

11 From the menu, select **File** → **Save As** to save the configuration data to a new archive file, or select **File** → **Save** to overwrite the existing archive file.

IMPORTANT: Save any configuration changes to a local or network drive so that if the device module fails, you can load your settings to a replacement device module. If the configuration file is not saved to a local or network drive, repeat the set-up steps after replacing a device module.

12 From the menu, select **File** → **Write Configuration to Device**.

4.4.8
CSS Configuration Parameters for the GCP 8000 Site Controller (Trunked Simulcast)

When and where to use:
Before proceeding with this process, complete the initial configuration of the device in Initial Configuration of a Device in CSS on page 95.

For configuration details of the GCP 8000 Site Controller at a trunked simulcast site, see "Multi-Site Site Controller" in the Site Controller Configuration & Service Help in the *CSS On-line Help*.

Process:

1 In the System tree, click **System** and complete the fields.

2 In the System tree, click **Sub-Band** and complete the fields in the two tabs.

3 In the System tree, click **Band Plan Configuration** and complete the fields in the two tabs.

4 In the System tree, click **Zone** and complete the fields in the two tabs.

5 In the System tree, click **Site** and complete the fields in the three tabs.

6 In the System tree, click **Channel** and complete the fields.

7 In the System tree, click **Subsite** and complete the fields.

8 In the System tree, click **Configuration** and complete the fields.

9 In the System tree, click **Network Services Configuration** and complete the fields on the three tabs.

NOTICE: For configuration details for DNS and RADIUS Services, see the *Authentication Services* manual. For configuration details for SYSLOG Services, see the *Centralized Event Logging*, manual.

10 In the System tree, click **Password Configuration** and complete the fields.

NOTICE: Password Configuration is only required if you have passwords entered for local accounts. This sets the password complexity and controls. For details on password complexity and controls see “Password Configuration” in *CSS Online Help*.

11 In the System tree, click **Data Configuration** and complete the fields in the four tabs.

12 From the menu, select **File** → **Save As** to save the configuration data to a new archive file, or select **File** → **Save** to overwrite the existing archive file.

IMPORTANT: Save any configuration changes to a local or network drive so that if the device module fails, you can load your settings to a replacement device module. If the configuration file is not saved to a local or network drive, repeat the set-up steps after replacing a device module.

13 Write the configuration data to the device, as follows:

- From the menu, select **File** → **Write Configuration to Device**.

4.4.9
CSS Configuration Parameters for the Conventional GCP 8000 Site Controller

When and where to use:
This section describes the configuration procedures for the selected Conventional GCP 8000 Site Controller using the CSS.

Before proceeding with this process, complete the initial configuration of the device in Initial Configuration of a Device in CSS on page 95.

For configuration details of the GCP 8000 Site Controller at a conventional site, see "Conventional Site Controller" in the Site Controller Configuration & Service Help in the *CSS On-line Help*.

Process:

1 In the System tree, click **Zone** and complete the field.

2 In the System tree, click **Configuration** and complete the fields.

3 In the System tree, click **Network Services Configuration** and complete the fields on the three tabs.

NOTICE: For configuration details for DNS and RADIUS Services, see the *Authentication Services* manual. For configuration details for SYSLOG Services, see the *Centralized Event Logging*, manual.

4 In the System tree, click **Password Configuration** and complete the fields.

NOTICE: Password Configuration is only required if you have passwords entered for local accounts. This sets the password complexity and controls. For details on password complexity and controls see “Password Configuration” in *CSS Online Help*.

5 From the menu, select **File** → **Save As** to save the configuration data to a new archive file, or select **File** → **Save** to overwrite the existing archive file.

IMPORTANT: Save any configuration changes to a local or network drive so that if the device module fails, you can load your settings to a replacement device module. If the configuration file is not saved to a local or network drive, repeat the set-up steps after replacing a device module.

6 Write the configuration data to the device, as follows:

- From the menu, select **File** → **Write Configuration to Device**.

4.5

Configuring Centralized Authentication on Devices in VoyenceControl

When and where to use: This process provides the procedures for configuring centralized authentication on devices using the VoyenceControl component of the Unified Network Configurator (UNC) application.

NOTICE: VoyenceControl does not apply for a K core or non-networked site.

Process:

1. Configure Domain Name Service (DNS) on the device. See “DNS Configuration on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.
2. Configure Authentication Sources for the device. See “Centralized Authentication Configuration on RF Site and VPM Devices with VoyenceControl" in the *Authentication Services* manual.
3. Configure RADIUS parameters for the device. See “Configuring RADIUS on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.
4. Set the Local Cache Size for Centralized Authentication for the device. See “Setting the Local Cache Size for Central Authentication on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.
5. Enable/Disable Centralized Authentication for the device. See “Centralized Authentication Configuration on RF Site and VPM Devices with VoyenceControl” in the *Authentication Services* manual.
6. Enable/Disable Centralized Event Logging for the device. See “Enabling/Disabling Centralized Event Logging on RF Site Devices and VPMs with EMC Smarts” in the *Centralized Event Logging* manual.

This page intentionally left blank.

Chapter 5

GCP 8000 Site Controller Optimization

This chapter contains optimization procedures and recommended settings relating to the GCP 8000 Site Controller.

5.1 GCP 8000 Site Controller Reference Oscillator Alignment

NOTICE: This alignment is for both active and standby site controllers at a repeater site only and when a TRAK is **Not** present.

After an active or standby site controller is installed, the reference oscillator must be aligned.

NOTICE: The site controllers must be turned on for at least one week before the reference oscillator is aligned.

The site controller reference oscillator must be aligned to within 1 ppb (parts per billion). The frequency reference used to make this alignment should be accurate to within 1 ppb. This accuracy typically requires test equipment with a double oven or a Rubidium reference oscillator.

The reference oscillator must be aligned:

- Upon installation of the site controller for all bands.
- Once every year after installation for TDMA systems for all bands.
- Once every two years after installation for FDMA, 700/800/900 MHz systems.
- Once every five years after installation for FDMA, UHF systems.
- FDMA, VHF systems do not require alignment after initial installation.

See Site Controller Configuration & Service Help > Site Controller Procedures > Aligning the Reference Oscillator in the *CSS Online Help* for the alignment procedures.

This page intentionally left blank.

Chapter 6

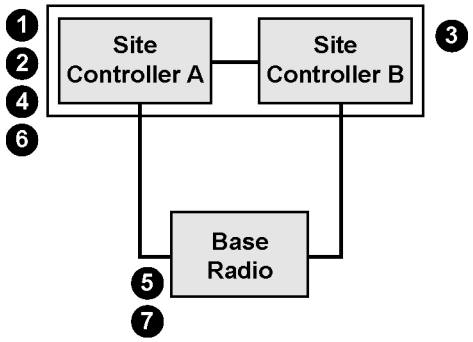
GCP 8000 Site Controller Operation

This chapter details tasks that are performed once the GCP 8000 Site Controller is installed and operational in the system.

6.1 Site Initialization for the Trunked GCP 8000 Site Controller (HPD and Repeater Site)

The GCP 8000 Site Controller at an HPD or repeater site follows this site initialization process.

Figure 42: Site Initialization (HPD and Repeater Site)



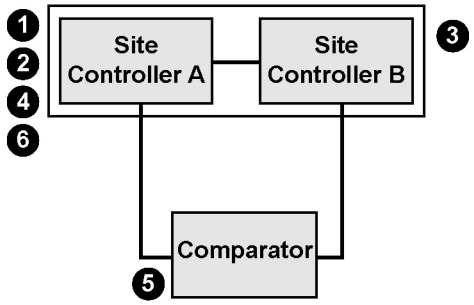
Remote_site_initialization

1. After the site controller is powered up, it enters standby mode and checks for status messages from the other site controller.
2. If status messages are not received before a time-out period, the site controller becomes active, monitors the LAN for base radios, and begins sending status messages.
3. When the standby site controller is powered up, it enters standby mode and receives status messages from the active site controller. The standby site controller remains in the standby mode.
4. When the active site controller detects a base radio on the LAN, it sends a report status message to the base radio through the site LAN. This activity takes place with all base radios simultaneously.
5. The base radio responds with a channel status reply to the active site controller. The base radio then begins to monitor periodic status messages from the active site controller.
6. The active site controller receives the channel status response from the base radio and begins to send background messages to the base radio, then sends a channel grant to the base radio.
7. The base radio enters the assigned operational state and keys up. It is now available for operation. If the zone controller has the greatest preference setting in the UNC, the base radio may be assigned as the control channel.

6.2 Site Initialization for the Trunked GCP 8000 Site Controller (Simulcast)

The GCP 8000 Site Controller at a simulcast site follows this site initialization process.

Figure 43: Site Initialization (Simulcast)



Prime_site_initialization

1 After the site controller is powered up, it enters standby mode and checks for status messages from the standby site controller.

2 If status messages are not received before a time-out period, the site controller becomes active, monitors the LAN for comparators, and begins sending status messages.

3 When the standby site controller is powered up, it enters standby mode and receives status messages from the active site controller. The standby site controller remains in standby mode.

4 When the active site controller detects a comparator on the LAN, it sends a report status message to the comparator through the site LAN. This activity takes place with all comparators simultaneously.

5 The comparator responds with a channel status reply to the active site controller. The comparator then begins to monitor periodic status messages from the active site controller.

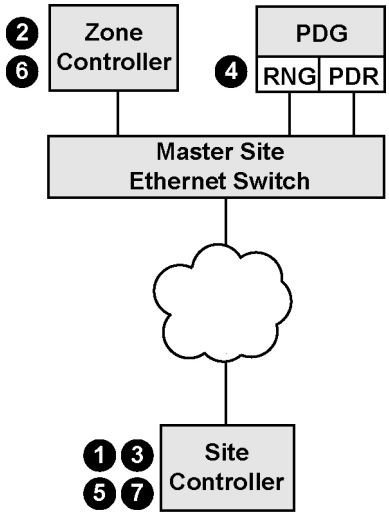
6 The active site controller receives the channel status response from the comparator and begins to send background messages to the comparator, then sends a channel grant to the comparator.

NOTICE: For specifics regarding the site controllers employed in a Geographical Redundant Prime Site, see the *Trunked IP Simulcast Prime Site* manual.

6.3 Master Site and Trunked GCP 8000 Site Controller Interaction During Site Initialization

In addition to the interactions at the site, there are also a number of transactions that take place between the GCP 8000 Site Controller and master site equipment during the site initialization. The following describes these interactions between the site controller, zone controller (ZC), and Radio Network Gateway (RNG) during the site initialization.

Figure 44: Site Initialization – Master Site Interaction



1. Information between the active site controller and the zone controller is exchanged during initialization.
2. The zone controller determines whether the site transits into wide area mode. When ready, the zone controller notifies the site controller to transit to wide area mode.
3. The site controller responds to the zone controller and initiates a connection with the RNG.
4. The RNG establishes the link with the site controller.
5. The site controller notifies the zone controller that the site is wide capable.
6. The zone controller sends a wide grant message to the site controller and updates the adjacent sites.
7. The site controller updates its system broadcast status (Network Available) and its status message (Wide Area).

6.4 Site Initialization of the Conventional GCP 8000 Site Controller

After the site controller is powered up, it enters active mode and waits for in-service signals from both consoles and conventional channels through a CCGW. There is no interaction between the conventional site controller and the master site except for configuration provisioning from UNC.

This page intentionally left blank.

Chapter 7

GCP 8000 Site Controller Maintenance

This chapter describes periodic maintenance procedures relating to the GCP 8000 Site Controller.

7.1 Fan Grill Cleaning Instructions

If the station equipment is installed in a dusty environment, take precautions to filter the air used for a forced cooling of the station. Excessive dust drawn across and into the device circuit modules by the cooling fans can adversely affect heat dissipation and circuit operation. In such installation, be sure to clean or replace external filtering devices periodically.

If dust has accumulated on the fan grills, cleaning the fan grills is recommended. When cleaning, take care to prevent dust from being pulled into the modules. Use a damp cloth to wipe the front of the fan grills. When removing the power supply, turn off the unit before proceeding.

7.2 GCP 8000 Site Controller Reference Oscillator Alignment

NOTICE: This alignment is for both active and standby site controllers at a repeater site only and when a TRAK is **Not** present.

After the GCP 8000 Site Controller is installed, the reference oscillator must be aligned.

NOTICE: The site controllers must be turned on for at least one week before the reference oscillator is aligned.

The site controller reference oscillator must be aligned to within 1 ppb (parts per billion). The frequency reference used to make this alignment should be accurate to within 1 ppb. This accuracy typically requires test equipment with a double oven or a Rubidium reference oscillator.

See Site Controller Configuration Service Help > Site Controller Procedures > Aligning the Reference Oscillator in the *CSS Online Help* for the alignment procedures.

This page intentionally left blank.

Chapter 8

GCP 8000 Site Controller Troubleshooting

This chapter provides fault management and troubleshooting information relating to the GCP 8000 Site Controller.

8.1 GCP 8000 Site Controller General Troubleshooting

Table 14: GCP 8000 Site Controller - General Troubleshooting

Problem	Troubleshooting
General connectivity problems	**1** If you have access to the equipment, check the LEDs to verify if each piece of equipment is connected and operational. See GCP 8000 Site Controller LEDs on page 149. **2** In the CSS, check the alarms of the site controller and all associated devices and links. **3** Verify that the IP address, subnet mask, Site Controller Number, and default gateway for the site controller is correct. In the CSS, send a diagnostic command to enable the site controller. **4** For a Repeater Site Controller or an HPD Site Controller (if present in a Tsub), verify that the DNS Hostname is correct. If the DNS Hostname was incorrect and then corrected, further corrections may be needed on the DNS server, UNC, and UEM. See the Troubleshooting chapter in the *Authentication Services* manual. **5** Verify if the physical cabling is firmly connected and is in good condition. Check for any sharp bends or kinks in cabling. Test suspected cabling for noise, continuity, attenuation, and crosstalk. Replace the cabling if necessary. **6** If the connection fails to operate normally, check the diagnostics, and if needed, contact the Motorola Solutions Support Center (SSC). **7** If the site controller still fails to operate properly, create a backup of the current configuration, then reinstall the software and reconfigure the site controller. **8** Replace the site controller if necessary.
Unit will not power up	**1** If you have access to the equipment, check the LEDs to verify if each piece of equipment is connected and is operational. See GCP 8000 Site Controller LEDs on page 149. **2** Check the power cabling and verify if the power source for the site controller is supplying the appropriate voltage. Connect the site con-

Table continued…

Problem	Troubleshooting
	troller to another power source or replace the power cabling if necessary. **NOTICE:** Check all power sources if there is more than one. **3** Check for any burn marks or physical damage to the site controller and check whether the site controller is properly grounded. **4** Replace the site controller if necessary.
Reference Service reported as not detected	**1** Verify that the Time Reference Configuration in CSS is properly configured. **2** Verify that the time reference source is operational.
Unable to perform a password reset	If the device module has been replaced and serial port access is not available to configure the IP address, the device may have the account locked out or the backplane slot has passwords enabled. Perform the following steps: **1** Move the device module to a different chassis or to a different slot in the backplane where local passwords are not configured. **2** Configure the IP address and reset the device through the front panel RS-232 serial service port using CSS. **3** Perform the local password reset operation (to clear account information stored in the FRU) through and Ethernet port link using CSS. **4** Move the device module back to the original chassis or slot. **5** Perform the local password reset operation again (to clear account information stored in the backplane). See “Connecting Through an Ethernet Port Link” and “Setting the Local Password Configuration in CSS”.

8.2 Troubleshooting Tools

Several tools are available for troubleshooting the GCP 8000 Site Controller:

- Unified Event Manager to monitor links and components
- Unified Network Configurator
- Configuration/Service Software (CSS)
- MOSCAD NFM

NOTICE: The Unified Event Manager (UEM) can be established as a more centralized fault management solution replacing the MOSCAD GMC. See the *Unified Event Manger* and the *UEM GMC MOSCAD Transition Guide* for details.

8.2.1 Troubleshooting GCP 8000 Site Controller Alarms in Unified Event Manager

Unified Event Manager is a fault management software tool that displays alarms for devices in the subsystem. For further details on the UEM, see the *UEM Online Help*.

The site controller monitors the state and activities throughout the site, and reports any relevant events to UEM. The site controller also reports the status and events of its subcomponents including the fan, GPS reference, internal switch, and power supply.

If a site controller is configured with an incorrect Site ID, the UEM may display two separate site objects (not only as a redundant group name) and the ZoneWatch application may also show “gray” for the site or zone. To correct this situation, re-configure the site controller with the correct Site ID, manually delete the incorrect site objects in the UEM, and rediscover the site controller in the UEM. If a UEM rediscovery operation is not performed after re-configuring the site controller with the correct Site ID, the UEM and ZoneWatch displays are not updated. After re-discovery, “refresh” the ZoneWatch.

NOTICE: In a GTR 8000 Expandable Site Subsystem, the base radio reports a failure of the power supply instead of the site controller. The site controller always shows the power supply as Operational or Enabled because the actual status of the power supply is provided by the base radio.

These options apply to site controllers in all hardware configurations, and include the systems supported by these configurations: HPD, repeater site subsystem, and circuit and IP simulcast site subsystems.

Table 15: GCP 8000 Site Controller Diagnostic Options

Option	Description
User Disabled	Requests that the selected site controller disable. If in a redundant configuration, after disabling, the site controller isolates itself from the other site controller and the RNG. If the site controller was the active site controller and the standby site controller is not isolated from the system, then the standby site controller becomes active and takes over operations at the site.
Enabled	Requests the selected site controller to enable.
Restart	Requests the selected site controller to reset. The site controller re-sets back in its current state.
Force Active*	Forces the third site controller to become active when in a Trunked IP Simulcast Prime Site Geographic Redundancy (TPSGR) sub-system. The other two site controllers go into standby, provided the network between all three site controllers is functional.

* = This option is only available for the third site controller at the secondary prime site in a Trunked IP Simulcast Prime Site Geographic Redundancy (TPSGR) subsystem.

8.2.1.1
Monitoring Links and Individual Components in Unified Event Manager

Use the Unified Event Manager (UEM) to monitor critical links and components in a device or in the system. Monitoring may take place remotely from a central operations center. Two types of monitoring include:

- Real-time monitoring of UEM Topology maps, which alert the user the “highest severity” of alarms of a particular subnet as they occur.
- Evaluation of UEM Active Alarms Window on a regularly scheduled basis.

See the *Unified Event Manager* manual or *UEM Online Help* for further details.

8.2.1.2
Analyzing Unified Event Manager Active Alarms Window

The Unified Event Manager (UEM) **Active Alarms** Window is useful for troubleshooting, because it captures alarms that may occur intermittently or during off-hours. For example, review the **Active Alarms** Window to correlate the reported loss of service with patterns of critical alarms, for the links and equipment.

When analyzing the **Active Alarms** Window, look for these types of patterns:

- Failures sent with time stamps on or about the same time.
- Failures from equipment attached to particular links. For example, routers, switches, base radios, site controllers, and comparators.
- Many devices are capable of sending out events that report both critical and non-critical events. Learn to distinguish between critical and non-critical events.

See the *Unified Event Manager* manual or *UEM Online Help*.

8.2.2
Device Troubleshooting in Unified Network Configurator

Use the Unified Network Configurator (UNC) to verify configuration data during system commissioning and later when you maintain or expand the system. Use UNC to do the following to the device:

- Verify configuration
- Correct configuration errors

See the *Unified Network Configurator* manual for further details.

8.2.3
Troubleshooting the GCP 8000 Site Controller in Configuration/ Service Software

The GCP 8000 Site Controller is locally or remotely configured or serviced through Configuration/ Service Software (CSS). The CSS provides access to alarms, status information, and configuration settings for the site controller.

The CSS is used for the following tasks, which are useful when troubleshooting the site controller. See the *CSS Online Help* for specific details and instructions when using these tasks:

- Enable and disable channels and services.
- View and save a log of site controller alarms.
- Verify the site controller configuration.
- Gather troubleshooting information and escalated to Motorola Solutions for evaluation.
- Check the active VLANs.

8.2.3.1
Troubleshooting the GCP 8000 Site Controller Using Broadcast RNG Link Status

NOTICE: The Broadcast link status is displayed in the Configuration/Service Software (CSS) status panel screen and might be used for troubleshooting.

The CSS status panel screen displays the following status data:

Table 16: Broadcast RNG Link Status Possible States

State	Description
Up	Broadcast RNG Link up: Data Site Controller successfully connected to the RNG via multicast.
Down	Broadcast RNG Link down: Failed multicast connection to the RNG. (Data Site Controller does not report this trap when Broadcast Data is disabled at the Site.)
Disabled	Broadcast RNG Link disabled: Broadcast data feature disabled at the site.

Table 17: Broadcast RNG Link Status Possible Causes

Cause	Description
No Reason	No Reason
linkFailure	Broadcast RNG Link down
userDisabled	User disabled broadcast date feature at the site

Table 18: Broadcast RNG Link Status Possible States and Causes

State	Cause
Up	No Reason
Down	linkFailure
Disabled	userDisabled
Disabled	No Reason

8.2.3.2
Diagnostic Tests for the GCP 8000 Site Controller

The GCP 8000 Site Controller is designed with internal diagnostic tests that occur on power-up and reset. Diagnostic tests are available for the control module and power supply. If a problem occurs during operation, it is reported as an alarm. All alarms are stored in the Alarm Log, accessible with Configuration/Service Software (CSS). The alarm log contains the name of the diagnostic test that failed and the time since the last power-up. Critical alarm conditions, alarms are reported directly to the Site Control Manager.

8.2.3.3
Local Password and SNMPv3 Passphrase Troubleshooting

The password reset mechanism in the Configuration/Service Software (CSS) application can be enabled/disabled. See “Secure Remote Access Configuration > Device Security Configuration - Security Services (Serial)” in the *CSS Online Help* for information. To obtain the keys for resetting either password or SNMPv3 passphrases for the device, contact Motorola Solutions Support Center (SSC).

NOTICE: The default values for the local passwords and SNMPv3 passphrases, as well as the keys for the local password reset procedure, may vary by system release. These default values and keys are treated as sensitive information and are provided to your organization through secured communication.

Table 19: Local Password and SNMPv3 Passphrase Troubleshooting

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Login Password
User is locked out of the local login, but knows SNMPv3 passphrases	✓	✗	See the *CSS Online Help* “SNMPv3 User Configuration”.	See the *CSS Online Help* “Resetting Device Passwords.”
User knows the local login, but not the SNMPv3 passphrases	✗	✓	See the *CSS Online Help* “Reset SNMPv3 Configuration (Serial)”.	See the *CSS Online Help* “Device Security Configuration – Security Services (Serial)”.
User knows both passphrases and local service password	✓	✓	See the *CSS Online Help* “SNMPv3 User Configuration”.	See the *CSS Online Help* “Device Security Configuration – Security Services (Serial)”.
User does not know SNMPv3 passphrase nor service account password	✗	✗	Contact Motorola Solutions SSC.	Contact Motorola Solutions SSC.

8.2.4
MOSCAD Network Fault Management

If MOSCAD Network Fault Management (NFM) equipment is supported at the site, additional status, and alarm information for a device can be viewed through the MOSCAD NFM.

Figure 45: MOSCAD Network Fault Management – Example

When an alarm condition occurs, the alarm device for one of the modules begins to flash red. Selecting the LED box opens an alarm pop-up window indicating details of the alarm. To view the status of all alarms for a particular module within the device, select the alarm LED box corresponding to the particular module. Alarms can be acknowledged by pressing the **Acknowledge** button on the screen.

See the *MOSCAD Network Fault Management Feature Guide* for details.

NOTICE: The Unified Event Manager (UEM) can be established as a more centralized fault management solution replacing the MOSCAD GMC. See the *Unified Event Manger* manual and the *UEM/GMC Transition Setup Guide* for details.

8.3 Failure of the Active Trunked GCP 8000 Site Controller

If the active site controller fails, and the standby site controller has a connection with the master site, then a site controller switchover occurs. During the switch over period, the standby site controller re-initializes and becomes the active site controller. Depending on the site preferences, Mobile Subscriber Units (MSUs) that are active on the site attempt to find an adjacent wide area site. MSUs register with the site and resumes the data services.

During the site controller switch over process, the system exhibits characteristics that are similar to SC-RNG, SC-BR, and SC-ZC link failures. The general sequence of activities during site controller failure is explained in the following:

1. The standby site controller detects the loss of the active site controller within 150 ms. The standby site controller begins sending TSP messages immediately after the switch over. The TSP contains new active site controller information.
2. Behavior for other devices in the system is similar to the behavior during an SC-RNG, SC-BR, and SC-ZC link failure.
3. The newly active site controller performs an initialization process (similar to the power-up initialization). During this initialization process, the base radios advertise that the site is in the local area mode. Depending on the site preferences, MSUs leave the site and search for a wide area site.

4 After the base radios receive the TSP messages from the newly active site controller, the base radios clean their database, but do not dekey. The base radios then begin to accept registration requests.

5 Adjacent sites broadcast that the site is in wide area mode. MSUs begin to register with the site. Any existing MSUs not registered with another site then begin another registration as the standby site controller and active site controller do not share databases. Holdoff timers (RRHOT and FRHOT) are used to prevent a large volume of MSUs from trying to register with the recovered site simultaneously.

8.4 Failure of Active and Standby GCP 8000 Site Controllers

If both the active and standby GCP 8000 Site Controllers fail, or if the active site controller fails and the standby is isolated from the system, the site controllers are inoperable and in failsoft mode. The MSUs leave the site and attempt to register with another site in wide area mode. In voice systems, the channels provide limited functionality and calls are made in failsoft mode.

The following are the general sequence of activities when both active and standby site controllers fail:

1 Channels detect the link failure within 500 ms (since TSP messages are not received from the site controllers). All the channels at the site dekey and the broadcast information ceases.

2 Behavior for other devices in the system is similar to the behavior during an SC-RNG, SC-BR, and SC-ZC link failure.

3 MSUs that are operating on the site scan through their adjacent site list and attempt to register with another site in wide area mode.

4 If one or both site controllers recover, the first site controller to recover initializes and becomes the active site controller. The base radios at the site then begin to accept registration requests and handle traffic after the site initialization has completed. Holdoff timers (RRHOT and FRHOT) are used to prevent a large volume of MSUs from trying to register with the recovered site simultaneously.

8.5 Geographically Redundant Configuration Site Controller Failure Scenarios

In the event both site controllers (SC1, SC2) fail at the primary prime site while the site is in Wide Area Trunking, the standby controller (SC3) at the secondary prime site becomes the active controller, and results in the loss of wide area operation for a brief period. The Zone Controller is still the call-processing controller for all existing calls.

Table 20: Geographically Redundant Configuration Site Controller Failure Scenarios

Type of Failure	Site Mode
Active controller fails at the primary prime site (SC1)	Standby site controller (SC2) at the primary prime site takes over, remains in wide area trunking.
Both site controllers fail at the primary prime site (SC1, SC2)	After a brief outage, the site controller at the secondary prime site (SC3) takes over and restores wide area trunking.
Active controller at the secondary prime site (SC3)	A Site Controller at the primary prime site (SC1 or SC2) activates if available and restore wide area.

Table continued…

Type of Failure	Site Mode
Active controller at the primary prime site (SC1) and LAN switch #1 fail	After a brief outage, wide area is restored after the site controller (SC3) and secondary prime site comparators go active.

8.6
Failure of the Conventional GCP 8000 Site Controller

Centralized Conventional Architecture

If the conventional site controller fails when the site is in the Wide Conventional mode, the use of conventional channel resources at the site continues. But, if the site controller fails in the Site Conventional mode or before the transition to Site Conventional mode, the conventional channel resources at the site stops operating.

Distributed Conventional Architecture and Conventional Master Site

If the conventional site controller fails when it is the active call controller in either type system, the subscriber radios may still be able to maintain communications using repeat functionality of the base radios or when the base radios are connected to a comparator. The repeat functionality of the comparators enable wide area repeat for subscribers.

8.7
Hold-Off Timers: CAHOT, FRHOT, and RRHOT

The GCP 8000 Site Controller uses several types of hold-off timers:

- CAHOT – Channel Access Hold-Off Timer. (Used only in HPD systems.) The CAHOT is used to determine how long an MSU holds off registering with the system, or performing a location update under failure conditions. The CAHOT value is one of the site controller parameters in the CSS.
- FRHOT – Failure Random Hold-Off Timer. The time value broadcasted by Wide Area sites next to a failed site. The MSU must wait a random time period up to a maximum of the FRHOT time before it registers to sites in Wide Area mode.
- RRHOT – Recovery Random Hold-Off Timer. The time value broadcasted by Wide Area sites next to a site that has recovered. The MSU is allowed to roam back to the recovered site in a random time period based on the RRHOT time.

When a site fails, the zone controller sends an FRHOT value > 0 to an adjacent site. The site controller compares the CAHOT value and FRHOT value, and broadcasts the larger of the two. If the default values for the hold-off timers are not changed, an MSU waits or holds off for as long as 16 minutes before resuming services. If multiple sites have failed, the FRHOT is 16 minutes per site. If the CAHOT value received is zero, then the MSU cannot run the Access Hold-off timer, but proceeds immediately with the registration message.

For HPD systems only:

- To set the CAHOT value, perform the following calculation: the number of MSUs in the system / 1666.7 mobility events per minute. The mobility events number is based on the ability of the zone controller to handle up to 100,000 mobility events per hour.
- For example, if the maximum number of MSUs in a system is 20,000, the hold-off timer is calculated as follows: 20,000 MSUs / 1666.7 mobility events per min = up to 11.9 minutes of hold-off per MSU.
- Another example is a system with 1000 MSUs. In this example, the calculation is: 1000 MSUs / 1666.7 mobility events per minute = .60 minutes or 1 minute. It is important that the CAHOT value is

calculated based on the actual number of users on the system. If the defaults are used, the length of the hold-off timer is excessive.

8.8 Motorola Solutions Support Center

Motorola Solutions Support Center (SSC) can help technicians and engineers resolve system problems, and ensure that warranty requirements are met. Check your contract for specific warranty information.

Motorola Solutions assigns a tracking ticket number that identifies each support call. This ticket number allows Motorola Solutions to track problems, resolutions, and activities for the call, and if possible, communicate the resolution and a status of call so that the SSC can note the resolution and close the ticket.

8.8.1 Information Necessary to Contact Motorola Solutions Support Center

Before calling the Motorola Solutions Support Center (SSC), log all steps taken to troubleshoot the problem and any results of those steps. The SSC can use this information to determine the appropriate support actions.

Listed is the following information to collect before calling the SSC:

- System ID number (such as 2CB5). Each zone in the system has a unique system ID number
- Location of the system
- Date the system was put into service
- Software and firmware versions
- Symptom or observation of the problem, such as:
  - When did it first appear?
  - Can it be reproduced?
  - Are there any other circumstances contributing to the problem (for example, loss of power)?
- Maintenance action preceding the problem, such as:
  - Upgrade of software or equipment
  - Changes to hardware or software configuration
  - Reload of software from a backup disk, CD, or DVD with the version and date

Dispatch Support:

- Site ID
- Description of problem
- Severity of issue

Tech Support:

- Site ID
- Billing information (If not being billed under contract)
- Name or model number of product causing the issue (Helps get you over to proper tech support group)

Return Authorization:

- Site ID
- Part Number and/or description of part
- How being billed
- Where it is being billed
- Where it is being shipped

8.8.2
Where to Call for Service

After collecting the required information and writing a detailed problem report, contact the Motorola Solutions Support Center (SSC) to help with the problem.

8.8.2.1
Motorola Solutions Support Center

The Motorola Solutions Support Center (SSC) is the primary Motorola Solutions contact. Call Motorola Solutions SSC:

- Before any software reload
- To confirm troubleshooting results and analysis before removing and replacing a Field Replaceable Unit (FRU) or Field Replaceable Equipment (FRE) to repair the system

Motorola Solutions SSC contact information:

- Phone: (800) 221-7144 for domestic calls and (302) 444–9800 for international calls
- Fax: (847) 725-4073

8.8.3
Subcontractors

The Motorola Solutions Service Subcontractor Assessment program ensures that service people Motorola Solutions contracts meet strict minimum requirements before they can work on any system. For more information on this program, contact the Motorola Solutions representative.

This page intentionally left blank.

Chapter 9

GCP 8000 Site Controller FRU/FRE Procedures

This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to the GCP 8000 Site Controller.

9.1 Required Tools and Equipment

The following items are necessary to bring to the replacement site when replacing any equipment:

- Electrostatic discharge (ESD) strap (Motorola Solutions part number RSX4015A, or equivalent)
- Service computer/laptop with Configuration/Service Software and Software Download Manager applications installed
- DB-9 Straight through serial cable
- Ethernet patch cable
- Crosstip and slotted screwdrivers
- TORX® driver set
- 1/2 drive torque wrench capable of torque settings to 110 in/lbs.

9.2 Field Replaceable Units (FRUs)

This section covers FRU kit numbers, part numbers, and procedures for replacing the FRUs.

9.2.1 GCP 8000 Site Controller FRU

Table 21: GCP 8000 Site Controller Field Replaceable Units

Component Type	FRU Kit Number	Replacement Procedure
GCP 8000 Site Controller module	DLN6966A	See Replacing the GCP 8000 Site Controller Module on page 136.
GCP 8000 Site Controller, Fan Assembly	DLN6898A	See Replacing the Fan Assembly on page 141.
GCP 8000 Site Controller Power Supply for DLN6966A	DLN6781A (0182516W14) or DLN6805A (0182516W20)	See Replacing the Power Supply on page 142.
GCP 8000 Site Controller Power Supply for DLN6569A	DLN6781A (0182516W14)	

9.2.2
Standalone GCP 8000 Site Controller Parts

Table 22: Standalone GCP 8000 Parts

GCP 8000 Part	Part Number	Replacement Procedure
GCP 8000 Site Controller Backplane	0180706H87	See Replacing a Standalone GCP 8000 Site Controller Backplane on page 144.
Power Supply Fan	5985167Y02	Order from North America Parts Organization at 800–422–4210 or the international number at 302–444–9842.

9.3
Replacing the GCP 8000 Site Controller Module

IMPORTANT: The site controller module can be hot swapped out without losing functionality. The standby site controller automatically becomes the active site controller and takes over if the active site controller is the one being swapped out.

Figure 46: GCP 8000 Site Controller Module

Prerequisites: Before replacing the site controller, pull configuration and hardware information from the site controller module into the Unified Network Configurator (UNC) by performing a “Pull All” procedure from the UNC. See the “Scheduling the Pull of Device Configurations” section in the *Unified Network Configurator* manual. This step may not be possible if communication is severed between the site controller and the UNC, or if the site controller is within a K core or non-networked site.

Procedure:

1. Wear an Electrostatic Discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout this procedure to prevent ESD damage to any components.

2. Locate the site controller module being replaced.
3. If the site controller module is non-operational, go to step 8.
4. Connect to the site controller Ethernet service port using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 99.
5. Save the site controller configuration to the laptop PC as follows:
   a. From the menu, select **File** → **Read Configuration From Device**.
   b. At the success message, click **OK**.

c From the menu, select **File** → **Save As**.

d On the **Properties** window, enter the ***<IP address>*** of the device. Click **OK**.

e Specify the directory location where you want to save the configuration file, type a meaningful name for the file. Press ENTER.

The site controller configuration is saved to the location indicated. The configuration file is reloaded later to the replacement site controller module.

6 For a trunked site controller, disable the site controller module, as follows:

a From the menu, select **Service** → **Status Panel Screen**.

The **Status Panel Screen** appears.

b Select the **Site Controller** tab.

c From the **User Requested Site Controller State** list box, select **User Disabled**.

The site controller module resets, after approximately two minutes, it is disabled. If this is the active site controller module, control of trunking switches over to the standby site controller module.

7 Disconnect the Ethernet cable from the service port on the site controller to be replaced.

8 Remove the fan assembly to gain access to the site controller module. See Replacing the Fan Assembly on page 141.

IMPORTANT: The site controller module can be swapped out without shutting the power off. The fan assembly, however, must be in place within a reasonable amount of time so the other site controller module does not overheat and shut down.

9 Label and disconnect any cabling on the front of the site controller module.

10 Loosen the two captive screws holding the site controller module to the chassis.

11 Using the handle, gently pull the used module straight out, along the guides on which it sits.

12 Slide in the replacement site controller module along the guiding rails until it is engaged. A slight push is needed to engage the module. For a replacement standalone site controller in a circuit simulcast subsystem, use the upper slot for the module. For a replacement standalone site controller in an IP simulcast subsystem, the site controller that has been assigned as site controller 1 must have the site controller module in the upper slot within the chassis, and the site controller that has been assigned as site controller 2 must have the site controller module in the lower slot within the chassis.

IMPORTANT: If the site controller module stops well before it is engaged, it is in an incorrect position. Either it is in the wrong slot or it is rotated 180 °. The module has a keying feature that prevents it from going all the way into an incorrect slot, or going into the correct slot but rotated 180 °. Do not try to force the module.

13 Secure the site controller module with the two captive screws.

14 Reconnect all the cabling to the correct ports as previously labeled.

15 Reinstall the fan assembly. See Replacing the Fan Assembly on page 141.

16 Perform basic device configuration through the serial port in Configuration/Service Software (CSS). See Connecting Through a Serial Port Link on page 96.

a Set the IP address of the device. Setting the Device IP Address in CSS on page 97.

b Set the serial security services. See Setting the Serial Security Services in CSS on page 98.

17 On systems with MAC Port Lockdown implemented, disable MAC Port Lockdown. The switch port where the colocated replacement device is connected to needs to be Unlocked before

connecting with CSS or performing a software download. See the *MAC Port Lockdown* manual for instructions on how to disable MAC Port Lockdown.

18 Open the Software Download Manager application, and perform the following:

CAUTION: Load the correct version of the software. A mismatch in software versions may occur when replacing the site controller module with an on-hand spare. A mismatch in software versions may cause a 'critical malfunction', or if when the site controller becomes active, it may bring the entire site into a configuration mode of operation. To exit base radios out of configuration mode, see CSS Procedures > Changing from Configuration to Normal Mode in the *CSS Online Help*.

a From the **Advanced Options** menu, select the transfer type.

b From the menu, select **File** → **File Manager**.

The Software Depot File Manager opens.

c From the menu, select **Component Operations** → **Import Fileset**.

The **Import a Fileset Into the Software Depot** dialog box appears.

d Click **Browse** and search for the `swdlv3.cfg` file, or follow the path `E:\swdl\swdlv1.cfg` or `swdlv3.cfg`. Click **Open**.

The file appears in the **Configuration File Path** field of the dialog box.

e Click **Generate**. Click **OK**.

The **Import a Fileset Into the Software Depot** dialog box closes and the software component appears in the **Components In the Software Depot** list of the **Software Depot File Manager** window.

f Exit the **Software Depot File Manager**.

19 For a conventional device, perform a single device software download to transfer and install the latest software using Software Download Manager as follows:

a Click **Open Single Device Mode**.

b Enter the ***<IP address>*** of the device and click **Connect**.

A **Security Level** screen appears.

c Choose the required security level. Click **OK**.

d In the **Select an Option** drop down list, select **Upgrade**.

e In the **Operations Type** drop down list, select **Transfer and Install**.

f In the **Application Type** drop down list, select the application to install.

g In the **Software Version** drop down list, select the appropriate software version.

h In the **Bank Selection** drop down list, select the bank to receive the software. Select **Automatic** to store the software in the bank that is more suitable for the device.

i Click **Start Operation**.

j In the window that appears, click **Proceed**

If the transfer was successful, the progress bar in the **Operation Status** tab displays green. If the transfer failed, the progress bar displays red.

20 Perform a site software download and installation for trunked ASTRO® 25 devices. See Performing a Site Download on page 156.

A site software download is not available for conventional devices.

CAUTION: It is crucial that a site software download is performed at the site to ensure that all devices are on the same software version, VLAN, and active bank. Failure to perform this step, results in the replacement site controller or base radios to have a mismatch in software versions. If a mismatch in software versions occurs, base radios may go into a configuration mode of operation with a reason of 'Invalid Software Version'.

21 Perform basic device configuration through the Ethernet port in Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 99.

a Set the current date and time. See Setting the Date and Time in CSS on page 102.

b Set up the local Password Configuration (optional). See Setting the Local Password Configuration in CSS on page 108.

An IP address must be configured to set up the local password. If the serial port access is not available to configure the IP address, the device may have the account locked out or the backplane slot has passwords enabled. Perform the following:

1 Move the device module to a different slot in the backplane where local passwords are not configured.

2 Configure the IP address and reset the device through the front panel RS-232 serial service port using CSS.

3 Perform the local password reset operation (to clear account information stored in the FRU) through and Ethernet port link using CSS.

4 Move the device module back to the original slot.

5 Perform the local password reset operation again (to clear account information stored in the backplane).

22 Complete the configuration of the Information Assurance features, as follows:

a Configure the SNMPv3 configuration and user credentials. See Changing SNMPv3 Configuration and User Credentials in CSS on page 103.

b Create, update, or delete an SNMPv3 user. See Adding or Modifying an SNMPv3 User in CSS on page 105.

c Verify the SNMPv3 credentials. See Performing an SNMPv3 Connection Verification in CSS on page 106.

d Set the SWDL transfer mode. See Setting the SWDL Transfer Mode in CSS on page 107.

e For a trunked site controller, configure DNS. See Chapter 7, "Configuring DNS with CSS" in the *Authentication Services* manual.

f Configure for SSH. See Chapter 4, "Configuring SSH for Devices at an RF Site" in the *Securing Protocols with SSH* manual or see "Device Security Configuration – Remote Access/Login Banner (Ethernet)" in the *CSS Online Help*.

g Restore the following Clear Protocols parameters in the Remote Access Configuration tab on the Device Security Configuration screen in CSS. See "Device Security Configuration – Remote Access/Login Banner (Ethernet)" in the *CSS Online Help*

h Enable RADIUS Authentication. See Chapter 7, "Configuring RADIUS Sources and Parameters with CSS" in the *Authentication Services* manual.

i Enable Centralized Authentication. See Chapter 7, "Enabling/Disabling Centralized Authentication with CSS" in the *Authentication Services* manual.

j Set the Local Cache Size for Centralized Authentication. See Chapter 7, "Setting the Local Cache Size for Central Authentication with CSS" in the *Authentication Services* manual.

k Enable Centralized Event Logging (if required by your organization). See Chapter 6, "Enabling/Disabling Centralized Event Logging on Devices with CSS" and Chapter 1, "Event

Logging Client Configuration" for proper hostnames in the *Centralized Event Logging* manual.

23 From CSS, restore the Codeplug Archive from backup. Reload the configuration into the replacement site controller module as follows:

a From the menu, select **File** → **Open**.

NOTICE: For comparator: If you were not able to back up the configuration from the previous comparator module, you can use the configuration from your system build book or use the default configuration file for the comparator module. Specific settings for the comparator module must still be configured. See the *CSS Online Help* for detailed configuration instructions.
For site controller: If you were not able to back up the configuration from the previous site controller module, you can use the configuration from your system build book, the default configuration file for the site controller module, the stored backup configuration file, or the configuration from the other site controller module. Specific settings for the site controller module must still be configured. See the *CSS Online Help* for site controller detailed configuration instructions.

b Locate and open the previously saved configuration file for the device.

c On the **Properties** window, click **OK**.

d When the **Progress Monitor** screen is complete, click **OK**.

e From the menu, select **File** → **Write Configuration To Device**. Click **OK**.

f On the Ethernet connection confirmation screen, click **OK**.

g On the **Connection** screen, enter the ***<IP Address>*** and click **Connect**.

h On the **SNMPv3 PassPhrase Prompt** dialog box, enter the **User Information** and **Passphrase Information**. Click **OK**. If Authentication Services are not enabled on a device, click **OK** when the dialog box appears.

i On the confirmation screen, click **OK**.

j When the **Progress Monitor** screen is complete, click **OK**.

The configuration from the file selected is loaded into the new site controller module.

24 Read the site controller, as follows:

a From the menu, select **File** → **Read Configuration From Device**.

b On the Confirmation screen, click **OK**.

c When the **Progress Monitor** screen is completed, click **OK**.

25 For a trunked site controller, enable the site controller module as follows:

a From the menu, select **Service** → **Status Panel Screen**.

The **Status Panel Screen** appears.

b Select the **Site Controller** tab.

c From the **User Requested Site Controller State** list box, select **Enabled**.

The site controller module is enabled after approximately two minutes.

26 Restore the 802.1x / MAC Port Lockdown feature as follows:

NOTICE: Substeps a, b, c apply only to HPD and repeater site configurations.

a Capture the MAC address on the switch for all devices connected to the site controller. See "Capturing the MAC Address of a Device Connected to a GCP 8000" in the *MAC Port Lockdown* manual.

b Update/verify the site controller MAC Port Lockdown Configuration. See Chapter 6, "Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 in CSS" and “Validating MAC Port Lockdown on a GCP 8000 or GPB 8000” in the *MAC Port Lockdown* manual.

c Update/verify the site controller 802.1x configuration on HPD and repeater site controllers. See "Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 in CSS" in the *802.1x Service Ports on Switches* manual.

NOTICE: Substep d can only be performed through VoyenceControl. It cannot be performed in CSS.

d (Optional), Enable the site controller 802.1x configuration on the Ethernet port for the simulcast site controller or conventional site controller devices. See "Enabling/Disabling 802.1x on a GCP 8000 Ethernet Service Port in VoyenceControl" in the *802.1x Service Ports on Switches* manual.

27 Replace the site controller in the Unified Network Configurator (UNC). See Chapter 4, “Replacing a Device” in the *Unified Network Configurator* manual.

28 Discover the site controller in the UEM, see the *Unified Event Manager* manual.

29 Verify that the site controller module is operating properly:

- The Link Status LED for the RJ-45 Service port on the front of the new site controller module is green.
- The Status LED on the front of the site controller is green.
- Use software tools, such as UEM and CSS, to verify the status of the equipment.

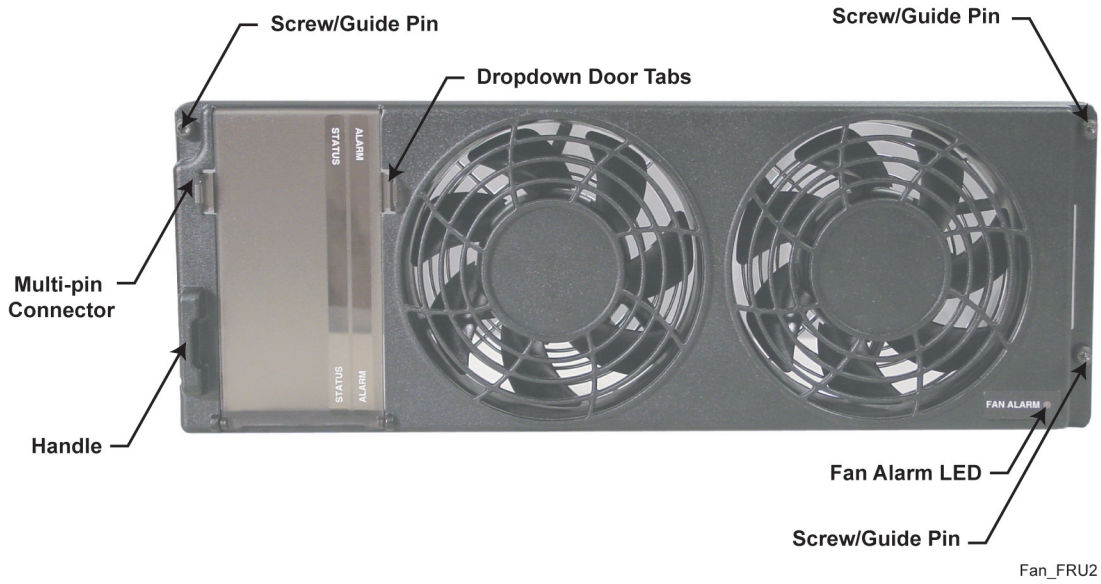
9.4 Replacing the Fan Assembly

WARNING: When removing a fan module, care should be taken to avoid contacting moving fan blades before and after removal with tools, hands, or other objects. If you are removing the fan module to access or replace the modules behind it, turn off the equipment power and allow the modules to cool before performing any work, as the surfaces of the modules can be extremely hot.

CAUTION: To prevent overheating, this fan must be in place at all times, except during servicing.

IMPORTANT: The fan assembly can be swapped out without shutting the power off. The replacement fan assembly must be in place within a reasonable amount of time so that the device module does not overheat and shut down.

Figure 47: Fan Assembly



When and where to use: Use this procedure to remove the fan module to replace the modules it covers.

Procedure:

1. Wear an Electrostatic Discharge (ESD) wrist strap and connect its cable to a verified good ground.

   CAUTION: Wear the ESD strap throughout this procedure to prevent ESD damage to any components.

2. Using a T20 bit, loosen the three captive screws on the front of the fan assembly, so they disengage from the chassis.
3. Using the handle on one end and the edge on the other side, gently pull the fan assembly straight out to disengage the connector.
4. Using the guide pins and the connector on the back of the new fan assembly, push the new fan assembly into place until it feels secured.
5. Using a T20 Bit, tighten the three captive screws on the front of the fan assembly. Torque to 17 ± 2 in-lb.
6. Verify that the fan assembly is operating properly, and the Fan Alarm LED is off. Use software tools such as Unified Event Manager (UEM) or Configuration/Service Software (CSS) to verify the status of the equipment.

9.5 Replacing the Power Supply

WARNING: The power supply module contains dangerous voltages that can cause electrical shock to people or damage to equipment.

IMPORTANT: The power supply can be swapped out without shutting the power off if the site controller is located in a GTR 8000 Expandable Site Subsystem and is connected to the Auxiliary Power input from a colocated GTR 8000 Base Radio. Otherwise, the site controller must be disabled and the power must be shut off before replacing it.

Figure 48: Power Supply

Procedure:

1. Wear an Electrostatic Discharge (ESD) wrist 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. If the power supply is within a standalone chassis, disable the site controller module(s) as follows:
   a. Connect to the site controller module Ethernet service port using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 99.
   b. From the menu, select **Service** → **Status Panel Screen**.

      The **Status Panel Screens** window appears.
   c. Select the **Site Controller** tab.
   d. In the **User Requested Site Controller State** list box, select **User Disabled**.

      The site controller module resets, and after approximately two minutes becomes disabled. In a redundant configuration, if this is the active site controller module, control switches over to the standby site controller module.
   e. Repeat substeps a through d if the other site controller module is within the same chassis.
3. Push the power button to Off on the power supply unit.
4. Using a T20 bit, loosen the two captive screws on the front of the power supply, so that they disengage from the chassis.

   WARNING: Let the power supply module cool before performing the following step, which exposes surfaces of the module that can be extremely hot.
5. Pull on the metal handle to disengage the power supply from the backplane, and remove it completely from the chassis.
6. Slide the replacement power supply module into place, pushing gently until it seats.
7. Using a T20, bit tighten the two captive screws.
8. Turn **On** the power button, and verify that the power supply is operating properly.

- The power supply Status LED is green.
- The power supply Alarm LED is off.
- The power supply Fan LED is off.
- Use software tools, such as Unified Event Manager, to check the alarms of the equipment.

9 Enable the site controller module(s) as follows:

a Connect to the site controller module Ethernet service port using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 99.

b From the menu, select **Service** → **Service Panel Screen**.

The **Service Panel Screens** window appears.

c Select the **Site Controller** tab.

d In the **User Requested Site Controller State** list box, select **Enabled**.

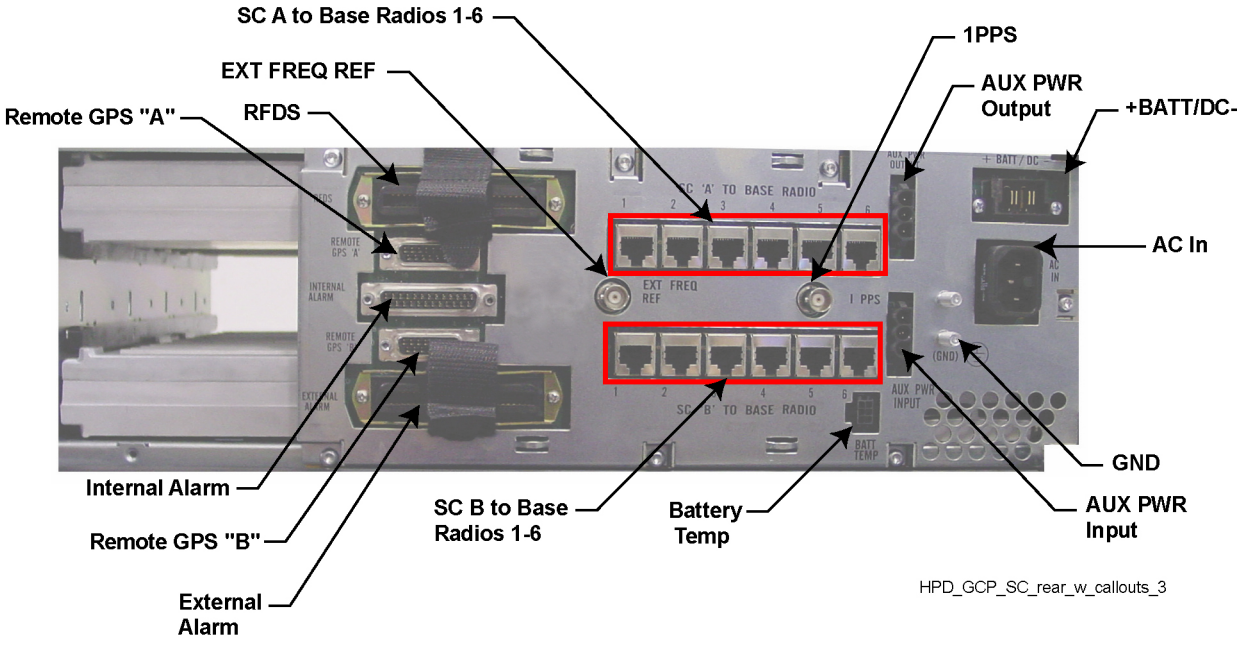
The site controller module is enabled after approximately two minutes.

e Repeat substeps a through d if the other site controller module is within the same chassis.

9.6 Replacing a Standalone GCP 8000 Site Controller Backplane

In a standalone GCP 8000 Site Controller, the backplane is the circuit board at the rear of the card cage, which connects the power supply and site controller modules.

Figure 49: GCP 8000 Site Controller Connections to Backplane Through Backplane Cover



NOTICE: The procedure assumes the following service access clearances:

- At least 2 ft access at the rear of the cabinet or rack, or

- At least 2 ft access on one side of the cabinet or rack, and at least 6 in. at the rear of the cabinet or rack

Procedure:

1. Wear an Electrostatic Discharge (ESD) strap and connect its cable to a verified good ground.

   CAUTION: Wear this ESD strap throughout this procedure to prevent ESD damage to any components.

2. If the site controller modules are not operational, skip to step 5.
3. For a trunked site controller, disable the site controller module as follows:
   a. Connect to the site controller module Ethernet service port using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 99.

      NOTICE: If all unused ports on the LAN switch are disabled, enable the desired port. See the *System LAN Switches* manual.

   b. From the menu, select **Service** → **Status Panel Screen**.

      The **Status Panel Screens** window appears.

   c. Select the **Site Controller** tab.
   d. In the **User Requested Site Controller State** list box, select **User Disabled**.

      The site controller module resets, and, after approximately two minutes, becomes disabled. In a redundant configuration, if this is the active site controller module, control switches over to the standby site controller module.

   e. Repeat substeps a through d if the other site controller module is within the same chassis.
4. Disconnect the Ethernet cable from the service port on the site controller module.
5. Push the power rocker switch to Off (O) on the power supply unit.
6. Label, then disconnect all cables from the site controller backplane.
7. Remove the power supply module from the chassis as follows:

   WARNING: Allow the power supply module to cool before performing the following step, which exposes surfaces of the module that can be extremely hot.

   a. Using a T20 bit, loosen the two captive screws on the front of the power supply, so that they disengage from the chassis.
   b. Pull on the metal handle to disengage the power supply module from the backplane, and remove it completely from the chassis.
8. Remove the fan assembly to gain access to the site controller modules. See Replacing the Fan Assembly on page 141.
9. Disengage the site controller modules from the backplane as follows:
   a. Using a T20 bit, loosen the two captive screws on the front of each module, so that they disengage from the chassis.
   b. Using their handles, gently pull the modules until they disengage from the backplane.
10. Remove the fan cable from the backplane, accessing it from the front of the chassis, with the backplane still secured to the chassis, as follows:
    a. Follow the fan cable with your hand from its connector at the front of the chassis to its connection to the backplane, through the card–cage section from which you removed the power supply module.
    b. Remove the fan cable multi-pin connector from the backplane.

NOTICE: Squeeze the top and bottom of the connector and pull the connector straight out from the backplane.

11 Using a T20 bit, remove the seven screws that secure the metal backplane cover and the backplane circuit board to the rear of the site controller chassis.

12 Remove the metal backplane cover and the backplane circuit board.

13 Place the new backplane circuit board in the same location and orientation as the one that you removed.

14 Seat the seven screws, previously removed, into the backplane circuit board and backplane cover. Start all screws before fully securing them.

15 Secure the new backplane circuit board and the backplane cover to the rear of the site controller chassis with the seven screws. Torque to 18 +/- 2 in.-lb.

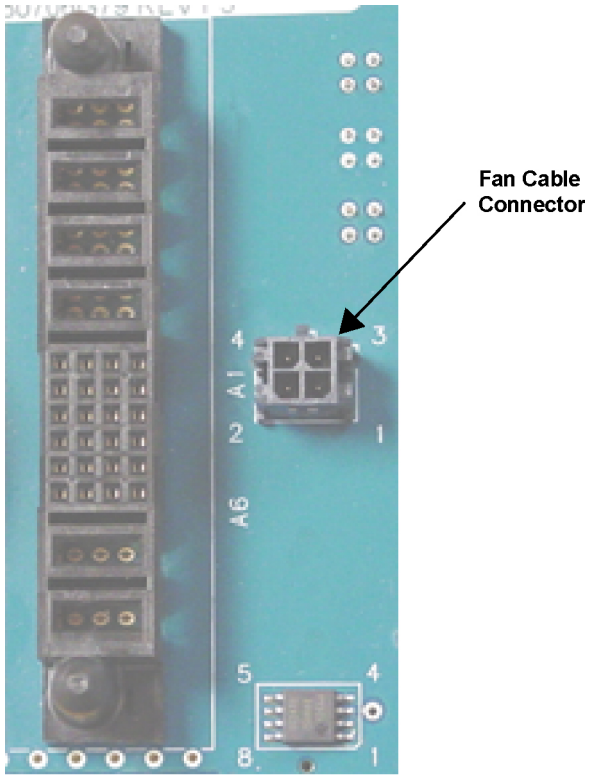
16 Connect the fan cable to the new backplane from the front of the chassis with the backplane secured to the chassis, as follows:

a Locate the port in the new backplane for the fan cable multi-pin connector.

b Follow the fan cable with your hand from its connector at the front of the chassis to the connector at the other end of the cable.

c Push the fan cable multi-pin connector, with the tab up, into the correct location in the backplane.

Figure 50: Fan Cable Connector



GTR_GCP_Fan_Cable_Connector

17 Slide the site controller modules into the new backplane. A slight push may be needed to engage the modules.

18 Secure the site controller modules to the chassis with the two captive screws on the front of each module.

19 Reinstall the fan assembly unit. See Replacing the Fan Assembly on page 141.

20 Slide the power supply into the chassis, pushing gently until it seats in the new backplane.

21 Tighten the two captive screws on the front of the power supply.

22 Reconnect all cables at the rear of the site controller.

23 Set the power supply rocker switch to On (1).

24 Enable the site controllers modules as follows:

a Connect to the site controller module Ethernet service port using Configuration/Service Software (CSS). See Connecting Through an Ethernet Port Link on page 99.

b From the menu, select **Service** → **Service Panel Screen**.

The **Service Panel Screens** window appears.

c Select the **Site Controller** tab.

d In the **User Requested Site Controller State** list box, select **Enabled**.

The site controller module is enabled after approximately two minutes.

e Repeat substeps a through d if the other site controller module is within the same chassis.

25 Disconnect the laptop PC from the site controller module.

26 Verify that the LEDs indicate the modules you removed and reinstalled are operational.

- The Status LEDs are green.
- The Alarm LEDs are off.
- The power supply Fan LED is off.

27 Verify proper operation using software tools, such as Unified Event Manager, and Configuration/Service Software (CSS).

28 Re-configure the Security Settings into the Backplane. See Setting the Serial Security Services in CSS on page 98.

This page intentionally left blank.

Chapter 10

GCP 8000 Site Controller Reference

This chapter contains supplemental reference information relating to GCP 8000 Site Controller.

10.1 Reset Button

The GCP 8000 Site Controller has a Reset button on the extended area on the front of the device. Each site controller module has its own RESET button.

The **RESET** button is used to reboot the device. Pressing the button for more than 3 seconds, results in a reset or reboot of the module. The button is set into the chassis, so it is difficult to accidentally engage.

10.2 GCP 8000 Site Controller LEDs

Green LEDs indicate that the device is fine. Yellow warns of a potential problem that requires attention, though not an immediate issue. Red is indicative of a problem requiring immediate attention.

LED colors and states in order of severity:

Green
Good/active

Green Flashing
Good, in progress, standby

Yellow
Warning

Yellow Flashing
Minor fault

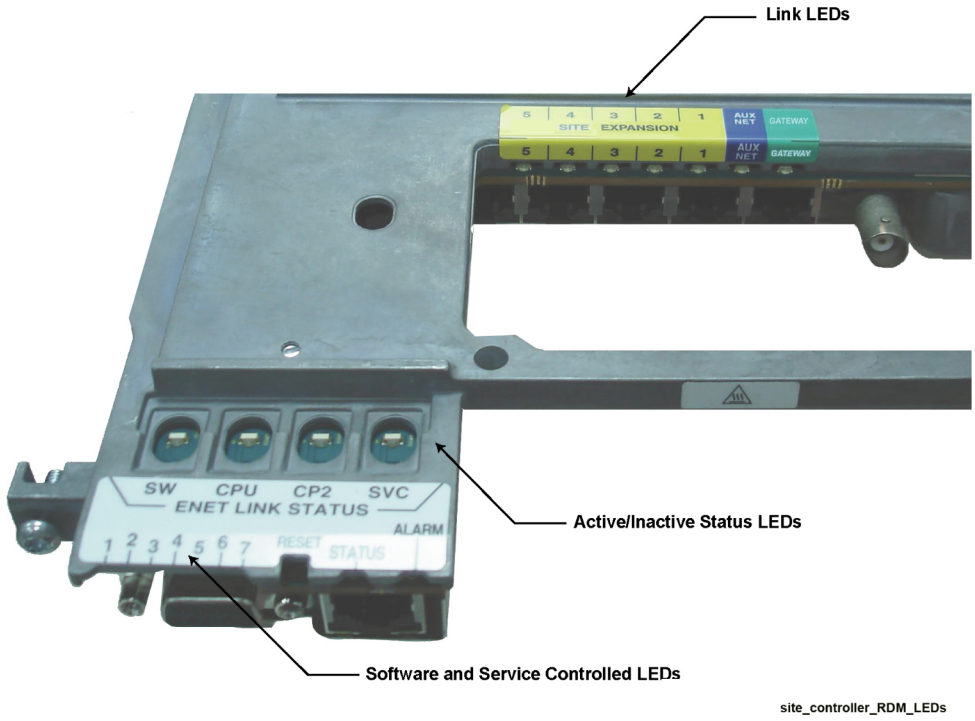
Red Flashing
Major fault

Red
Critical

10.2.1 GCP 8000 Site Controller Software and Services-Controlled LEDs

Software and Services-Controlled LEDs are visible on the front of a GCP 8000 Site Controller with the service door open.

Figure 51: GCP 8000 Site Controller – Software and Services-Controlled LEDs



10.2.1.1

GCP 8000 Site Controller Software-Controlled LEDs

NOTICE: The trunking and ZC Link LEDs are only valid if the GCP 8000 Site Controller is the active or standby site controller in a fully Enabled state. In a Disabled or Critical Malfunction (CR Malf) state, the LEDs are off. A site controller in one of these states does not know the state of the site nor does it try to communicate with the zone controller.

Table 23: Trunked GCP 8000 Site Controller Software-Controlled LEDs

LED	Application Use	Green On	Green Blinking	Yellow On	Yellow Blinking	Red Blinking	Red On	Off
1	SC state	Active	Standby	Disabled (User Req)			CR Malf (includes VV failure for SWDL)	
2	RNG link	Link Up				Establishing link with RNG		CR Malf or Disabled state, standby, data unconfigured

Table continued…

LED	Application Use	Green On	Green Blinking	Yellow On	Yellow Blinking	Red Blinking	Red On	Off
3	Trunking State	Wide Area		Site Off		Local area (site trunking)	Failsoft (IV&D only)	CR Malf or disabled state, standby
4	ZC Link	Active	Standby				Down	CR Malf or Disabled state

Table 24: Conventional GCP 8000 Site Controller Software-Controlled LEDs

LED	Application Use	Green On	Green Blinking	Yellow On	Yellow Blinking	Red Blinking	Red On	Off
1	SC state	Enabled		Disabled (User Req)			CR Malf	
2	Unused							Unused
3	Unused							Unused
4	Unused							Unused

10.2.1.2

GCP 8000 Site Controller Services-Controlled LEDs

NOTICE: The hardware controls LED 7, the Hardware Active LED. When active, it indicates that the site controller has ownership of the site controller shared external interfaces.

Table 25: GCP 8000 Site Controller Services-Controlled LEDs

LED	Services Use	Green On	Green Blinking	Yellow On	Yellow Blinking	Red Blinking	Red On	Off
5	SWDL/ VLAN		Version validation or auto-VLAN detection	SWDL with common VLAN	SWDL with split VLAN		Not in SWDL with split VLAN	Not in SWDL with Common VLAN
6	Local hardware failure (all hardware including GNSS)			Warning (such as fan unplugged)	Minor hardware failure	Major hardware failure	Critical hardware failure (such as inoperable fans or switch failure)	Good – no faults
7	Hardware Active	Active						Inactive

10.2.2

GCP 8000 Site Controller Status and Alarm LEDs

The status and alarm LED assignment for the GCP 8000 Site Controller are shown and definitions for each status follow the assignment table.

Table 26: GCP 8000 Site Controller Status and Alarm LED Assignment

LED	No Power	Lamp Test	Failure	Impaired	Booting Up	Online
Status LED (green)	Off	On	Off	On	Flash	On
Alarm LED (red)	Off	On	On	Flash	Off	Off

Table 27: GCP 8000 Site Controller Status/Alarm LEDs Definitions

Status	Definitions
No Power	The device is currently without power, both primary power and auxiliary power. The No Power state tells the service technician that there is a fundamental problem.
Lamp Test	The Lamp Test state is used to verify if the indicators are operational.
Booting Up	The Booting Up state indicates that the device is booting or is undergoing diagnostics and is not yet ready to place into service. Even though no failure or impairment is identified, the device is not ready to place into service.
Online	The site controller is fully operational, whether in Active or Standby mode. The Online state is used to indicate that the site controller is fully operational. It may be in a Standby mode or In service. The Online state indicates that the site controller should not be removed as it is possibly involved in active calls. The Standby mode is included in this state, it is important that a field technician should not remove a standby site controller without first informing the system of what he is about to do. This keeps the system from switching over to the standby site controller as it is pulled from the frame.
Impaired	The site controller is not fully operational due to internal or external causes. Some corrective action must be taken to return to 100% functionality. The impaired state also indicates that the current state does not equal the User Requested State of the site. For example, a site in the Site Trunking state due to the diagnostic state from the Network Manager has the Online state. If the site is staying out of Wide Trunking due to a reason other than the User Requested State, such as zone controller Link failure, the Impaired LED is lit. The device state, Enabled/Disabled, is always User Requested. Therefore, the Impaired LED is not shown for this state.
Failure	This status indicates a failure that is fixed only through replacement. If something other than a hardware fault is causing the state, the status is Impaired.

If both site controllers are disabled, one site controller still provides the site reference to the base radios, so the channels can maintain failsoft functionality.

10.2.3

GCP 8000 Site Controller Active/Inactive Status LEDs

The four active/inactive status LEDs are found on the top of the service port area of each site controller module. They are visible by opening the service door.

Table 28: GCP 8000 Site Controller Active/Inactive Status LEDs

Active/Inactive LEDs	Description
SW	Status of connection between the active site controller and the standby site controller.
CPU	Status of connection between the active CPU and the stand-by site controller.
CP2	Status of connection between the site controller and the base radio
SVC	Status of connection between the site controller and the service computer/laptop.

Table 29: GCP 8000 Site Controller Active/Inactive LEDs

Information State	Link Status LED
Link Inactive	Off
Link Established (assumes no activity)	Green
Link Active	Yellow or Amber

10.2.4

GCP 8000 Site Controller Link LEDs

The Link LEDs include the LEDs associated with the service port, site controller expansion ports, Net AUX port, and the gateway port.

Table 30: GCP 8000 Site Controller Link LEDs

LED	Link Inactive	Link Established (assumes no activity)	Link Active
Activity LED (yellow/amber)	Off	Off	Yellow/Amber - constant
Link LED (green)	Off	Green - constant	Green - constant

10.2.5

GCP 8000 Site Controller Power Supply LEDs

The POWER switch on the front of the power supply is used to enable or disable the DC outputs of the power supply for the GCP 8000 Site Controller.

The power supply has three LEDs, which provide a visual image of the operating condition of the power supply.

Table 31: GCP 8000 Site Controller Power Supply LEDs

LED	Explanation
Alarm	Red LED: When illuminated, it indicates the power supply is no longer operating within its design specifications.
Status	Green LED: When illuminated, it indicates the power supply is operating within its design specifications.
Fan	Red LED: When illuminated, it indicates the fan for the power supply is no longer functioning as per its design specifications.

10.2.6
GCP 8000 Site Controller Fan Assembly LED

The fan assembly has one LED, the Fan Alarm, on the front in the corner. The LED provides a visual image of the operating condition of the fan assembly.

Table 32: GCP 8000 Site Controller Fan Assembly LED

LED color	Explanation of State
Off	Operational, or Off
Red (constant)	Failure

Chapter 11

GCP 8000 Site Controller Disaster Recovery

This chapter provides references and information that will enable you to recover a GCP 8000 Site Controller in the event of failure.

11.1 Recovering the GCP 8000 Site Controller

When and where to use:
Follow this procedure to recover the GCP 8000 Site Controller.

Procedure:

1. To replace, install, connect power, and cable the site controller, see GCP 8000 Site Controller Hardware Installation on page 58.
2. To replace the site controller module only, see Replacing the GCP 8000 Site Controller Module on page 136 and follow steps 1 through 15.
3. To replace other hardware devices within the chassis, see GCP 8000 Site Controller FRU/FRE Procedures on page 135.
4. To perform basic device configuration and SWDL download, see Replacing the GCP 8000 Site Controller Module on page 136 and follow steps 16 through 29.

11.2 Performing a Single Device Download

Procedure:

1. Connect an Ethernet straight through cable between the Ethernet port on the service computer/ laptop and the Ethernet service port on the site controller or appropriate LAN switch. See Connecting Through an Ethernet Port Link on page 99.
2. Open the Software Download Manager application.

   CAUTION: Load the correct version of the software. There is a possibility of a mismatch in software versions when replacing the transceiver module with an on-hand spare. If a mismatch in software versions occurs, this mismatch may cause the base radio at the site to go into a configuration mode of operation with a reason of 'Invalid Software Version'. To exit out of configuration mode, see “CSS Procedures > Changing from Configuration to Normal Mode” in the *CSS Online Help*.
   If a mismatch in software versions occurs with a site controller, this mismatch may cause a 'critical malfunction', or if it becomes active, to bring the entire site into a configuration mode of operation.
3. Download and install the necessary software onto the site controllers and devices as follows:
   a. From the menu, select **File** → **File Manager**.

      The Software Depot File Manager opens.

b From the menu, select **Component Operations** → **Import Fileset**.

The **Import a Fileset Into the Software Depot** dialog box appears.

c Click **Browse** and search for the `swdlv3.cfg` file, or follow the path `E:\swdl\swdlv1.cfg` or `swdlv3.cfg`. Click **Open**.

NOTICE: Choose the `swdlv1.cfg` file if STR 3000, QUANTAR®, or ASTRO-TAC® 9600 devices are mixed with G-Series devices at a site.

The file appears in the **Configuration File Path** field of the dialog box.

d Click **Generate**. Click **OK**.

The **Import a Fileset Into the Software Depot** dialog box closes and the software component appears in the **Components In the Software Depot** list of the **Software Depot File Manager** window.

e Exit the **Software Depot File Manager**.

f From Software Download Manager, click **Open Single Device Mode**.

g Enter the ***<IP address>*** of the device and click **Connect**.

A **Security Level** screen appears.

h Choose the required security level. Click **OK**.

i In the **Select an option** window, select **Upgrade**.

j In the **Operations Type** drop down list, select **Transfer and Install** .

k In the **Application Type** drop down list, select the application to install.

l In the **Software Version** drop down list, select the appropriate software version.

m In the **Bank Selection** drop down list, select the bank to receive the software. Select **Automatic** to store the software in the bank that is more suitable for the device.

n Click **Start Operation**.

o In the window that appears, click **Proceed**.

If the transfer was successful, the progress bar in the **Operation Status** tab displays green. If the transfer failed, the progress bar displays red.

11.3 Performing a Site Download

Procedure:

1. Connect an Ethernet straight through cable between the Ethernet port on the service computer/ laptop and the Ethernet service port on the site controller or appropriate LAN switch. See Connecting Through an Ethernet Port Link on page 99.
2. Open the Software Download Manager application.

CAUTION: Load the correct version of the software. There is a possibility of a mismatch in software versions when replacing the transceiver module with an on-hand spare. If a mismatch in software versions occurs, this mismatch may cause the base radio at the site to go into a configuration mode of operation with a reason of 'Invalid Software Version'. To exit out of configuration mode, see “Changing from Configuration to Normal Mode” procedure in the *CSS Online Help*.
If a mismatch in software versions occurs with a site controller, this mismatch may cause a 'critical malfunction', or if it becomes active, to bring the entire site into a configuration mode of operation.

3 From the **Advanced Options** menu, select the transfer type.

4 For a **trunked site controller**, download and install the necessary software onto the site controllers and devices as follows:

a From the menu, select **Action** and choose one of the following:

- **Use DNS Server:** This is the default option and is recommended for most cases.
- **Use Standard ASTRO IPs (non-Tsub):** Legacy option which relies upon a built-in IP Plan rather than the DNS Server. This option is not supported for Trunking Subsystems (Tsubs).
- **DNS Override:** Use when running the Software Download Manager from a server that is not joined to the ASTRO® 25 system domain. In order to use a DNS server in the ASTRO® 25 system domain, the **Override DNS Server** dialog box is used to specify the DNS server IP address (defaults to the ASTRO® 25 system level DNS server).
- **Load DNS File:** Use only in situations where a custom DNS configuration file has been provided. Typically, this option is selected when the site IP addresses are not configured to be part of an ASTRO® 25 system.

b From the menu, select **File** → **File Manager**.

The **Software Depot File Manager** opens.

c From the menu, select **Component Operation** → **Import Fileset**.

The **Import a Fileset Into the Software Depot** dialog box appears.

d Click **Browse** and search for the `swdlv3.cfg` file, or follow the path `E:\swdl\swdlv1.cfg` or `swdlv3.cfg`. Click **Open**.

NOTICE: Choose the **swdlv1.cfg** file if STR 3000, QUANTAR®, or ASTRO-TAC® 9600 devices are mixed with G-Series devices at a site.

The file appears in the **Configuration File Path** field of the dialog box.

e Click **Generate**. Click **OK**.

The **Import a Fileset Into the Software Depot** dialog box closes and the software component appears in the **Components In the Software Depot** list of the **Software Depot File Manager** window.

f Exit the **Software Depot File Manager**.

g From Software Download Manager, click **Open Site Mode**.

h In the **ASTRO 25 Site Type**, select the type of site.

i Select the **Zone**, **Site**, and if applicable, the **Subsite**. The Subsite ID is only available when the Site ID is between 1-64.

j Click **Connect**.

k If the device supports SNMPv3 protocol, a pop-up window appears with the security level option. Choose the required security level. Click **OK**.

NOTICE: Depending on the size of the system, the window takes a few minutes to update.
If the Ethernet connection to the site uses the Site Controller Service Port, you might need to enter an 802.1x login account to connect to the SC Service Port. An 802.1x account is a centrally managed account.

The system connects to the specified zone and site.

l If this is a simulcast site, from the **Site View** tab, click the icon in the front of **Prime LAN** folder and **Subsite** folders.

The entries under the **Running Version** column display the current version. The **VLAN** column displays the VLANs for all devices.

m In the **Operation Type**, select **Transfer and Install**.

n In the **Application Type**, select one of the following:

- For an HPD site: select both **HPD Site Controller** and **HPD Base Radio**.
- For a Repeater site: select both **Repeater Site Controller** and **Site Repeater**.
- For a Simulcast site: select both **Multisite Site Controller** and **Multisite Base Radio**.
- For a simulcast site with a GPB 8000 Reference Distribution Module: select **Multisite Base Radio**, and **Reference Distribution Module**

o In the **Software Component** drop-down list, select the version for each site type.

NOTICE: Both the site controller and base radio software must be chosen as part of the site software download.

p In the **Simultaneous Channels Install** drop down list, select the number of the channels to install simultaneously.

Software Download Manager always installed all channels. For example, setting the **Simultaneous Channels Install** field to a specific number value means that those amount of channels are installed simultaneously.

NOTICE: The **Simultaneous Channels Install** field decreases the installation time. A warning is displayed if the site goes into failsoft, due to this setting.

q Click **Start Operation**.

NOTICE: If the **Start Operation** button is grayed out, SWDL has determined that there is a problem performing this operation to the selected devices. The button becomes active, when the appropriate operation set details are selected.
If a fileset is damaged, the Transfer operation stops. Import a correct fileset and repeat the operation.

r In the window that appears, click **Proceed**.

The Transfer operation begins first. After the transfer is successfully completed, SWDL begins the Install operation.

If the install was successful, the **Operation Status** bar displays green. If the install failed, the **Operation Status** bar displays red.

s Verify that the selected devices have installed the desired version of software.

NOTICE: After installation, the new software version is present in the **Running Version** column. If the new version is not present, it indicates a problem.
For more information, consult the “Fixing a Transfer Failure” section of the Software Download Manager manual.

In many cases, a second attempt at transferring the software corrects the failure. If further attempts continue to fail, contact System Support.

This page intentionally left blank.