System Release 7.13

ASTRO® 25
INTEGRATED VOICE AND DATA

HPD – GTR 8000 SITE SUBSYSTEM

July 2013

6871022P89-B

Copyrights

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 contact for further information.

Trademarks

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.

Document History

Version	Description	Date
6871022P89–A	Original release of the *HPD – GTR 8000 Site Subsystem* manual.	November 2012
6871022P89–B	Second release of the *HPD – GTR 8000 Site Subsystem* manual.	July 2013

Contents

List of Figures

List of Tables

List of Processes

List of Procedures

About This Manual

This manual provides descriptive and procedural information on the GTR 8000 Site Subsystem. Included in the manual are descriptions of the components of the GTR 8000 Site Subsystem and their function, specifications for the various configurations, and procedures on installation, configuration, optimization, operation, troubleshooting, and FRU/FRE replacement. Finally, a reference section provides information on LED indicators and RFDS equipment specifications.

This manual is intended for technicians and system operators as a resource for understanding and installing the GTR 8000 Site Subsystem, after they have attended the Motorola formal High Performance Data training. The manual should be used 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:

- Chapter 1 GTR 8000 Site Subsystem Description. This chapter provides a high-level description of GTR 8000 Site Subsystem and the function it serves on your system.
- Chapter 2 GTR 8000 Site Subsystem Theory of Operations. This chapter explains how the GTR 8000 Site Subsystem works in the context of your system.
- Chapter 3 GTR 8000 Site Subsystem Installation. This chapter details installation procedures relating to the GTR 8000 Site Subsystem.
- Chapter 4 GTR 8000 Site Subsystem Configuration. This chapter details configuration procedures relating to GTR 8000 Site Subsystem.
- Chapter 5 GTR 8000 Site Subsystem Optimization. This chapter contains optimization procedures and recommended settings relating to GTR 8000 Site Subsystem.
- Chapter 6 GTR 8000 Site Subsystem Maintenance. This chapter describes periodic maintenance procedures relating to GTR 8000 Site Subsystem.
- Chapter 7 GTR 8000 Site Subsystem Operation. This chapter details tasks that you perform once the GTR 8000 Site Subsystem is installed and operational on your system.
- Chapter 8 GTR 8000 Site Subsystem Troubleshooting. This chapter provides fault management and troubleshooting information relating to GTR 8000 Site Subsystem.
- Chapter 9 GTR 8000 Site Subsystem FRU Procedures. This chapter lists the Field Replaceable Units (FRUs) and Field Replaceable Entities (FREs) and includes replacement procedures applicable to GTR 8000 Site Subsystem.
- Chapter 10 GTR 8000 Site Subsystem Reference. This chapter contains supplemental reference information relating to GTR 8000 Site Subsystem.
- Chapter 11 GTR 8000 Site Subsystem Disaster Recovery. This chapter provides references and information that enables you to recover the GTR 8000 Base Radio and GCP 8000 Site Controller in the event of a failure.

Helpful Background Information

Motorola 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 communications site. This may be purchased on CD 9880384V83, by calling the North American Parts Organization at 800–422–4210 or the international number at 302–444–9842.
System Documentation Overview	For an overview of the ASTRO® 25 system documentation, open the graphical user interface for the ASTRO® 25 system documentation set and select the **System Documentation Overview** link. This opens a file that includes: • ASTRO® 25 system release documentation descriptions • ASTRO® 25 system diagrams • ASTRO® 25 system glossary For an additional overview of the system, review the architecture and descriptive information in the manuals that apply to your system configuration.
Dynamic System Resilience	Provides all the information required to understand, operate, maintain, and troubleshoot the Dynamic System Resilience feature.
HPD Standalone System - Infrastructure	Proves the information required to understand and operate the GTR 8000 Site Subsystem in an ASTRO® 25 High Performance Data System.

1 GTR 8000 Site Subsystem Description

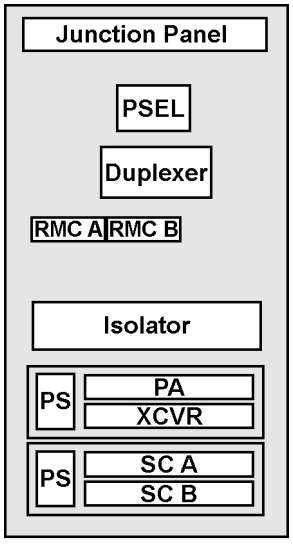
This chapter provides a high-level description of GTR 8000 Site Subsystem and the function it serves on your system.

1.1 Overview – GTR 8000 Site Subsystem

The GTR 8000 Site Subsystem includes a GCP 8000 Site Controller (with redundant modules), one GTR 8000 Base Radio, and RFDS components in a rack. The site controller and base radio in the rack are the same as the standalone versions, with similar internal connections within the rack between the site controller, base radio, and RFDS equipment.

The standard configuration for the GTR 8000 Site Subsystem, as used in a remote site, is shown in the figure.

Figure 1-1 GTR 8000 Site Subsystem - Components

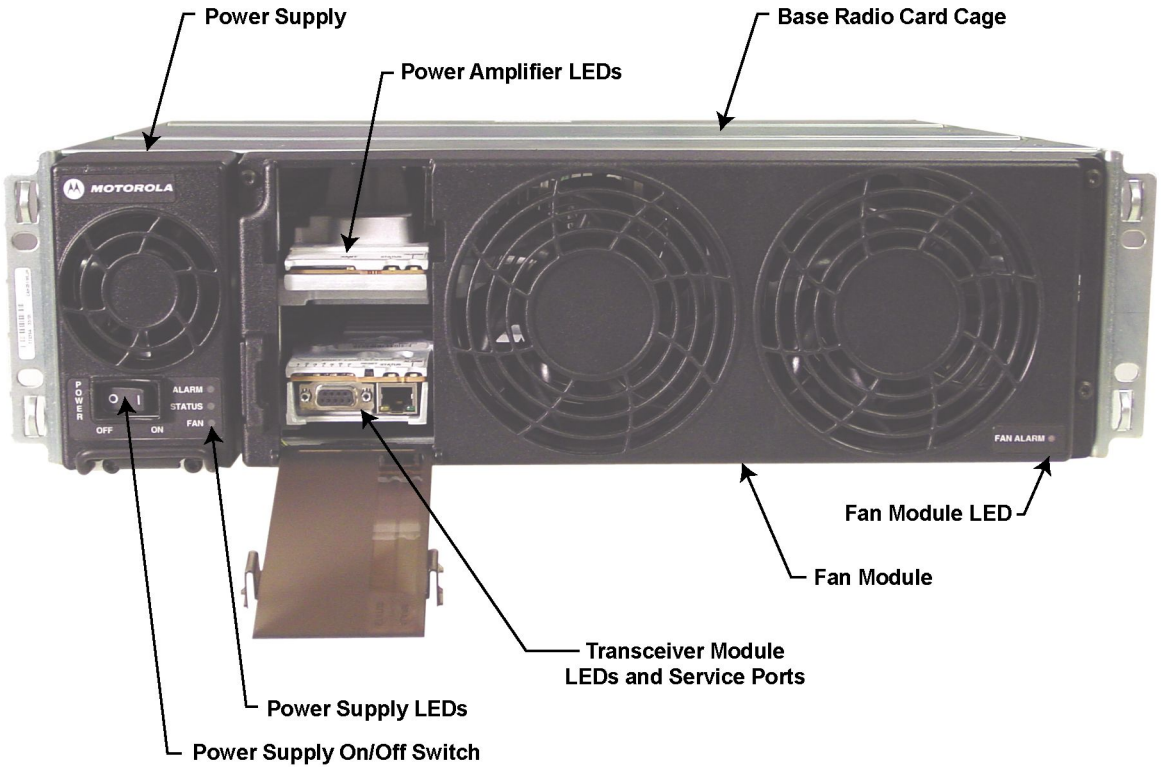


HPD_site_subsystem_config

1.2 GTR 8000 Base Radio Overview

The term "base radio" or "BR" is used to denote the transceiver and associated modules providing the functionality for **one** channel. As viewed in these applications, one "base radio" is in a GTR 8000 Site Subsystem configuration.

Figure 1-2 GTR 8000 Base Radio



The GTR 8000 Site Subsystem provides the radio frequency (RF) link between the system GCP 8000 Site Controller and the subscriber/mobile radios. The base radio captures inbound signals through external receive (Rx) antennas from the subscriber / mobile radios and then amplifies, filters, and demodulates the signals into data packets which are forwarded to the site controller. The site controller routes these packets upstream to a base site zone controller for further processing and routing.

The site controller receives digitized data and control packets from the zone controller and routes them to a specified base radio. The base radio extracts the control instructions from the packets and uses them for internal management such as channel frequency assignment. The base radio maps the digital data packets to discreet voltage levels which are then used to modulate an RF carrier. The modulated RF carrier is amplified and may be combined with other RF channels, filtered and routed to the transmission (Tx) antenna(s).

The base radio's home channel must be assigned a home channel preference level through the channel record in the Unified Network Configurator (UNC) for the zone controller. Settings for the base radio are made through the Unified Network Configurator (UNC) and Configuration/Service Software (CSS). See the Configuration chapter.

The base radio consists of a transceiver module, power amplifier module, fan module, and power supply. The transceiver module includes the functionality for the exciter, receiver, and station control. The base radio software, configuration, and network management, as well as inbound/outbound traffic handling, are performed through this transceiver module. On-board serial and Ethernet ports are on this module for local servicing through CSS and Unified Network Configurator (UNC). The power amplifier module amplifies the low-level modulated RF signal from the transceiver module and delivers the amplified signal on the path to the transmit antenna. The power supply module supports the transceiver and power amplifier modules, and can also provide auxiliary power to a connected site controller or a receive multicoupler/low noise amplifier (RMC/LNA).

Radio Frequency Distribution System (RFDS) provides the interface between the base radio and the site antennas and between the power amplifier and the site antennas.

NOTE

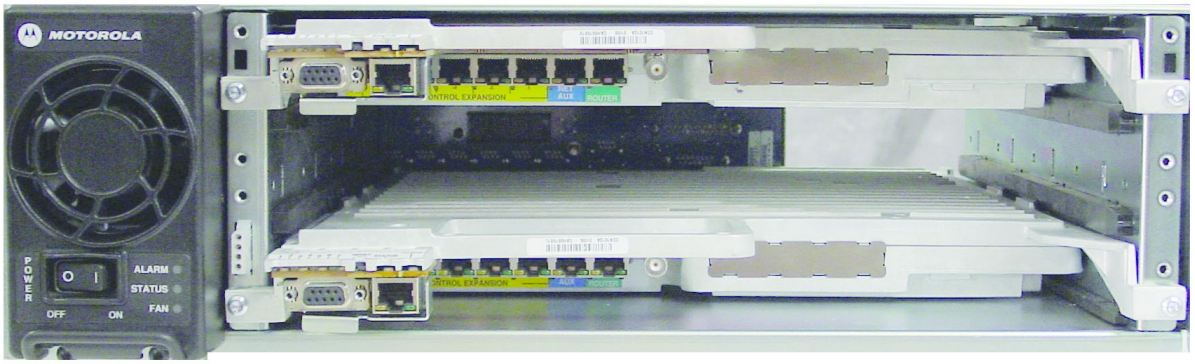
RFDS information provided in this documentation pertains to the RFDS equipment supplied by Motorola.

1.3 GCP 8000 Site Controller Modules

The GTR 8000 Site Subsystem is designed to work with the GCP 8000 Site Controller modules. For HPD applications, the site controller modules manage resources at the site, support frequency referencing, and the base radio data channel, handle the mobile subscriber unit (MSU) mobility messaging to/from the zone controller, and handle data messaging to/from the Radio Network Gateway (RNG).

One site controller module acts as the active module and the second module as the standby. The redundancy ensures that any single point of failure at the site does not reduce overall functionality.

Figure 1-3 GCP 8000 Site Controller Module



HPD_GCP8000_site_controller_front_wo_cover1

For details on the GCP 8000 Site Controller modules and configuration, see the *GCP 8000 Site Controller* documentation.

1.4 RFDS Components

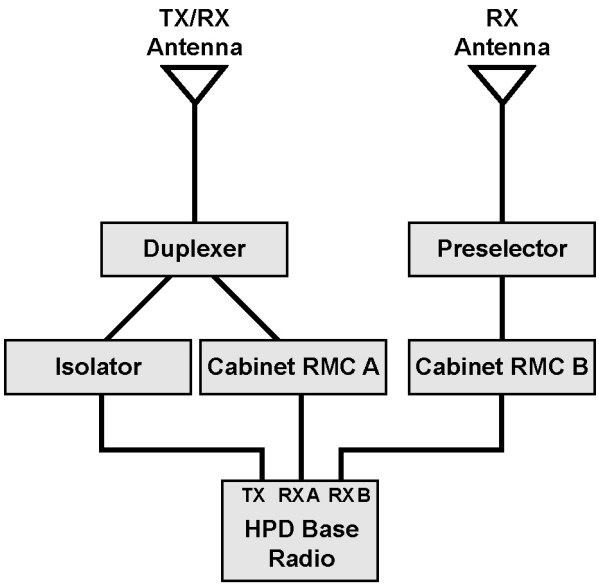
The RFDS components provide the conditioning and distribution of inbound/outbound signaling between the base radio and the antennas. The RF distribution components within the GTR 8000 Site Subsystem consist of the following:

- **External Dual Circulator/Isolator tray:** The tray includes an External Dual Circulator, Circulator Load, and Low Pass/Harmonic Filter to provide high isolation against intermodulation.
- **Duplexer:** Sends transmission to a full-duplex transmit/receive antenna as shown in the figure. Also receives input for one of the inbound paths from the full-duplex transmit/receive antenna, as described in the following section.
- **Receive Multicouplers/low noise amplifiers (RMCs/LNAs):** Cabinet RMCs A and B as shown in the figure.
- **Preselector:** For inbound path B.

One inbound path (receive path A) is captured through the full-duplex transmit/receive antenna (receive path A), and the other inbound path comes through the receive antenna (receive path B). On path A, the inbound signaling is received over the duplex antenna and passes through the duplexer which provides bandpass filtering on the receive signal. The inbound signal is sent to the RMC/LNA module A, which provides low noise amplification and a 4-way splitter. From the splitter, the receive signal is then sent to the base radio's RX-A port.

The second inbound path (path B) originates at the receive antenna and passes into a preselector which filters undesired energy from the receive signal. The output of the preselector is routed to the second receive multicoupler in the rack (RMC B). The RMC/LNA module amplifies, levels, and divides the signal before distribution to the base radio's RX-B port. This figure illustrates the transmit and receive paths of the GTR 8000 Site Subsystem.

Figure 1-4 GTR 8000 Site Subsystem - Transmit/Receive Paths



HPD_site_subsystem_txrx_path

A junction panel near the top of the rack is used for connection to receive and duplex antennas.

1.5 GTR 8000 Base Radio in an HPD Application

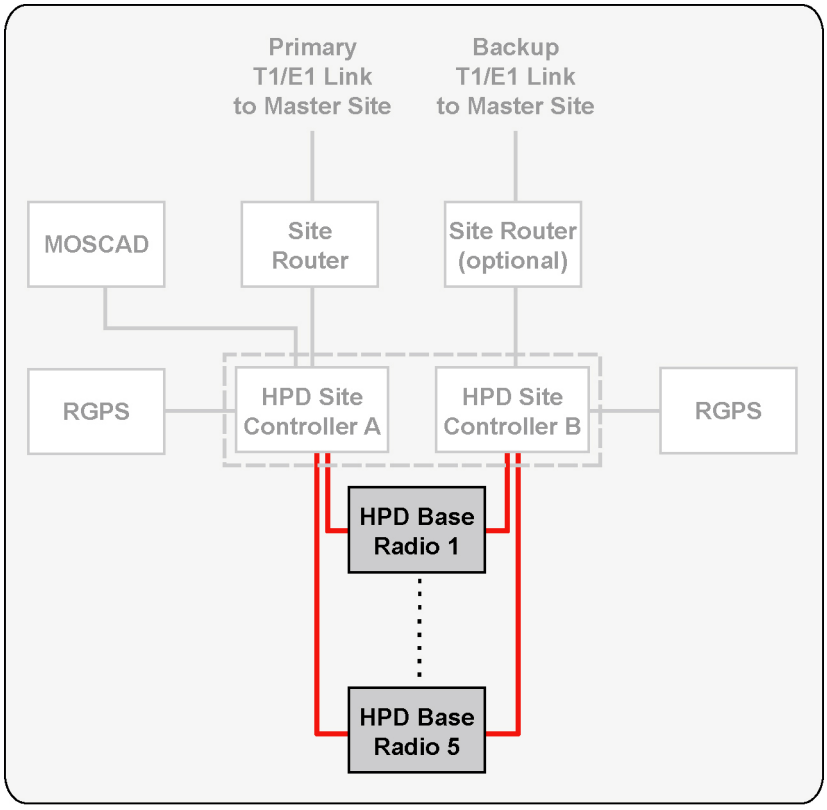
The ASTRO® 25 High Performance Data (HPD) system is a wireless data network designed for delivering mission-critical IP traffic between mobile data subscribers and customer host equipment. The high performance data system provides an efficient and reliable wireless transport medium for standard IP packet transfer, with raw data rates up to 96 kbps. This data rate allows service for medium bandwidth applications, including still image transfers, vehicle location services, and constrained web browsing services.

The base radio provides a full-duplex RF interface to Mobile Subscriber Units (MSUs). The base radio is available for 25 kHz HPD operation in the 700 MHz or 800 MHz bands. The base radio has an Ethernet connection to the redundant site controller.

The base radio uses Radio Link Adaptation (RLA) to provide high-speed, reliable, enhanced data performance when communicating traffic with MSUs. RLA uses adaptive modulation techniques, with slower, and more reliable modulation for control signaling and retries, and faster modulation methods when traffic is successfully being delivered between the base radio and MSUs.

The base radio is implemented with 2X receiver diversity. This receiver diversity enhances the inbound signals from the MSUs on the channel.

Figure 1-5 GTR 8000 Base Radios in HPD Remote Site



HPD_RS_comp_base_radio

The base radio uses Time Division Multiplex (TDM) frames for random access channels, reserved access channels, and broadcast messages. All carriers in the system are synchronized by a Global Positioning System (GPS) so that transmission slots are synchronized across sites. The base radio is able to schedule inbound/outbound traffic for half-duplex MSUs so that outbound traffic intended for the MSU does not conflict with inbound random or reserved access traffic from the MSU.

1.6 GTR 8000 Site Subsystem Specifications

This section details the GTR 8000 Base Radio and GTR 8000 Site Subsystem specifications. For the specifications for the GCP 8000 Site Controller, see the *GCP 8000 Site Controller* manual.

The following G-Series Product Specifications references the TIA specifications for the base radio. This includes the following Methods and Performance recommendations:

Phase 1 (includes Linear Simulcast):

- Methods: TIA-102.CAAA-C, “Digital C4FM/CQPSK Transceiver Measurements Methods” September 2008
- Performance: TIA-102.CAB-C, “Land Mobile Radio Transceiver Performance Recommendations, Project 25 – Digital Radio Technology, C4FM/CQPSK Modulation” January 2010

Phase 2:

- Methods: TIA-102.CCAA, “Two-Slot Time Division Multiple Access Transceiver Measurement Methods” August 2011
- Performance: TIA 102.CCAB, “Two-Slot Time Division Multiple Access Transceiver Performance Recommendations” October 2011

1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz)

The following lists the general, transmitter, receiver, FCC ID, and Industry Canada specifications for the GTR 8000 Base Radio.

1.6.1.1 General Specifications for GTR 8000 Base Radio (700/800 MHz)

Table 1-1 General Specifications for GTR 8000 Base Radio (700/800 MHz)

General Specifications	
Model Number	T7039A
Number of Channels	1
Size (H x W x D)	133mm x 483 x 457mm (5.25" x 19" x 18")
Weight	21 kg (46 lbs)
Temperature Range	
Operating:	-22 to 140 °F (-30 to 60 °C)
Storage:	-40 to 185 °F (-40 to 85 °C)
Operating Altitude	Up to 1800 meters (6000 feet) above mean sea level
Power Requirements	AC: 90-264 VAC, 47-63 Hz DC: 43.2-60 VDC
Power Consumption	AC: 450 W DC: 410 W
Power Supply Type	Switching
Battery Revert	Included
Input/Output Impedance	50 Ohms
Antenna Connector Types	
Tx:	N female
Rx:	BNC female
Frequency Stability	External Reference
Frequency Generation	Synthesized

1.6.1.2 Transmitter Specifications GTR 8000 Base Radio (700/800 MHz)

Table 1-2 Transmitter Specifications for GTR 8000 Base Radio (700 MHz and 800 MHz)

Transmitter Specifications	
Frequency Range	769-775, 775-776, 851-870 MHz
Power Output*	2-50 W
Channel Spacing	25 kHz
Modulation	QPSK, 16 QAM, 64 QAM
Electronic Bandwidth	Full Bandwidth
Error Vector Magnitude	10%
Spurious and Harmonic Emissions Attenuation	90 dB
Emissions Designators	17K7D7D
Adjacent Channel Power Ratio	
25 kHz offset, 22 kHz BW:	58 dB
37.5 kHz offset, 25 kHz BW:	65 dB
Tx Noise in Rx Band	-142 dBc/Hz
Intermodulation Attenuation	80 dB

* Full transmitter output power is available during battery revert.

NOTE

The output power reference plane is the output connector of the power amplifier. The loss of the transmitter output cable (PA output to back of base radio) is 4% at 800 MHz. However, the base radio software allows the transmitter output power to be set at 10% above rated value.

1.6.1.3 Receiver Specifications GTR 8000 Base Radio (700/800 MHz)

Table 1-3 Receiver Specifications for GTR 8000 Base Radio (700 MHz and 800 MHz)

Receiver Specifications	
Frequency Range	792-825 MHz
Sensitivity 1% Bit Error Rate Static (BER)	
64 QAM:	-98 dBm
QAM/QPSK:	-104 dBm
QPSK:	-111dBm
Faded Sensitivity 1% Bit Error Rate TU50 (BER)	
64 QAM:	-90 dBm

Table 1-3 Receiver Specifications for GTR 8000 Base Radio (700 MHz and 800 MHz) (cont'd.)

Receiver Specifications	
QAM/QPSK:	-96 dBm
QPSK:	-101 dBm
Faded Sensitivity 5% Bit Error Rate HT200 (BER)	
64 QAM:	-90 dBm
Faded Sensitivity 2% Bit Error Rate HT200 (BER)	
QAM/QPSK:	-94 dBm
Faded Sensitivity 1% Bit Error Rate HT200 (BER)	
QPSK:	-98 dBm
Intermodulation Rejection*	80 dB
Adjacent Channel Rejection*	50 dB
Spurious and Image Response Rejection*	85 dB
Intermediate Frequencies	
1st:	73.35 MHz
2nd:	2.16 MHz
Electronic Bandwidth	Full Bandwidth
Blocking Immunity	90 dB
Conducted Spurious	-57 dBm
Bit Error Rate Floor	0.01%
Co-Channel Rejection QPSK	11 dB

* Reference signal is QPSK

1.6.1.4 FCC ID GTR 8000 Base Radio (700/800 MHz)

Table 1-4 FCC ID for GTR 8000 Base Radio (700 MHz and 800 MHz)

FCC Identification			
Frequency Range	**Type**	**Power Output**	**Type Acceptance Number**
769-775, 775-776 MHz	Transmitter	2-50 W	ABZ89FC5812B
851-870 MHz	Transmitter	2-50 W	ABZ89FC5810B
792-825 MHz	Receiver	N/A	ABZ89FR5811B

1.6.1.5 Industry Canada GTR 8000 Base Radio (700/800 MHz)

Table 1-5 Industry Canada for GTR 8000 Base Radio (700 MHz and 800 MHz)

IC Approval Number	Frequency Range	Type	Power Output	IC Model Number
109AB-5812B	Tx 768–776 MHz, Rx 798–806 MHz	HPD	Variable 2–50 Watts (average)	T7039–700 B
109AB-5810B	Tx 851–869 MHz, Rx 806–824 MHz	HPD	Variable 2–50 Watts (average)	T7039–800 B

1.6.2 Specifications for GTR 8000 Site Subsystem (700/800 MHz)

The following lists the general, transmitter, receiver, and FCC ID specifications for the GTR 8000 Site Subsystem.

1.6.2.1 General Specifications for GTR 8000 Site Subsystem

Table 1-6 General Specifications for GTR 8000 Site Subsystem (700 MHz and 800 MHz)

General Specifications	
Model Number	T7133A
Number of Channels	1
Height	27 RU, 50.4 in. (128 cm)
Footprint (W x D)	20.8 x 24.8 in. (52.8 x 62.9 cm)
Weight (fully configured)	225 lbs (102 kg)
Temperature Range	
Operating:	-22 to 140 °F (-30 to 60 °C)
Storage:	-40 to 185 °F (-40 to 85 °C)
Operating Altitude	Up to 1800 meters (5900 feet) above mean sea level Above 1800 meters (5900 feet), the derating is 1.5 °C/km (0.8 °F/1000 feet) Above 3000 meters (9800 feet), the peak power derating for the Tx filter and phasing harness is 1 dB/1km (0.3 dB/1000 feet) Maximum operational altitude is 5000 meters (16900 feet)
Power Supply Input	AC: 90-264 VAC, 47-63 Hz DC: 43.2–60 VDC
Power Consumption	AC: 631 W DC: 490 W

Table 1-6 General Specifications for GTR 8000 Site Subsystem (700 MHz and 800 MHz) (cont'd.)

General Specifications	
Power Supply Type	Switching
Battery Revert	Included
Input/Output Impedance	50 Ohms
Antenna Connector Type	N female
Channel Spacing	25 kHz
Modulation	64 QAM, 16 QAM, QPSK
Frequency Stability	GPS synchronized
Frequency Generation	Synthesized

1.6.2.2 Transmitter Specifications for GTR 8000 Site Subsystem

Table 1-7 Transmitter Specifications for GTR 8000 Site Subsystem (700 MHz and 800 MHz)

Transmitter Specifications, including RFDS	
Frequency Range	764-776, 851-870 MHz
Average power output per channel	1-27 W
Error Vector Magnitude	10%
Spurious and Harmonic Emissions Attenuation	90 dB
Emissions Designators	17K7D7D
Adjacent Channel Power Ratio	
25 kHz offset, 22 kHz BW:	58 dB
37.5 kHz offset, 25 kHz BW:	65 dB
Intermodulation Attenuation	90 dB

Full transmitter output power is available during battery revert at the junction panel.

1.6.2.3 Receiver Specifications for GTR 8000 Site Subsystem

Table 1-8 Receiver Specifications for GTR 8000 Site Subsystem (700 MHz and 800 MHz)

Receiver Specifications, including RFDS	
Frequency Range	792-825 MHz
Electronic Bandwidth	Full Bandwidth
Sensitivity 1% Bit Error Rate Static (BER)	
64 QAM:	-101 dBm
16 QAM:	-108 dBm
QPSK:	-115 dBm

Table 1-8 Receiver Specifications for GTR 8000 Site Subsystem (700 MHz and 800 MHz) (cont'd.)

Receiver Specifications, including RFDS	
Faded Sensitivity 1% Bit Error Rate TU50 (BER)	
64 QAM:	-93 dBm
16 QAM:	-99 dBm
QPSK:	-104 dBm
Faded Sensitivity 5% Bit Error Rate HT200 (BER)	
64 QAM:	-93 dBm
Faded Sensitivity 2% Bit Error Rate HT200 (BER)	
16 QAM:	-97 dBm
Faded Sensitivity 1% Bit Error Rate HT200 (BER)	
QPSK:	-101 dBm
Intermodulation Rejection*	75 dB
Adjacent Channel Rejection*	50 dB
Spurious and Image Response Rejection*	90 dB
Intermediate Frequencies	
1st:	73.35 MHz
2nd:	2.16 MHz
Blocking Immunity	90 dB
Conducted Spurious	-57 dBm
Bit Error Rate Floor	0.01%
Co-Channel Rejection QPSK	11 dB

* Reference signal is QPSK

1.6.2.4 FCC ID for GTR 8000 Site Subsystem

Table 1-9 FCC ID for GTR 8000 Site Subsystem (700 MHz and 800 MHz)

FCC Identification			
Frequency Range	**Type**	**Power Output**	**Type Acceptance Number**
769-776 MHz	Transmitter	2-27 W	ABZ89FC5812
851-870 MHz	Transmitter	2-27 W	ABZ89FC5810
792-825 MHz	Receiver	N/A	ABZ89FR5811

2 GTR 8000 Site Subsystem Theory of Operations

This chapter explains how the GTR 8000 Site Subsystem works in the context of your system.

For an understanding of the way that GTR 8000 Site Subsystem components contribute to a base station; review the modules that provide the Base Radio functionality, the modules that provide RF distribution functionality (RFDS), and the modules that connect GTR 8000 Site Subsystems to the rest of the site (backplanes and junction panels).

2.1 Functions of the GTR 8000 Base Radio Modules

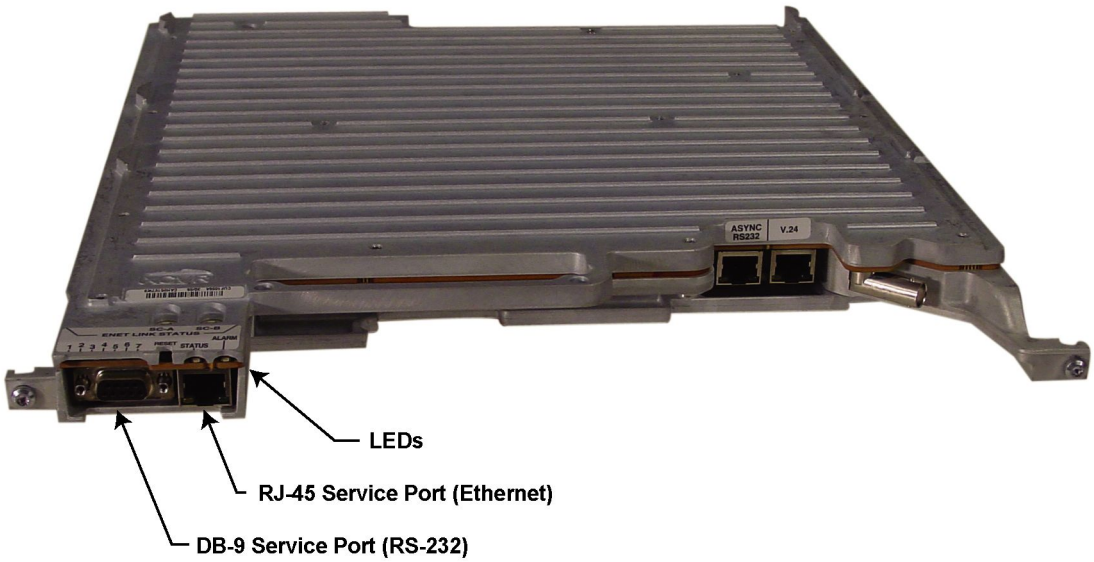
The following lists GTR 8000 Base Radio modules:

- Transceiver (XCVR) module
- Power amplifier module
- Fan module
- Power supply module

2.1.1 Function of the Transceiver Module

The transceiver (XCVR) module provides the control, exciter, and receiver functions for the base radio.

Figure 2-1 Transceiver Module (Front View)



GTR8000_XCVR_Front1

The XCVR generates the station reference, which typically must be locked on to one of many possible external sources. The external source can be either the site controller TDM clocks or the external reference operating at 5 and 10 MHz.

The XCVR SPI bus allows communication with its receiver and exciter circuitry, as well as the power supply and power amplifier modules.

There are two circuit boards in the XCVR:

- **XCVR Control Board**: Performs the control management, digital signal processing, and transmit and receive data formatting for the base radio.
- **XCVR RF Board**: Contains DC power conversion/regulation and performs receiver and exciter functions.

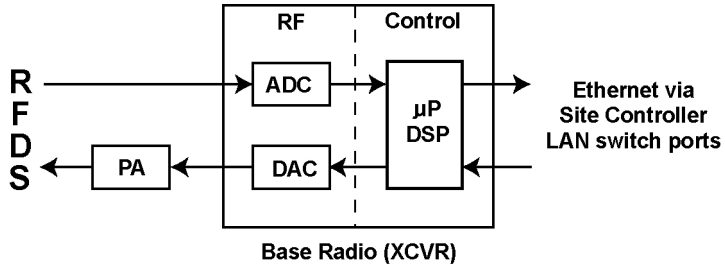
2.1.1.1 Transceiver Control Board

The main operating software for the base radio is loaded in the XCVRs control section. As the main manager for the base radio, the XCVR control board provides operational control over the other station modules. It handles three types of information flow, in the following ways:

- Serves as a gateway between the network and RF functionality, by distributing the RF payload to and from the network.
- Supports operational and diagnostic functions with digital control data (for example: site information, channel assignments, and identification numbers for call processing).
- Ensures the flow of other network management configuration information.

This figure shows the information flow through the transceiver control and RF sections for HPD systems.

Figure 2-2 GTR 8000 Base Radio HPD Information Flow



HPD_GTR8000_RF_Ethernet_Flow1

2.1.1.2 Transceiver RF Board

In addition to DC power conversion/regulation, the XCVR RF board provides circuitry for the following exciter and receiver functions.

2.1.1.2.1 Exciter

The exciter on the XCVR RF board provides the transmitter functions for the base radio. The exciter circuitry generates a low-level, modulated RF signal that passes to the power amplifier. It supports various modulation types as well as bandwidths up to 25 kHz, through software programming.

The exciter also provides a controlled output power level to the power amplifier.

2.1.1.2.2 Receiver

The receiver provides dual receiver inputs for dual diversity. The receiver also provides enhanced diagnostic capabilities using an on board noise source generator. It includes a wide tuning range (electronic varactor-tuned) preselector. The preselector is electronically tuned to the desired receive frequency anywhere between 792 MHz and 825 MHz. The preselector is best suited for:

- Low density RF environments
- Stations with external multicouplers
- Stations with requirements for multi-frequency operation beyond 14 MHz.

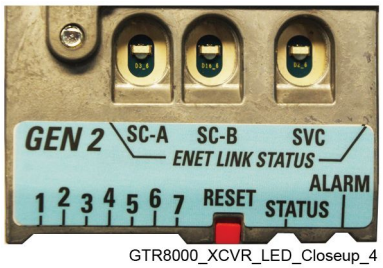
2.1.1.3 Transceiver External Interfaces

The transceiver external interfaces include seven external ports, a switch, and LEDs. See 3.4.6 Connections – Front, page 3-26 for the service ports. See 10.1 LEDs, page 10-1 for the LED states.

2.1.1.3.1 Transceiver Switch

There is one multifunction Reset switch on the front of the transceiver module, accessible through the drop-down door to the left of the fans. The Reset switch has two functions:

Figure 2-3 Transceiver Reset Switch (viewable through the drop-down door)



GTR8000_XCVR_LED_Closeup_4

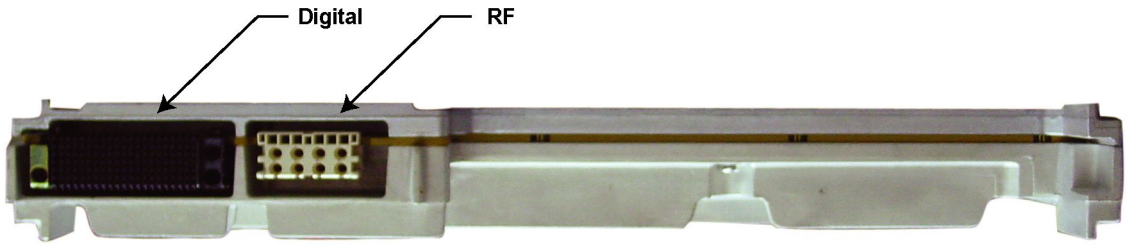
Table 2-1 Transceiver Front Reset Switch Functions

User Action	Result
Press switch for less than 1 second	Service Mode (LED 3 lights amber)
Press switch for more than 3 seconds, then release	Transceiver Control Module Reset

2.1.1.3.2 Transceiver Ports (Rear)

The transceiver interconnects to the backplane using a 120-pin HVDML digital connector and 8-pack RF connector, as shown in the figure. These connections handle multiple signals including power supply communications, power amplifier communications, fan interface, and peripheral interface. The digital connection receives alarm data and the site controller TDM signals, which are used to pass reference and control data to the receiverbase radio.

Figure 2-4 Transceiver Module (Backplane Connections)



GTR8000_XCVR_Rear1

- **Single Receiver Input:** An RJ-45 Ethernet port on the backplane is cabled to a site LAN switch for this channel. The backplane also provides an RF connection to the transceiver for receive (Rx) path A.
- **Dual Receiver Input:** RJ-45 Ethernet ports on the backplane are cabled to corresponding ports on the site controller backplanes (HPD). The backplane also provides RF connections to the transceiver for receive (Rx) paths A and B (TDMA)(HPD and TDMA).

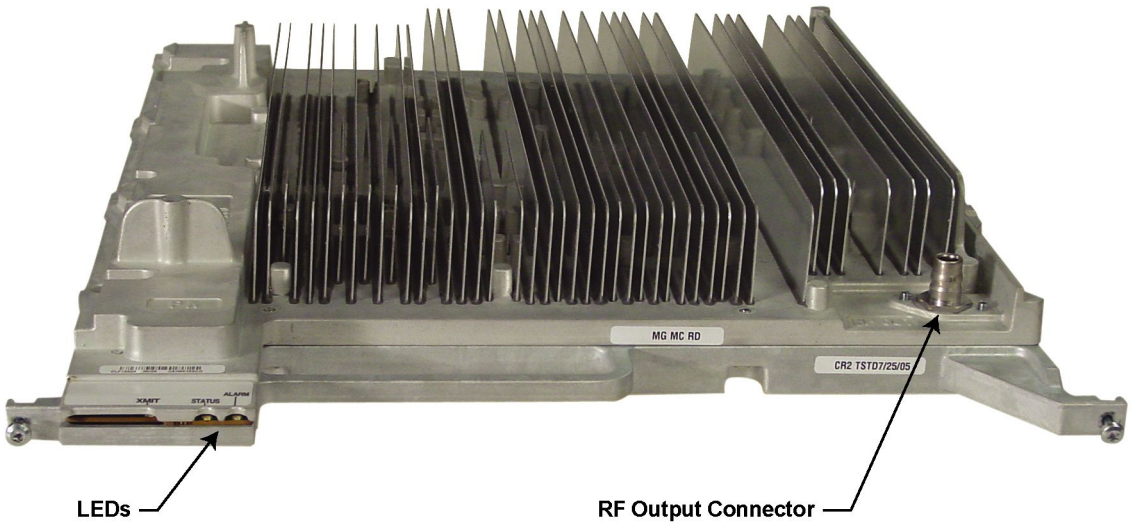
2.1.2 Function of the Power Amplifier Module

The Power Amplifier (PA) is a forced convection-cooled RF power amplifier. It accepts a low-level modulated RF signal from the transceiver module, and amplifies it for transmission through the site transmit antenna. Also, to complete the Cartesian correction loop (linearization method), it provides a low-level RF feedback signal to the transceiver module to achieve the required transmitter linearity.

Transmit power output can be set using Configuration/Service Software (CSS). See 4.4.7 Configuring Tx Power Values and Battery Type, page 4-24 in the Configuration chapter.

The power amplifier also performs functions related to the fan module, including reporting of the fan module status and supplying power to the fan power bus.

Figure 2-5 Power Amplifier Module



GTR8000_NonXS_PA_Front1

The power amplifier is comprised of six internal modules:

- Core Board
- Converter Board
- Driver Amplifier Board
- Final Amplifier Board
- Distribution Board
- Output Circuitry

2.1.2.1 Power Amplifier Input/Output Connections

There are three electrical connection assemblies on the power amplifier:

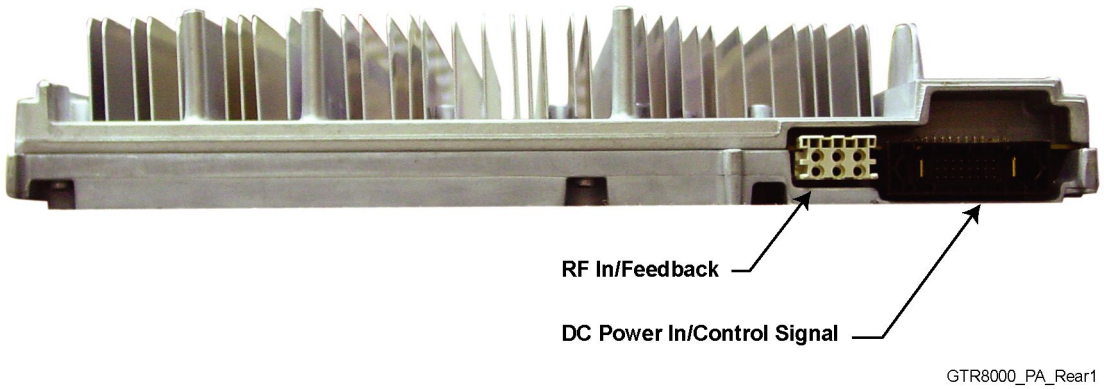
- RF output (front QN "quick-N" connector) on the front of the power amplifier module

  NOTE

  This is cabled to the N-type female bulkhead connection at the rear of the base radio housing.

- DC power supply/control signal (backplane connection)
- RF input/feedback (backplane connection).

Figure 2-6 Power Amplifier (Backplane Connections)



2.1.3 Function of the Fan Module

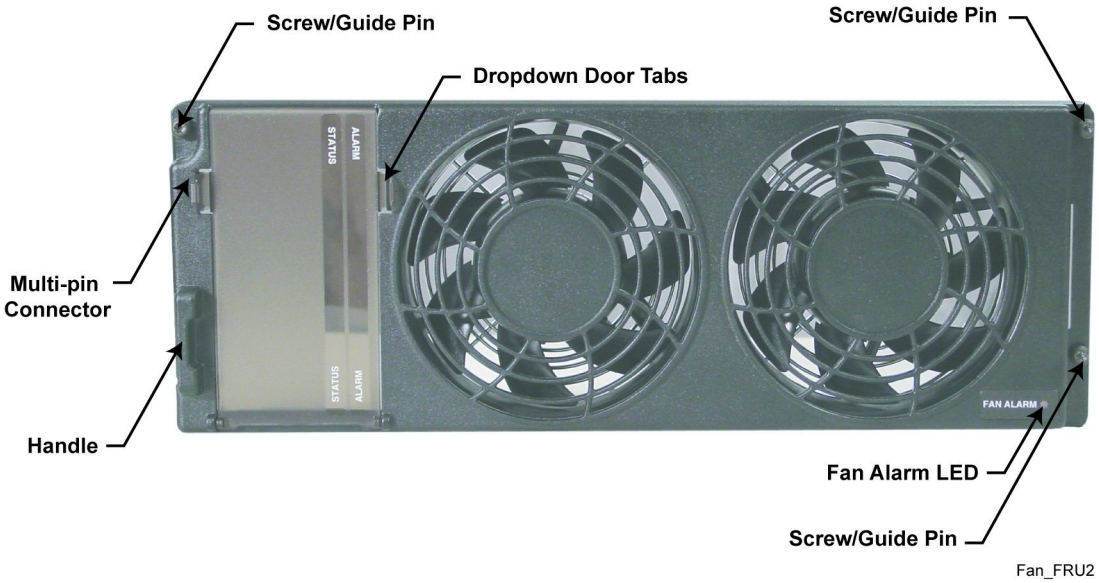
The fan module provides intermittent forced air cooling for the power amplifier, and transceiver modules. The fan module houses two 119 mm axial fans which deliver a total of approximately 160 cubic feet per minute of airflow. Nominal fan speed is 4100 revolutions per minute. A thermostat behind the fan module controls each fan. If the fan speed for either fan falls below 30% of the rated speed, a built-in speed sensor on each fan turns on the red Fan Alarm LED.

The fan module connects to the base radio backplane through a 4-pin port on the front of the base radio chassis.

NOTE

The power supply module has its own fan which provides independent airflow.

Figure 2-7 Fan Module



2.1.4 Function of the Power Supply

The power supply operates from either an AC or DC input and provides the DC operating voltage for the base radio.

Figure 2-8 Power Supply

HPD_Power_Supply_FRU.jpg

When operating from an AC source (90 to 264 VAC, 47-63 Hz), the supply generates two 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 AC mode, the power supply provides a separate battery charger which can be used to maintain the charge on a 48 VDC nominal system, positive or negative ground, if installed. The supply generates two DC output voltages of 29 V with respect to 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. Whether in AC, Battery Revert, or DC Only mode, at a voltage of 42 V or lower, the power supply shuts down in order to not damage any connected battery bank. Once this condition occurs, the power supply starts only after the applied voltage exceeds 45 V.

The battery charger is not usable when operating from a DC input power source. This DC source must be located in the same building as the base radio / repeater, and it must meet the requirements of a SELV circuit.

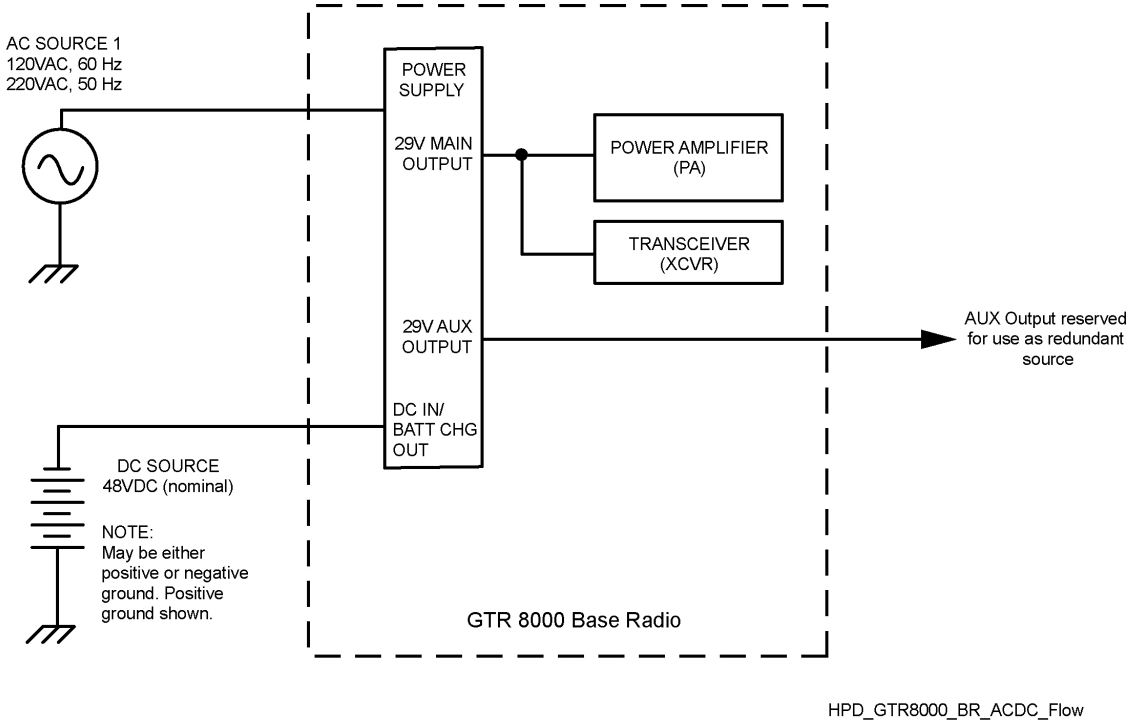
The power supply contains several switching-type power supply circuits as follows:

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

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

2.1.4.1 AC/DC Power Distribution – Base Radio

Figure 2-9 AC and DC Power Distribution in the GTR 8000 Base Radio



If present, the base radio operates from AC power as the preferred power source. When AC power is not available, the base radio switches to operate from the DC source. Operation returns to the AC source when the AC source is restored. Switchover 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 power amplifier and the transceiver. The Auxiliary output of the power supply is not used within the base radio, but is reserved for use as a redundant power input to other site components such as the site controller.

2.1.4.2 Power Supply Battery Charger

The power supply includes 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 may be 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 A-hr 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.

2.1.4.3 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 3.4.3.4 Mounting the Battery Temperature Sensor, page 3-21.

IMPORTANT

Continuous operation with a disconnected sensor is not recommended.

2.1.4.4 ON/OFF Switch for Power Supply and Battery Charger

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

Table 2-2 ON/OFF Switch - States for Power Supply and Battery Charger

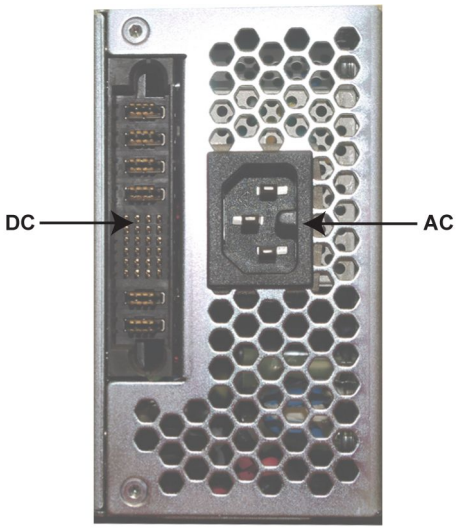
Switch Position	Power Supply State	Battery Charger State
ON (1)	• Power Factor Correction (PFC) section is active (AC input only) • Main DC converter runs to create the MAIN and AUX DC outputs	Can be started if desired (AC input only)
OFF (0)	• Main DC converter is turned OFF and the MAIN and AUX DC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

2.1.4.5 Power Supply Module Backplane Connections

Table 2-3 Power Supply Module Backplane Connections

Port/Type	Description
AC	Input only
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 2-10 Power Supply Connections (Rear)



G_Series_PS_Rear1

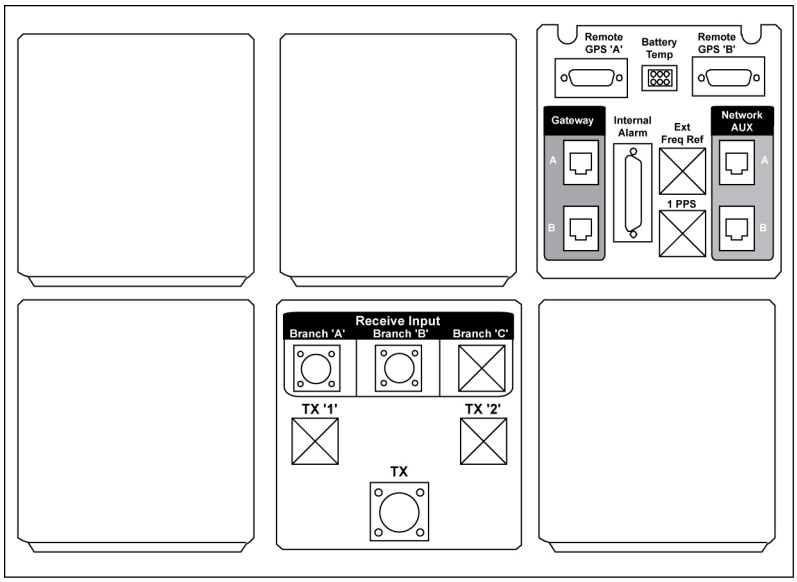
2.2 Function of the GCP 8000 Site Controller

See “GCP 8000 Site Controller Functions” in the *GCP 8000 Site Controller* manual for functions of the site controller used in a GTR 8000 Site Subsystem at an HPD site.

2.3 Junction Panels

The junction panels for the GTR 8000 Site Subsystem provides locations for all the connections to external devices. Locations for receive (Rx) and transmit (Tx) connectors are integrated in the junction panel in the lower center position as shown in the figure.

Figure 2-11 Junction Panel with Primary Subpanel #1



All other connector locations are provided through additional subpanels, such as the Primary Subpanel #1, in the top right position as shown in the figure.

2.4 Power Distribution Module

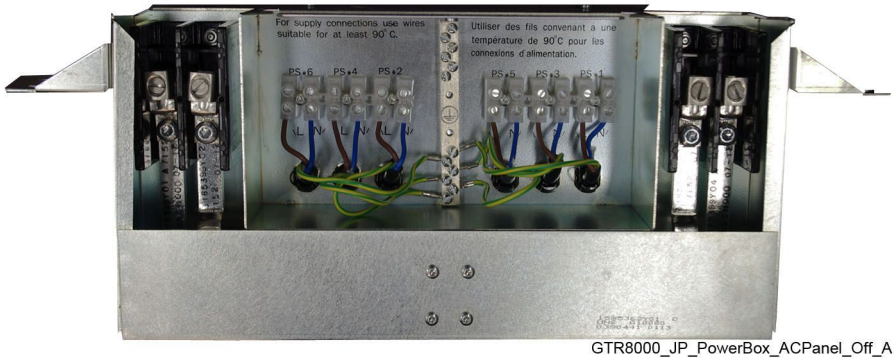
The power distribution module located with the junction panel in a GTR 8000 Site Subsystem provides connections for customer-provided AC and DC inputs. One or two DC inputs can be connected to the DC section of the power distribution module. For each base radio, there must be a single, separate AC source with the proper power rating connected to the appropriate terminals in the AC section, where it is then fed to the corresponding AC power supply input.

The number of **outputs** from the power distribution module depends on the configuration purchased. Two AC outputs from the power distribution module are used (one for the base radio and one for the site controller).

For additional information about power distribution in a GTR 8000 Site Subsystem, see the following sections:

- 2.1.4.1 AC/DC Power Distribution – Base Radio, page 2-8
- 2.5 Backplanes and Card Cages, page 2-14

Figure 2-12 Power Distribution Module (Access Panel Removed)

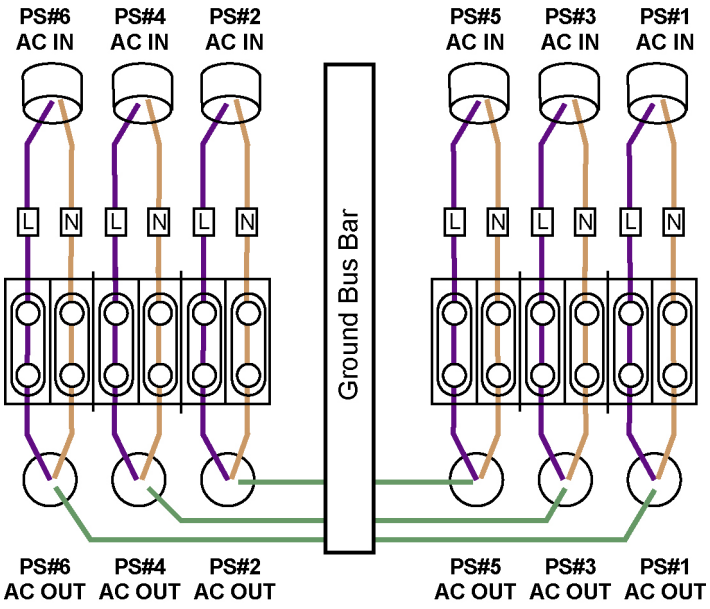


GTR8000_JP_PowerBox_ACPanel_Off_A

This block diagram shows the AC distribution block of the power distribution module. In the diagram:

- "L" indicates "Line" or "Hot" AC power feed.
- "N" indicates "Neutral" AC power feed.
- Input cable ground wires should be terminated to the ground bus bar.

Figure 2-13 Power Distribution Module- AC Distribution Block Diagram



GTR8000_JP_PowerBox_AC_DistrBlock

2.4.1 Splitting the Battery Pack

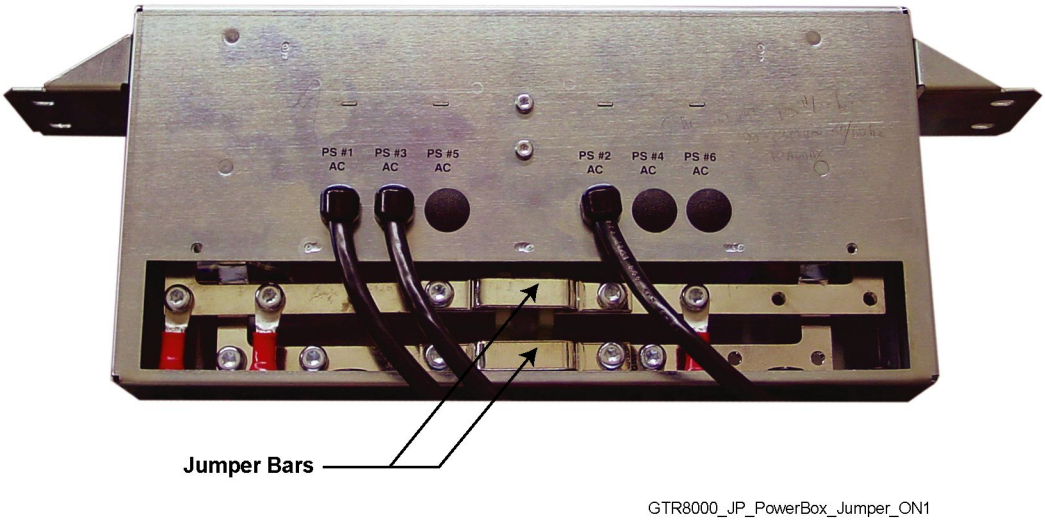
The GTR 8000 Site Subsystem is designed to receive DC power from a single DC source. The power distribution module at the junction panel is shipped with the DC busses interconnected to ensure that the single source is available for all power supplies contained within the subsystem.Two sets of DC input terminals are provided to reduce the current supplied through any one set of DC input cables to a value within the rating of the DC cables maximum size (2 AWG).

NOTE

Each DC input termination is rated for a maximum of 108A.

If only one DC power source is connected, the jumpers must be in place to provide DC power to the entire subsystem. This figure shows the jumpers in place (the power distribution module has 6 AC output cables. There are only three shown in this figure).

Figure 2-14 Power Distribution Module with Jumper Bars in Place



2.4.1.1 Removing the DC Bus Bars in the Power Distribution Module

Prerequisites:
The procedure assumes the following service access clearances:

- At least 2 ft access at the rear of the rack
- At least 2 ft access on one side of the rack, and at least 6 inches at the rear of the rack

When and where to use:
If operation with a split DC bus is desired, the DC jumpers can be easily removed from the bus bars by performing the following task.

Motorola does not recommend operating with a split DC bus. The customer should consider the impacts on system availability when operating with a split DC bus.

Potentially hazardous voltages are present in the power distribution panel. Input power sources should be de-energized before removing access covers. If input power cannot be de-energized at the source, this procedure should only be performed by properly trained service personnel using appropriate safety precautions for working on energized equipment.

Procedure Steps

1	Locate the access cover on the junction panel power distribution module (accessible from the rear of the rack, immediately below the AC power output cables).
2	Remove the access cover by removing the two retaining screws.
3	Remove the two screws that secure each jumper to the bus bars.
4	Carefully remove each jumper from the assembly.
5	Retain the jumpers and screws in a secure location in case jumper reinstallation is needed at a later date.
6	Reinstall the cover plate removed in step 1.

2.5 Backplanes and Card Cages

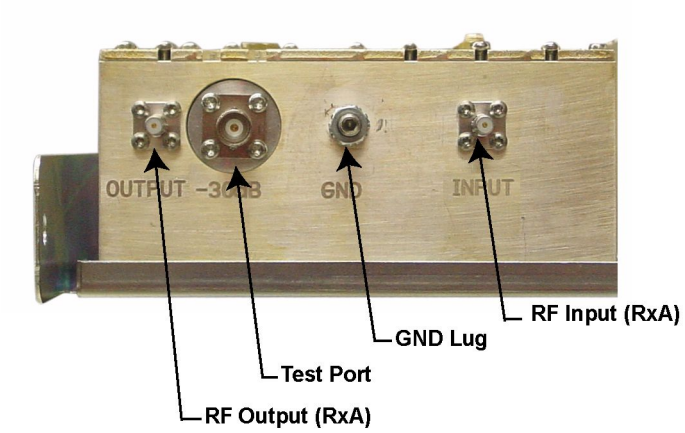
Card cages for the base radio are created with a welded and riveted design. Each card cage has a backplane. For base radios, customers make the connections to the backplane. See 3.4.5 Connections – Rear, page 3-24 in the Installation chapter.

2.6 RFDS Modules

The Radio Frequency Distribution System (RFDS) equipment included in your base radio depends on what options were purchased from Motorola. The following lists all RFDS equipment available for your system.

2.6.1 RFDS - Site Preselector

Figure 2-15 Preselector Filter



GTR8000_RFDS_Preselector_Front_2

The preselector provides a first level of band pass filtering for inbound RF signals. RF input and output connectors on the front of the device are cabled to the junction panel and a receive multicoupler.

The site preselector also has a built-in 30 dB coupler attached to a BNC connector on the front of the filter. That coupler port can be used for diagnostics and test purposes. For instance, a test signal can be injected on that port without having to disconnect the site from the antenna.

2.6.2 RFDS - (RMCs/LNAs)

RMC and LNA are used interchangeably in this documentation when referring to the receive multicoupler/low noise amplifier modules. This table describes components that are common to both Site RMCs/LNAs and Cabinet RMCs/LNAs.

Table 2-4 Receive Multicoupler (RMC) Internal Components

Circuit	Description
Balanced Amplifier	A balanced amplifier design has been chosen, in order to achieve redundancy, improved intercept point, and improved input matching. It splits the receive signal into two identical branches. Each branch contains a low noise amplifier, a programmable attenuator and a driver. At the output, the two branches are combined.
Splitter	The splitter provides multiple outputs. Each output is isolated from the others to prevent unwanted interactions between the receivers. The programmable step attenuator used to adjust output level is at the input of the splitter.
Alarm Circuit	Measured current is compared to a threshold and an alarm signal is set if the threshold is exceeded. The status and alarm LED are controlled by the digital circuit block as well.
Power Supply	Each amplifier branch has its own 5V regulator for redundancy reasons. The alarm circuitry is fed by a separate 5V regulator as well.

The following are additional features for the Cabinet RMCs/LNAs:

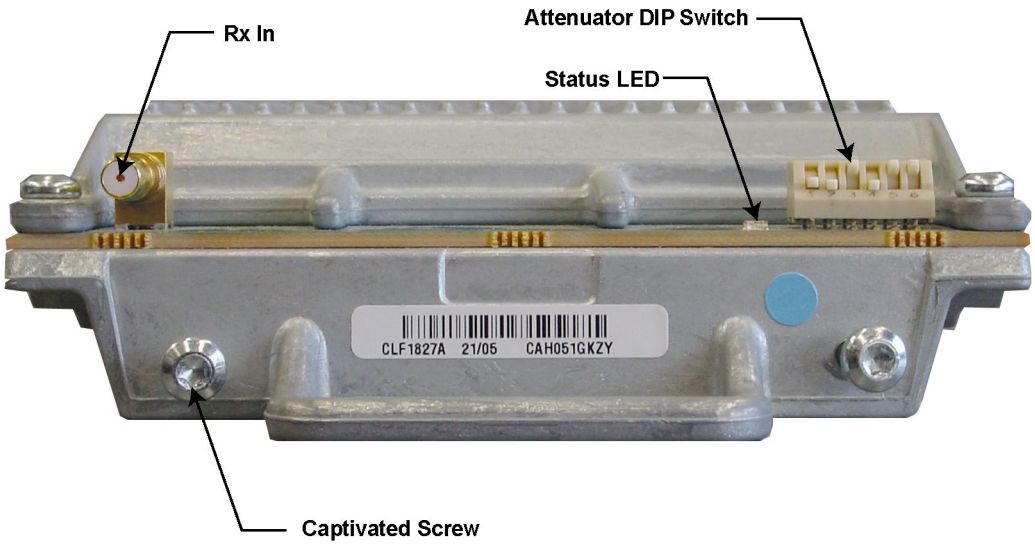
- Each RMC/LNA has a built-in 29 V to 7.5 V DC/DC converter.

- Power sharing between the two RMC/LNAs provides PSU redundancy.
- A green and a red LED visible from the front of the module indicate power supply and alarm state.

2.6.2.1 Cabinet Receive Multicouplers/Low Noise Amplifiers (Cabinet RMCs/LNAs)

The Cabinet RMC/LNA module employs a balanced amplifier, selectable attenuators, and a balanced divider to route Rx signals to the base radio module in the cabinet.

Figure 2-16 Cabinet RMC/LNA Module (Front View)

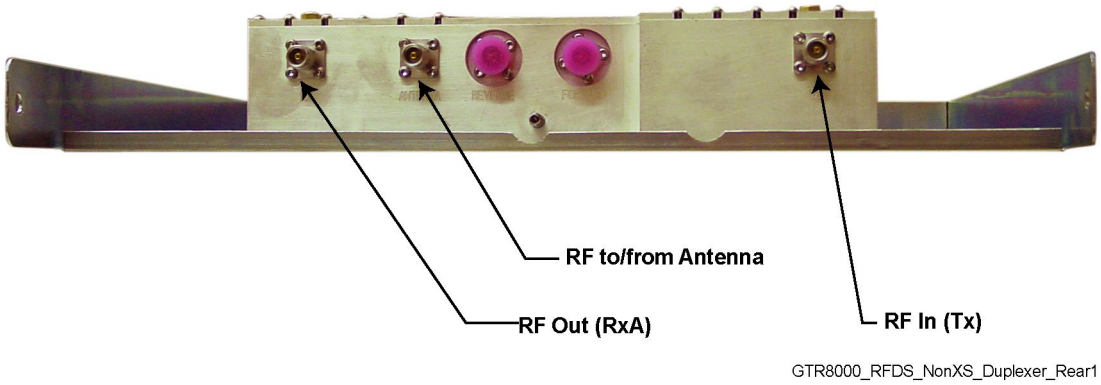


GTR8000_RFDS_XS_RMC_Cabinet_Front1

2.6.3 RFDS - Duplexer

In GTR 8000 Site Subsystems, the duplexer prepares transmit (Tx) signals for the duplex (Tx/Rx) antenna. It also processes inbound path A receive (RX-A) signals.

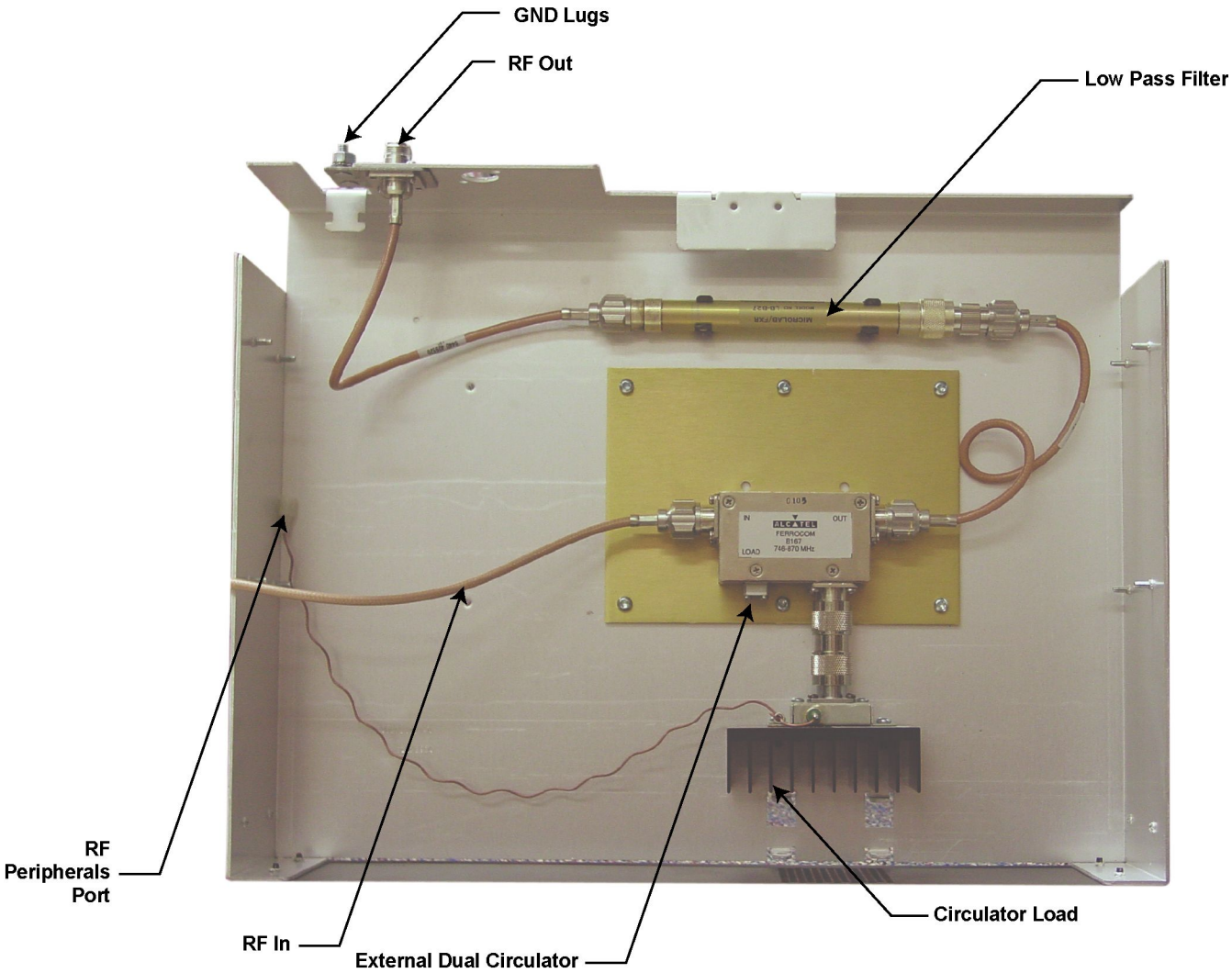
Figure 2-17 Duplexer (Rear View)



2.6.4 RFDS - External Dual Circulator/ Isolator Tray

In GTR 8000 Site Subsystems, the External Dual Circulator module isolates the base radio equipment from any intermodulation. A low pass filter and circulator load are on the tray with the External Dual Circulator. The circulator load dissipates reflected power. It includes a cable that connects to the RF Peripherals port on the base radio backplane to provide temperature monitoring.

Figure 2-18 External Dual Circulator/Isolator Tray



3 GTR 8000 Site Subsystem Installation

This chapter details installation procedures relating to the GTR 8000 Site Subsystem.

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 (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 Steps

1. Prepare the site to comply with the Motorola requirements and specifications for the equipment, as listed in the Motorola *Standards and Guidelines for Communication Sites* manual. The base radio may be installed in a suitable, restricted access, indoor enclosure in any location suitable for electronic communications equipment. Other codes and guidelines that may apply to the location must also be met. See 3.2 General Safety Precautions, page 3-2.

2. Inspect and inventory all racks, cabinets, cables, and other equipment with a Motorola representative to ensure that the order is complete. See 3.3 General Installation Standards and Guidelines, page 3-8.

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 System Support Center (SSC). See 3.3.12 General Installation/Troubleshooting Tools, page 3-15 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 3.4 GTR 8000 Site Subsystem Hardware Installation, page 3-17.

6. Connect all necessary cables within a rack and between the racks for system interconnection. See 3.4.6 Connections – Front, page 3-26, 3.4.5 Connections – Rear, page 3-24, and 3.4.7.1 Junction Panel Connections, page 3-27.

7. Run a preliminary check of a site before applying power.

8 See 3.6 Device Software Installation Prerequisites, page 3-29 for a list of items you need access to before installing the software.

9 See 3.8 Installing Devices Using the UNC, page 3-33 to discover the base radio and to load OS software images from the UNC.

10 See 4.4 Configuring a Device Using CSS, page 4-3 to program the configurations into the base radio using CSS.

11 See 4.5 Using VoyenceControl to Configure Centralized Authentication on Devices, page 4-30 to program the base radio using 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 *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.

NOTE

The installation process requires preparation and knowledge of the site before installation begins. Review installation procedures and precautions in the Motorola *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:

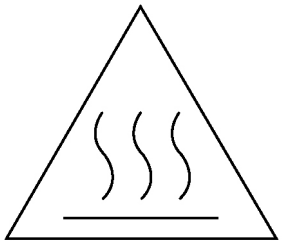
- Read and follow all warning notices and instructions marked on the product or included in this manual before installing, servicing, or operating the equipment. Retain these safety instructions for future reference.
- If troubleshooting the equipment while power is on, be aware of the live circuits.
- 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 *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 extremely 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 3-1 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.

WARNING

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 *Standards and Guidelines for Communications Sites* manual requirements.

CAUTION

All Tx and Rx RF cables must be connected to a surge protection device according to the Motorola *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-trained personnel.

3.2.1 GTR 8000 Base Radio Supplemental Safety Installation Requirements

The Supplemental Safety and Installation Requirements include the following:

- The GTR 8000 Base Radio must be installed in a suitable, in-building enclosure. A restricted access location is required when installing this equipment into the end system.
- The base radio contains a Class 1 built-in power supply component. This component is equipped with an appliance inlet for connecting to an AC input, as well as DC input terminals which meet SELV DC circuit requirements.
- When installing the equipment, all requirements of relevant standards and local electrical codes must be fulfilled.
- The maximum operating ambient temperature of this equipment is 60 °C. The maximum operating altitude is 3000 meters above sea level.
- The 28.6 VDC output from the power supply to the PA is at an energy hazard level (exceeds 240 VA). When installing into the end system, care must be taken so as not to touch the output wires.
- When the GTR 8000 Base Radio / Repeater is used in a DC reverting system, the DC power supply must be located in the same building as the GTR 8000 Base Radio, and it must meet the requirements of a SELV circuit.

3.2.2 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.

3.2.2.1 Disconnect Device Permanently Connected

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

3.2.2.2 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.

3.2.2.3 Connection to Primary Power

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

3.2.2.4 Replaceable Batteries

WARNING

Risk of Explosion if the battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

3.2.3 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.

3.2.4 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.

3.2.4.1 Lifting Equipment Racks Horizontally

In some cases, equipment racks are shipped in the horizontal position. Use the appropriate lifting apparatus to lift the racks upright. Comply with all applicable health and safety regulations, and any other regulations applicable to lifting heavy equipment.

WARNING

Crush Hazard could result in death, personal injury, or equipment damage.

Do not use the eyenuts mounted on the top of the rack to lift the rack upright from a horizontal position. The eyenuts are not designed to lift horizontally and could fail resulting in damage to the equipment or injury to personnel .

3.2.4.2 Lifting Equipment Racks Vertically

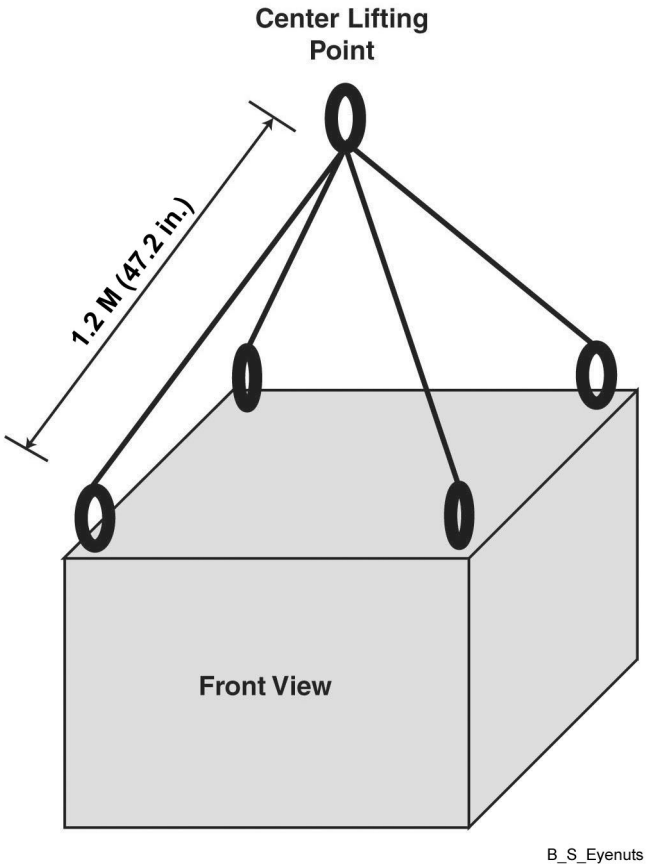
Some equipment racks have four M10 eyenuts mounted in the top of the rack. Use these eyenuts to lift the equipment rack vertically. Before using these eyenuts, visually check them and the rack hardware for any damage that may have occurred during shipping.

WARNING

Do not use the eyenuts if damage is apparent. Contact Motorola for replacements.

Use all four eyenuts when lifting the equipment rack. The minimum distance from each eyenut to the lifting point is 1.2 meters (47.2 in). Using a shorter length than specified could cause the eyenuts to fail. This figure shows the minimum lengths and proper lifting angles using the eyenuts.

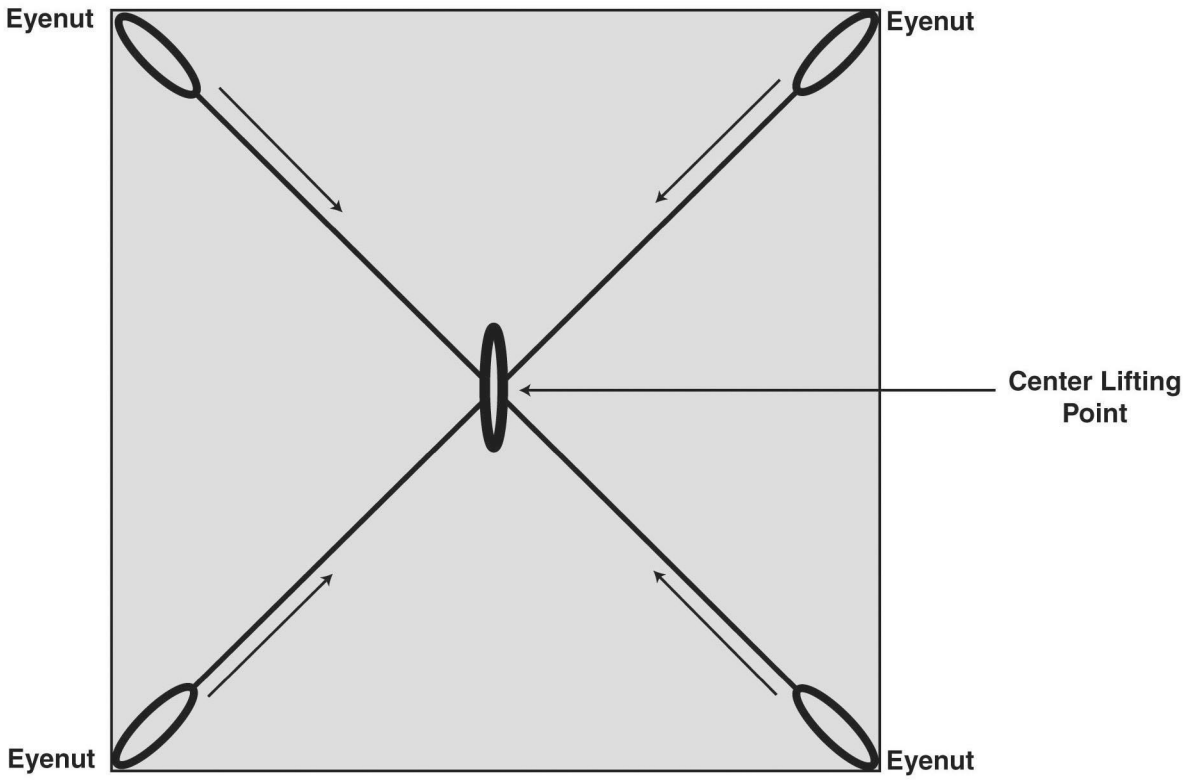
Figure 3-2 Lengths and Angles for Lifting Using the Eyenuts



If eyenuts are removed or become loose, install them properly before lifting the equipment rack. Tighten the eyenuts and bolt assembly by hand. Correct eyenut tightness and alignment are crucial to ensure that the eyenut assembly performs to its intended lifting capacity. Align the eyenuts to point towards the center lifting point of the cabinet and tightened to between 90 to 120 in.-lb torque.

This figure shows the proper alignment of the eyenuts.

Figure 3-3 Proper Alignment of the Eyenuts



3.3 General Installation Standards and Guidelines

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

- Equipment installation
- Antenna installation

Review installation information specifically for the GTR 8000 Site Subsystem in 3.4 GTR 8000 Site Subsystem Hardware Installation, page 3-17.

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 *Standards and Guidelines for Communication Sites* manual for more information.

Table 3-1 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 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 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 representative.

CAUTION

Do not tamper with factory configuration settings for these devices. These include software configuration, firmware release, password, and physical connections. Motorola 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.

NOTE

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 *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 provided by the field engineer or consult the Motorola 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.

3.3.5 General Floor Mounting Procedure for Cabinets or Racks

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 Steps

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 is 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 *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 provided by Motorola. Also see the Motorola *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 provided by Motorola.
- Ensure that cables do not exceed the minimum bend radius as outlined in the Motorola *Standards and Guidelines for Communication Sites* manual.

CAUTION

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

NOTE

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 *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 *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 specified by the customer.
- 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.

SUGGESTION

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

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

- For a 120 VAC, 60 Hz application, the AC supply breaker must be rated for a continuous current of 20 A. For a 220 VAC, 50 Hz application, the AC supply breaker must be rated for a continuous current of 10 A minimum, not to exceed 20 A.
- Individual DC breakers are not used. For information involving the sizing of cables and DC power distribution, see the *Standards and Guidelines for Communication Sites* manual.
- Site installation must include a single current interrupting device on the DC input distribution (fuse or circuit breaker) rated for the application loading, not to exceed 200 A. For each standalone device, the DC supply breaker should be rated for a continuous current of 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 heavy gauge stranded cable is advised to minimize voltage drop. Examples of the resistance of some heavy gauge wire are:

Table 3-2 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)]

See 3.4.3.3 DC Power Connection Wire Gauge Calculations, page 3-20 for additional guidelines on the cable sizing.

3.3.9 General Electrostatic Discharge Recommendations

Electronic components, such as circuit boards and memory modules, can be extremely 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.

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
- Ni-MH 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 System Support Center (SSC). See 8.4 Using Motorola Solution Support Center, page 8-6.

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 XP Home Edition
    - Windows XP Professional
    - Windows Vista (all editions)

- ♦ Windows 7 (all editions)

- Hardware Requirements:
  - Processor:
    - ♦ 1 GHz or higher Pentium grade
  - Processor Memory:
    - ♦ 1 GB RAM recommended for Windows XP
    - ♦ 2 GB RAM recommended for Windows Vista and Windows 7
  - 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 provided by the Field Engineer or Motorola Field Representative for the system, one of the Motorola Solution 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 8.4 Using Motorola Solution Support Center, page 8-6.
- The Motorola System Service Subcontractor Assessment program ensures that service people contracted by Motorola meet strict minimum requirements before they can work on any system. For more information on this program, contact the Motorola representative.

3.3.13.1 Site-Specific Information

When the Motorola 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

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

3.4 GTR 8000 Site Subsystem Hardware Installation

The following is information specific to the GTR 8000 Base Radio and GTR 8000 Site Subsystem.

3.4.1 Placement and Spacing

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

For the GTR 8000 Site Subsystem, recommended clearance 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 rack.

Side and rear access:

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

To maintain this clearance, the following is recommended:

- If there is less than 2 ft rear access, do not install more than two racks side by side, and allow at least 2 ft access on at least one side of each rack.

3.4.2 Floor Mounting of the GTR 8000 Site Subsystem

Figure 3-4 is the footprint diagram for the GTR 8000 Site Subsystem.

Figure 3-4 GTR 8000 Site Subsystem - Floor Mounting Detail

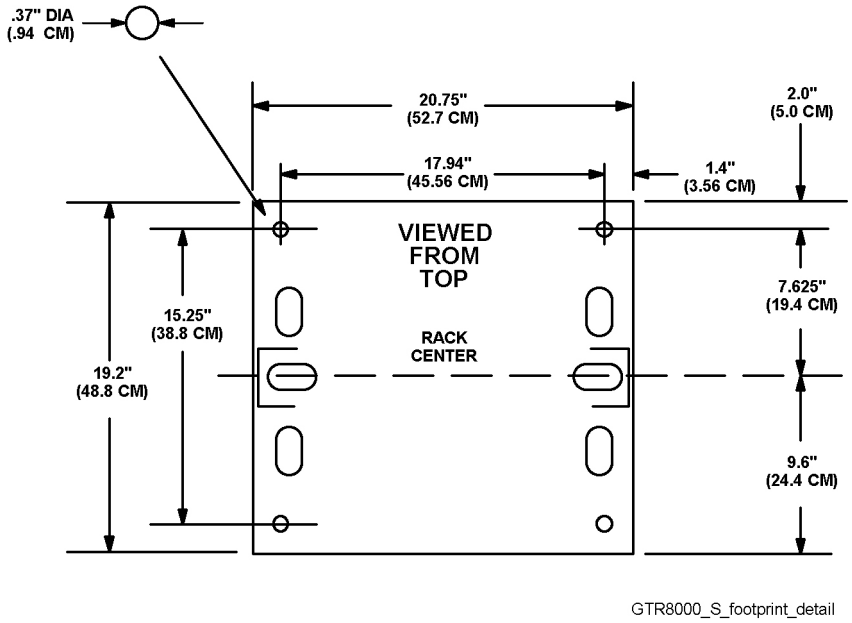
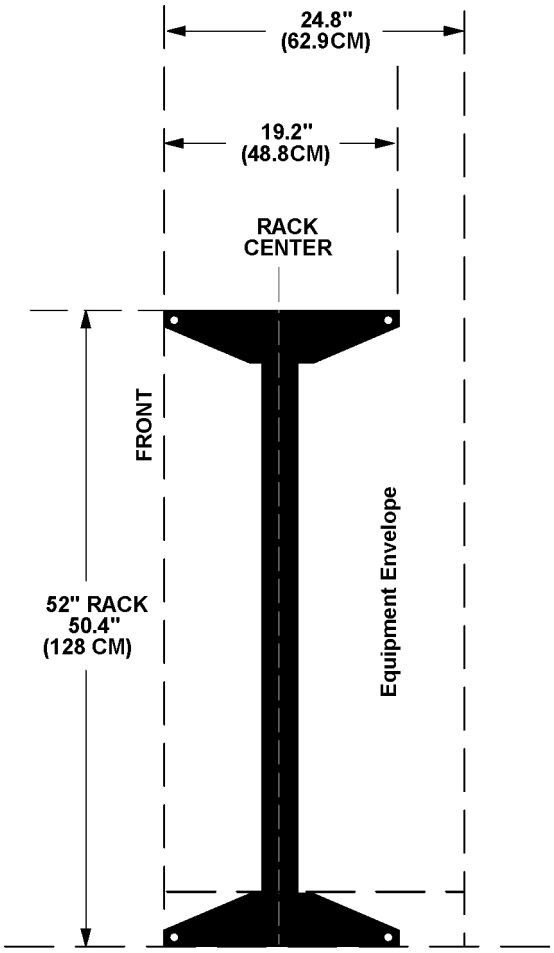


Figure 3-5 provides a side view.

Figure 3-5 GTR 8000 Site Subsystem (Open Rack Version) - Side View



GTR8000_S_footprint_side

3.4.3 Connecting Power

This section covers topics on connecting power cables to the base radio and the power distribution module, calculating the length of wire for various gauges, and mounting the battery temperature sensor.

3.4.3.1 Connecting Power Cables to a GTR 8000 Base Radio

For the base radio, customer-provided AC and DC inputs connect to the power supply through the backplane of the base radio. See 3.4.5 Connections – Rear, page 3-24.

3.4.3.2 Connecting Power Cables to a Power Distribution Module

In a GTR 8000 Site Subsystem, the power distribution module located with the junction panel provides connections for customer-provided AC and DC inputs. One or two DC inputs can be connected to the DC section of the power distribution module. For the base radio, there must be a single, separate AC source with the proper power rating connected to the appropriate terminals in the AC section, where it is then fed to the corresponding AC power supply input.

NOTE

Each DC input termination is rated for a maximum of 54A.

For additional information about power distribution in GTR 8000 Site Subsystems, see the following sections:

- 2.1.4.1 AC/DC Power Distribution – Base Radio, page 2-8
- 2.4 Power Distribution Module, page 2-11.

3.4.3.3 DC Power Connection Wire Gauge Calculations

Since the power supply disconnects itself from the DC input when it senses that DC voltage has dropped to 42 VDC, it is important to minimize the voltage drop in the DC power supply loop (the total length of the 48 VDC "hot" wire and the DC return wire) to no more than 1 V total. Minimizing the voltage drop ensures that the maximum energy is removed from the battery before disconnecting the power supply from the DC input line.

A GTR 8000 Site Subsystem transmitting at 50 W draws up to 7.4 A current when operating from a 54 V source (nominal 48 VDC system). As voltage decreases (due to the standby battery discharging) the current increases proportionally (since the base radio appears to be a constant power load). At the low voltage disconnect point (42 V for a nominal 48 VDC system), the current is up to 9.5 A. If a single pair of 2 AWG wire is used to connect the battery to the junction panel, the maximum length of a single conductor would be 335 ft. Use of smaller gauge wire would reduce this length depending on the resistance of the wire. To determine the maximum length of wire for wire other than 2 AWG, the following relationship can be used:

- Length (ft) = V/I/R

where:

- V = voltage drop in one leg of the loop (max = 0.5 V)
- I = current drawn by the base radio during DC operation (12A)
- R = resistance of the wire being considered (in Ohms per ft)

3.4.3.3.1 Power Connection Wire Gauge Maximum Distances

For common wire sizes, the maximum distances shown in this table apply.

Table 3-3 Power Connection Wire Gauge Maximum Distances

AWG	Resistance (ohm/1000 ft)	Maximum Distance (meter/ft)
2	0.1563	102.1m (335 ft)
3	0.1970	81m (265 ft)
4	0.2485	64m (210 ft)

Table 3-3 Power Connection Wire Gauge Maximum Distances (cont'd.)

AWG	Resistance (ohm/1000 ft)	Maximum Distance (meter/ft)
5	0.3133	51m (165 ft)
6	0.3951	40m (130 ft)

In some installations, local codes may require the installation of wire heavier than 2AWG. In these situations, a local splice box can be used to reduce the incoming wire to the 2AWG needed for connection to the input terminal box. The splice box should be located as close as possible to the junction panel.

3.4.3.4 Mounting the Battery Temperature Sensor

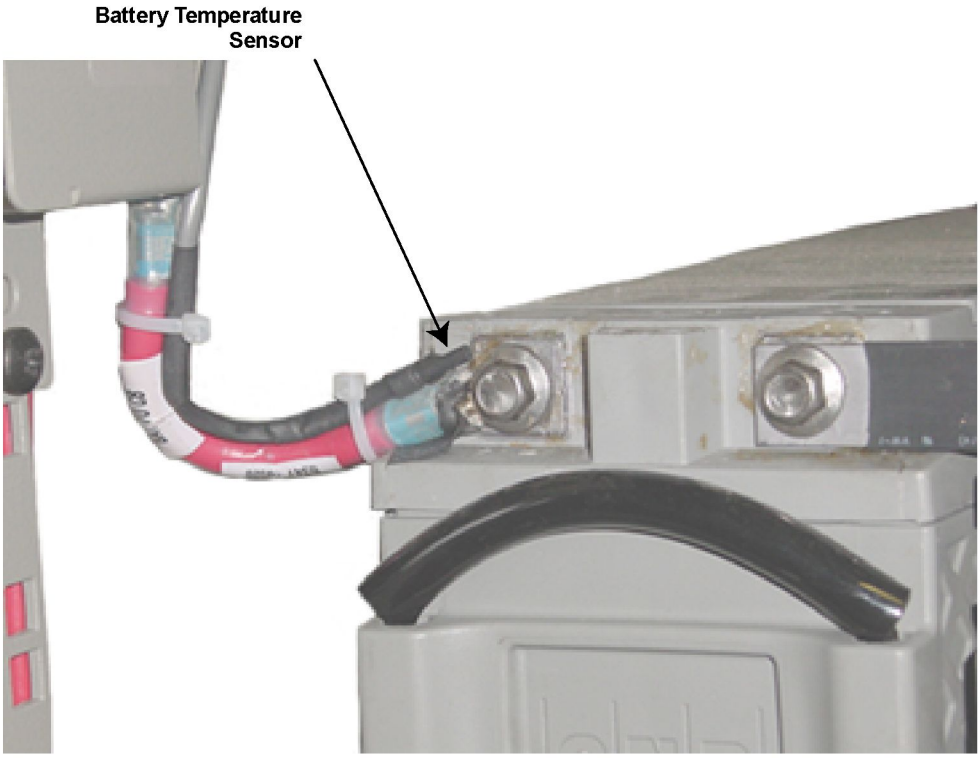
A 40 ft battery temperature sensor cable is shipped with your device. This three-wire cable carries a voltage signal to the power supply from a sensor element which must be mounted close to the storage battery. Voltage is proportional to the battery temperature and the diagnostic circuitry in the power supply module. The 40 ft cable can be extended to a total length of 190 ft using 50 ft extensions (Motorola part number 3084827Y04. See 8.4 Using Motorola Solution Support Center, page 8-6.

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 3-6.

Figure 3-6 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 3-7.

Figure 3-7 Battery Temperature Sensor Example 2

3.4.4 Grounding

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

IMPORTANT

Ground the battery system, either positive or negative, at the battery. The DC input (battery charger output) of the power supply is floating with respect to earth ground. The power supply can therefore be used in either positive ground or negative ground DC systems. The appropriate terminal (+ or -) of the DC system should be connected to protective earth at the battery. These instructions assume that all telephone lines, antenna cables, and AC or DC power cables have been properly grounded and lightning-protected.

3.4.4.1 GTR 8000 Base Radio Grounding

Procedure Steps

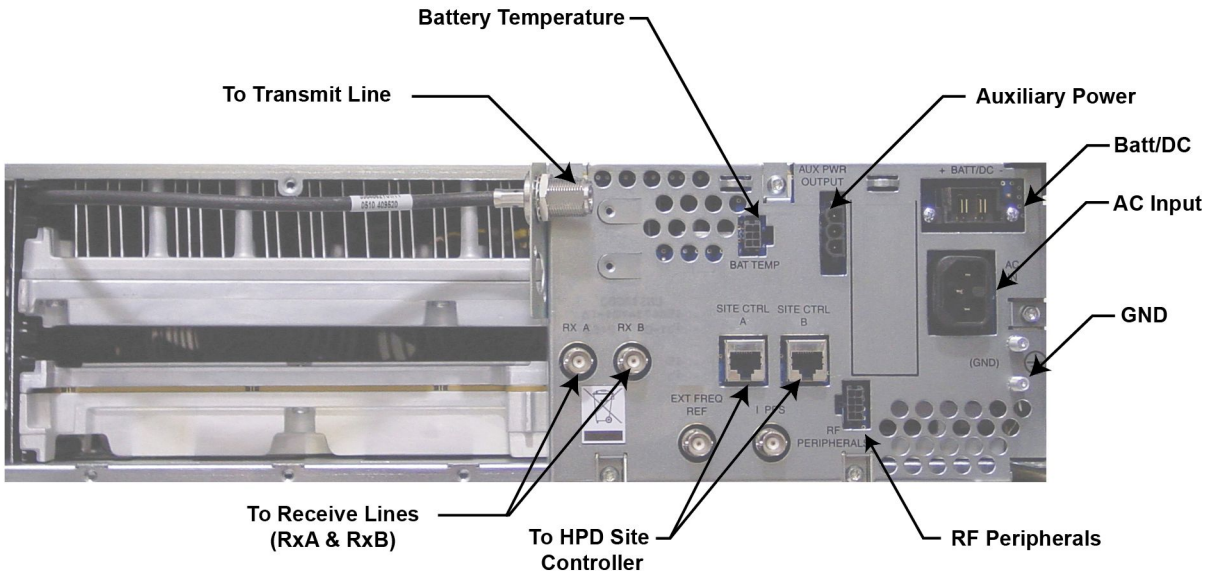
1 Take the ground wire already attached to the two grounding lugs at the rear of the base radio, and connect the other end to the rack grounding bar.

2 Tighten the ground lock nut to 60 in-lbs (6.94 newton-meters).

3.4.5 Connections – Rear

The GTR 8000 Base Radio connects with each of the site controllers and to the transmit and receive paths.

Figure 3-8 Base Radio – HPD Backplane



HPD_GTR8000_base_radio_rear2

Table 3-4 GTR 8000 Base Radio Connections (Backplane)

Port / Type	Device it connects to:	Port / Type	Description
SC A port, RJ-45	Site Controller module A	Base radio port, RJ-45	Connects to site controller A base radio port for this channel. **NOTE** The length of the cable between the site controller and the base radio should be no greater than 30 feet.
SC B port, RJ-45	Site Controller module B	Base radio port, RJ-45	Connects to site controller B base radio port for this channel.
RX-A, BNC	Receive line A	BNC	RF coax to receive path for Rx antenna.
RX-B, BNC	Receive line B	BNC	RF coax to receive path for antenna B.
Transmit port, N-type	Transmit line	N-type	RF coax to transmit antenna.
Aux Pwr Output	Site Controller or RMC/LNA	Aux Pwr Input	The auxiliary output power can be used to provide secondary power to the site controller or receive multicouplers (Site RMCs/LNAs).
Bat Temp, 6-pin	Battery temperature sensor		Connection to temperature sensor, allowing for temperature compensated battery charging.
RF Peripherals	RF peripheral sensor ports		Antenna relay and presence detect, external circulator load temperature (external wattmeter not supported).
Batt/DC	DC power supply or battery	Batt/DC	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 (8AWG; 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 120/240 VAC nominal power source.
Rx-C			Not in use

Table 3-4 GTR 8000 Base Radio Connections (Backplane) (cont'd.)

Port / Type	Device it connects to:	Port / Type	Description
EXT FREQ REF			Not in use
1 PPS			Not in use

3.4.6 Connections – Front

Two service ports are accessible through a drop-down door to the left of the fans. The remaining ports are behind the fan module.

Figure 3-9 GTR 8000 Base Radio – Front

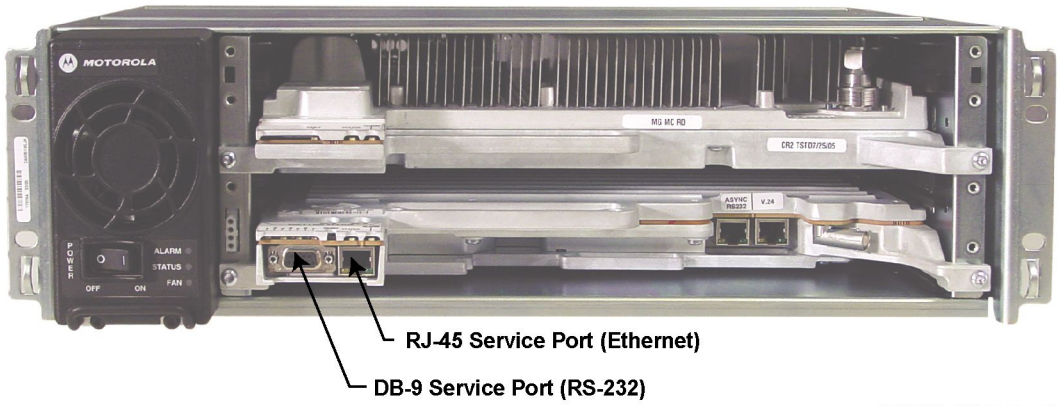


Table 3-5 GTR 8000 Base Radio Connections (Front)

Port / Type	Description
Service port, RJ-45	Connects to service PC for local access using Configuration/Service Software. Also may be used for localized software downloads. **NOTE** The RJ-45 service port supports only 10 Mb half duplex operation.
Service port, DB-9	Connects to service PC for initial configuration of the base radio IP address.
Reference frequency input, BNC	Connection port to service monitor for frequency calibration.

3.4.7 Junction Panel Connections for the GTR 8000 Site Subsystem

The junction panels for the GTR 8000 Site Subsystem provides locations for all the connections to external devices. Cables provided by Motorola include the specific connectors for the junction panel on one end and the subsystem equipment on the other end.

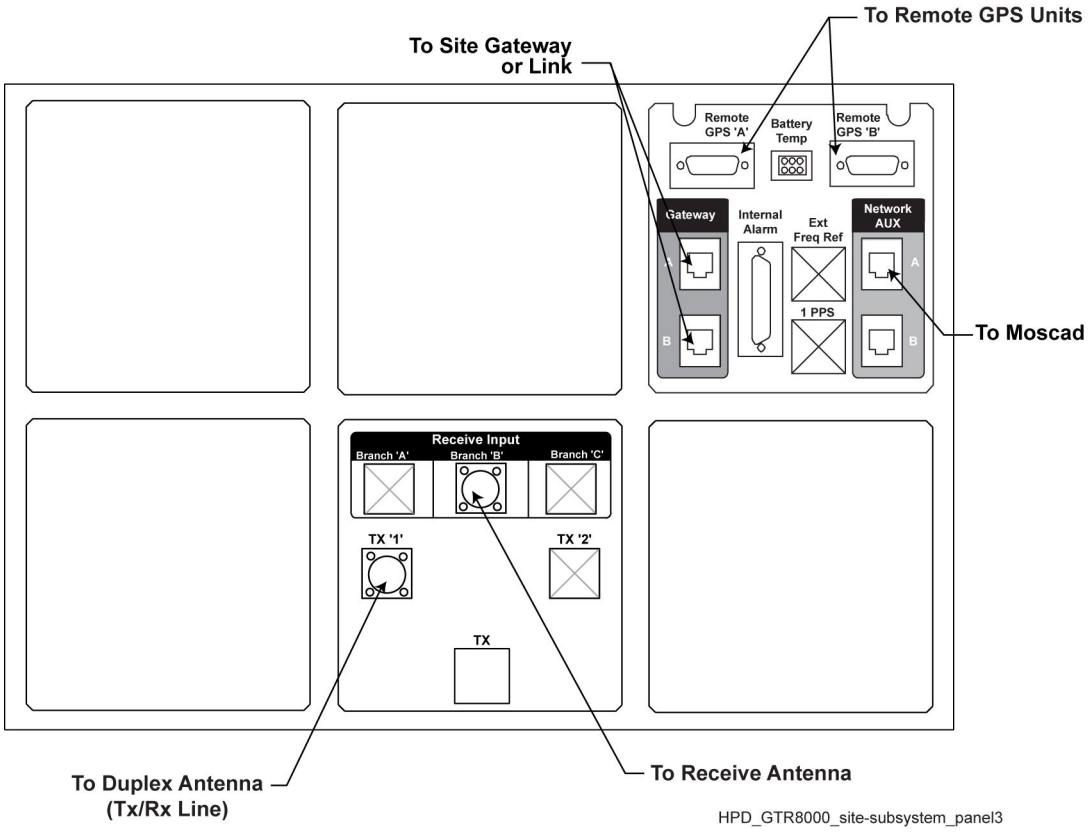
IMPORTANT

Do not remove the label from a connector location until you insert the connector.

3.4.7.1 Junction Panel Connections

External connections can be made at the GTR 8000 Site Subsystem. The RF connections are also illustrated in the Rx and Tx path diagrams in 1.4 RFDS Components, page 1-3.

Figure 3-10 Junction Panel for the GTR 8000 Site Subsystem



NOTE

For HPD Overlay sites, the Gateway A and B connections link directly to Site Switches A and B instead of Gateways.

Table 3-6 GTR 8000 Site Subsystem Junction Panel Connections

Port / Type	Device this connects to:	Port / Type	Description
GatewayA port, RJ-45	Primary Site Gateway	LAN 1, RJ-45	Ethernet link between site controller A and the primary site gateway.
GatewayB port, RJ-45	Secondary Site Gateway (optional)	LAN 1, RJ-45	Ethernet link between site controller B and secondary site gateway (if installed).
Network AUX A, RJ-45	MOSCAD Network Fault Management (NFM)	LAN Port 1, RJ-45	Ethernet link for MOSCAD NFM device.
Network AUX B, RJ-45	Auxiliary site equipment such as a site gateway	LAN 1, RJ-45	This port is available for devices that need to be connected to the network, including a site gateway, if it is included at the site.
Battery Temp	Backup Battery Temperature Sensor		See battery temperature sensor instructions for connection requirements.
Remote GPS A, DB-15	Lightning Arrestor / RGPS Unit A	Line terminals	See the *GCP 8000 Site Controller* manual for terminal connection details on the lightning arrestor.
Remote GPS B, DB-15	Lightning Arrestor / RGPS Unit B	Line terminals	See *GCP 8000 Site Controller* manual for terminal connection details on the lightning arrestor.
Rx-B, N-type	Receive antenna		RF coax to receive antenna.
Rx-A, N-type	Transmit/receive antenna		RF coax to transmit/receive antenna.
Internal Alarm, DB-25			Not in use.

3.5 Installation/Troubleshooting Tools

In addition to the general tools needed for site installation activities, a service monitor is used specifically for testing the equipment.

To place an order, contact Motorola at:

Phone: 1-800-422-4210 ext. 6883

TTY Phone: 1-866-522-5210

Motorola Online users: Web: http://www.motorola.com/businessonline

Fax: 1-800-622-6210

3.5.1 Quick Connect RF Coaxial Adapters for GTR 8000 Base Radio Support

The GTR 8000 Base Radio employs a number of "QN" and "QMA" Quick Connect RF connectors in its design. The following RF adapters are available from Motorola and can be used to connect test equipment to the various station devices for troubleshooting purposes.

Table 3-7 Quick Connect RF Coaxial Adapters for GTR 8000 Base Radio Support

Type	Adapter / Connector description	Motorola Part Number
"N"/QN	Female "N" to Male QN	5886055Y01
"N"/QN	Female "N" to Female QN	5886055Y10
"N"/QN	Male "N" to Male "QN"	5886055Y05
QN	Right Angle Male QN cable plug for RG-400 coax	2871002H01
QN	Right Angle Male QN cable plug for RG-213 coax	2886067Y01
N/QMA	Female "N" to Male QMA	5886055Y06
N/QMA	Female "N" to Female QMA	5886055Y07
QMA/QMA	Female QMA to Female QMA	5886055Y08
QMA/QMA	Male QMA to Male QMA	5886055Y09
7/16/QN	Female 7/16 to male QN	5886055Y03
7/16/QN	Male 7/16 to Male QN	5886055Y02
7/16/QN	"Female 7/16 to female QN Intermod test adaptor"	5886055Y04
7/16/QN	"Male 7/16 to female QN Intermod test adaptor"	5886055Y11

3.6 Device Software Installation Prerequisites

When and where to use:
This process provides a list of items to have access to before you can complete the device software installation and begin the configuration procedures in the “Configuration” chapter.

Process Steps

1 Transfer and install new software to a device using Software Download Manager. See 3.7 Using Software Download, page 3-31.

2 Ensure that the ASTRO® 25 system CDs and DVDs are available to you. Specifically, you need the Motorola Device OS Image CDs. See 3.8.2 Loading Device OS Images to the UNC, page 3-36.

3 Ensure that you have the user names, passwords, and procedures to access the devices on the network. For specific user names and passwords to access devices on the network, contact your system administrator.

Set up the users in the IT Admin group in Active Directory Users and Computers. See the *Authentication Services* manual.

---

4 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

NOTE

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

---

5 Ensure that you have the default credentials (local accounts, central authentication, and SNMPv3) for the device being installed, as well as updated passwords for those types of accounts (so that you can change the password once you install the device). Contact your system administrator, if you do not have this information. See the *SNMPv3* manual or see 8.2.4.2 Resetting Passwords and SNMPv3 Passphrases, page 8-5 for more information.

6 Ensure that the device is configured 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.

7 

NOTE

This step is applicable to systems with AAA Servers, Domain Controllers, or Syslog Servers.

To use the VoyenceControl component of the Motorola 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
- *Securing Protocols with SSH* manual

3.7 Using Software Download

The Software Download (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.

Data transfer can be installed using the following methods:

- Clear SWDL – transfer operations without security, based on the File-Transfer Protocol (FTP)
- Secure SWDL – transfer operations are encrypted, based on the Secure File-Transfer Protocol (SFTP)

NOTE

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.

IMPORTANT

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.

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

Software Download can be accomplished in two ways:

- Site Software Download – is a Network Management application that allows you to transfer and install application software from any location within a network. The software download application resides on the Network Management Client computer and a computer loaded with the CSS application. From either of the computers, you can select device types to which to download software. Site Software Download allows you to select the zone, site, device types, and software download operation to perform.
- 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 computer loaded with the CSS application either connected directly to the device or connected to the network.

NOTE

Conventional devices, GPB 8000 Reference Distribution Modules, and 3600 base radios are supported only in single device mode.

SWDL transfers and installs software to the GCP 8000 Site Controllers through a direct connection to the front Ethernet port. For the GCM 8000 Comparator, SWDL transfers and installs software only through the network LAN switch. 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 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 is done in the background without interruption of services at the site. An install causes the site controller to reset and load the RAM from the bank that was installed with the new software.

NOTE

- When performing a site software download, the site controller coordinates the software transfer for all base radios, receivers and/or comparators installed at the site.
- A site software download can only be performed on a trunked ASTRO® 25 system.

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 computer with CSS or a network management client before software download is performed on the site.

The system downloads software to the site controllers, comparators, receivers, and/or base radios 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* 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.

3.8 Installing Devices Using 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.

The UNC is not applicable for K1/K2 or non-networked sites.

Process Steps

1	Discover the device in the UNC. See 3.8.1 Discovering a Device with the UNC, page 3-34.
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 3.8.2 Loading Device OS Images to the UNC, page 3-36.
4	Enable FTP services on the UNC. See 3.8.3.1 Enabling FTP Service, page 3-38.
5	Transfer and install the OS image to the device. See 3.8.3.2 Transferring and Installing the OS Image, page 3-38.
6	Inspect the device properties for the transferred and installed software. See 3.8.3.3 Inspecting Device Properties for Transferred and Installed Software, page 3-42.
7	Disable FTP services for the UNC. See 3.8.3.4 Disabling FTP Service, page 3-43.

3.8.1 Discovering a Device with 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.

NOTE

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 Steps

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 base radio.
2	Log on to the UNC Wizard from the Network Management (NM) client, by double-clicking the **Internet Explorer** icon on the desktop. **Step result:** The Internet Explorer browser opens.

3 Enter: **`http://ucs-unc0<Y>.ucs:9443/UNCW`** in the **Address** field.

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

Step result: The UNC Wizard launches and a login dialog box appears.

---

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

Step result: The UNC Wizard appears.

---

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

Step result: 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**, **Site ID**, and then click **Submit**.

Step result: 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).

Step result: The UNC client launches and then a login dialog box appears.

---

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

Step result: VoyenceControl launches.

NOTE

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

---

10 Press F7 (Schedule Manager).

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

---

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

NOTE

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, select **RF Site Level Configuration**, **Channel** to verify the devices. Choose **Zone**, if multiple zones exist.

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

3.8.2 Loading Device OS Images to the UNC

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

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 Steps

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.

Step result: The UNC **Server Administration** menu appears.

2 Select **OS Images Administration** from the menu. Press ENTER.

Step result: The OS **Images Administration** menu appears.

3 Select **Load new OS images** from the menu. Press ENTER.

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

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

Step result: The drive light starts blinking on the server.

5 When the drive light stops blinking, press ENTER.

Step result: The OS images load on the UNC.

6 Select **View OS Images** from the menu. Press ENTER.

Step result: The device software image appears.

7 Select **Eject CD** from the menu. Press ENTER.

Step result: The media ejects from the drive on the server.

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

9 To log out of the server. Press ENTER.

Step result: The **User Configuration Server Administration** menu appears.

10 Press ENTER again.

Step result: The prompt appears.

3.8.3 Loading Software to a Device

NOTE

These procedures are for a single device download. For a site download, see 3.7 Using Software Download, page 3-31.

The following procedures describe how to load software images onto Unified Network Configurator (UNC) and download and install this software to the device. However, before installing the software, FTP service must be enabled.

3.8.3.1 Enabling FTP Service

Prerequisites:
Before installing the OS software, enable FTP services.

Procedure Steps

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.

Step result: The UNC **Server Administration** menu appears.

2 Select **Unix Administration** from the menu. Press ENTER.

Step result: The **Unix Administration** menu appears.

3 Select **FTP Services** from the menu. Press ENTER.

Step result: The **FTP Services** menu appears.

4 Select **Enable FTP service** from the menu. Press ENTER.

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

3.8.3.2 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 Steps

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

NOTE

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).

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

Figure 3-11 VoyenceControl Welcome Page

NOTE

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

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

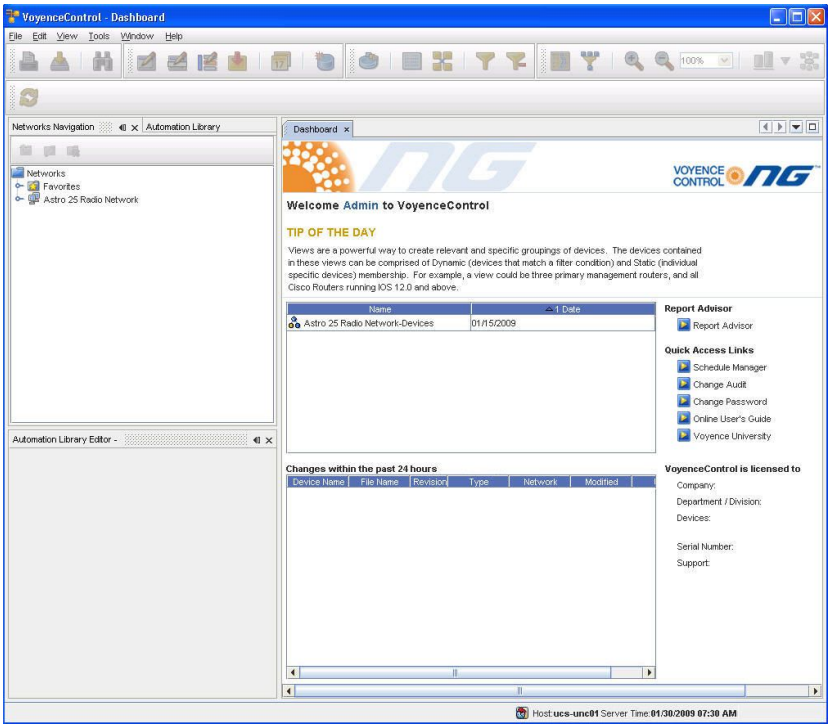
Step result: A VoyenceControl client session launches with the login window.

Figure 3-12 VoyenceControl Login Window

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

Step result: The **VoyenceControl Dashboard** appears.

Figure 3-13 VoyenceControl Dashboard



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

Step result: The list of options expands.

5 Double-click **Motorola <device>** from the navigation pane.

Step result: The view opens and all currently discovered devices appear.

---

6 Select **Tools → OS Inventory** from the menu.

NOTE

You can also press F9 to select the OS Inventory.

Step result: A list of the OS images appears.

---

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

NOTE

These images were automatically created during the 3.8.2 Loading Device OS Images to the UNC, page 3-36 procedure.

---

8 Under **Networks** in the navigation pane, select one or more devices from the same device class, right-click the selections, then choose **Update OS Image** from the menu.

Step result: The **Select OS Image** window appears.

---

9 Select **Software Image**. Click **Next**.

Step result: The **Update OS Image** window appears.

---

10 Select each device that appears in the **Selected Devices** section.

Step result: This associates a version to a device instance.

NOTE

In most cases, the “summary of device partitions” are already set up and the values in step 10 through step 13 must be verified.

---

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

NOTE

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

---

12 Select the image for this device from the **Selected Image** section.

NOTE

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

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

---

13 Click **Add**.

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

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

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

NOTE

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

15 Click **Schedule**.

Step result: The **Schedule Push Job** window appears.

16 Configure the schedule information. Click **Approve and Submit**.

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

NOTE

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

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

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

3.8.3.3 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 Steps

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

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

NOTE

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

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

Step result: The **Device Properties** window appears.

NOTE

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

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

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

Step result: The **Chassis** property tree expands.

5 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.

NOTE

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

3.8.3.4 Disabling FTP Service

When and where to use:
After the transfer and installation of the software, disable the FTP service.

Procedure Steps

1 Launch an 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.

Step result: The **UNC Server Administration** menu appears.

2 Select **Unix Administration** from the menu. Press ENTER.

Step result: The **Unix Administration** menu appears.

3 Select **FTP Services** from the menu. Press ENTER.

Step result: The **FTP Services** menu appears.

4 Select **Disable FTP service** from the menu. Press ENTER.

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

5 Back out of the menus by pressing Q three times.

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

7 Enter: **`exit`** again.

Step result: You have successfully logged out of the application.

8 Close the PuTTY connection.

4 GTR 8000 Site Subsystem Configuration

This chapter details configuration procedures relating to GTR 8000 Site Subsystem.

Proper software/hardware configuration for the GTR 8000 Site Subsystem requires the following activities:

- Updating factory-installed HPD base radio application software
- Setting parameters in a configuration file stored on the transceiver module that impacts both base radio and RF Distribution System (RFDS) functionality
- Setting DIP switches on RFDS receive multicoupler/low noise amplifier (RMC/LNA) modules

NOTE

For configuration of the GCP 8000 Site Controller, see the *GCP 8000 Site Controller* manual.

4.1 Configuration Software

Configuring a device requires loading two software applications on the service computer: 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.

NOTE

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 K1/K2 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 program locally provides the means to test the site before making it available for system operation.

4.2 Discovering Devices in the UNC

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

Process Steps

1 Use the UNC Discovery Wizard to:

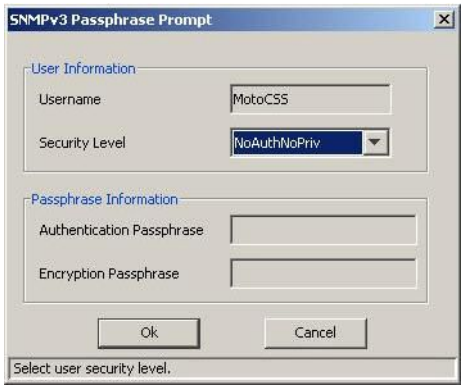
- Discover the devices.
- Upload configurations for the devices.
- Generate changes for non-compliant devices.

2 Approve jobs (if any).

4.3 Security/Authentication Services

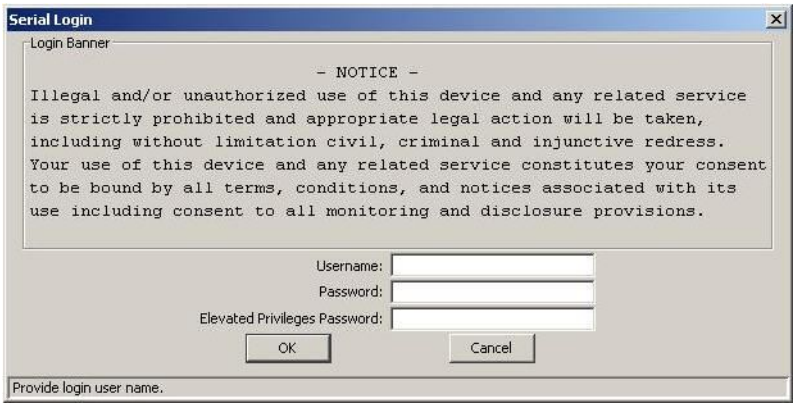
If the device supports SNMPv3 protocol, a pop-up dialog box appears displaying the SNMPv3 Password Prompt when logging in to a device through Configuration/Service Software (CSS) using an Ethernet connection. Enter your Authentication Password and Encryption Password if the chosen security level requires inserting these credentials. If Authentication Services are not enabled on a device, click **OK** when the pop-up window appears. For configuration details, see the *Information Assurance Features Overview*, *Software Download*, and *SNMPv3* manuals. See Figure 4-1.

Figure 4-1 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. If Authentication Services are enabled on a device, enter your Username, Password, and Elevated Privileges Password, if the chosen security level requires inserting these credentials. 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. See Figure 4-2.

Figure 4-2 CSS Login Banner



4.4 Configuring a Device Using CSS

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

NOTE

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 Using CSS

Prerequisites:
CSS must be loaded on the computer.

When and where to use:
Follow this process to initially configure a device using CSS.

Process Steps

1 Perform the following configuration steps that require a serial connection. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.

   a. Set the IP address of the device. See 4.4.3.1 Setting the Device IP Address Using CSS, page 4-6.

   b. Set the serial security services. See 4.4.3.2.1 Setting the Serial Security Services Using CSS, page 4-8.

2 Perform the following configuration steps that require an Ethernet connection. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

   a. Set the current date and time in CSS. See 4.4.5.1 Setting the Date and Time Using CSS, page 4-13.

   b. Change the SNMPv3 configuration and user credentials from CSS on a selected device in the site. See 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14.

   c. Create, update, or delete an SNMPv3 user. See 4.4.5.2.1 Adding or Modifying an SNMPv3 User Using CSS, page 4-17.

   d. Verify the SNMPv3 credentials. See 4.4.5.2.2 Performing an SNMPv3 Connection Verification Using CSS, page 4-18.

   e. Configure DNS using the CSS. See Chapter 7, “Configuring DNS Using CSS” in the *Authentication Services* manual.

   f. Set the SWDL transfer mode. See 4.4.5.4 Setting the SWDL Transfer Mode Using CSS, page 4-19.

   g. Configure for SSH. See Chapter 4, “Configuring SSH for RF Site Devices and VPMs Using CSS” in the *Securing Protocols with SSH* manual.

   h. Enable RADIUS Authentication using the CSS. See Chapter 7, “Configuring RADIUS Sources and Parameters Using CSS” in the *Authentication Services* manual. Make sure that the devices have been added to the RADIUS servers on the domain controllers as RADIUS clients.

   i. Enable Centralized Authentication using the CSS. See Chapter 7, “Enabling/Disabling Centralized Authentication Using CSS” in the *Authentication Services* manual.

   j. Set the Local Cache Size for Centralized Authentication using the CSS. See Chapter 7, “Setting the Local Cache Size for Central Authentication Using CSS” in the *Authentication Services* manual.

   k. Customize the login banner text using CSS (optional). See 4.4.5.3 Customizing the Login Banner Using CSS, page 4-19.

   l. Enable Centralized Event Logging using CSS (if required by your organization). See Chapter 6, “Enabling/Disabling Centralized Event Logging on Devices Using CSS” in the *Centralized Event Logging* manual.

   m. Set the NTP Server Settings. See 4.4.5.5 Setting the NTP Server Settings, page 4-20.

3 Set up the local Password Configuration using the CSS (optional). See 4.4.5.6 Setting Up the Local Password Configuration Using the CSS, page 4-21.

4 Program the device. See 4.4.6 CSS Configuration Parameters for the GTR 8000 Base Radio (HPD), page 4-23.

4.4.2 Connecting Through a Serial Port Link

Prerequisites:
This procedure assumes that the Configuration/Service Software (CSS) application is loaded on your computer. See the *Private Network Management Client* manual if necessary. This procedure describes the steps required to perform a serial connection.

When and where to use:
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 Steps

1 Connect a serial cable to a laptop or computer 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 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**.

Step result: The **Connection Screen** dialog box appears.

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

Step result: 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 computer.

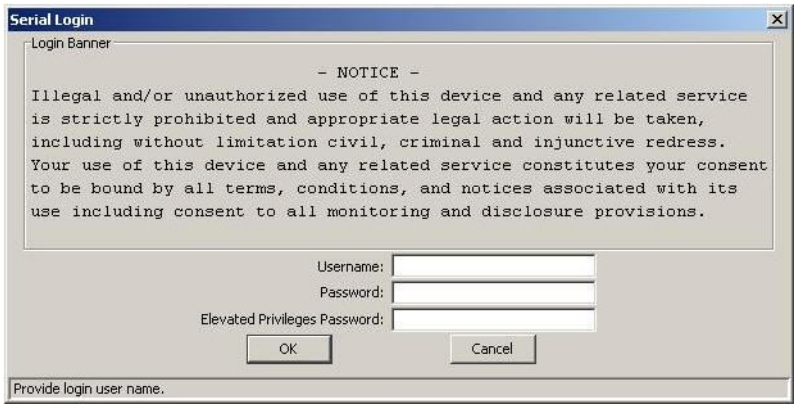
6 In the **Baud Rate** field, select the baud rate with which you want to communicate with the device.

- Baud Rate 19200

7 Click **Connect**.

Step result: A login/password prompt screen appears.

Figure 4-3 CSS Login Banner



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

- If a domain controller is available on the network, type 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, type the **Username** and **Password** for the local bts_service account.
- If the **Elevated Privileges Password** field is active, type the **Elevated Privileges Password** that was set up for this device.

NOTE

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. See 4.4.3.2.1 Setting the Serial Security Services Using CSS, page 4-8 to configure Authentication Services on the device.

9 Click **OK** to access the device and close the dialog box.

Step result: The blank CSS main window appears.

NOTE

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 are configuration parameters in the Configuration/Service Software (CSS) using a serial connection.

4.4.3.1 Setting the Device IP Address Using 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 8.2.4.2 Resetting Passwords and SNMPv3 Passphrases, page 8-5.

NOTE

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

Procedure Steps

1. Connect to the device using Configuration/Service Software (CSS) through a serial port link. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.
2. Select **Tools → Set IP Address/Box Number** from the menu.

   Step result: 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. Click **OK** to close the dialog box.
6. Click **Reset** to initiate a hardware restart.

   Step result: SNMPv3 user credentials reset to their factory default values.
7. Click **Close** to close the dialog box.
8. Proceed to 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14 to reconfigure the SNMPv3 user credentials.

4.4.3.2 Serial Security Services Using CSS

This section describes how to enable the secure services and change the device password. Perform these steps before changing the SNMPv3 configuration and user credentials from Configuration/Service Software (CSS) 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 Software Downloads (SWDL). Only certain SWDL 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 Chapter 7, “Enabling/Disabling Centralized Authentication Using 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 Using CSS

Prerequisites:
Ensure 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 8.2.4.2 Resetting Passwords and SNMPv3 Passphrases, page 8-5. 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 Steps

1 Connect to the device using CSS through a serial port link. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.

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

Step result: The **Security Services Configuration** dialog box opens.

3 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**. 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**.

Step result: A **Change Account Password** dialog box opens.

7 Enter the old password, then enter a new password and confirm the new password before clicking **Change Password**.

8 Click **OK** to save the new password.

Step result: The **Change Account Password** dialog box closes.

4.4.3.3 Resetting SNMPv3 User Credentials to Factory Defaults Using CSS

Prerequisites:
Ensure the required credentials information (local service account password and elevated privileges password) to configure the site devices are available 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 Solution 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 Steps

1. Connect to the device using CSS through a serial port link. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.

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

   Step result: The **Reset SNMPv3 Configuration** dialog box opens.

3. Click **Reset SMPv3 Configuration**.

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

4. Click **Exit**.

   Step result: The **Reset SNMPv3 Configuration** dialog box closes.

5. To reboot the device for the SNMPv3 user credentials to take effect:
   a. From the menu, select **Tools → Set IP Address/Box Number** or **Set IP Address/BR_CM Pairing Number**.

      Step result: The dialog box appears.

   b. Click **Reset**.

      Step result: The device reboots.

6. Proceed to 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14.

4.4.4 Connecting Through an Ethernet Port Link

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

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

Procedure Steps

1 Connect a computer (either laptop or desktop) to a device:

a. Connect an Ethernet straight through cable between the Ethernet port on the computer and the appropriate LAN switch either locally at a site or remotely through the network.

- For a base radio or receiver, set the IP address of the laptop to the 192.168.1.x subnet (where x is any number between 2 and 253). Configure the speed/duplex setting of the computer Ethernet interface to 10 Mb half duplex.
- For a site controller or comparator, set the IP address of the laptop to an address on the subnet of the local site, which varies depending on the site and zone numbers.
- For a comparator, the 10/100Base-T LAN is not the default Ethernet port setting. To set the correct port speed and duplex, see the *CSS Online Help*.

NOTE

Normally the computer is connected to the appropriate LAN switch either locally or remotely through the network. Do not connect directly to a device unless downloading the software individually to that device.

b. Start the computer.

2 Open the CSS application.

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

Step result: The **Connection Screen** appears.

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

5 If connected through the LAN switch, specify the IP address for the device in the **Ethernet Settings** area. Perform one of the following actions:

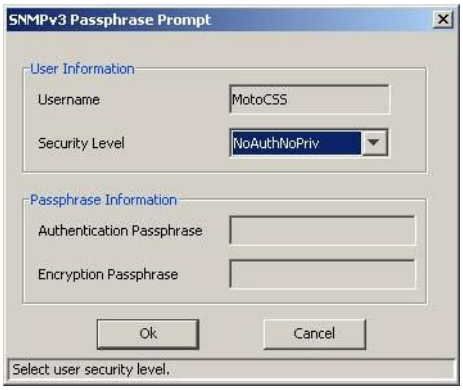
If...	Then...
If you know the IP address for the device,	perform the following actions: 1. Enter the IP address for the device in the **Device IP Address** field. 2. Go to step 6.
Trunked Device: If you do not know the IP address, but know the system identification of the device (the zone, site, subsite, and device ID of the device),	perform the following actions: 1. Click **Fetch DNS Entry** to open the **DNS IP Address Calculation Screen** dialog box. 2. Select the desired device type from the **Device** list box. 3. Enter the proper values in the **Zone**, **Site**, **Subsite**, and **Device ID** fields. **NOTE** Some fields, such as **Subsite**, do not allow entries for some devices. Therefore, select the device first. 4. Click **OK**. **Step result**: The Domain Name Services (DNS) information of the device automatically appears in the **Device IP Address** field. 5. Go to step 6.
Conventional Device: If you do not know the IP address,	perform the following actions: 1. Establish a serial connection to the device. See 4.4.2 Connecting Through a Serial Port Link, page 4-4. 2. For a base radio, receiver or comparator, select **Tools → Set IP Address/BR_CM Pairing Number**. For a site controller or Reference Distribution Module (RDM), select **Set IP Address/Box Number**. 3. Read the IP address from the **Device IP Address** field. 4. Re-establish an Ethernet connection and repeat steps 1 through 4. 5. Enter the IP address for the device in the **Device IP Address** field. 6. Go to step 6.

6 If connected directly to the Ethernet service port of the device, click **Front Panel Ethernet**.

7 Click **Connect** to make the connection.

Step result: If this device is SNMPv3-capable, an **SNMPv3 Passphrase Prompt** dialog box appears. Go to step 9.

Figure 4-4 SNMPv3 Passphrase Prompt



NOTE

For Windows XP computers: If after clicking **Connect**, a "comm.Error" is encountered when connecting to the front panel Ethernet port on a base radio or receiver, follow the procedure in step 8 to repair the local area connection (LAN) or high-speed Internet connection.

8 The front panel Ethernet port on base radios and receivers have a fixed IP address (192.168.1.1). However the Ethernet MAC ID for each front panel connection is unique to each base radio and receiver. A communication error can occur when configuring multiple base radios and receivers through the front panel Ethernet port. When connected to the initial base radio or receiver, Windows XP associates the fixed IP address of the front panel port with the front panel Ethernet MAC ID. When connecting to the next base radio or receiver, the Address Resolution Protocol (ARP) cache is not cleared and causes a communication error. This procedure clears the ARP cache and allows for a new Ethernet MAC ID to be associated with the fixed IP address.

a. In Windows XP, from the **Start** menu, select **Settings → Network Connections → Local Area Connection**

b. Click the **Support** tab and select **Repair**.

Step result: The **Repair Local Area Connection** window opens and displays the different caches that are cleared.

c. Reconnect the Ethernet cable to the front panel Ethernet port, if not connected.

9 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.

NOTE

See 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14 to configure or change SNMPv3 configuration and user credentials on the device.

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

Step result: The parameters download from the device to the computer. 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 are configuration parameters in the Configuration/Service Software (CSS) using an Ethernet connection.

4.4.5.1 Setting the Date and Time Using 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 from a remote Configuration/Service Software (CSS).

NOTE

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

Procedure Steps

1 Connect to the device using CSS through an Ethernet port link. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

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

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

Step result: The date and time is set.

4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS

Prerequisites:
Ensure that you have the required SNMPv3 credentials information (Authentication passphrase, Encryption passphrase, and Authoritative Engine ID) to configure the device available 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 8.2.4.2 Resetting Passwords and SNMPv3 Passphrases, page 8-5. 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.

NOTE

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 Steps

1 Connect to the device using CSS through an Ethernet port link. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

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

Step result: The **SNMPv3 Login/Connection** dialog box appears with **MotoAdmin** as the selected SNMPv3 user.

3 Enter the appropriate **Authentication** and **Encryption Passphrases** in the fields.

NOTE

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: 1. Enter the IP address for the device in the **Device IP Address** field. 2. Go to step 5.
If you do not know the IP address, but know the system identification of the device (the zone, site, subsite, and device ID of the device),	perform the following actions: 1. Click **Fetch DNS Entry** to open the **DNS IP Address Calculation Screen** dialog box. 2. Select the desired device type from the **Device** list box. 3. Enter the proper values in the **Zone**, **Site**, **Subsite**, and **Device ID** fields. NOTE Some fields, such as **Subsite**, do not allow entries for some devices. Therefore, select the device first. 4. Click **OK**. **Step result**: The Domain Name Services (DNS) information of the device automatically appears in the **Device IP Address** field. 5. Go to step 5.

5 Click **OK**.

Step result: A connection is made with the selected device, the entered **SNMPv3 admin** passphrases are authenticated, and the **Configure SNMPv3 Users** dialog box appears. If the connection fails, a message appears.

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

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

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 **Security Level** list in the **User Information** form, select the security level.

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.

Step result: The security level of the selected user is set.

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.

---

8 To change the Authentication Passphrase for the selected SNMPv3 user (if applicable to the selected security level):

a. In the **Authentication Passphrase** form, enter the passphrase into the **Old Passphrase** field.

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.

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

a. 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):

a. In the **Encryption Passphrase** form, enter the old passphrase into the **Old Passphrase** field.

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. 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):

a. In the **Authoritative Engine ID** section, select the desired current engine ID from the **Current Engine ID List**.

b. Enter the new engine ID into the **New Engine ID** field.

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 4.4.5.2.1 Adding or Modifying an SNMPv3 User Using CSS, page 4-17.

4.4.5.2.1 Adding or Modifying an SNMPv3 User Using CSS

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

Procedure Steps

1 In the Configuration/Service Software (CSS), log in using the appropriate credentials.

Step result: The **Configure SNMPv3 Users** dialog box appears.

2 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.

Step result: A **Confirmation** dialog box appears and asks if you want to continue.

3 Click **Yes**.

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

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

NOTE

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

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

6 Click **Cancel** to exit the **Configure SNMPv3 Users** dialog box.

Step result: The **Configure SNMPv3 Users** dialog box closes, and the CSS main window returns.

4.4.5.2.2 Performing an SNMPv3 Connection Verification Using 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 Steps

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.
2. When the passphrase prompt screen opens, select the configured security level and enter the required passphrases.
3. Click **OK** if the connection was successful.

4.4.5.3 Customizing the Login Banner Using CSS

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

Procedure Steps

1. Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.
2. From the menu, select **Security → Device Security Configuration → Remote Access/Login Banner (Ethernet)**.

   Step result: The **Remote Access/Login Banner** screen appears displaying the **Remote Access Configuration** tab.
3. 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 Using CSS

This procedure sets the Software Download (SWDL) transfer mode before performing a SWDL on the device.

When and where to use:
Follow this procedure to set the SWDL transfer mode to FTP (clear) or SFTP (secure) for the device.

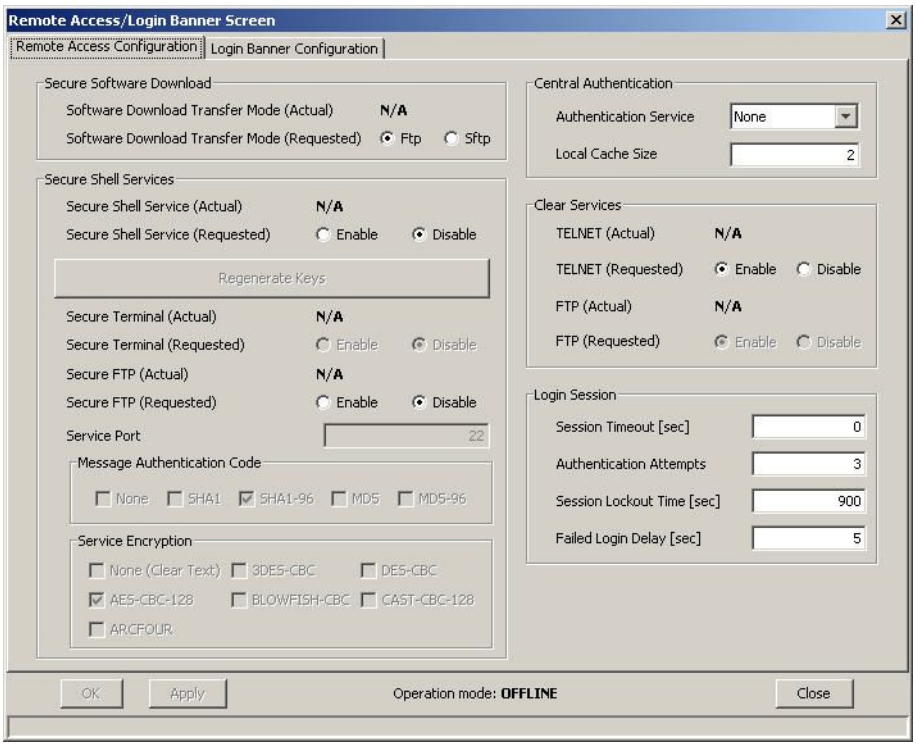
Procedure Steps

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

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

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

Figure 4-5 Remote Access Configuration Tab



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

NOTE

Secure SHell (SSH) service and Secure FTP services are automatically set to **Enabled** and grayed out when you choose **Sftp**.

4.4.5.5 Setting the NTP Server Settings

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

For security purposes, the base radio or receiver can restrict NTP messages from only the site controller. This restriction can be accomplished by configuring two site controller IP addresses into the **NTP Server IP Address** fields on the base radio or receiver.

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

When the IP addresses exceed the total, removing IP addresses allows the Unified Event Manager (UEM) to be identified as the current manager and can handle traps for the device.

4.4.5.6 Setting Up the Local Password Configuration Using the 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*.

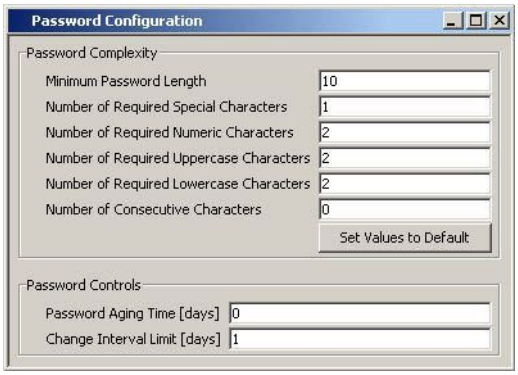
Procedure Steps

1 Connect to the device using Configuration/Service Software (CSS) through an Ethernet port link. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

2 In the navigation pane, click the **Password Configuration** element.

Step result: The **Password Configuration** window appears.

Figure 4-6 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 GTR 8000 Base Radio (HPD)

Prerequisites:
Before proceeding with this process, complete the initial configuration of the device in 4.4.1 Initial Configuration of a Device Using CSS, page 4-3.

When and where to use:
Use this process as a guide to configure the base radio for the HPD GTR 8000 Site Subsystem. For configuration parameters, see the following in the *CSS Online Help*:

- **GTR 8000 Base Radios:** HPD Remote/Expandable Site
- **GCP 8000 Site Controllers:** Site Controller > Configuration & Service Help > HPD Site Controller

Process Steps

1. Connect to the base radio through an Ethernet port link and then read the configuration file from the base radio. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.
2. Click **System** in the tree view and enter a hexadecimal value (between 001 and FFE) in the **System Id** field.
3. Click **Site** in the tree view and complete the fields.
4. Click **Channel** in the tree view and complete the fields.
5. Click **Configuration** in the tree view and complete the fields on all four tabs.

As part of RMC configuration, the DIP switches must be set on the RMC/LNA modules. See 4.4.9 Setting RMC System Gain, page 4-29.

6 Click **Network Services Configuration** in the tree view and complete the fields on the three tabs.

NOTE

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.

7 Click **Password Configuration** in the tree view and complete the fields.

NOTE

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

8 Select **File → Save As** from the menu to save the configuration data to a new archive file or **File → Save As** from the menu to overwrite an existing archive file.

IMPORTANT

Be sure to save any configuration changes to a local or network drive so that if the device fails, you can load your settings to a replacement device. If the configuration file is not saved to a local or network drive, you will need to repeat the setup steps after replacing a device.

9 Select **File → Write Configuration to Device** from the menu to write the configuration data to the device.

4.4.7 Configuring Tx Power Values and Battery Type

When and where to use:
As part of the site configuration process, the **Battery Type**, **Tx Power Level (Battery Backup)**, and **Tx Power Out** on the **Hardware Configuration** tab in Configuration/Service Software (CSS) must be configured.

Procedure Steps

1 Open CSS.

2 Connect to the device through an Ethernet port link and then read the configuration file from the device. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

3 From the navigation tree, select **Configuration**.

Step result: The **Configuration** window appears.

4 Select the **Hardware Configuration** tab.

5 Enter a value in the field labeled **Tx Power Out (Watts)**.

6 Enter a value in the field labeled **Tx Power Level Battery Backup (Watts)**.

7 Select the **Battery Type** (manufacturer and model, or select the generic listing for the class of battery).

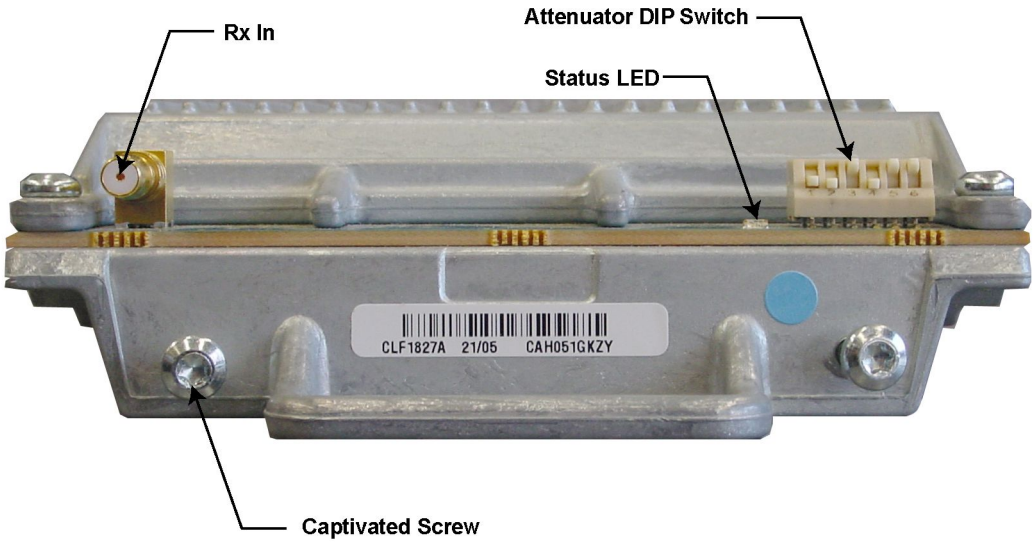
8 From the menu, select **File → Save** or **File → Save As** to save the configuration to an archive on your local or network drive.

9 From the menu, select **File → Write Configuration to Device** to write the configuration to the device.

4.4.8 Setting RMC Attenuation

To adjust the RF gain for different configurations, the attenuation level applied to receivers can be set from the DIP switches (on the front of Cabinet RMC/LNA modules).

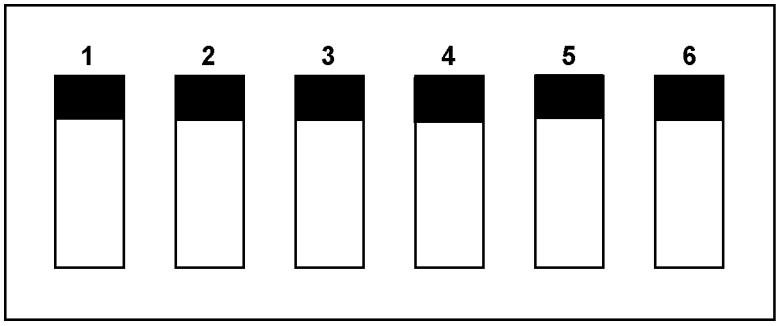
Figure 4-7 Cabinet RMC/LNA Module (Front View)



GTR8000_RFDS_XS_RMC_Cabinet_Front1

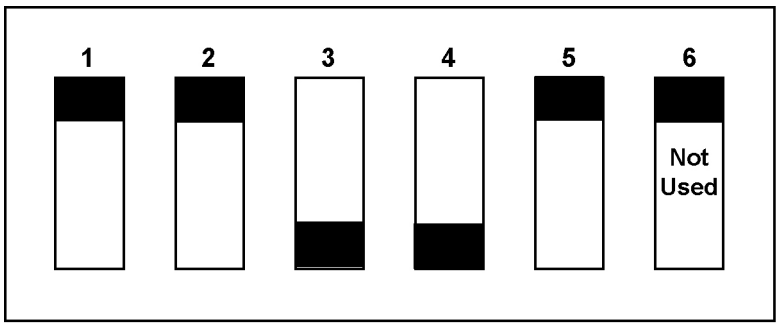
The following are examples of how the DIP switch positions (0 and 1) create a binary system for setting dB attenuation values.

Figure 4-8 RMC DIP Switch Example: 0 dB



HPD_GTR8000_RFDS_RMC_Dipswitch2

Figure 4-9 RMC DIP Switch Example: 12 dB



HPD_GTR8000_RFDS_RMC_Dipswitch1

To determine how to set each DIP switch for your configuration, see Table 4-1.

- **RMC Attenuator for Single Cabinet Sites with No Site RMC:** If your configuration displays in the Single Cabinet with No Site RMC Switch Settings table, set the DIP switches on your Cabinet RMC/LNA modules to the positions indicated in that table for your configuration. If your configuration does **not** display in this table, it does not include Cabinet RMC/LNA modules or it does not use the DIP switch settings on your Cabinet RMC/LNA modules. See Table 4-2 RMC Attenuator Settings for Single Cabinet Sites with No Site RMC.

4.4.8.1 RMC Attenuator DIP Switch Settings

NOTE

Although the DIP switches on the RMC/LNA modules are numbered starting with the number 1 on the left, as shown in the RMC DIP Switch examples, this table starts with the number 5 on the left because switch 5 represents the most significant digit in the binary system that the switches provide for setting a dB value.

Table 4-1 RMC Attenuator DIP Switch Settings

Required Attenuation (dB)	Position 5	Position 4	Position 3	Position 2	Position 1
0dB	0	0	0	0	0
1dB	0	0	0	0	1
2dB	0	0	0	1	0
3dB	0	0	0	1	1
4dB	0	0	1	0	0
5dB	0	0	1	0	1
6dB	0	0	1	1	0
7dB	0	0	1	1	1
8dB	0	1	0	0	0
9dB	0	1	0	0	1
10dB	0	1	0	1	0

Table 4-1 RMC Attenuator DIP Switch Settings (cont'd.)

Required Attenuation (dB)	Position 5	Position 4	Position 3	Position 2	Position 1
11dB	0	1	0	1	1
12dB	0	1	1	0	0
13dB	0	1	1	0	1
14dB	0	1	1	1	0
15dB	0	1	1	1	1
16dB	1	0	0	0	0
17dB	1	0	0	0	1
18dB	1	0	0	1	0
19dB	1	0	0	1	1
20dB	1	0	1	0	0
21dB	1	0	1	0	1
22dB	1	0	1	1	0
23dB	1	0	1	1	1
24dB	1	1	0	0	0
25dB	1	1	0	0	1
26dB	1	1	0	1	0
27dB	1	1	0	1	1
28dB	1	1	1	0	0
29dB	1	1	1	0	1
30dB	1	1	1	1	0
31dB	1	1	1	1	1

4.4.8.2 RMC Attenuator Settings for Single Cabinet Sites with No Site RMC

The required attenuation dB values shown in this table are also displayed on the Receive Multicoupler (RMC) Configuration tab in Configuration/Service Software (CSS), which must be used to set up system gain according to your configuration.

Cabinet RMC Settings must be the same in each cabinet. These settings provide maximum system dynamic range.

Table 4-2 RMC Attenuator Settings for Single Cabinet Sites with No Site RMC

System Noise Figure (dB)	System Input Intercept (dBm)	RFDS Gain (dB)	Cabinet RMC Attenuator Setting (dB)
4.5	4.8	13	0
4.8	5.8	12	1
5.2	6.7	11	2
5.6	7.7	10	3
6.1	8.6	9	4
6.6	9.6	8	5
7.2	10.5	7	6
7.8	11.3	6	7
8.5	12.2	5	8
9.3	13.0	4	9
10.1	13.8	3	10
10.9	14.6	2	11
11.7	15.3	1	12
12.6	15.9	0	13
13.5	16.5	–1	14
14.4	17.1	–2	15
15.4	17.6	–3	16
16.3	18.0	–4	17
17.3	18.4	–5	18
18.2	18.7	–6	19
19.2	19.0	–7	20
20.2	19.2	–8	21

4.4.9 Setting RMC System Gain

When and where to use:
System gain is automatically calculated when GTR 8000 Site Subsystem is selected as the configuration. The system gain entered differs depending on whether a Tower Top Amplifier (TTA) for this base radio is installed:

- **With a TTA**, calculate system gain from the antenna to the transceiver.
- **Without a TTA**, calculate system gain from the junction panel to the base radio.

Procedure Steps

1 Open Configuration/Service Software (CSS).

2 Connect to the device through an Ethernet port link and then read the configuration file from the device. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

3 Select **File → Read Configuration from Device** from the menu.

4 Select **Configuration** from the navigation tree in the left pane.

Step result: The Configuration window appears.

5 Select the **Receive Multicoupler (RMC) Configuration** tab.

6 Select **GTR 8000 Site Subsystem** configuration in the GTR 8000 Base Radio field.

Step result: Site RMC Attenuation is automatically calculated and displayed. System Gain is automatically calculated and displayed as 9 dB.

7 Select **File → Save** or **File → Save as** from the menu to save your RMC configuration to an archive on your local or network drive.

8 Select **File → Write Configuration to Device** from the menu to save your RMC configuration to the device.

Step result: The resulting system gain and site RMC attenuation are automatically used by the RMCs.

4.5 Using VoyenceControl to Configure Centralized Authentication on Devices

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.

VoyenceControl does not apply for a K1/K2 or non-networked site.

Process Steps

1. Configure Domain Name Service (DNS) on the device. See “Configuring DNS on RF Site and VPM Devices Using VoyenceControl” in the *Authentication Services* manual.
2. Configure Authentication Sources for the device. See “Configuring Authentication Sources for RF Site and VPM Devices Using VoyenceControl in the *Authentication Services* manual.
3. Configure RADIUS parameters for the device. See “Configuring Radius Parameters for RF Site and VPM Devices Using 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 Using VoyenceControl” in the *Authentication Services* manual.
5. Enable/Disable Centralized Authentication for the device. See “Enabling/Disabling Centralized Authentication on RF Site and VPM Devices Using 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 VPM's Using VoyenceControl” in the *Centralized Event Logging* manual.

5 GTR 8000 Site Subsystem Optimization

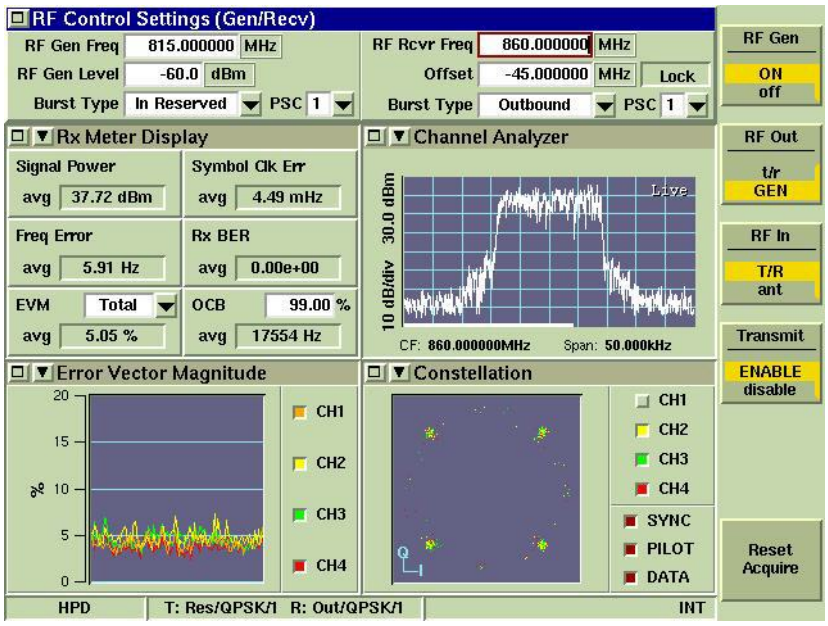
Your Motorola Field Representative or Motorola System Support Center (SSC)t can advise you on optimization activities required for your system, if any. See 8.4 Using Motorola Solution Support Center, page 8-6 in the Troubleshooting section of the documentation.

This chapter contains optimization procedures and recommended settings relating to GTR 8000 Site Subsystem.

5.1 Testing the GTR 8000 Site Subsystem Performance with a Service Monitor (for HPD)

The HPD Service Monitor is a diagnostic tool that may be used with an HPD base radio or HPD modem to test and measure the transmitter and receiver characteristics. The HPD service monitor can generate HPD signaling and can provide diagnostic information for received signaling.

Figure 5-1 HPD Service Monitor - Test Screen (Aeroflex 3900 Series Service Monitor)



The HPD Service Monitor may be connected with an HPD base radio to perform the following diagnostic tests (for additional tests, see the HPD service monitor manual). These tests are designed to determine whether the equipment is operating within specification. If it fails to meet specification, service may be required on an HPD base radio.

- **Measure Transmit Power:** See 5.1.3 Measuring HPD BR Tx Power, Frequency Accuracy, and Tx EVM, page 5-4.
- **Measure Frequency Accuracy:** See 5.1.3 Measuring HPD BR Tx Power, Frequency Accuracy, and Tx EVM, page 5-4.
- **Measure Error Vector Magnitude (EVM) for Transmitter:** See 5.1.3 Measuring HPD BR Tx Power, Frequency Accuracy, and Tx EVM, page 5-4.

- **Measure Receiver Sensitivity:** See 5.1.4 Measuring HPD BR Rx Sensitivity and Rx BER, page 5-8.
- **Measure Bit Error Rate (BER) for Receiver:** See 5.1.4 Measuring HPD BR Rx Sensitivity and Rx BER, page 5-8.

For additional information about using the service monitor, see the HPD service monitor manual or online help (accessed through the **Help** button on the front of the service monitor).

5.1.1 Setting Up the HPD Service Monitor for Testing the Base Radio

Procedure Steps

1 Plug a power cable into the AC port at the rear of the service monitor.

2 Connect a USB mouse to one of the two USB ports in the rear of the Service Monitor.

NOTE

The following procedures assume that a USB mouse is connected. If not, for instructions to "click" or "select" you can use the **TAB** and arrow buttons on the front of the service monitor. For instructions to select a soft key on the right side of the screen, use the unlabeled buttons on the front of the service monitor, pressing the button located next to the soft key on the screen.

3 Configure the Speed/Duplex setting in the PC's Ethernet interface to 10 Mb Half Duplex.

4 Connect to the base radio's transceiver module in CSS through an Ethernet connection. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

5 Select **Service → Test and Measurement Screen** from the menu.

Step result: The Test and Measurement Screen dialog box appears.

6 Disable the channel using the base radio being tested.

NOTE

The test procedures require the base radio's Rx and Tx cables to be connected to the HPD service monitor. Any calls present on the channel associated with the base radio are dropped from that channel. It is recommended that you disable the channel before performing the test procedures, so that the system does not attribute the loss of channel to a failure.

If the base radio is not already in service mode, click **Change to Service Mode**

Step result: A configuration dialog box appears.

7 Click **OK**.

Step result: The base radio does through a reset sequence to change modes. This reset sequence takes a few minutes.

8 After the base radio resets, re-open the Test and Measurement screen.

9 If measuring the base radio's transmit signal, connect the Tx connector at the rear of the base radio to the T/R (Transmit/Receive) port on the front of the service monitor. (Both are N-type RF connectors.)

10 If measuring the base radio's receive signal, connect the RX-A and RX-B ports at the rear of the base radio to the GEN port on the front of the service monitor, using a splitter.

11 Press the green power button on the front of the service monitor.

12 If the Test Screen is not displayed (see Figure 5-1), press the **Test** button on the front of the service monitor.

13 Locate the specifications for the base radio being tested. See 1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz), page 1-6.

14 If no further testing is needed, click **Change to Normal Mode** to return the base radio to normal operation.

5.1.2 Performing In-band Power Meter User Calibration

When and where to use:
The Aeroflex 3900 series High Performance Data (HPD) service monitor has two forms of power measurement:

- Broadband is similar to the working of an in-line wattmeter.
- In-band is performed after the RF signal is down converted to baseband by a Digital Signal Processor (DSP).

If the HPD service monitor runs continuously, it requires periodic calibration. Re-calibration is required only if the User Calibration Threshold is exceeded. The service monitor displays a flag at the bottom indicating to re-calibrate to maintain the accuracy indicated in the User Calibration Threshold.

For an HPD signal, only the in-band power meter is available. The in-band power measurement accuracy without a user calibration is ±1 dB. User calibration improves the accuracy at a specific frequency, bandwidth, and temperature by using the broadband power meter to correct the in-band power measurement. This correction occurs when an in-band user calibration is performed.

Procedure Steps

1 Press the **UTILS** button on the service monitor twice.

Wait for approximately 1 second or more before pressing the **UTILS** button the second time.

Step result: The **Utility Menu** screen appears.

2 Select **User Calibration** from the drop-down menu.

Step result: The **User Calibration** screen appears.

3 Click **Run User Calibration** in the upper right corner of the **User Calibration** screen.

The default user calibration setting is 1.0 dB. This setting means that a user re-calibration is not indicated on the HPD service monitor until the in-band power measurement has a potential of 1.0 dB error in the measurement (same as the basic in-band power meter accuracy). For HPD, a 0.5 dB value or lower is more appropriate. This value may require more frequent re-calibrations, but it provides better performance.

Step result: A **User Calibration** message box appears instructing you to remove all connectors from the ports.

4 Remove all connectors from the ports. Click **Continue**.

Step result: A progress bar appears showing the progress of the calibration process. The calibration completes in approximately 2 min.

Failure to remove all connectors and cables from the ports causes an inaccurate user calibration. Any connectors present causes a variation on the impedance seen by the instrument during calibration.

5.1.3 Measuring HPD BR Tx Power, Frequency Accuracy, and Tx EVM

In this procedure, the service monitor receives and provides readings on transmissions from the base radio.

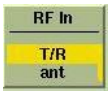
Prerequisites:
Setting Up the HPD Service Monitor for Testing the Base Radio.

Procedure Steps

1 Perform the service monitor setup steps in 5.1.1 Setting Up the HPD Service Monitor for Testing the Base Radio, page 5-2.

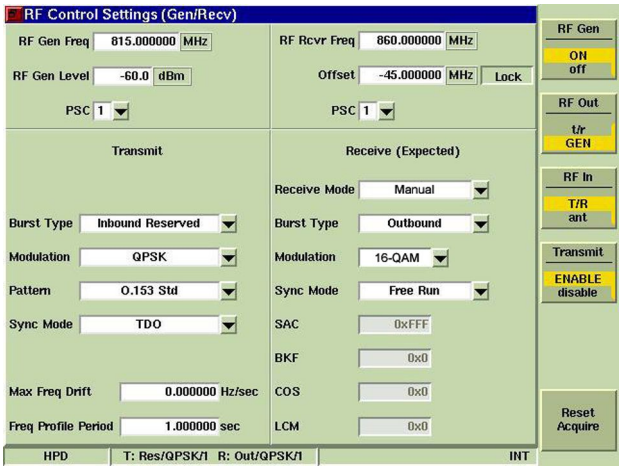
2 Configure the service monitor T/R port to receive transmissions from the base radio, as follows:

- Click the **T/R** soft key under **RF In** on the right side of the screen.



3 Maximize the RF Control Settings window, by clicking the upper left corner of the window.

Figure 5-2 HPD Service Monitor - RF Control Settings Window (Aeroflex 3900 Series Service Monitor)



4 Set RF Receiver Frequency, as follows:

a. Click the **RF Rcvr Freq** field in the upper right quadrant of the RF Control Settings window.

b. Press the number buttons on the front of the service monitor to enter a value in the **RF Rcvr Freq** field.

c. If **MHz** is not already displayed to the right of the RF Receiver Frequency value you entered, press the unlabeled button on the front of the service monitor next to the **MHz** soft key.

NOTE

The value entered should be within the frequency range specification for the GTR 8000 Base Radio configuration being tested. See 1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz), page 1-6 in the Description chapter of this documentation.

5 Select **1** from the drop-down list for Pilot Sync Code **(PSC)** in the upper right quadrant of the RF Control Settings window.

6 Make the following selections in the "Receive (Expected)" quadrant of the RF Control Settings window:

a. Select **Manual** from the drop-down list for **Receive Mode**.

b. Select **Outbound** from the drop-down list for **Burst Type**.

c. Select **16-QAM** from the drop-down list for **Modulation**.

d. Select **Free Run** from the drop-down list for **Sync Mode**.

7 Minimize the RF Control Settings window, by clicking the upper left corner of the window. (See Figure 5-1.) Modulation Type is not visible in the minimized RF Control Settings window but displays with Burst Type and PSC at the bottom of the screen.

Step result: The minimized RF Control Settings window is visible at the top of the screen as long as all subscreens are minimized. The Modulation Type is not visible in the minimized RF Control Settings window but displays with Burst Type and PSC at the bottom of the screen.

---

8 From CSS, select **Service → Test and Measurement Screen** from the menu.

---

9 In the CSS Test and Measurement Screen:

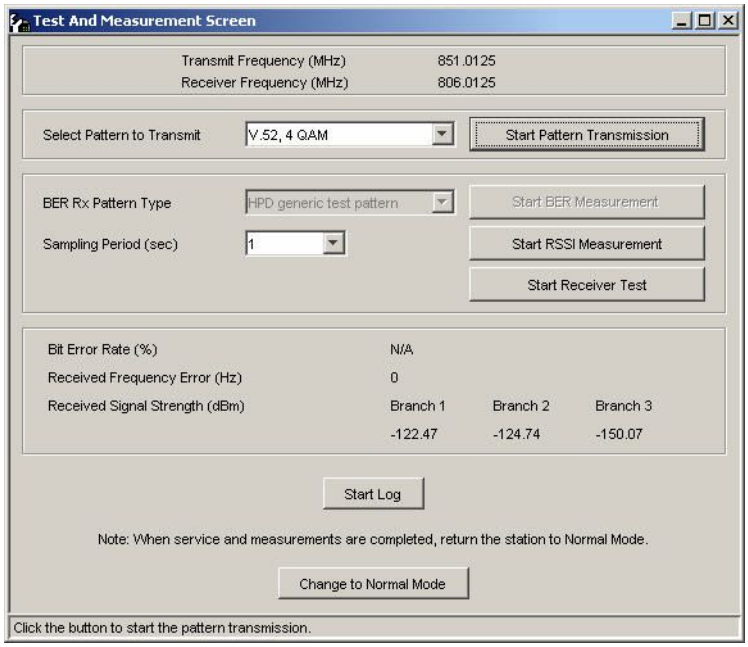
a. Click **Change to Service Mode**.

b. Re-open the **Test and Measurement Screen** after the base radio resets.

c. Key up the base radio for 16-QAM modulation by selecting **16-QAM** in the **Select Pattern to Transmit** field.

d. Click **Start Pattern Transmission**

Figure 5-3 CSS Test and Measurement Screen



---

10 Display the base radio's transmission readings on the service monitor's Rx Meter subscreen, as follows:

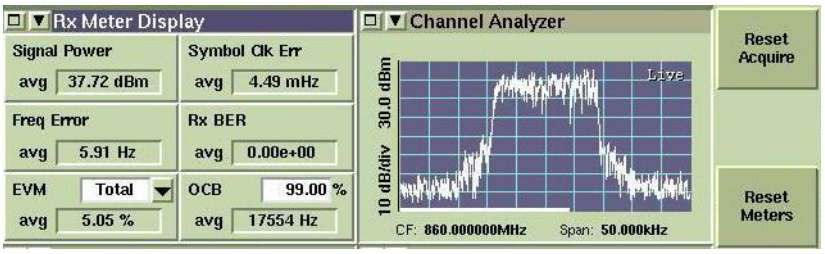
a. Click the Rx Meter subscreen.

Step result: A panel of soft keys displays on the right side of the screen, including two **Reset** keys.

b. Click the **Reset Acquire** soft key on the right side of the screen. This re-synchronizes the test set with the incoming signal.

c. Click the **Reset Meters** soft key on the right side of the screen. This stops, clears, and restarts the acquisition of data for the data display fields.

Figure 5-4 HPD Service Monitor - Rx Meter Subscreen, Reset Soft Keys (Aeroflex 3900 Series Service Monitor)



11 Compare the value that displays in the **Signal Power** field to the base radio Tx Power Out specification **that matches your base radio configuration.** See 1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz), page 1-6 in the Description chapter of this documentation.

NOTE

Be sure to account for cable loss in this comparison.

NOTE

The output power reference plane is the output connector of the power amplifier. The loss of the transmitter output cable (PA output to the back of the base radio) is 4% at 700 MHz and 800 MHz. However, the base radio software allows the transmitter output power to be set at 10% above rated value.

12 Note the value that displays in the **Freq. Error** field. Tolerance should be +/- 50 Hz.

13 Note the value that displays in the **EVM avg** field. The value should be less than or equal to 10%.

14 If no further testing is needed, click **Change to Normal Mode** to return the base radio to normal operation.

5.1.4 Measuring HPD BR Rx Sensitivity and Rx BER

When and where to use:
Use this procedure to test:

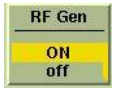
- **Rx Sensitivity:** Does the 1% Bit Error Rate (BER) meet specifications for the GTR 8000 Base Radio configuration?
- **Rx BER:** Does -70 dBm produce a 0.01% Bit Error Rate (BER) or better, as expected?

Procedure Steps

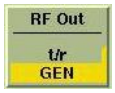
1 Perform the service monitor setup steps in 5.1.1 Setting Up the HPD Service Monitor for Testing the Base Radio, page 5-2.

2 Using the soft keys on the right side of the screen, configure the service monitor GEN port to generate inbound signaling to the base radio, as follows:

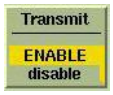
a. Click the **on** soft key under **RF Gen**.



b. Click the **gen** soft key under **RF Out**.

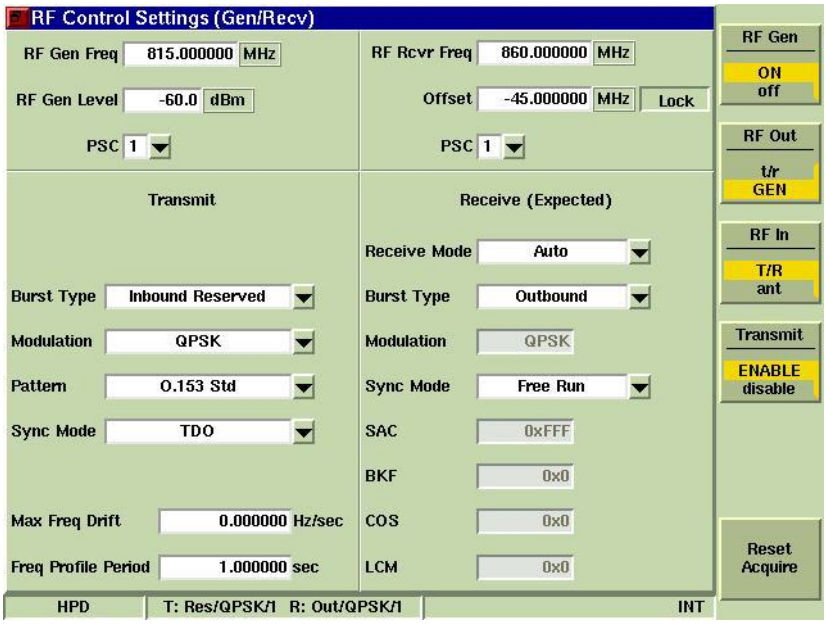


c. Click the **enable** soft key under **Transmit**.



3 Maximize the RF Control Settings window, by clicking the upper left corner of the window.

Figure 5-5 HPD Service Monitor - RF Control Settings Window (Aeroflex 3900 Series Service Monitor)



Step result: All RF Control Settings fields display, as shown.

---

4 Select the following values in the Transmit quadrant of the RF Control Settings window:

a. Select **Inbound Reserved** for the **Burst Type**.

b. Select a **Modulation Type**.

NOTE

The selection should be a modulation type from HPD Receive Sensitivity 1% BER specifications, which include:

- 64 QAM (Quadrature Amplitude Modulation)
- 16 QAM
- QPSK (Quadrature Phase Shift Keying)

See 1.6 GTR 8000 Site Subsystem Specifications, page 1-5 in the Description chapter of this documentation.

c. Select **TDO** for the **Sync Mode**.

d. Select **0.153 Std** for the **Pattern**.

---

5 Select **Free Run** for the **Sync Mode** in the Receive (Expected) quadrant of the RF Control Settings window.

---

6 Select the following values in the upper left quadrant of the RF Control Settings window:

a. Click the **RF Gen Freq** field and use the number buttons on the front of the service monitor to enter a value.

NOTE

The value entered should be within the Frequency Range specification for the HPD base radio configuration being tested. See 1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz), page 1-6 in the Description chapter of this documentation.

b. Click the **RF Gen Level** field and enter a dBm value, depending on the length of cable between the service monitor and the base radio.

NOTE

The value you enter should match the Receive Sensitivity 1% BER specifications for the HPD base radio's configuration, for the Modulation Type you selected. See 1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz), page 1-6 in the Description chapter of this documentation.

c. Select **1** from the drop-down list for Pilot Sync Code **(PSC)**.

---

7 Minimize the RF Control Settings window, by clicking the upper left corner of the window.

Step result: The minimized RF Control Settings window is visible at the top of the screen as long as all subscreens are minimized. See Figure 5-1. Modulation Type is not visible in the minimized RF Control Settings window but displays with Burst Type and PSC at the bottom of the screen.

---

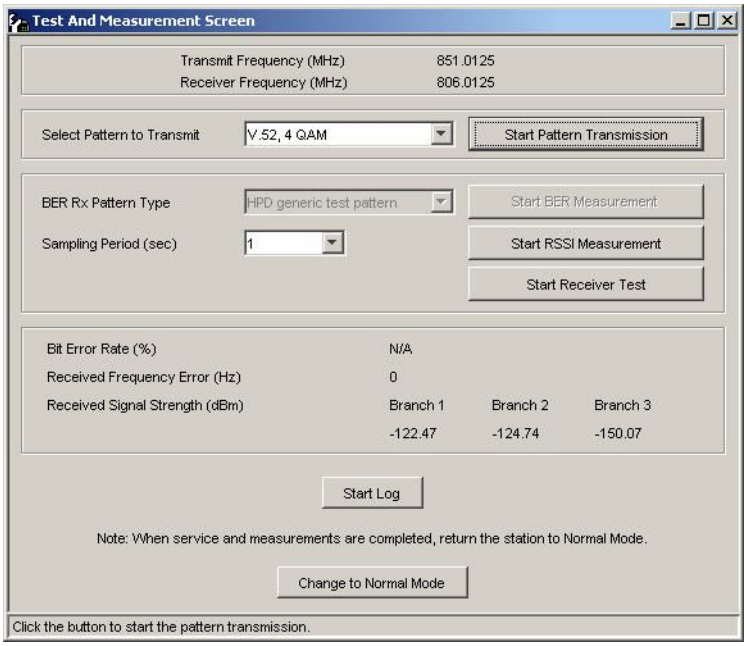
8 Connect to the base radios transceiver module in CSS through an Ethernet connection. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

---

9 Setup the Test and Measurement Screen to display the received BER through CSS, as follows:

a. Select **Service → Test and Measurement Screen** from the menu.

Figure 5-6 CSS Test and Measurement Screen



b. Click **Change to Service Mode**.

This keys up the base radio in service mode.

c. Re-open the **Test and Measurement Screen** after the base radio resets.

d. Select a pattern that matches the Modulation Type selection for the RF Control Settings in the service monitor.

NOTE

To match the QPSK Modulation Type on the service monitor screen, select the 4 QAM pattern in CSS.

e. Click **Start Pattern Transmission**.

f. Click **Start BER Measurement**.

10 Display the base radio's transmission readings on the service monitor Rx Meter subscreen, as follows:

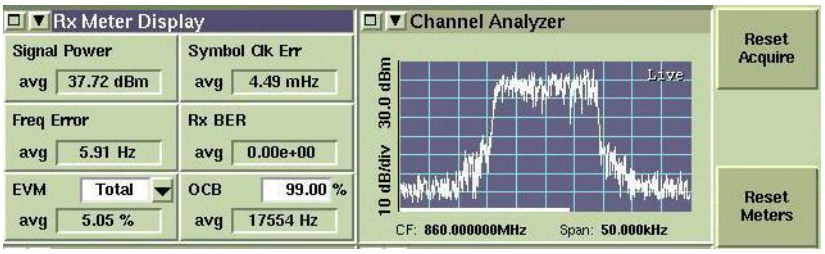
a. Click the Rx Meter subscreen.

Step result: A panel of soft keys displays on the right side of the screen, including two **Reset** keys.

b. Click the **Reset Acquire** soft key on the right side of the screen. This re-synchronizes the test set with the incoming signal.

c. Click the **Reset Meters** soft key on the right side of the screen. This stops, clears, and restarts the acquisition of data for the data display fields.

Figure 5-7 HPD Service Monitor - Rx Meter Subscreen and Soft Keys (Aeroflex 3900 Series Service Monitor)



11 On the RF Control Settings window of the service monitor, enter lower values in the **RF Gen Level** field until 1% BER is displayed on the CSS Test and Measurement screen. Compare the value in the **RF Gen Level** field to the Receive Sensitivity 1% BER specifications for the HPD base radio configuration. See 1.6.1 Specifications for GTR 8000 Base Radio (700/800 MHz), page 1-6 in the Description section of this documentation.

NOTE

Be sure to take the cable and splitter loss into account.

12 Enter -70 dBm in the **RF Gen Level** field.

NOTE

This should produce a 0.01% or better BER on the Test and Measurement screen in CSS. If it does not, contact Motorola System Support Center (SSC). See 8.4 Using Motorola Solution Support Center, page 8-6 in the Troubleshooting chapter of this document.

13 When finished testing, perform the following steps in CSS in the **Test and Measurement Screen**:

a. Click **Stop BER Measurement**.

b. Click **Stop Pattern Transmission**.

14 If no further testing is needed, click **Change to Normal Mode** to return the base radio to normal operation.

5.1.5 Checking Receiver Sensitivity (Self-test Method)

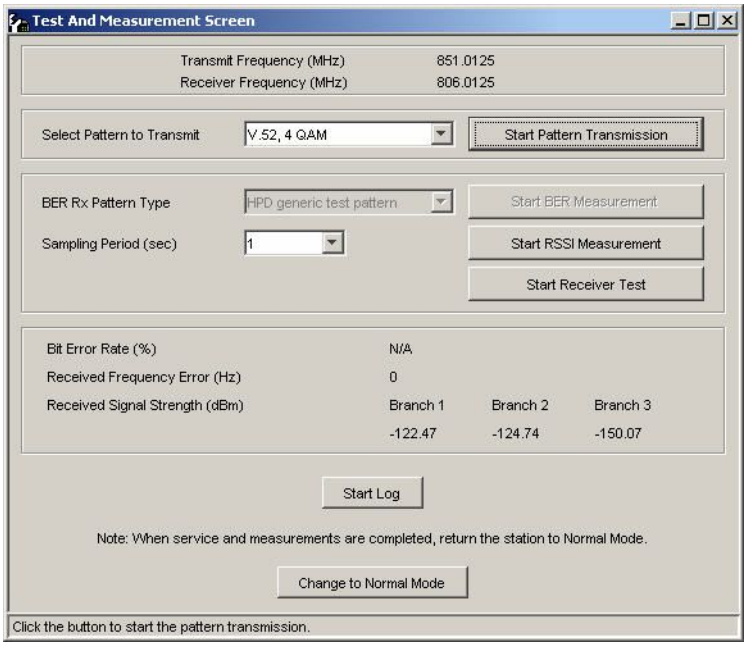
When and where to use:
This procedure explains how to check the receiver sensitivity for the station without any test equipment. The receiver uses a factory calibrated low-level noise source at the receiver input to check performance. This procedure can be performed remotely.

Procedure Steps

1 Connect to the base radios transceiver module in CSS through an Ethernet connection. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

2 From CSS, select **Service → Test and Measurement Screen** from the menu in CSS.

Figure 5-8 CSS Test and Measurement Screen



3 Reset the base radio:

a. If the base radio is not already in service mode, click **Change to Service Mode**.

Step result: A confirmation dialog box appears.

b. Click **OK**.

Step result: The base radio begins a reset sequence to change modes, which take a few minutes.

c. After the base radio resets, re-open the Test and Measurement Screen dialog box as described in step 2.

4 Select **Start Receiver Test**.

Step result: A confirmation dialog box appears indicating the test progress. After a few seconds, the test will conclude with a pass or fail message.

5 Click **OK**.

6 If no further testing is needed, click **Change to Normal Mode** to return the base radio to normal operation.

6 GTR 8000 Site Subsystem Maintenance

This chapter describes periodic maintenance procedures relating to GTR 8000 Site Subsystem.

6.1 Fan Grill Cleaning Instructions

CAUTION

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 GTR 8000 Site Subsystem Operation

This chapter details tasks that to perform once the GTR 8000 Site Subsystem is installed and operational on your system.

7.1 Base Radio Operational States for HPD

The base radio can be in one of four operational states, depending on how it is currently handling packets from the site controller.

- Standby
- Idle
- Assigned
- Isolated

During initialization, the base radio powers up into the **standby** state and waits for a status packet from the site controller. After initial contact with the site controller has been made, the base radio will enter **idle** mode and send a status message back to the site controller (indicating that it is ready for assignment). The site controller responds with a channel grant message, and the base radio is enabled for service. If the base radio has a greater home channel preference setting (than other base radios at the site), then the zone controller assigns the base radio as the home channel at the site.

After a base radio has been **assigned**, it can begin to handle inbound/outbound traffic. In case where the base radio fails to receive a number of consecutive status packets from the site controller, it enters **isolated** mode and dekeys. This isolated mode is reported in Unified Event Manager.

If the base radio becomes operational again and receives status packets from the site controller, it replies again with a channel status message. The site controller may then respond with a channel grant, and the base radio becomes enabled for service again.

8 GTR 8000 Site Subsystem Troubleshooting

This chapter provides fault management and troubleshooting information relating to GTR 8000 Site Subsystem.

GTR 8000 Site Subsystem troubleshooting requires an understanding of hardware-based and software-based diagnostics, as well as testing tools. Support is available from Motorola to assist with all steps in the troubleshooting process.

8.1 General Troubleshooting

Table 8-1 GTR 8000 Site Subsystem General Troubleshooting

Problem	Troubleshooting
General connectivity problems	1. If you have access to the equipment, check the LEDs to verify that each piece of equipment is connected and operational. See 10.1 LEDs, page 10-1. 2. In CSS, check the alarms of the base radio and all associated devices and links. 3. Verify the configuration of the base radio through CSS. Verify that the IP address for the base radio is correct. In CSS, send a diagnostic command to enable the base radio. 4. Verify that the DNS Hostname for the base radio 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 that the physical cabling is firmly connected and 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. Run ping, traceroute, pathping, and other network administration commands to identify any link or intermediate devices (switch or routers) with high latency or connection problems. 7. If the connection fails to operate normally, send a restart command to the base radio through CSS. Consider cycling power to the base radio if necessary. 8. If the base radio still fails to operate properly, create a backup of the current configuration, then reinstall the software and reconfigure the base radio. 9. Replace the base radio if necessary.
Unit will not power up	1. If you have access to the equipment, check the LEDs to determine which equipment is connected and operational. See 10.1 LEDs, page 10-1. 2. In CSS, check the alarms for the base radio. 3. Check the power cabling and verify that the power source for the base radio is supplying the appropriate voltage. Try connecting the base radio to another power source or replace the power cabling if necessary.  **NOTE** Check all power sources as there may be more than one. 4. Check for any physical damage to the modules and check whether the modules were properly grounded. 5. Replace any defective modules.

8.2 Troubleshooting Tools

Several tools are available for viewing and monitoring equipment and troubleshooting suspecting problems:

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

In addition, see 3.5.1 Quick Connect RF Coaxial Adapters for GTR 8000 Base Radio Support, page 3-29 for testing system performance:

8.2.1 Using Unified Event Manager to Monitor Links and Components

Use Unified Event Manager (UEM) to monitor critical links and components 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 faults as they occur.
- Evaluation of UEM Active Alarms Window on a regularly scheduled basis.

8.2.1.1 Analyzing Unified Event Manager Active Alarm 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, you can review the **Active Alarms Window** to correlate reported loss of service with patterns of critical alarms for links and equipment.

When analyzing the **Active Alarms Window**, look for the following patterns:

- Failures sent with time stamps on or about the same time.
- Failures from related equipment:
  - Cards in the same device
  - Equipment part of the same subsystem.

Many devices send 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* for further details.

8.2.1.2 Diagnostic Options in UEM

This table summarizes the base radio diagnostic options in the Unified Event Manager (UEM).

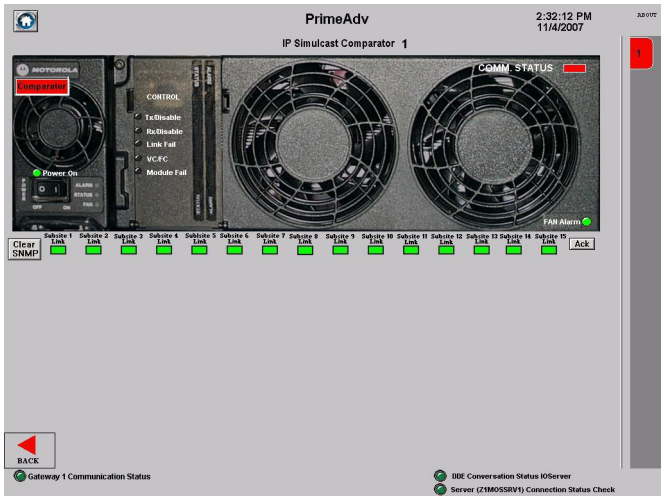
Table 8-2 Base Radio Diagnostic Options in UEM

Option	Description
Restart	Requests that the base radio perform a reset.
Service	Requests that the base radio enters service mode, allowing a technician to make alignment adjustments and run other tests while the base radio is offline.
Enabled	Requests that the base radio enter the enabled mode and handle traffic.

8.2.2 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 8-1 MOSCAD Network Fault Management



When an alarm condition occurs, the alarm box 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* manual for details.

8.2.3 Using Unified Network Configurator for Troubleshooting

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.

8.2.4 Using Configuration/Service Software for GTR 8000 Base Radio Troubleshooting

The GTR 8000 Base Radio can be locally or remotely configured or serviced through Configuration/Service Software (CSS). CSS provides access to alarms, status information, and configuration settings for the base radio.

Use CSS for the following tasks which may be useful when troubleshooting the base radio. See the *CSS Online Help* for specific details and instructions when performing these tasks.

- Enable and disable channels and services.
- View and save a log of alarms.
- Verify the configuration.
- Gather troubleshooting information that can be escalated to Motorola for evaluation.

8.2.4.1 Alarm Log from Internal Diagnostic Tests

The base radio has been 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.

8.2.4.2 Resetting Passwords and SNMPv3 Passphrases

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 Solution Support Center (SSC).

NOTE

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 8-3 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 local login, but knows SNMPv3 passphrases	✓	✗	See the *CSS Online Help* “SNMPv3 User Configuration”.	See the *CSS Online Help* “Resetting Device Passwords.”
User knows 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)”

Table 8-3 Local Password and SNMPv3 Passphrase Troubleshooting (cont'd.)

Scenario	SNMPv3 Passphrase Known	Local Password Known	To Reset SNMPv3 Passphrase	To Reset Local Login Password
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 SSC.	Contact Motorola SSC.

8.3 Site Controller Failure – Impact on GTR 8000 Base Radio for Trunked Operation

If the link fails between the base radio and the site controller, the base radio dekeys and does not handle any MSU traffic. MSUs attempt to operate on another channel at the site. If another channel is not available, the MSUs attempt to register at another site.

For HPD operation, the base radio receives external frequency reference and network time synchronization from the active site controller over the Ethernet link. If a loss of the external time and frequency reference source, the base radio continues to maintain its own time and frequency stability to continue operations for a specified amount of time without degradation. Afterwards, operation continues with minimal degradation.

8.4 Using Motorola Solution Support Center

Motorola Solution 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 assigns a tracking ticket number that identifies each support call. This ticket number allows Motorola 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.

8.4.1 Gathering Information Before Calling Motorola

Before calling the Motorola Solution 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.

Collect the following information:

- 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

8.4.2 Where to Call for Service

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

8.4.2.1 Motorola Solution Support Center

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

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

8.4.3 Use of Subcontractors

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

9 GTR 8000 Site Subsystem FRU Procedures

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

GTR 8000 Site Subsystem is comprised of numerous field replaceable units (FRUs) and field replaceable parts. If a FRU or part must be replaced, it is essential to obtain the precise FRU kit number or part number and to review the replacement procedures provided, including all safety precautions and system impact information.

9.1 Field Replaceable Units (FRUs) and Parts

When ordering field replaceable units (FRUs), you need the FRU Kit Number. When ordering field replaceable parts, you need the Part Number. Contact Motorola System Support Center (SSC) as needed for numbers not provided here (for cables that are internal to a GTR 8000 Site Subsystem, the part numbers are not listed in this documentation, but you can locate the part number on the cable itself before contacting Motorola System Support Center (SSC)). See 8.4 Using Motorola Solution Support Center, page 8-6 in the Troubleshooting section of this documentation.

WARNING

To guard against personal injury and/or damage to equipment, switch the base radio to Service Mode when performing service. The GTR 8000 Base Radio periodically keys up to pseudo train its linear transmitter autonomously when it is not assigned by the zone controller. Tx Inhibiting the base radio also prevents the transmitter from keying. Remember to switch the base radio back to Normal Mode when service is complete.

9.1.1 GTR 8000 Site Subsystem Field Replaceable Units

Table 9-1 GTR 8000 Site Subsystem Field Replaceable Units

Component Type	FRU Kit Number	Replacement Procedure
Transceiver Module (700/800 MHz)*	DLN6885A	9.5 Replacing a Transceiver Module, page 9-7
Fan Module	DLN6898A	9.6 Removing/Replacing the Fan Module, page 9-13
AC/48V DC Power Supply	DLN6781A (0182516W14)	9.7 Replacing a Power Supply, page 9-15
Power Amplifier Module (700/800 MHz)	DLN6895A	9.9 Replacing a Power Amplifier, page 9-19
GCP 8000 Site Controller	DLN6569A	See the *GCP 8000 Site Controller* manual.

Table 9-1 GTR 8000 Site Subsystem Field Replaceable Units (cont'd.)

Component Type	FRU Kit Number	Replacement Procedure
Power Distribution Module	0184847Y01	9.14 Replacing the Power Distribution Module, page 9-33

* The transceiver field replacement units are not compatible with ASTRO® 25 base radio software distributed before July 2013. BEFORE installing the replacement transceiver, ensure that all base radios at the site meet the minimum software version requirements listed. Contact Motorola Customer Support at 800-422-4210 if you do not have access to compatible software. See xx for details.

9.1.2 GTR 8000 Site Subsystem Field Replaceable Parts

Table 9-2 GTR 8000 Site Subsystem Field Replaceable Parts

Component Type	Part Number	Replacement Procedure
Power Supply Fan Module	5985167Y02	9.8 Replacing a Power Supply Fan, page 9-17
GTR 8000 Base Radio Backplane	0180706K30	9.15 Replacing the GTR 8000 Base Radio Backplane, page 9-36
Site Preselector	CFF6065A	9.10 Replacing Filters/Preselectors in a GTR 8000 Site Subsystem, page 9-22
Cabinet LNA Module (Cabinet RMC)	DLN1306A	9.11 Replacing a Cabinet RMC/LNA Module, page 9-24
External Dual Circulator Tray	DLN1317A	9.12 Replacing the Dual Circulator/Isolator Modules, page 9-27
Duplexer 700 MHz	9184718Y01	9.13 Replacing a Duplexer, page 9-32
Duplexer, 800 MHz	9184718Y02	9.13 Replacing a Duplexer, page 9-32

9.1.3 GTR 8000 Site Subsystem Individual Customer Replacement Parts on External Dual Circulator Tray

Table 9-3 GTR 8000 Site Subsystem Individual Customer Replaceable Parts on External Dual Circulator Tray

Component Type	Part Number	Replacement Procedure
Dual Circulator	0185172Y01	9.12 Replacing the Dual Circulator/Isolator Modules, page 9-27
Circulator Load	TLN3391A	9.12 Replacing the Dual Circulator/Isolator Modules, page 9-27
Low Pass/Harmonic Filter	9185202U04	9.12 Replacing the Dual Circulator/Isolator Modules, page 9-27

9.2 Required Tools and Equipment

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

- Electrostatic discharge (ESD) strap (Motorola part number RSX4015A, or equivalent)
- Laptop PC with Configuration/Service Software and Software Download 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.

9.3 Transceiver Hardware Generations

As of July 2013, the GTR 8000 Base Radio and the GPW 8000 Receiver are shipped with a new generation of transceiver hardware (referred to in this manual as GEN 2). The hardware updates are intended to extend the life of the device as seamlessly as possible. This section details relevant differences and compatibility requirements for GEN 1 and GEN 2 hardware.

9.3.1 Transceiver Software and Feature Compatibilities

The GEN 2 transceiver hardware is backwards compatible and interchangeable with GEN 1 transceiver hardware on ASTRO® 25 7.7 and later systems. GEN 1 transceivers can no longer be ordered; however, spare inventory of GEN 1 transceivers can still be used as FRU replacements.

All ASTRO® 25 system features are supported on GEN 1 and GEN 2 transceivers, with the following exceptions.

Table 9-4 System Feature Exceptions

Feature	GEN 1 Transceiver	GEN 2 Transceiver
X2 TDMA	Supported	Not Supported

GEN 2 transceiver hardware is not compatible with ASTRO® 25 GTR 8000 Base Radio software distributed before July 2013. The transfer operation fails if you perform a software download using a Software Download (SWDL) Package that was released before July 2013,

BEFORE installing a FRU replacement or expansion channel at an existing site, ensure that you are using the latest available Software Download (SWDL) Package and that all base radios at the site meet the minimum software version requirements listed. Contact Motorola Customer Support at 800-422-4210 if you do not have access to compatible software.

Table 9-5 Minimum Software Download Version Requirements

ASTRO® 25 System Release	HPD BR
7.6 and earlier	Not Supported
7.7	HPDBR_R07.7X.023
7.8	HPDBR_R07.8X.033
7.9	HPDBR_R07.9X.049
7.11	HPDBR_R07.BX.098
7.12	HPDBR_R07.CX.051
7.13	HPDBR_R07.DX.073
7.14 and later	Any Version

CAUTION

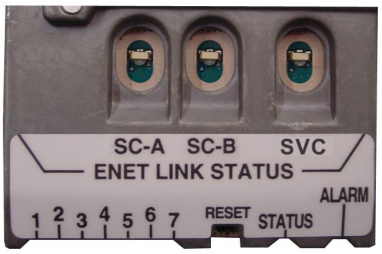
It is crucial that a site software download is performed at a trunked ASTRO® 25 site to ensure that all devices are on the same software version, VLAN, and active bank. Failure to perform this step, results in the replacement transceiver or expansion channel to have a mismatch in software versions. If a mismatch in software versions occurs, the transceiver may go into a configuration mode of operation with a reason of 'Invalid Software Version'.

9.3.2 Identifying Transceiver Hardware Generation

Label

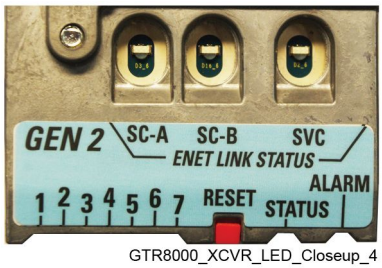
GEN 1 and GEN 2 transceiver modules can be identified by examining the physical hardware label. GEN 2 modules have a light blue label with 'GEN 2' clearly noted on it, while GEN 1 modules have a white label with no GEN identification.

Figure 9-1 GEN 1 Transceiver Module



GTR8000_XCVR_LED_Closeup_1

Figure 9-2 GEN 2 Transceiver Module



GTR8000_XCVR_LED_Closeup_4

CSS

GEN 1 and GEN 2 transceiver modules already installed in a system can be identified through the **Hardware Version** screen of the Configuration/Service Software (CSS).

9.3.3 Transceiver FRU Number Mappings

Table 9-6 Transceiver FRU Number Mappings

Transceiver FRU Number	GEN 1 (Shipped before Nov 2013)	GEN 2 (Shipped starting July 2013)
Transceiver Module (700/800 MHz)	DLN6566A	DLN6885A

9.4 Power Amplifier Hardware Generations

Starting in July 2013, the GTR 8000 Base Radio is shipped with a new generation of power amplifier hardware (referred to in this manual as GEN 2). The hardware updates extend the life of the base radio as seamlessly as possible. This section details relevant differences and compatibility requirements for GEN 1 and GEN 2 hardware.

9.4.1 Power Amplifier Software and Feature Compatibilities

The GEN 2 power amplifier hardware is fully backwards compatible and completely interchangeable with GEN 1 power amplifier hardware. GEN 1 power amplifiers can no longer be ordered; however, spare inventory of GEN 1 power amplifiers can be used as Field Replaceable Unit (FRU) replacements.

All ASTRO® 25 system features are supported on GEN 1 and GEN 2 power amplifiers. All ASTRO® 25 system release software is supported on GEN 1 and GEN 2 power amplifiers.

9.4.2 Identifying Power Amplifier Hardware Generation

Label

GEN 1 and GEN 2 power amplifier modules can be identified by examining the physical hardware label. GEN 2 modules have a light blue label with ‘GEN 2’ clearly noted on it, while GEN 1 modules have a white label with no GEN identification.

Figure 9-3 GEN 1 Power Amplifier Module

GTR8000_PA_LED_Closeup

Figure 9-4 GEN 2 Power Amplifier Module

GTR8000_PA_LED_Closeup1

CSS

GEN 1 and GEN 2 power amplifier modules already installed in a system can be identified through the **Hardware Version** screen of the Configuration/Service Software (CSS).

9.4.3 Power Amplifier FRU Number Mappings

Table 9-7 Power Amplifier FRU Number Mappings

Power Amplifier FRU Number	GEN 1 (Shipped before Nov 2013)	GEN 2 (Shipped starting July 2013)
Power Amplifier Module (700/800 MHz)	DLN6567A	DLN6895A

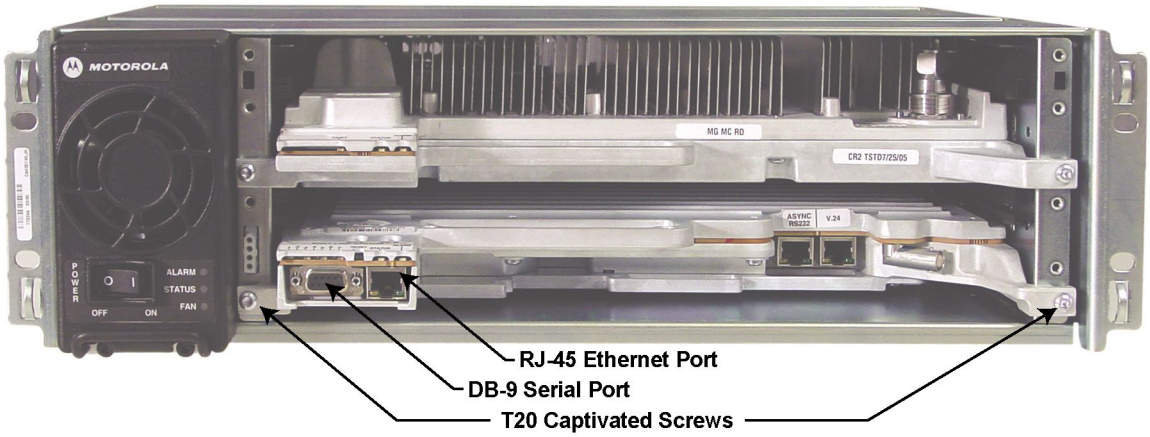
9.5 Replacing a Transceiver Module

Prerequisites:
Before replacing the transceiver, pull configuration and hardware information from the transceiver into the Unified Network Configurator (UNC) by performing a “Pull All” procedure from the UNC. For instructions on “How to Perform a Pull All” procedure, see the *Unified Network Configurator* manual. This step may not be possible if communication is severed between the transceiver and the UNC. If this scenario exists, perform any one of the following:

- Use the last known good configuration files from the UNC
- Extract the configuration files from the transceiver directly

This figure shows the captive screws that secure the transceiver module to the chassis in the base radio configuration.

Figure 9-5 Transceiver Module (Inside Chassis)



Procedure Steps

1 Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground. Be sure to wear this strap throughout this procedure to prevent ESD damage to any components.

2 Locate the transceiver module being replaced.

3 If the transceiver module is not operational, go to step 8.

4 Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

5 Save the base radio configuration to the laptop PC as follows:

a. Select **File → Read Configuration From Device** from the menu. Click **OK**.

b. Select **File → Save As** from the menu.

c. Enter the IP address of the transceiver module on the Properties Screen. Click **OK**.

d. On the Save window, select the directory where you want to save the configuration file, type a meaningful name for the file (use ".cpl" as the extension or do not type an extension). Press ENTER.

Step result: The base radio configuration is saved to the location you indicated. The configuration file will be reloaded later to the replacement transceiver.

---

6 Disable the channel before replacing the module, so that the system does not attribute the loss of channel to a failure.

NOTE

It is not necessary to turn off the power supply for the transceiver module being replaced, as the modules are designed to be swapped out with the power on. If you choose to turn off the power, set the rocker switch on the front of the associated power supply to the Off (0) position.

a. Select **Service → Test & Measurement Screen** from the menu.

b. Click **Change to Service Mode**.

Step result: The base radio is disabled.

---

7 Disconnect the Ethernet cable from the service port on the transceiver being replaced.

---

8 Remove the fan module to gain access to the transceiver module. See 9.6 Removing/Replacing the Fan Module, page 9-13.

IMPORTANT

Although the transceiver module is designed to be swapped out without shutting the power off, minimize the amount of time that the fan module is removed, so the circuitry that remains powered on does not overheat and shut down.

---

9 Using a T20 bit, loosen the two captive screws on the front of the transceiver module, so that they disengage from the chassis.

---

10 Using the handle, gently pull the transceiver module straight out, along the guides on which it sits.

---

11 Slide in the replacement transceiver module along the guiding rails until it is engaged. A slight push may be needed to engage the module.

IMPORTANT

If the transceiver 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.

Step result: LEDs on the transceiver turn on when it is engaged.

---

12 Secure the transceiver module to the chassis with the two captive screws on the front of the module.

13 Reinstall the fan module. See 9.6 Removing/Replacing the Fan Module, page 9-13.

NOTE

If you chose to turn off the power, set the rocker switch on the front of the associated power supply to the On (1) position.

14 Perform basic device configuration using the serial port. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.

a. Set the **IP Address** and the **Box Number** for the new device module. See 4.4.3.1 Setting the Device IP Address Using CSS, page 4-6.

b. Set the Serial Security Services Using CSS. See 4.4.3.2.1 Setting the Serial Security Services Using CSS, page 4-8.

15 Disconnect the laptop PC from the transceiver's serial port.

16 Perform basic device configuration using the Ethernet port. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

a. Set the current date and time in CSS. See 4.4.5.1 Setting the Date and Time Using CSS, page 4-13.

b. Set up the local Password Configuration using the CSS (optional). See 4.4.5.6 Setting Up the Local Password Configuration Using the CSS, page 4-21.

17 Complete the configuration of the Information Assurance features using CSS, as follows:

a. Change the SNMPv3 configuration and user credentials from CSS. See 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14.

b. Create, update, or delete an SNMPv3 user. See 4.4.5.2.1 Adding or Modifying an SNMPv3 User Using CSS, page 4-17.

c. Verify the SNMPv3 credentials. See 4.4.5.2.2 Performing an SNMPv3 Connection Verification Using CSS, page 4-18.

d. Set the SWDL transfer mode. See 4.4.5.4 Setting the SWDL Transfer Mode Using CSS, page 4-19.

e. Configure DNS using the CSS. See Chapter 7, “Configuring DNS Using CSS” in the *Authentication Services* manual.

f. Configure for SSH. See Chapter 4, “Configuring SSH for RF Site Devices and VPMs Using CSS” in the *Securing Protocols with SSH* manual or see “Device Security Configuration Remote Access/Login Banner (Ethernet)” in the *CSS Online Help*.

NOTE

Make sure to Restore the Clear Protocols parameters.

g. Enable RADIUS Authentication using the CSS. See Chapter 7, “Configuring RADIUS Sources and Parameters Using CSS” in the *Authentication Services* manual.

h. Enable Centralized Authentication using the CSS. See Chapter 7, “Enabling/Disabling Centralized Authentication Using CSS” in the *Authentication Services* manual.

i. Set the Local Cache Size for Centralized Authentication using the CSS. See Chapter 7, “Setting the Local Cache Size for Central Authentication Using CSS” in the *Authentication Services* manual.

j. Enable Centralized Event Logging using the CSS (if required by your organization). See Chapter 6, “How to Enable/Disable Centralized Event Logging on Devices Using CSS” and Chapter 1, “Event Logging Client Configuration” for proper hostnames in the *Centralized Event Logging* manual.

k. Set the NTP Server Settings. See 4.4.5.5 Setting the NTP Server Settings, page 4-20.

---

18 Open the Software Download application.

CAUTION

Make sure to 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*.

---

19 Perform a single device software download to transfer and install the latest base radio software using Software Download as follows:

a. From Software Download, select **File → File Manager** from the menu.

Step result: The **Software Depot File Manager** opens.

b. Select **Component Operations → Import Fileset** from the menu.

Step result: The **Import a Fileset Into the Software Depot** dialog box appears.

c. Click **Browse** and search for the **swdlv3.cfg** file on the CD. Click **Open**.

d. Click **Generate** to add the file to the Components In the Software Depot list. Click **OK**.

e. Exit the Software Depot File Manager.

f. From Software Download, select the appropriate ASTRO® 25 system Site Type, and the relevant zone and site information.

g. Select the **Single Device Mode** tab. Click **Continue**.

Step result: An informational warning appears.

h. Click **OK**.

i. Enter the IP address of the transceiver module being programmed. Click **Continue**.

j. In the Select an Option window, select **Upgrade Software Application**. Click **Continue**.

k. Select **HPD Base Radio** for the Application Type.

l. Select **Transfer and Install** for the Operations Type.

m. For Software Component, select a configuration fileset from the drop-down list.

n. Select **Start Operation**.

Step result: The software is transferred and installed on the device. This transfer takes several minutes to complete. When completed, the two progress bars on the Transfer and Install window display "100%" and a completion message displays in the Transfer message box.

---

20 Reload the base radio configuration file on to the new transceiver, using CSS as follows:

a. Select **File → Open** from the menu.

b. Locate and open the previously saved configuration file for the base radio.

NOTE

If you were not able to back up the base radio configuration from the previous base radio, you can use the configuration from your system build book or use the default base radio configuration file. Specific settings for the base radio must still be configured. See the *CSS Online Help* for GTR 8000 Base Radio for detailed configuration instructions.

c. Click **OK**.

d. Select **File → Write Configuration To Device** from the menu. Click **OK**.

Step result: The configuration from the file you selected is loaded into the base radio. Communication with the base radio is not available until the reset is complete.

---

21 Enable the base radio from CSS, as follows:

a. From CSS, select **Service → Test And Measurement Screen** from the menu.

b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

---

22 Disconnect the laptop PC from the transceiver.

---

23 Perform a site software download and installation. See 11.3 Performing a Site Download, page 11-7.

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 transceiver or expansion channel to have a mismatch in software versions. If a mismatch in software versions occurs, the transceiver may go into a configuration mode of operation with a reason of 'Invalid Software Version'.

---

24 Disconnect the PC Ethernet from the local LAN.

---

25 On systems with SNMPv3 enabled, enable passphrase information. For procedures to enable passphrases, see the *SNMPv3* manual.

---

26 On systems with MAC Port locking, disable the locking and then re-enable the locking with the MAC address of the base radio. The device being replaced may be connected to an Ethernet port on a switch which implements MAC Port locking (HP switch or site controller). If so, the Ethernet switch port must be unlocked and relocked to the MAC address of the replacement device. See the *MAC Port Lockdown* manual for instructions on how to disable and enable MAC Port locking.

NOTE

Following the device restoration, if it was connected to an HP switch port, the HP switch port may have been disabled due to an unexpected MAC address. If so, re-enable the port on the HP switch.

---

27 Replace the transceiver in the UNC. See Chapter 4, "Replacing a Device" in the *Unified Network Configurator* manual.

---

28 Discover the base radio in the UEM, see the *Unified Event Manager* manual.

---

29 Verify that the transceiver module is operating properly:

- The Status LED on the front of the transceiver is green.
- Proper operation is confirmed using software tools, such as UEM, and the Transmitter Metering Screen in Configuration/Service Software (CSS).

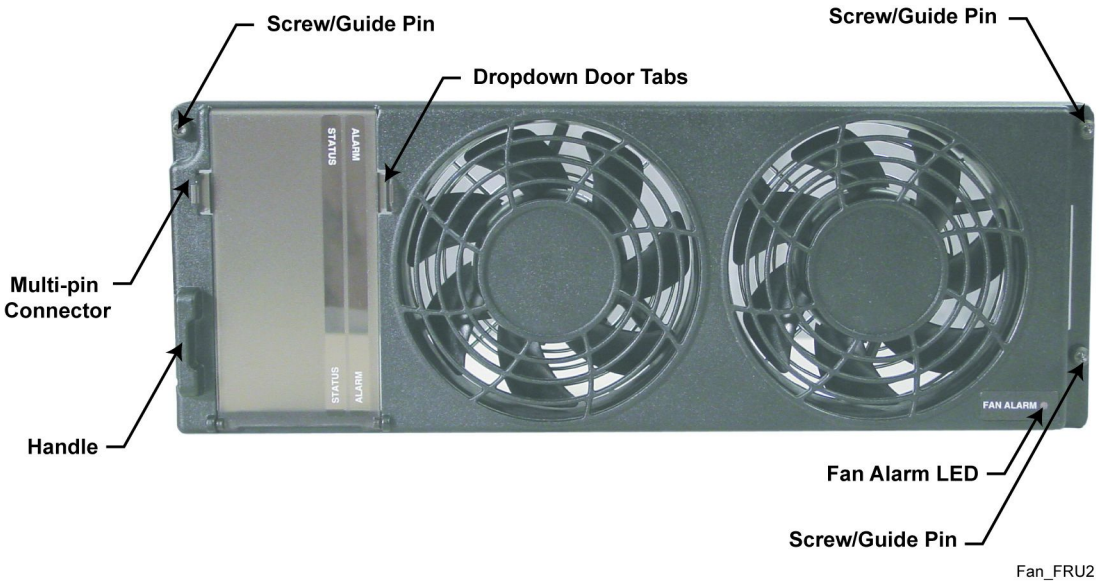
9.6 Removing/Replacing the Fan Module

When and where to use:
This procedure can be used to remove the fan module to replace the modules it covers (transceiver, power amplifier, or site controller modules). The fan assembly is designed to be swapped out without shutting the power off. However, minimize the amount of time before the new fan is operational, so the modules do not overheat and shut down.

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, it is recommended that you 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.

Figure 9-6 Fan Assembly (Front View)



Procedure Steps

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 Using a T20 bit, loosen the three captive screws on the front of the fan assembly, so that 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 secure.

5 Tighten the three captive screws. Torque to 17 ± 2 in-lb.

6 Verify that the fan assembly is operating properly, and that the fan's Alarm LED is off.

You can also use software tools, such as Unified Event Manager, to view any alarms.

9.7 Replacing a Power Supply

Prerequisites:
The power supply output is directly mapped to a PA/transceiver combination. Removal of a power supply results in a loss of the associated transmit channel until the replacement power supply is inserted and turned ON. It is recommended that you disable the channel before replacing the module, so the system does not attribute the loss of channel to a failure. For a GTR 8000 Site Subsystem, a power supply can be removed without disabling the site controllers if they are cabled to auxiliary power. Auxiliary power is available from the base radio connected to a power supply.

WARNING

The Power Supply module contains dangerous voltages which can cause electrical shock to people or damage to the equipment.

Figure 9-7 Power Supply

HPD_Power_Supply_FRU.jpg

Procedure Steps

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 Disable the channel using the power supply module being replaced.

NOTE

It is recommended that you disable the channel before replacing the module, so that the system does not attribute the loss of channel to a failure.

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

3 Push the power rocker switch to Off (0) 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

It is recommended that you 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 FRU power supply into place, pushing gently until it seats.

7 Tighten the two captive screws on the front of the power supply.

8 Turn the power button to On, 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.
- Proper operation is confirmed using software tools, such as Unified Event Manager, and the Power Supply Metering Screen in Configuration/Service Software (CSS).

9 Enable the base radio as follows:

a. From CSS, select **Service → Test & Measurement Screen** from the menu.

b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

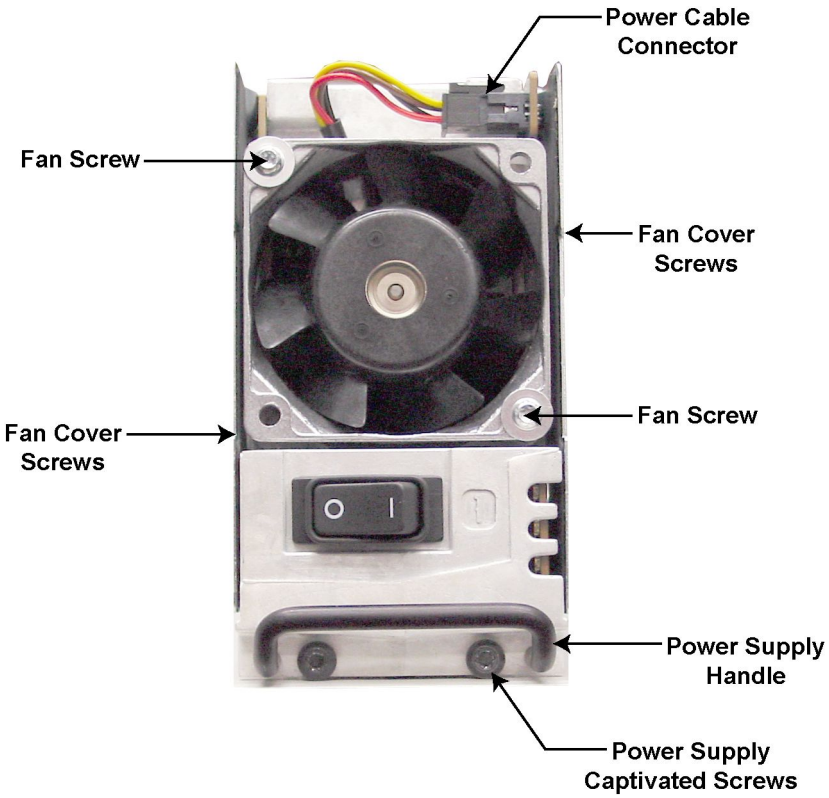
9.8 Replacing a Power Supply Fan

Prerequisites:
Replacing the power supply fan requires that the entire power supply module is removed. The power supply output is directly mapped to a PA/transceiver combination. Removal of a power supply results in a loss of the associated transmit channel until the replacement power supply is inserted and turned ON. It is recommended that you disable the channel before replacing the module, so that the system does not attribute the loss of channel to a failure. For a GTR 8000 Site Subsystem, a power supply can be removed without disabling site controllers if they are cabled to auxiliary power. Auxiliary power is available from any base radio still connected to a power supply.

WARNING

The power supply module contains dangerous voltages which can cause electrical shock to people or damage to the equipment.

Figure 9-8 Power Supply Fan



Procedure Steps

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 Disable the channel using the power supply fan being replaced, so the system does not attribute the loss of channel to a failure:

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

---

3 Set the rocker switch on the front of the power supply to Off (0).

---

4 Using a T20 bit, loosen the two captive screws on the front of the power supply module, so that they disengage from the chassis.

WARNING

It is recommended that you 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 Remove the black fan cover from the power supply module:

a. Using a T15 bit, remove the four screws that connect the cover to the sides of the power supply module.

b. Slide the cover off (tilting the top edge out and lifting the bottom edge above the power supply handle).

---

7 Disconnect the power cable located above the fan.

---

8 Remove the two screws that secure the fan to the power supply.

---

9 Remove the fan and insert the new fan.

---

10 Secure the fan to the power supply with the two screws.

---

11 Attach the power cable for the fan to the connection on the power supply.

---

12 Replace the black fan cover:

a. Slide the cover on, tilting the bottom edge in, past the power supply handle.

b. Using a T15 bit, insert and tighten the four screws that connect the cover to the sides of the power supply module.

---

13 Slide the FRU power supply into place, pushing gently until it seats.

---

14 Tighten the two captive screws on the front of the power supply module.

---

15 Turn the power button to On, 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 and the fan is operating.
- Proper operation is confirmed using software tools, such as Unified Event Manager, and the Power Supply Metering Screen in Configuration/Service Software (CSS).

16 Enable the base radio as follows:

a. From CSS, select **Service → Test & Measurement Screen** from the menu.

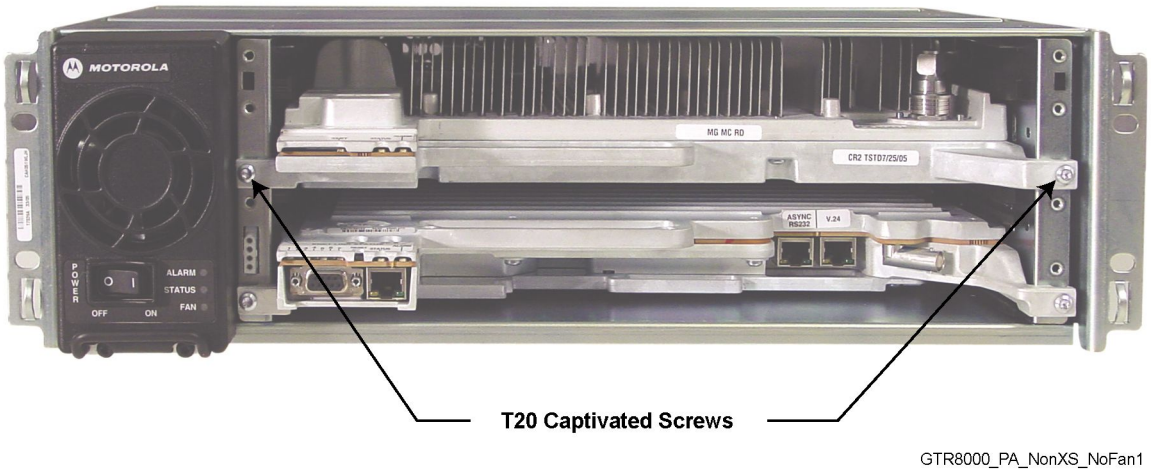
b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

9.9 Replacing a Power Amplifier

Prerequisites:
It is recommended that you disable the channels before replacing the module, so that the system does not attribute the loss of channel to a failure. You can disable a channel using the Unified Event Manager or the Configuration/Service Software (CSS). It is not necessary to turn off the power supply for the power amplifier module you are replacing, as the power amplifier modules are designed to be swapped out with the power on. If you choose to turn off the power, set the rocker switch on the front of the associated power supply to the Off (0) position.
This figure shows the captive screws that secure the power amplifier module to the chassis in the GTR 8000 Base Radio.

Figure 9-9 Power Amplifier (Within Chassis)



Procedure Steps

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 base radio is not operational, go to step 4.

3 Disable the channel associated with the power amplifier module being replaced, so that the system does not attribute the loss of channel to a failure..

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

4 

NOTE

It is not necessary to turn off the power supply for the power amplifier module you are replacing, as the power amplifier modules are designed to be swapped out with the power on.

If you choose to turn off the power, set the rocker switch on the front of the associated power supply to the Off (0) position.

5 Remove the fan module to gain access to the power amplifier module. See 9.6 Removing/Replacing the Fan Module, page 9-13.

IMPORTANT

The power amplifier module is designed to be swapped out without shutting the power off. However, minimize the amount of time that the fan is removed, so the circuitry that remains powered on does not overheat and shut down.

CAUTION

It is recommended that you let the power amplifier module cool before performing the following step, which exposes surfaces of the module that can be extremely hot.

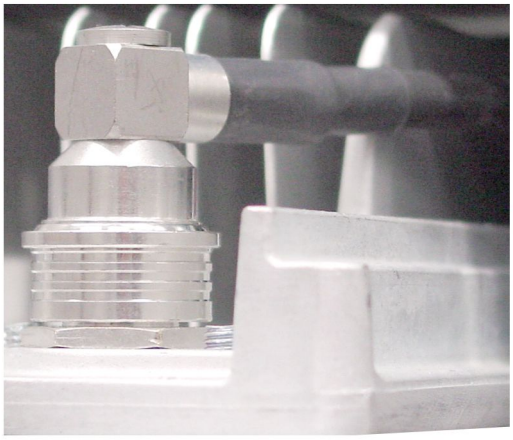
6 Using a T20 bit, loosen the two captive screws on the front of the power amplifier module so that they disengage from the chassis.

7 Remove the RF output QN connector from the front of the power amplifier module, as follows.

a. Pull the power amplifier out of the chassis far enough so that the QN (quick-N) RF output connector is accessible.

b. Disconnect the cable from the power amplifier.

Figure 9-10 Power Amplifier RF Cable (Front)



GTR8000_XCVR_RFCable_On

8 Using the handle, gently pull the power amplifier module straight out, along the guides on which it sits.

9 Reconnect the RF cable to the RF output QN connector on the front of the power amplifier module, as follows:

a. While holding the RF cable, slide in the replacement power amplifier module along the guiding rails until the RF cable connector can reach the RF connection on the front of the module.

b. Push the RF cable connector onto the module's connector until it snaps securely into place.

10 Slide in the replacement power amplifier module until it engages with the backplane. A slight push may be needed to engage the module.

IMPORTANT

If the power amplifier 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 °.

11 Secure the power amplifier module to the chassis with the two captive screws on the front of the module.

12 Reinstall the fan module. See 9.6 Removing/Replacing the Fan Module, page 9-13.

NOTE

If you chose to turn off the power, set the rocker switch on the front of the associated power supply to the On (1) position.

13 Verify that the power amplifier is operating properly.

- The power amplifier Status and Transmit LEDs are green.
- The Alarm LED is off.
- Proper operation is confirmed using software tools, such as Unified Event Manager, and the Transmitter Metering Screen in Configuration/Service Software (CSS).

14 Enable the base radio as follows:

a. From CSS, select **Service → Change to Normal Mode** from the menu.

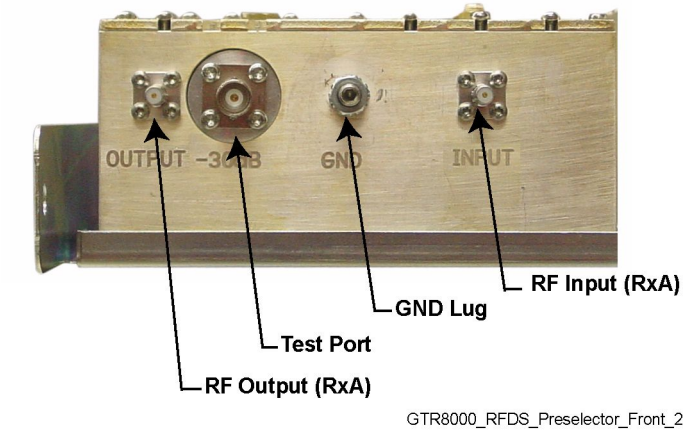
b. Click **Change to Service Mode**.

Step result: The base radio is enabled.

9.10 Replacing Filters/Preselectors in a GTR 8000 Site Subsystem

When and where to use:
If you are using the following procedure to replace one preselector filter, you can replace it without shutting the power down.

Figure 9-11 Preselector Filter



WARNING

Shock hazard. GTR 8000 Site Subsystems contain dangerous voltages which can cause severe electrical shock or damage to the equipment. Set the rocker switches on the front of the associated power supplies to the off position before servicing this component in the subsystem.

Procedure Steps

1 Wear an electrostatic discharge (ESD) 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 Disable all channels at the site that are using the transmit filter module being replaced:

NOTE

Using Unified Event Manager or CSS to disable the channel ensures that calls in progress complete before the channel shuts down.

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The channel is disabled.

3 Set the rocker switches on the front of the power supplies to the OFF (0) position.

4 Remove the filter tray from the rack, as follows:

a. Label and disconnect the RF input, RF output, and ground cables from the front of the preselector.

b. Using a T30 bit, remove the two screws which secure the filter tray to the rack.

c. Slide the tray out the front of the rack.

5 Perform one of the following actions:

If...	Then...
If you are replacing an individual filter,	perform the following actions: 1. Remove the T20 screws that secure the filter to the tray. 2. Remove the filter. 3. Place the new filter in the tray in the same location and orientation as the filter you are replacing. 4. Secure the new filter to the existing tray using the T20 screws previously removed. 5. Go to step 6, using the existing tray
If you are replacing the entire tray including the filter or filters,	perform the following action: • Go to step 6, using the replacement tray.

6 Install the filter tray in the rack:

a. Slide the filter tray into the appropriate location through the front of the rack.

b. Secure the slide rail to the rack using the two screws which were previously removed.

c. Reconnect the RF input, RF output, and ground cables to the preselector.

7 Set the rocker switches on the front of the power supplies to the On (1) position, to power up the GTR 8000 Site Subsystem.

8 Enable the channels as follows:

a. From CSS, select **Service → Test & Measurement Screen** from the menu.

b. Click **Change to Normal Mode**.

Step result: The channels are enabled.

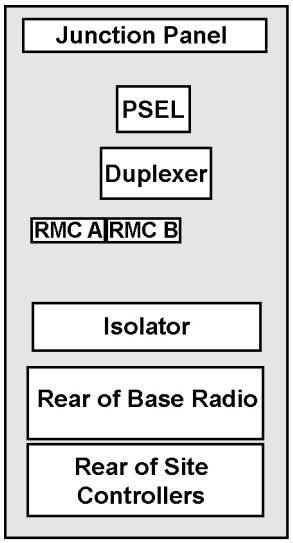
9 Verify that the GTR 8000 Site Subsystem is operating properly using fault management software, including:

- Unified Event Manager
- Transmitter Metering Screen in Configuration/Service Software (CSS)

9.11 Replacing a Cabinet RMC/LNA Module

Prerequisites:
The RMC/LNA modules and backplane connections are designed so that the modules can be swapped out without shutting the power down. In addition, the GTR 8000 Site Subsystem is designed with dual receive paths, so it may be possible to replace one RMC/LNA module without losing the channels provided by the subsystem. However, system performance may be degraded. If you choose to power down the subsystem, it causes any affiliated subscribers to relocate to another channel at the site or another channel at an adjacent site. It is recommended that you disable the channels before powering down, so that the system does not attribute the loss of channel to a failure. You can disable a channel using Unified Event Manager or the Configuration/Service Software (CSS).
This figure shows the GTR 8000 Site Subsystem with two Cabinet RMC/LNA modules

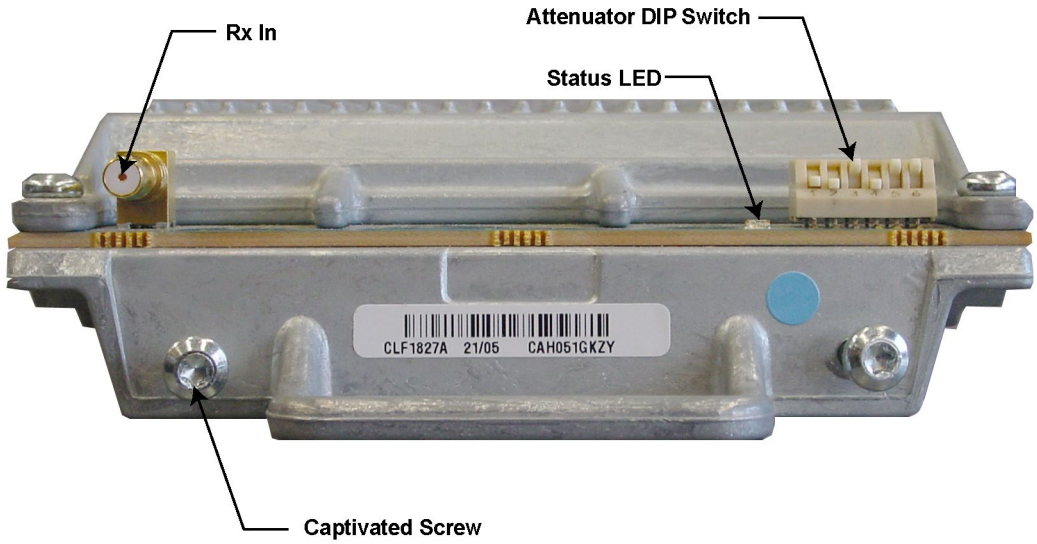
Figure 9-12 Cabinet RMC/LNA Modules in a GTR 8000 Site Subsystem (Rear View)



HPD_site_subsystem_config_rear_view

This figure shows an individual Cabinet RMC/LNA module.

Figure 9-13 Cabinet RMC/LNA Module (Front View)



GTR8000_RFDS_XS_RMC_Cabinet_Front1

Procedure Steps

1 Wear an electrostatic discharge (ESD) 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 Disable all channels at the site if you choose to shut down the power as follows:

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

---

3 If you choose to shut down the power, set the rocker switches on the front of the power supplies to the Off (0) position.

---

4 Remove the individual Cabinet RMC/LNA module as follows:

a. Label and disconnect the QMA input connectors from the front of the RMC/LNA module. The QMA connectors can be disconnected by hand.

b. Using a T20 bit, remove the two captive screws which secure the RMC module to the tray.

c. If you are removing the center RMC/LNA module, the rack ground bar must be temporarily moved out of the way. Using a T30 bit, remove the screws which attach the ground bar to the rack and move the bar to one side. Note the screw locations in the bar so you can re-attach it in the same position. Retain the screws for use in re-attaching the ground bar. Do not remove any ground cables from the ground bar.

d. Using the handle, gently pull the module straight out, along the guides on which it sits.

---

5 Set the DIP switches on the new Cabinet RMC/LNA module, using the instructions in 4.4.8 Setting RMC Attenuation, page 4-25.

---

6 Install the replacement Cabinet RMC/LNA module as follows:

a. Slide in the module along the guiding rails.

b. Secure the module to the chassis using the two T20 captive screws.

c. If it is the center RMC/LNA that you are replacing, the ground bar must be re-secured. Move the ground bar to its original position and re-attach with the T30 screws.

d. Reconnect the RF input cables to the QMA connector on the front of the RMC/LNA module.

---

7 If you chose to shut down the power, set the rocker switches on the front of the power supplies to the On (1) position.

---

8 If the base radios were disabled, enable the channels as follows:

a. From CSS, select **Service → Test & Measurement Screen** from the menu.

b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

---

9 Verify that the GTR 8000 Site Subsystem is operating properly using fault management software, including:

- Unified Event Manager
- Configuration/Service Software (CSS)

---

10 Verify that the RMC/LNA modules are operating properly.

- The Status LED on the front of each RMC/LNA module should be green.
- The red Alarm LED on the front of each RMC/LNA module should be off.

9.12 Replacing the Dual Circulator/Isolator Modules

Prerequisites:
Powering down the base radio caused any affiliated subscribers to relocate to another channel at the site or another channel at an adjacent site. It is recommended that you disable the channel before powering down, so that the system does not attribute the loss of channel to a failure. You can disable a channel using Unified Event Manager or the Configuration/Service Software (CSS).

When and where to use:
These modules can be replaced individually, or if you order them together, you may receive the modules already secured to a tray. For GTR 8000 Site Subsystems, the following RFDS modules are assembled in a tray:

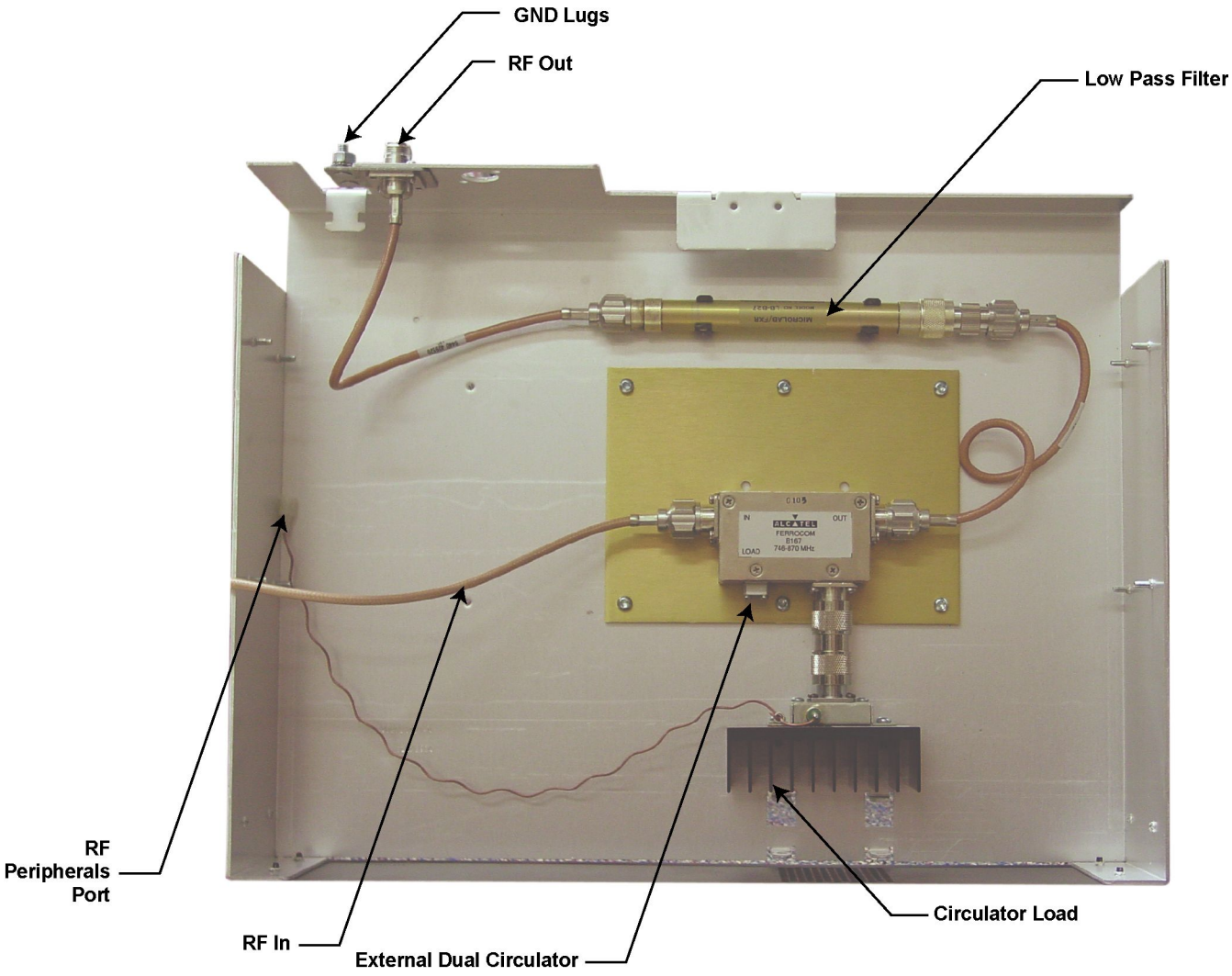
- External Dual Circulator/Isolator
- Circulator Load (a module connected directly to the External Dual Circulator module)
- Low Pass/Harmonic Filter

WARNING

Shock hazard. The GTR 8000 Site Subsystem contains dangerous voltages which can cause electrical shock or damage to the equipment. Set the power supply switches for the affected equipment to the Off (0) position when servicing this component in the GTR 8000 Site Subsystem.

This figure shows these modules installed on a tray.

Figure 9-14 Dual Circulator/Isolator Tray (Top View)



Procedure Steps

1 Wear an electrostatic discharge (ESD) 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 Set the rocker switch on the front of the power supply to the OFF (0) position.

3 Disable the base radio as follows:

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

4 Remove the filter tray from the rack, as follows:

a. Label and disconnect the RF input, RF output, and ground cables from the tray.

b. Disconnect the Circulator Load temperature cable at the inline connector (which disconnects it from the cable leading to the RF Peripherals port on the base radio backplane).

c. Using a T30 bit, remove the two screws which secure the tray to the rack.

d. Slide the tray out the front of the rack.

5 Perform one of the following actions:

If...	Then...
If you are replacing an individual External Dual Circulator/Isolator module,	perform the following actions: 1. Label and disconnect the RF input and RF output cables from the External Dual Circulator module. 2. Unscrew the connector that secures the Circulator Load to the External Dual Circulator module. 3. Remove the screws that secure the circulator baseplate to the tray. 4. Remove the circulator module including the circulator load module that extends beyond the baseplate. 5. Place the new External Dual Circulator module in the tray in the same location and orientation as the module you are replacing. 6. Secure the new External Dual Circulator module baseplate to the tray using the screws previously removed. 7. Connect the RF input and RF output cables to the new External Dual Circulator module. 8. Connect the Circulator Load to the External Dual Circulator module. 9. Go to step 6, using the existing tray.
If you are replacing an individual Circulator Load,	perform the following actions: 1. Unscrew the connector that secures the Circulator Load to the External Dual Circulator module. 2. Remove the Circulator Load module. 3. Place the new Circulator Load module on the tray in the same position and orientation as the module you removed. 4. Secure the new Circulator Load to the External Dual Circulator module by tightening the connector. 5. Connect the Circulator load cable to the RF Peripherals port on the base radio backplane. 6. Go to step 6, using the existing tray.

If...	Then...
If you are replacing an individual Low Pass/Harmonic Filter module,	perform the following actions: 1. Label and disconnect the RF input and RF output cables from the Low Pass/Harmonic Filter module. 2. Pull up firmly to release the Low Pass Filter module from the two semi-circular clips holding it in place. 3. Insert the new Low Pass Filter module into the semi-circular clips using the same orientation as the module you are replacing. 4. Connect the RF input and RF output cables to the new Low Pass/Harmonic Filter module. 5. Go to step 6, using the existing tray.
If you are replacing the entire tray including all of its modules,	perform the following actions: • Go to step 6, using the replacement tray.

6 Install the tray in the rack:

a. Slide the tray into the appropriate location through the front of the rack.

b. Secure the slide rail to the rack using the two screws which were previously removed.

c. Reconnect the RF input, RF output, and ground cables.

d. Reconnect the Circulator Load temperature cable at the inline connector (which connects it to the cable leading to the RF Peripherals port on the base radio backplane).

7 Set the rocker switches on the front of the power supplies to the On (1) position.

8 Enable the base radio as follows:

a. From CSS, select **Service → Test & Measurement Screen** from the menu.

b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

9 Verify that the GTR 8000 Site Subsystem is operating properly using fault management software, including:

- Unified Event Manager
- Transmitter Metering Screen in Configuration/Service Software (CSS)

9.13 Replacing a Duplexer

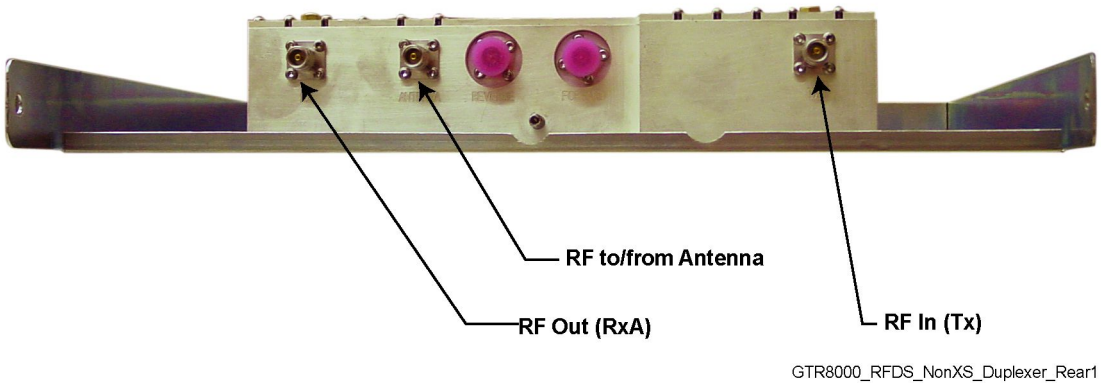
Prerequisites:
Powering down the GTR 8000 Site Subsystem causes any affiliated subscribers to relocate to another channel at the site or another channel at an adjacent site. It is recommended that you disable the channel before powering down, so that the system does not attribute the loss of channel to a failure. You can disable a channel using Unified Event Manager or the Configuration/Service Software (CSS).

WARNING

Shock hazard. The GTR 8000 Site Subsystem contains dangerous voltages which can cause electrical shock or damage to the equipment. Set the power supply switches for the affected equipment to the Off (0) position when servicing this component in the GTR 8000 Site Subsystem.

This figure shows the duplexer installed on a tray in the GTR 8000 Site Subsystem.

Figure 9-15 Duplexer Module



Procedure Steps

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 Disable the base radio connected to the duplexer being replaced

a. Connect to the base radio's transceiver module Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

3 Set the rocker switch on the front of the power supply to the OFF (0) position.

4 Remove the duplexer tray from the rack, as follows:
   a. Label and disconnect the Rx output, Tx input, antenna output, and ground cables from the duplexer.
   b. Using a T30 bit, remove the two screws which secure the tray to the rack.
   c. Slide the tray out the front of the rack.

5 Remove the duplexer from the tray, by removing the T20 screws that attach it to the tray.

6 Install the new duplexer in the tray, as follows:
   a. Place the new duplexer in the tray, in the same location and orientation as the module that you removed.
   b. Secure the replacement duplexer to the tray, using the T20 screws you previously removed.

7 Re-install the duplexer tray in the rack, as follows:
   a. Slide the tray into the front of the rack.
   b. Using a T30 bit, secure the tray to the rack with the two screws you previously removed.
   c. Reconnect the Rx output, Tx input, Antenna output, and ground cables to the duplexer.

8 Set the rocker switch on the front of the power supply to the ON (1) position.

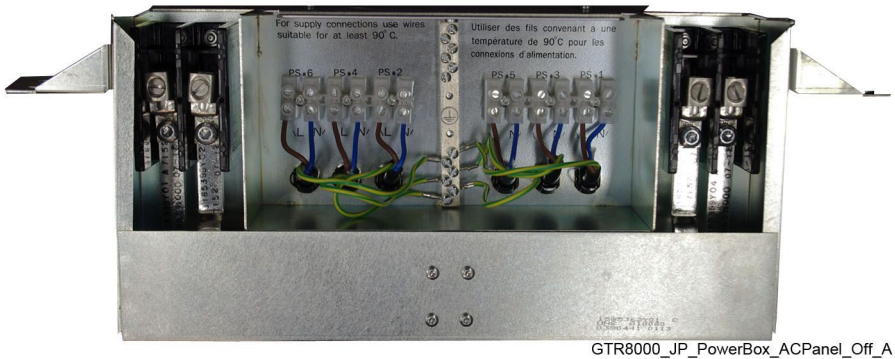
9 Enable the base radio as follows:
   a. From CSS, select **Service → Test & Measurement Screen** from the menu.
   b. Click **Change to Normal Mode**.

   Step result: The base radio is enabled.

9.14 Replacing the Power Distribution Module

Prerequisites:
Powering down the GTR 8000 Site Subsystem causes any affiliated subscribers to relocate to another channel at the site or another channel at an adjacent site. It is recommended that you disable the site before powering down, so that the system does not attribute the loss of channel to a failure. You can disable a site using Unified Event Manager or the Configuration/Service Software (CSS).
This figure shows the power distribution module with the terminal block access panel removed. The power distribution module is wired for six AC outputs, not three as shown in the figure.

Figure 9-16 Power Distribution Module (Access Panel Removed)

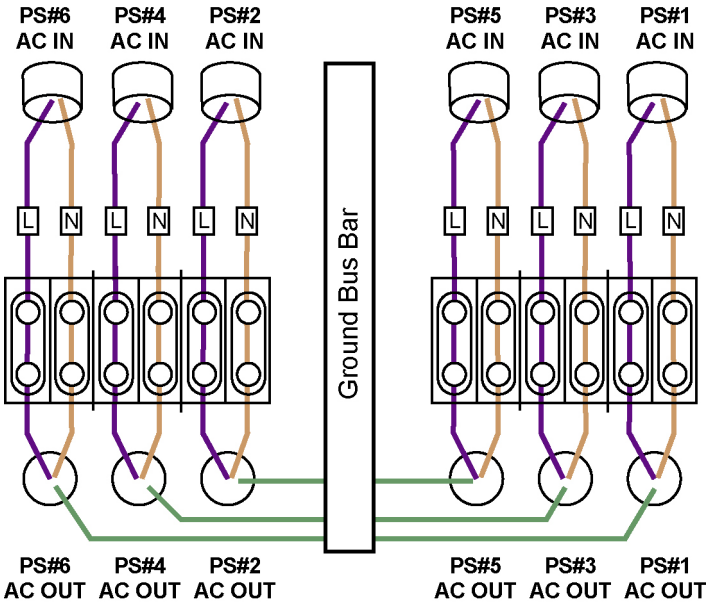


GTR8000_JP_PowerBox_ACPanel_Off_A

This figure shows AC distribution block of the power distribution module. In the figure:

- "L" indicates "Line" or "Hot" AC power feed.
- "N" indicates "Neutral" AC power feed.
- Input cable ground wires should be terminated to the ground bus bar.

Figure 9-17 Power Distribution Module – AC Distribution Block Diagram



GTR8000_JP_PowerBox_AC_DistrBlock

NOTE

The procedure assumes the following service access clearances:

- At least 2 ft access at the rear of the rack
- At least 2 ft access on both sides of the rack

CAUTION

The power distribution module and its cables are heavy. To avoid injury and damage to the equipment, have another person help lift and support the equipment when installing or removing the distribution module.

WARNING

Shock hazard. GTR 8000 Site Subsystems contain dangerous voltages which can cause electrical shock or damage to the equipment. Remove the AC and DC sources when servicing the power distribution module. Electrical installation work shall be carried out in accordance with the current edition of the NFPA 70 and local building codes. Where required, only a qualified and licensed electrician shall be used for all electrical installations.

Procedure Steps

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 Disable the site, as follows:

a. Connect to the appropriate site controller using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Status Panel Screen** from the menu.

c. Select the **Site Info** tab.

d. In the **User Requested Site State** select **Site OFF**.

Step result: The site is disabled.

3 Set all the AC supply breakers to the OFF position and open up the DC battery disconnects to power down the entire GTR 8000 Site Subsystem. Also shut down any other base radio racks which are connected to the GTR 8000 Site Subsystem.

4 Label and disconnect all input AC and DC power cables from the power distribution module.

5 Ensure that all power cables in the subsystem are free to be removed.

- Disconnect all power connectors from the AC and DC ports on the base radio and site controller backplanes.
- If the cables are tied to the rack, remove the ties.

6 Disengage the power distribution module from the junction panel by removing the two screws on each side of the power distribution module, using a T30 bit.

7 Lift the power distribution module to remove it, and feed the power cables to remove them from the rack.

8 Place the new power distribution module next to the junction panel in the same position and orientation as the module you removed.

9 Secure the power distribution module to the junction panel by securing the two screws on each side of the power distribution module to the junction panel, using a T30 bit

10 Connect the new module's power cables to the appropriate backplane input ports. For backplane connection information, see 2.5 Backplanes and Card Cages, page 2-14.

11 Reconnect all input AC and DC input power cables to the appropriate ports in the power distribution module. See Figure 9-17for the terminal block connections.

12 Secure the cables to the rack with cable ties.

13 Set all the AC supply breakers to the ON position and connect the DC battery to power up the GTR 8000 Site Subsystem. Also restore power to any other base radio racks which are connected to the GTR 8000 Site Subsystem.

14 Set the power supply rocker switches to On (1).

15 Enable the site, as follows:

a. Connect to the appropriate site controller using Configuration/Service Software (CSS).

b. Select **Service → Status Panel Screen** from the menu.

c. Select the **Site Info** tab.

d. In the **User Requested Site State** field, select **Wide Trunking**.

Step result: The site is enabled.

16 Verify that the subsystem is operating properly using software tools, including:

- Unified Event Manager
- Power Supply Metering Screen in Configuration/Service Software (CSS)

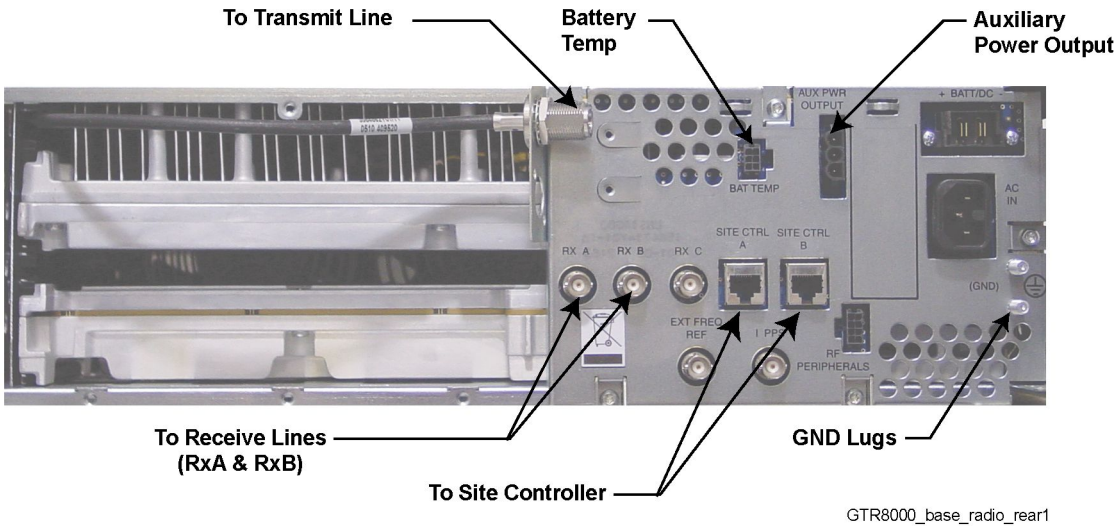
9.15 Replacing the GTR 8000 Base Radio Backplane

Prerequisites:
The procedure assumes the following service access clearances:

- At least 2 ft access at the rear of the rack
- At least 2 ft access on one side of the rack, and at least 6 inches at the rear of the rack

When and where to use:
In a GTR 8000 Site Subsystem configuration, the “backplane” is the circuit board at the rear of the card cage which connects the power supply, transceiver, and power amplifier. This figure shows the metal cover that must be removed to access the backplane and the ports for cables that must be disconnected to remove the cover.

Figure 9-18 GTR 8000 Base Radio (Backplane Cover)



Procedure Steps

1 Wear an electrostatic discharge (ESD) strap and connect its cable to a verified good ground. Be sure to wear this strap throughout this procedure to prevent ESD damage to any components.

2 If the base radio is not operational, go to step 4.

3 Disable the base radio.

NOTE

Powering down the base radio causes any affiliated subscribers to relocate to another channel at the site or another channel at an adjacent site. It is recommended that you disable the channel before powering down, so that the system does not attribute the loss of channel to a failure. You can disable a channel using Unified Event Manager or the Configuration/Service Software (CSS).

a. Connect to the device module's Ethernet service port using Configuration/Service Software (CSS). See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

b. Select **Service → Test & Measurement Screen** from the menu.

c. Click **Change to Service Mode**.

Step result: The base radio is disabled.

4 Push the power rocker switch to Off (0) on the power supply unit.

5 Label, then disconnect all cables from the base radio backplane.

NOTE

There is an RF output cable from the power amplifier which connects through a metal bulkhead to the left of the backplane. This cable does not need to be disconnected. However, to access the backplane screw behind the metal bulkhead, remove the two screws securing the bulkhead to the inner chassis at the left of the backplane using a T20 bit.

6 Remove the power supply module from the chassis as follows:

a. Using a T20 bit, loosen the two captive screws on the front of the power supply, so that they disengage from the chassis.

WARNING

It is recommended that you let the power supply module cool before performing the following step, which exposed surfaces of the module that can be extremely hot.

b. Pull on the metal handle to disengage the power supply module from the backplane, and remove it completely from the chassis.

7 Remove the fan assembly module to gain access to the transceiver and power amplifier modules. See 9.6 Removing/Replacing the Fan Module, page 9-13.

8 Disengage the transceiver module and the power amplifier 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.

WARNING

It is recommended that you let the power amplifier module cool before performing the following step, which exposes surfaces of the module that can be extremely hot.

b. Using their handles, gently pull the modules until they disengage from the backplane.

9 Using a T20 bit, remove the screw that secures the tab on the right EMI spring panel. See Figure 9-20.

NOTE

Removing the left EMI spring panel is optional.

10 Carefully slide the EMI spring panel forward, noting how the panel is affixed onto the power supply guide rail. The panel does not need to be completely removed.

11 Remove the fan cable from the backplane, 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's multi-pin connector from the backplane.

SUGGESTION

Squeeze the top and bottom of the connector and pull the connector straight out from the backplane.

---

12 Remove the five screws, using a T20 bit, that secure the metal backplane cover and the backplane circuit board to the rear of the base radio chassis.

---

13 Remove the metal backplane cover and the backplane circuit board.

---

14 Place the new backplane circuit board in the same location and orientation as the one that you removed.

---

15 Replace the backplane cover and insert and start the five screws previously removed.

---

16 Secure the new backplane circuit board and the backplane cover to the rear of the base radio chassis by torquing the screws to 18 +/- 2 in.-lbs.

---

17 Reinstall the metal bulkhead that holds the RF output cable from the power amplifier, using the two screws previously removed to secure it to the inner chassis at the left of the backplane.

---

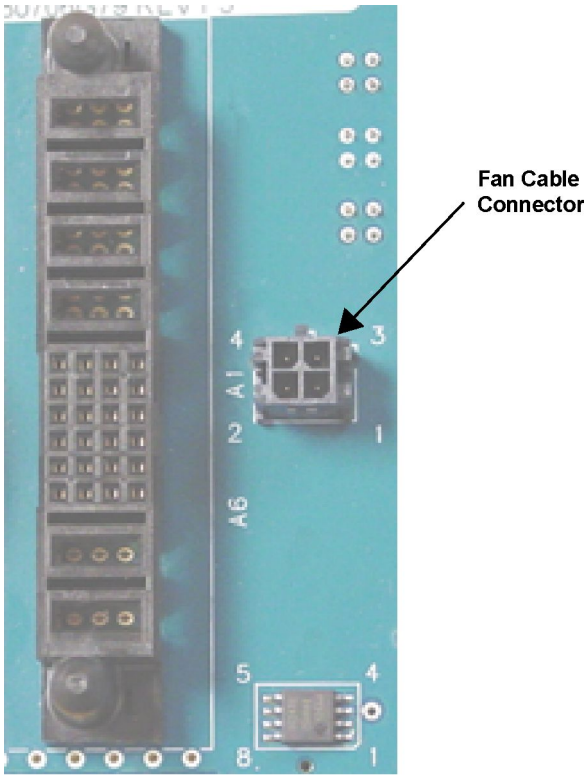
18 Connect the fan cable to the new backplane, from the front of the chassis, with the backplane secured to the chassis, as follows:

a. Locate the port in the new backplane for the fan cable's 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's multi-pin connector, with the tab up, into the correct location in the backplane.

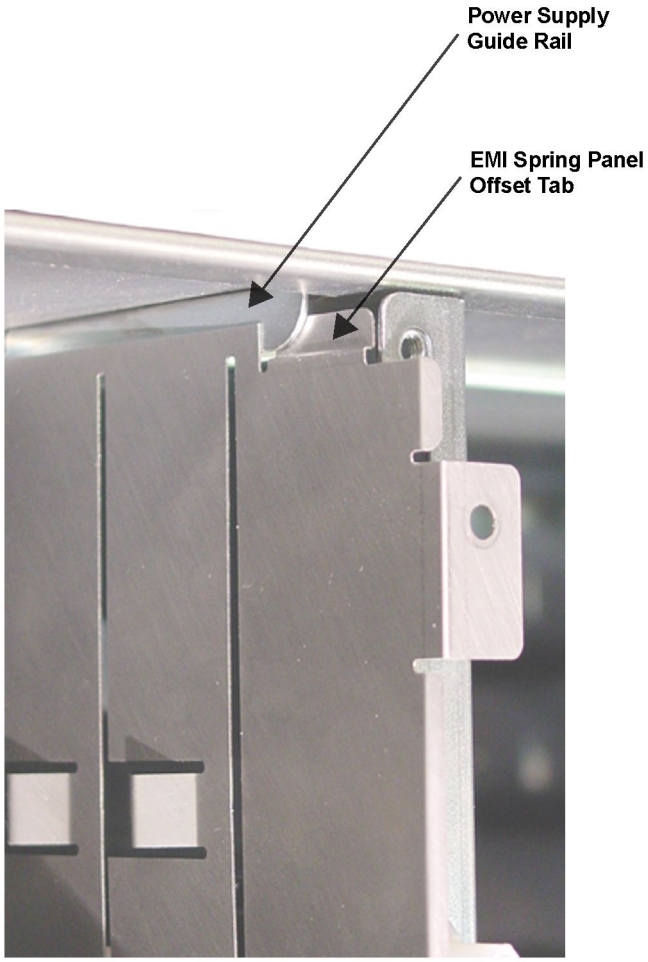
Figure 9-19 Fan Cable Connector



GTR_GCP_Fan_Cable_Connector

19 Slide the EMI spring panel back into the cabinet, making sure that the offset tabs on the panel are to the right (inside) of the power supply guide rail, making sure that the panel does not catch on the fan cable.

Figure 9-20 EMI Spring Panel Guide Rail Alignment



GTR_GCP_EMI_panel_alignment

20 Reinstall the screw into the EMI spring panel tab.

21 Slide the transceiver and power amplifier modules into the new backplane. A slight push may be needed to engage the modules.

22 Secure the transceiver and power amplifier modules to the chassis with the two captive screws on the front of each module.

23 Reinstall the fan assembly unit. See 9.6 Removing/Replacing the Fan Module, page 9-13.

24 Slide the power supply into the chassis, pushing gently until it seats in the new backplane.

NOTE

If the power supply does not seat properly, remove it and adjust the EMI spring panel properly against the mounting flange.

25 Tighten the two captive screws on the front of the power supply.

26 Reconnect all cables at the rear of the base radio.

27 Set the power supply rocker switch to On (1).

28 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.

29 Enable the base radio as follows:

a. From CSS, select **Service → Test & Measurement Screen** from the menu.

b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

30 Verify proper operation using software tools, such as:

- Unified Event Manager
- Configuration/Service Software (CSS)

31 Re-configure the Security Settings into the Backplane. See 4.4.3.2.1 Setting the Serial Security Services Using CSS, page 4-8.

10 GTR 8000 Site Subsystem Reference

This chapter contains supplemental reference information relating to GTR 8000 Site Subsystem.

Reference information for GTR 8000 Site Subsystem includes LED states and specifications for individual RFDS modules.

10.1 LEDs

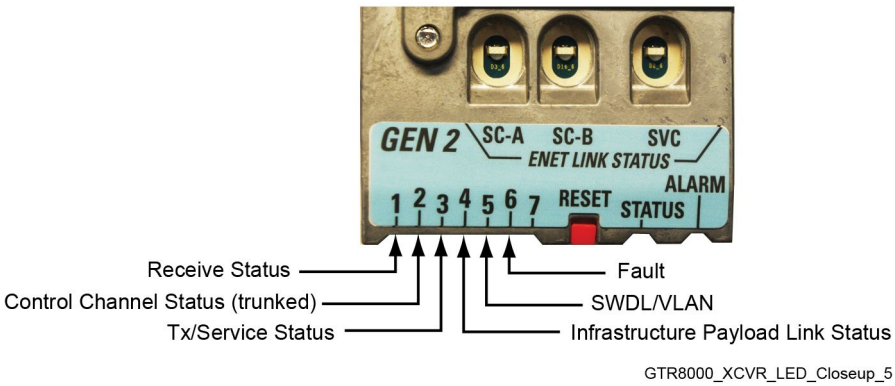
Many of the LEDs on the GTR 8000 Base Radio devices provide an indication for one or more the following conditions:

- **Lamp Test:** The Lamp Test state is used to verify that the indicators are operational. For Lamp Test, the LEDs stay in this state for only a second or less.
- **Failure:** Indicates a failure that can only be fixed through replacement. If something other than a hardware fault is causing the state, Impaired is noted.
- **Impaired:** The device is not fully operational due to internal or external causes. Some corrective action must be taken to get back to 100% operation.
- **Booting Up:** The device is not in service due to running of diagnostics or initializing.
- **Online:** Indicates that the device is fully operational.

The LEDs for the transceiver and power amplifier modules can be viewed through the door next to the fans, with the door opened, or closed.

10.1.1 GTR 8000 Base Radio Transceiver LEDs

Figure 10-1 Transceiver LEDs (viewable through a drop-down door)



10.1.1.1 Transceiver Status and Alarm LEDs

The Status LED is green, and the Alarm LED is red. These LEDs are either off, on, or blinking depending on the condition of the transceiver.

Table 10-1 Transceiver Status and Alarm LEDs

Condition	Green (Status LED)	Red (Alarm LED)
No Power	Off	Off
Lamp Test (During Test)	On	On
Impaired Operation	On	Blinking
Critical Failure	Off	On
Booting Up	Blinking	Off
Operational	On	Off

Note: To get detailed information on current operation and fault status, use the CSS Status Panel screen.

10.1.1.2 Transceiver Ethernet Link Status LEDs

The following LEDs indicate Ethernet link and status connections between the transceiver, LAN, and the front panel service port.

Table 10-2 Transceiver Ethernet Link Status LEDs

LED Name	Indication	LED Status
ENET SC-A (external connection to SITE CTRL A on the rear of the chassis)	Ethernet link inactive (Remote PHY/MAC not detected.)	Off
	Ethernet link established (Remote PHY/MAC detected and auto-negotiation completed.)	Green
	Ethernet link active (Actively transmitting or receiving data.)	Amber (blinking)
ENET SC-B (external connection to SITE CTRL B on the rear of the chassis)	Ethernet link inactive (Remote PHY/MAC not detected.)	Off
	Ethernet link established (Remote PHY/MAC detected and auto-negotiation completed.)	Green
	Ethernet link active (Actively transmitting or receiving data.)	Amber (blinking)
ENET SVC (front panel service port)	Ethernet link inactive (Remote PHY/MAC not detected.)	Off
	Ethernet link established (Remote PHY/MAC detected and auto-negotiation completed.)	Green
	Ethernet link active (Actively transmitting or receiving data.)	Amber (blinking)

10.1.1.3 Transceiver Application-Controlled LEDs

The application-controlled LEDs can be green, red, or amber depending on the conditions.

Table 10-3 Transceiver Application-Controlled LEDs

Condition	LED 1 Receive Status	LED 2 Control Channel Status	LED 3 Tx/Service Status	LED 4 Infrastructure Payload Link Status
Booting Up*	Green	Green	Green	Green
Lamp Test	Amber	Amber	Amber	Amber
Receiver Inhibited	Amber (blinking)			
Receiver Active	Green			
RF Channel Interference	Red (blinking)			
Monitor Before Data Transmit	Green			
Illegal Carrier	Red (blinking)			
Control Channel (Operating)		Green		
Control Channel (Failsoft)		Green (blinking)		
Service Mode			Amber	
Transmitter Inhibited			Amber (blinking)	
Infrastructure Link Connected (V.24, IP, and 4–wire/V.24)				Green
Partial Infrastructure Link Established (V.24 link established, 4–wire link not established)				Amber
Infrastructure Link Disconnected (V.24, IP, and 4–wire/V-24)				Green (blinking)

* During a normal boot up sequence, LEDs 1 through 4 blink from left to right and from right to left continuously for several seconds.

10.1.1.4 Transceiver Services-Controlled LEDs

For the service-controlled LEDs, the color of all LEDs must be observed to interpret the condition of the transceiver.

Table 10-4 Transceiver Services-Controlled LEDs

Condition	LED 5 SWDL/VLAN	LED 6 Fault	LED 7
Lamp Test	Amber	Amber	Amber
Receiver Inhibited		Red	
Receiver Reference Failure		Red	

Table 10-4 Transceiver Services-Controlled LEDs (cont'd.)

Condition	LED 5 SWDL/VLAN	LED 6 Fault	LED 7
Transmitter Inhibited		Red	
SWDL (Software Download transfer in progress)	Green		
Warning		Amber	
Minor Hardware Failure		Amber (blinking)	
Major Hardware Failure		Red (blinking)	
Critical Hardware Failure		Red	
VSWR Fault		Red	

10.1.2 Power Amplifier LEDs

Figure 10-2 Power Amplifier LEDs, viewable through a drop-down door

GTR8000_PA_LED_Closeup1

The power amplifier LED color must be observed to interpret the power amplifiers condition. For example:

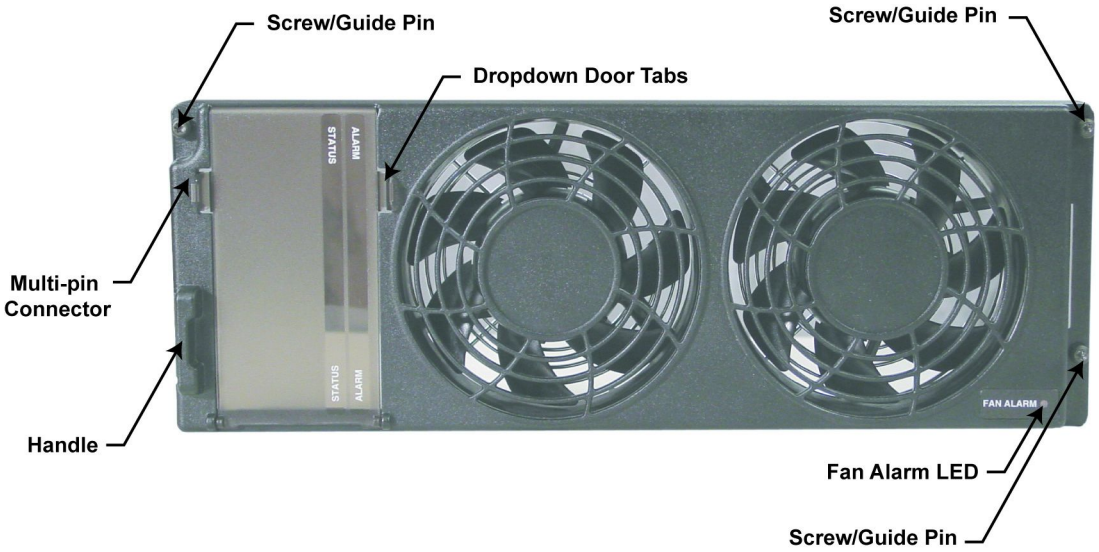
- If the Alarm LED is red and the Transmit and Status LEDs are not lit, the condition is “PA Failure” and the power amplifier module should be replaced.

Table 10-5 Power Amplifier LEDs

Condition	Transmit (XMIT)	Status	Alarm
Power Off	Off	Off	Off
Lamp Test	Amber	Green	Red
Not Transmitting	Off	Green	Off
Transmitting at Full Requested Output Power	Green	Green	Off
Transmitting at Less Than Requested Power	Amber	Green	Red
PA Failure	Red	Off	Red
Receive Only	Off	Off	Off
Transmitter Inhibited	Off	Green	Red (blinking)

10.1.3 Fan Module LED

Figure 10-3 Fan Module-Alarm LED (lower right corner)



The fan module has one Fan Alarm LED visible on the lower right corner of its front panel. The Alarm is red during Lamp Test (for a second or less), and remains red if there is a fan failure. A fan failure alarm occurs if the built-in speed sensor detects if either fan drops 30% below rated speed. A red Fan Alarm indicates that the fan module must be replaced.

NOTE

The fan operates at full capability for at least seven days after the fan alarm first occurs, allowing normal operation without requiring an immediate service call.

10.1.4 Power Supply LEDs

Figure 10-4 Power Supply Module

HPD_Power_Supply_FRU.jpg

The power supply has three LEDs visible from the front panel. To interpret its condition, observe the color of all the power supply LEDs. For example:

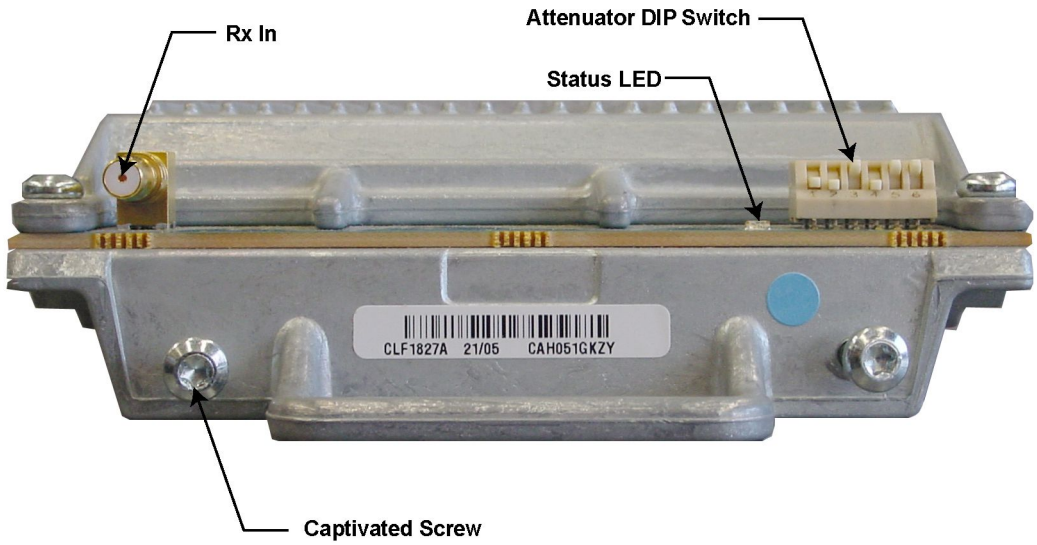
- If the Alarm and Fan LEDs are red and the Status LED is green, the condition is "Lamp Test"
- If the Alarm LED is red and the Fan and Status LEDs are not lit, the condition is "Power Supply Failure"

Table 10-6 Power Supply LEDs

Condition	Fan	Status	Alarm
Power Off	Off	Off	Off
Lamp Test	Red	Green	Red
Online	Off	Green	Off
Impaired	Off	Green	Red (blinking)
Power Supply Failure	Off	Off	Red
Power Supply Fan Failure	Red	Off	Red

10.1.5 RMC/LNA Alarm and Status LEDs

Figure 10-5 Cabinet RMC/LNA Module



Receive multicouplers/low noise amplifiers (RMCs/LNAs) have a green Status LED and red Alarm LED next to the DIP switches. These LEDs are either off or on, depending on the condition of the module, as indicated in the table.

Table 10-7 RMC/LNA Module LED States

Information State	Alarm LED (red)	Status LED (green)
No Power	Off	Off
Failure	On	Off
Online	Off	On

10.2 RFDS Equipment Specifications

This section provides specifications for all the RFDS equipment:site preselector filter, duplexer, and receiver multicoupler / low noise amplifier.

10.2.1 Site Preselector Filter Specifications

Table 10-8 Site Preselector Filter Specifications

	Site Preselector Spec Limit (700/800 MHz)	Typical
Frequency range	792-825 MHz	
Insertion loss	1 dB	0.6 dB
VSWR max.	1.5:1	1.3:1
Tx selectivity	75 dB	78 dB
Test Port Coupling		-30 dB
Input Connector	QMA	
Output Connector	QMA	
Test Port Connector	BNC	
Test Port Coupling	-30 dB	
Test Port Coupling	-30 dB	

10.2.2 Duplexer Specifications

Table 10-9 Duplexer Specifications

	Duplexer Spec Limit (700/800 MHz)	Typical	Notes
Tx Frequency range	764-776 MHz or 851-870 MHz		
Rx Frequency range	792-806 MHz or 806–825 MHz		
Insertion loss Tx	1 dB	0.5 dB	
Insertion loss Rx	1 dB	0.6 dB	
VSWR max.	1.5:1	1.23:1	
Rx isolation	80 dB	85 dB	
Tx isolation	80 dB	85 dB	
Passive Intermodulation	-120 dBc		2 x 43 dBm
Antenna Connector	QN		

Table 10-9 Duplexer Specifications (cont'd.)

	Duplexer Spec Limit (700/800 MHz)	Typical	Notes
Rx/Tx Output Connector	QN		
Rx/Tx Output Connector	QN	QN	

10.2.3 Site Receiver Multicoupler/Low Noise Amplifier (RMC/LNA) Specifications

Table 10-10 Site Receiver Multicoupler/Low Noise Amplifier (RMC/LNA) Specifications

	Site RMC/LNA Spec Limit	Site RMC/LNA Typical	Notes
Frequency range	776–824 MHz		
Attenuator range	0-31 dB		
Default attenuator setting	1 dB		Factory preset
Default Gain Primary Output Expansion Outputs	 9 dB 11.8 dB	 10.5 dB 12.3 dB	Factory preset
Noise Figure Primary Output Expansion Outputs	 2.6 dB 2.4 dB	 2.0 dB 1.8 dB	Factory preset
Third Order output intercept Primary Output Expansion Outputs		 23 dBm 25 dBm	Factory preset
Input connector type	QMA		
Output connector type Primary Output Expansion Outputs	 QMA BNC (3)		
VSWR max	1.5:1		All ports

10.2.4 Cabinet Receiver Multicoupler/Low Noise Amplifier (RMC/LNA) Specifications

Table 10-11 Cabinet Receiver Multicoupler/Low Noise Amplifier (RMC/LNA) Specifications

	Cabinet RMC/LNA Spec Limit	Cabinet RMC/LNA Typical	Notes
Frequency range	776–824 MHz		
Attenuator range	0-31 dB		

Table 10-11 Cabinet Receiver Multicoupler/Low Noise Amplifier (RMC/LNA) Specifications (cont'd.)

	Cabinet RMC/LNA Spec Limit	Cabinet RMC/LNA Typical	Notes
Default attenuator setting No Site RMC With Site RMC	 0 dB 10 dB		Factory preset
Default Overall Gain No Site RMC With Site RMC	 15 dB 5 dB	 16.3 dB 6.4 dB	Factory preset
Noise Figure No Site RMC With Site RMC	 2.4 dB 4.5 dB	 1.7 dB 3.7 dB	Factory preset
Third Order output intercept No Site RMC With Site RMC		 29 dBm 24 dBm	Factory preset
Input connector type	QMA		
Output connector type	Harting 6–way		
VSWR max	1.5:1		All ports

11 GTR 8000 Site Subsystem Disaster Recovery

This chapter provides references and information that assist in the recovery the GTR 8000 Base Radio and GCP 8000 Site Controller in the event of a failure.

11.1 Recovery Sequence for GTR 8000 Base Radio

Process Steps

1. Replace the GTR 8000 Base Radio transceiver module. See 9.5 Replacing a Transceiver Module, page 9-7.
2. Perform basic device configuration using the serial port. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.
   a. Set the IP address of the device. See 4.4.3.1 Setting the Device IP Address Using CSS, page 4-6.
   b. Set the serial security services. See 4.4.3.2.1 Setting the Serial Security Services Using CSS, page 4-8.
3. Perform basic device configuration using the Ethernet port. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.
   a. Set the current date and time in CSS. See 4.4.5.1 Setting the Date and Time Using CSS, page 4-13.
   b. Set up the local Password Configuration using the CSS (optional). See 4.4.5.6 Setting Up the Local Password Configuration Using the CSS, page 4-21.

4 Complete the configuration of the Information Assurance features using CSS, as follows:

a. Change the SNMPv3 configuration and user credentials from CSS. See 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14.

b. Create, update, or delete an SNMPv3 user. See 4.4.5.2.1 Adding or Modifying an SNMPv3 User Using CSS, page 4-17.

c. Verify the SNMPv3 credentials. See 4.4.5.2.2 Performing an SNMPv3 Connection Verification Using CSS, page 4-18.

d. Set the SWDL transfer mode. See 4.4.5.4 Setting the SWDL Transfer Mode Using CSS, page 4-19.

e. Configure DNS using the CSS. See Chapter 7, “Configuring DNS Using CSS” in the *Authentication Services* manual.

f. Configure for SSH. See Chapter 4, “Configuring SSH for RF Site Devices and VPMs Using CSS” in the *Securing Protocols with SSH* manual or see “Device Security Configuration Remote Access/Login Banner (Ethernet)” in the *CSS Online Help*.

NOTE

Make sure to Restore the Clear Protocols parameters.

g. Enable RADIUS Authentication using the CSS. See Chapter 7, “Configuring RADIUS Sources and Parameters Using CSS” in the *Authentication Services* manual.

h. Enable Centralized Authentication using the CSS. See Chapter 7, “Enabling/Disabling Centralized Authentication Using CSS” in the *Authentication Services* manual.

i. Set the Local Cache Size for Centralized Authentication using the CSS. See Chapter 7, “Setting the Local Cache Size for Central Authentication Using CSS” in the *Authentication Services* manual.

j. Enable Centralized Event Logging using CSS (if required by your organization). See Chapter 6, “How to Enable/Disable Centralized Event Logging on Devices Using CSS” and Chapter 1, “Event Logging Client Configuration” for proper hostnames in the *Centralized Event Logging* manual.

k. Set the NTP Server Settings. See 4.4.5.5 Setting the NTP Server Settings, page 4-20.

---

5 Open the Software Download application.

CAUTION

Make sure to 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 transceiver to go into a configuration mode of operation with a reason of ‘Invalid Software Version’. To exit the base radio out of configuration mode, see CSS Procedures > Changing from Configuration to Normal Mode in the *CSS Online Help*.

---

6 Perform a single device software download to transfer and install the latest software using Software Download as follows:

a. Select **File → File Manager** from the menu.

Step result: The **Software Depot File Manager** opens.

b. Select **Component Operations → Import Fileset** from the menu.

Step result: The **Import a Fileset Into the Software Depot** dialog box appears.

c. Click **Browse** and search for the **swdlv3.cfg** file on the CD. Click **Open**.

d. Click **Generate** to add the file to the Components In the Software Depot list. Click **OK**.

e. Exit the Software Depot File Manager.

f. From Software Download, select the appropriate ASTRO 25 system Site Type, and the relevant zone and site information, and if applicable, the Subsite. The Subsite ID is only available when the Site ID is between 1-64.

g. Select **Single Device Mode**.

h. Enter the **<IP address>** of the device. Click **Continue**.

i. In the Select an option window, select **Upgrade Software Application**. Click **Continue**.

j. Select either **HPD Base Radio** for the Application Type.

k. Select **Transfer and Install** for the Operation Type.

l. For Software Component, select a configuration fileset from the drop-down list.

m. Select **Start Operation**.

Step result: The software is transferred and installed on to the device. The transfer and install takes several minutes to complete. When completed, the two progress bars on the Transfer and Install window display 100% and a completion message displays in the Transfer message box.

---

7 Restore Codeplug Archive from backup in CSS. Reload the base radio configuration file on to the new base radio, as follows:

a. Select **File → Open**.

b. Locate and open the previously saved configuration file for the base radio.

NOTE

If you were not able to back up the base radio configuration from the previous base radio, you can use the configuration from your system build book or use the default base radio configuration file. Specific settings for the base radio must still be configured. See the *CSS Online Help* for detailed configuration instructions.

c. Click **OK** on the Properties window.

d. Select **File → Write Configuration To Device**. Click **OK**.

Step result: The configuration from the file you selected is loaded into the new base radio. Communication with the base radio is not available until the reset is complete.

---

8 Enable the base radio in CSS as follows:

a. Select **Service → Mode Screen**.

b. Click **Change to Normal Mode**.

Step result: The base radio is enabled.

9 Disconnect the laptop PC from the transceiver.

10 Perform a site software download (SWDL) with the SNMPv3 package (if SNMPv3 is desired) of the device and associated site devices. See 11.3 Performing a Site Download, page 11-7.

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 transceiver or expansion channel to have a mismatch in software versions. If a mismatch in software versions occurs, the transceiver may go into a configuration mode of operation with a reason of 'Invalid Software Version'.

11 Disconnect the PC Ethernet from the local LAN.

12 On systems with SNMPv3 enabled, enable passphrase information. For procedures to enable passphrases, see the *SNMPv3* manual.

13 On systems with MAC Port Lockdown, disable the locking and then re-enable the locking with the MAC address of the base radio. The device being replaced may be connected to an Ethernet port on a switch which implements MAC Port Lockdown (HP switch or site controller). If so, the Ethernet switch port must be unlocked and relocked to the MAC address of the replacement device. See the *MAC Port Lockdown* manual for instructions on how to disable and enable MAC Port Lockdown.

NOTE

Following the device restoration, if it was connected to an HP switch port, the HP switch port may have been disabled due to an unexpected MAC address. If so, re-enable the port on the HP switch.

14 Replace the base radio in the UNC. See Chapter 4, "Replacing a Device" in the *Unified Network Configurator* manual.

15 Discover the base radio in the UEM. See the *Unified Event Manager* manual.

16 Verify that the base radio is operating properly:

- The Status LED on the front of the transceiver is green.
- Proper operation is confirmed using software tools, such as UEM, and the Transmitter Metering Screen in Configuration/Service Software (CSS).

11.2 Recovery Sequence for GCP 8000 Site Controller

Process Steps

1 Replace the GCP 8000 Site Controller module. See Chapter 9, “How to Replace the GCP 8000 Site Controller Module” in the *GCP 8000 Site Controller* manual.

2 Perform basic device configuration via the serial port. See 4.4.2 Connecting Through a Serial Port Link, page 4-4.

   a. Set the IP address of the device. See 4.4.3.1 Setting the Device IP Address Using CSS, page 4-6.

   b. Set the serial security services. See 4.4.3.2.1 Setting the Serial Security Services Using CSS, page 4-8.

3 Perform basic device configuration via the Ethernet port. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

   a. Set the current date and time in CSS. See 4.4.5.1 Setting the Date and Time Using CSS, page 4-13.

   b. Set up the local Password Configuration using the CSS (optional). See 4.4.5.6 Setting Up the Local Password Configuration Using the CSS, page 4-21.

4 Complete the configuration of the Information Assurance features using CSS, as follows:

a. Change the SNMPv3 configuration and user credentials from CSS. See 4.4.5.2 Changing SNMPv3 Configuration and User Credentials Using CSS, page 4-14.

b. Create, update, or delete an SNMPv3 user. See 4.4.5.2.1 Adding or Modifying an SNMPv3 User Using CSS, page 4-17.

c. Verify the SNMPv3 credentials. See 4.4.5.2.2 Performing an SNMPv3 Connection Verification Using CSS, page 4-18.

d. Set the SWDL transfer mode. See 4.4.5.4 Setting the SWDL Transfer Mode Using CSS, page 4-19.

e. For a trunked site controller, configure DNS using the CSS. See Chapter 7, “Configuring DNS Using CSS” in the *Authentication Services* manual.

f. Configure for SSH. See Chapter 4, “Configuring SSH for RF Site Devices and VPMs Using CSS” in the *Securing Protocols with SSH* manual or see “Device Security Configuration Remote Access/Login Banner (Ethernet)” in the *CSS Online Help*.

NOTE

Make sure to Restore the Clear Protocols parameters.

g. Enable RADIUS Authentication using the CSS. See Chapter 7, “Configuring RADIUS Sources and Parameters Using CSS” in the *Authentication Services* manual.

h. Enable Centralized Authentication using the CSS. See Chapter 7, “Enabling/Disabling Centralized Authentication Using CSS” in the *Authentication Services* manual.

i. Set the Local Cache Size for Centralized Authentication using the CSS. See Chapter 7, “Setting the Local Cache Size for Central Authentication Using CSS” in the *Authentication Services* manual.

j. Enable Centralized Event Logging using the CSS (if required by your organization). See Chapter 6, “How to Enable/Disable Centralized Event Logging on Devices Using CSS” and Chapter 1, “Event Logging Client Configuration” for proper hostnames in the *Centralized Event Logging* manual.

---

5 Perform a site software download (SWDL) with the SNMPv3 package (if SNMPv3 is desired) of the device and associated site devices. See 11.3 Performing a Site Download, page 11-7.

---

6 Restore Codeplug Archive from backup. Reload the configuration file on to the new site controller using CSS, as follows:

a. Select **File → Open** from the menu. Locate and open the previously saved configuration file for the device.

NOTE

If you were not able to back up the configuration from the previous site controller, you can use the configuration from your system build book or use the default configuration file. Specific settings for the site controller must still be configured. See the *CSS Online Help* for detailed configuration instructions.

b. Click **OK** on the Properties window.

c. Select **File → Write Configuration To Device** from the menu. Click **OK** on the confirmation message.

Step result: The configuration from the file you selected is loaded into the new site controller.

---

7 Enable the site controller using CSS as follows:

a. Select **Service → Service Panel Screen** from the menu.

b. From the Service Panel Screens window, select the **Site Controller** tab.

c. From the User Requested Site Controller State list box, select **Enabled**.

Step result: The site controller module is enabled after approximately two minutes.

8 Restore the 802.1x / MAC Port Lockdown feature as follows:

a. Capture the MAC address of the device on the GCP 8000 switch for all devices connected to the GCP 8000 Site Controller. See "How to Capture 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 Using 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 site controllers. See "Enabling/Disabling 802.1x and MAC Port Lockdown for GCP 8000 Using CSS" in the *802.1x Service Ports on Switches* manual.

9 Replace the site controller in the UNC. See Chapter 4, "Replacing a Device" in the *Unified Network Configurator* manual.

10 Discover the site controller in the UEM. See the *Unified Event Manager* manual.

11.3 Performing a Site Download

Procedure Steps

1 Connect an Ethernet straight through cable between the Ethernet port on the computer and the Ethernet service port on the site controller. The laptop IP address must be set to an address on the subnet of the local site, which varies depending on the site and zone numbers. See 4.4.4 Connecting Through an Ethernet Port Link, page 4-9.

2 Open the Software Download application.

CAUTION

Make sure to 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 as follows:

a. Select **File → File Manager** from the menu.

Step result: The **Software Depot File Manager** opens.

b. Select **Component Operations → Import Fileset** from the menu.

Step result: The **Import a Fileset Into the Software Depot** dialog box appears.

c. Click **Browse** and search for the **swdlv3.cfg** file on the CD. Click **Open**.

d. Click **Generate** to add the file to the Components In the Software Depot list. Click **OK**.

e. Exit the Software Depot File Manager.

f. From Software Download, select the appropriate **ASTRO 25 Site Type**.

g. Select the **Zone**, **Site**, and if applicable, the **Subsite**. The Subsite ID is only available when the Site ID is between 1-64.

h. Click **Connect**.

Step result: The system connects to the specified zone and site.

i. Select **Transfer and Install** for the Operations Type.

j. Select the Application Type:

- For an HPD site: select both **HPD Site Controller** and **HPD Base Radio**.

Both the site controller and base radio software must be chosen as part of the Site Software Download.

k. Select a Software Component from the drop-down list.

l. Click **Start Operation** to download and install the software.

Step result: The site devices are all loaded with the new software.