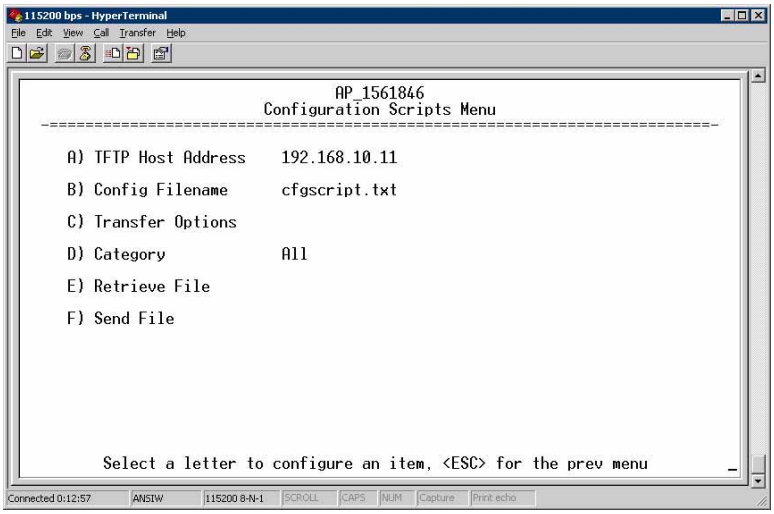

Figure 3-92. Configuration Scripts Menu

- **TFTP Host Address**—IP address of the computer on which the TFTP server resides. [**Any valid IP address**]
- **Config Filename**—Name of file containing this unit's configuration profile that will be transferred to the TFTP server. The configuration information is in plain-text ASCII format. [**Any 40-character alphanumeric string**] May require a sub-directory, for example: **config\mercury-config.txt**. (See *Configuration Scripts Menu* on Page 119 for more information.)

NOTE: The filename field is used to identify the desired incoming file and as the name of the file exported to the TFTP server. Before exporting a unit's configuration, name it in a way that reflects the radio's services or other identification.

- **Transfer Options**—A menu for configuring the TFTP transfer.
- **Category**—The category of parameters to send or receive.
- **Retrieve File**—Initiate the file transfer of the configuration file from TFTP server into the transceiver.
- **Send File**—Initiate the file transfer from the transceiver's current configuration file to TFTP server.

NOTE: See *Upgrade Procedure* on Page 117 for details on setting up the TFTP server.

Sample of Configuration Script File

A sample configuration script file is provided as part of every firmware release. Firmware images and sample files are available free-of-charge at: **www.GEmds.com/Resources/TechnicalSupport/.**

The name of the specific file includes the firmware revision number, represented by the "x" characters in the following example: **mercury-config-x_x_x.txt**.

Editing Configuration Files

Once a Remote unit□s operation is fine-tuned, use the *Configuration Scripts Menu* on Page 119 to save a copy of the configuration onto a PC. Once the file is saved on the PC, you can use it as a source to generate modified copies adjusted to match other devices. Modify the configuration files using a text editor or an automated process. (These applications are not provided by GE MDS).

We recommend that you review and update the following parameters for each individual unit. Change other parameters as necessary. Save each resulting file with a different name. We recommend using directories and file names that reflect the location of the unit to facilitate later identification.

Table 3-10. Common User-Alterable Parameters

Field	Comment	Range
IP Address	Unique for each individual radio.	Any legal IP address
IP Gateway	May change for different groups or locations.	Any legal IP address
Device Name	Should reflect a specific device. This information will appear in Management System headings.	Any 20-character alphanumeric string
Location	Used only as reference for network administration.	Any 40-character alphanumeric string

Editing Rules

- Only include parameters you want to change from the default value.
- Change only the parameter values.
- Capitalization counts in some field parameters.
- Comment Fields:
  a. Edit or delete anything on each line to the right of the comment delineator, the semicolon (;).
  b. Comments can be of any length, but must be on the same line as the parameter, or on a new line that begins with a semicolon character.
  c. Comments after parameters in files exported from a transceiver do not need to be present in your customized files.
- Some fields are read-only. These are designated by □(RO)□ in the configuration sample file.

Ping Utility Menu

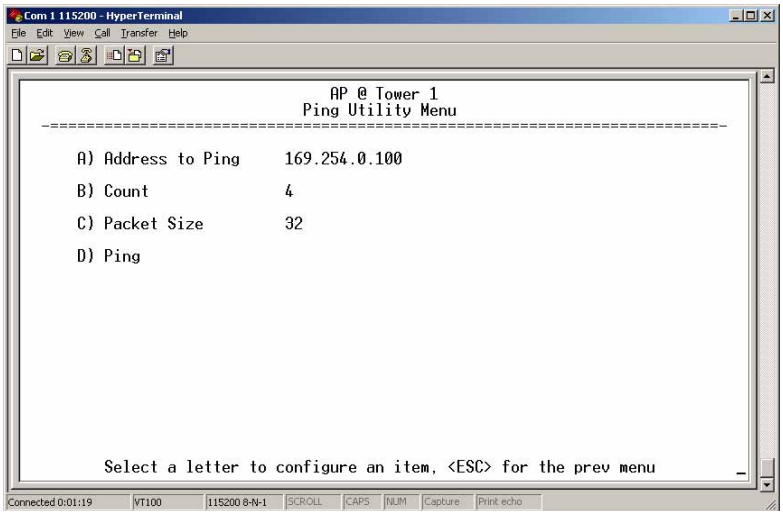

Figure 3-93. Ping Utility Menu

- **Address to Ping** – Address to send a Ping. [**Any valid IP address**]
- **Count** – Number of Ping packets to be sent.
- **Packet Size** – Size of each Ping data packet (bytes).
- **Ping** – Send Ping packets to address shown on screen.

  This screen is replaced with a detailed report of Ping activity (see example in Figure 3-94). Press any key after viewing the results to return to this menu.

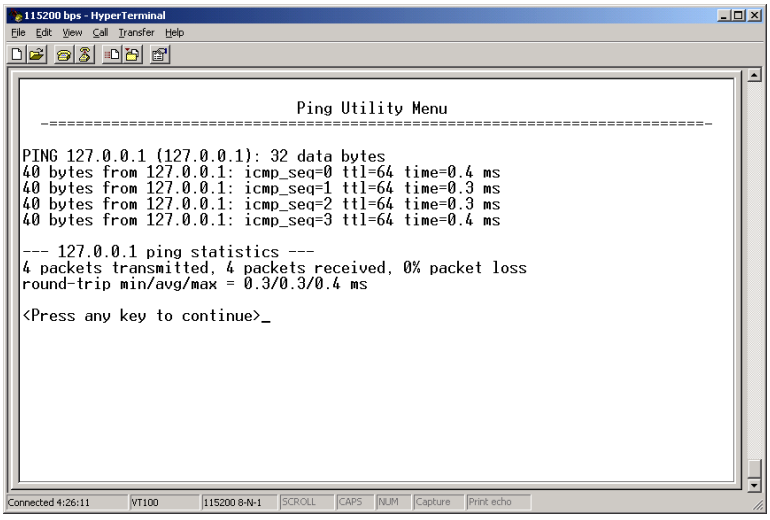

Figure 3-94. Ping Results Screen

Authorization Codes

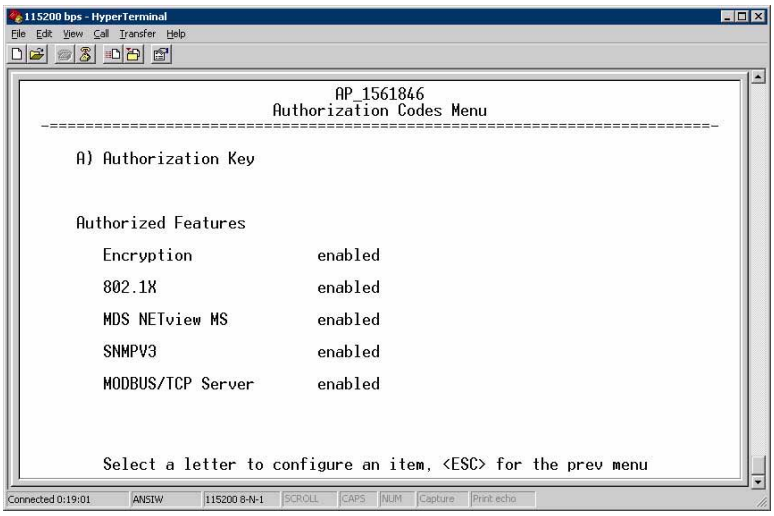

Figure 3-95. Authorization Codes Menu

- **Authorization Key**—For entering an Authorization Key into the transceiver's non-volatile memory.
- **Authorized Features**—List of the transceiver's authorized features. Each item shows **enabled** or **disabled** according to the settings allowed by the Authorization Key entered into the radio.

Reset to Factory Defaults

Use the **Reset to Factory Defaults** selection on the Maintenance/Tools Menu to return all configurable settings to those set at the factory prior to shipping. Use this selection with caution, as you will lose any custom settings you have established for your transceiver, and will need to re-enter them using the menu system.

To prevent accidental use of the command, a "challenge" question is presented at the bottom of the screen when this choice is selected (see Figure 3-96 on Page 124). To proceed, enter **y** for yes or **n** for no, and then press Enter. (You may also press the Escape key on your keyboard to exit this command without making any changes.)

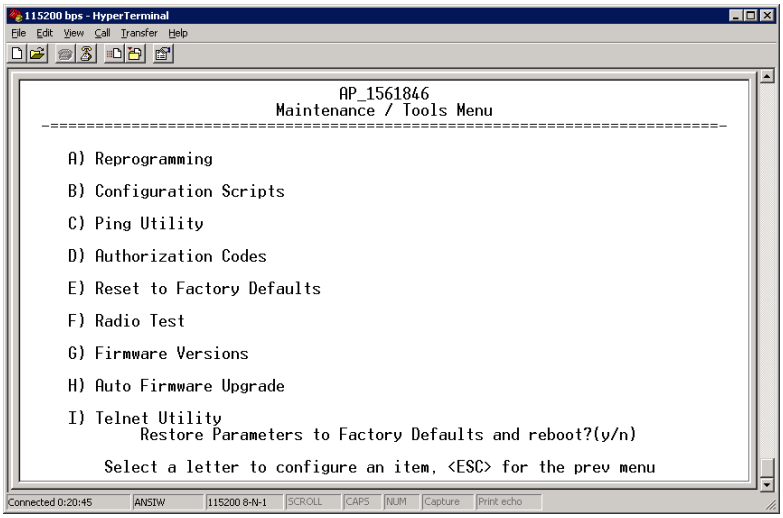

Figure 3-96. Reset to Factory Defaults Action
(Note challenge question at bottom of screen)

3.12.1Auto Firmware Upgrade Menu (AP Only)

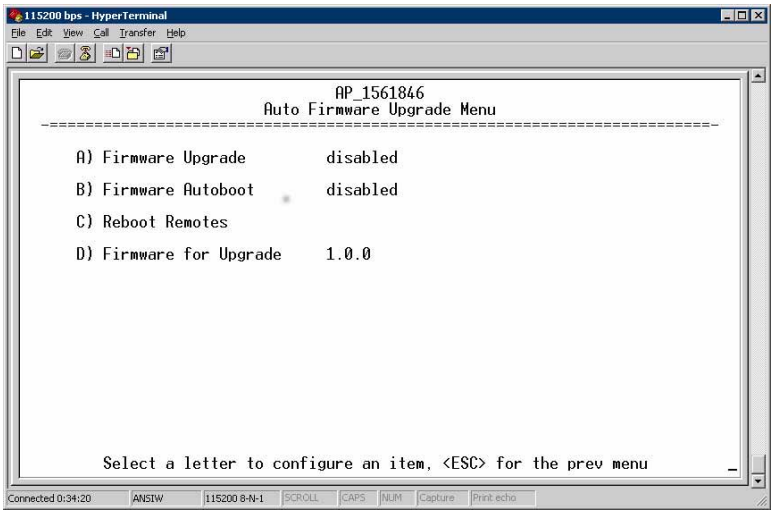

Figure 3-97.Auto Firmware Upgrade Menu

- **Firmware Upgrade** – Causes all of the Remotes associated to this AP to read the AP's specified (by **Firmware for Upgrade**) firmware version (active or inactive), and download it via TFTP to the inactive image if the Remote does not already have that firmware version.
- **Firmware Autoboot** – Boot connected remotes to **Firmware for Upgrade** (see below).
- **Reboot Remotes** – Determines how a Remote behaves once it has downloaded new firmware from the AP as part of an auto-upgrade. When enabled, the Remotes reboot to the new firmware.

NOTE: To use the Auto Upgrade/Reboot feature, both the AP and Remotes must already be running version 2.1.0 or newer firmware.

- **Firmware for Upgrade** – Specifies the firmware version that the Remotes should download, if they do not already have it.

Radio Test Menu

Using this menu, you can manually key the radio transmitter for performance checks and set several parameters that will be used when the Radio Mode is set to **Test**.

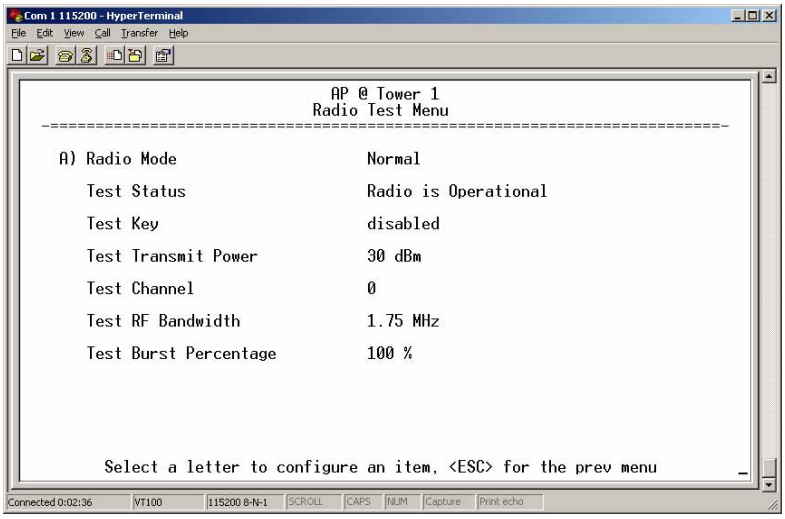

Figure 3-98. Radio Test Menu

NOTE : Using Test Mode disrupts traffic through the radio. If the unit is an Access Point, it will disrupt traffic through the *entire* network. The Test Mode function is automatically limited to 10 minutes. *Only use Test Mode for brief measurements*.

- **Radio Mode** – Sets/displays the radio's operating mode. To change the setting, press **A** on the PC's keyboard and press the Spacebar to toggle between the two settings. Press the Enter key to select the desired state. [**Normal, Test; Normal**]
- **Test Status** – This read-only parameter shows the current state of the radio.
  [**Radio is Operational, Reconfiguring the Radio, Ready to KEY**]

The following parameters are read-only unless **A) Radio Mode** is first selected and set to **Test**. In Test Mode, these items become selectable, and you can set their entries using the Spacebar or with a numeric entry, followed by pressing the Enter key.

- **Test Key** – Sets/displays keying status of the radio's transmitter. Use the Spacebar to view selections. [**disabled, enabled; disabled**]

- **Test Transmit Power** – Sets/displays the transmitter's power setting. Make a numerical entry within the allowable range. [**-30 to +30 dBm**]
- **Test Channel** – Sets/displays the radio's test channel number. Make a numerical entry within the allowable range. [**0-13; 0**]
- **Test RF Bandwidth** – Sets/displays the transmitter's bandwidth for testing. Use the Spacebar to view selections. [**1.75. 3.5 MHz; 1.75 MHz**]
- **Test Burst Percentage** – Sets/displays the percentage of Burst size to use for testing. Make a numerical entry within the allowable range. [**0-100%; 100**]

Spectrum Analyzer Menu (Remote Only)

Using this menu, you can enable or disable the remote's spectrum analyzer mode (Figure 3-99 on Page 126). When enabled, the remote displays through the terminal a spectrum analyzer view of its transmit power and frequency (Figure 3-100 on Page 127).

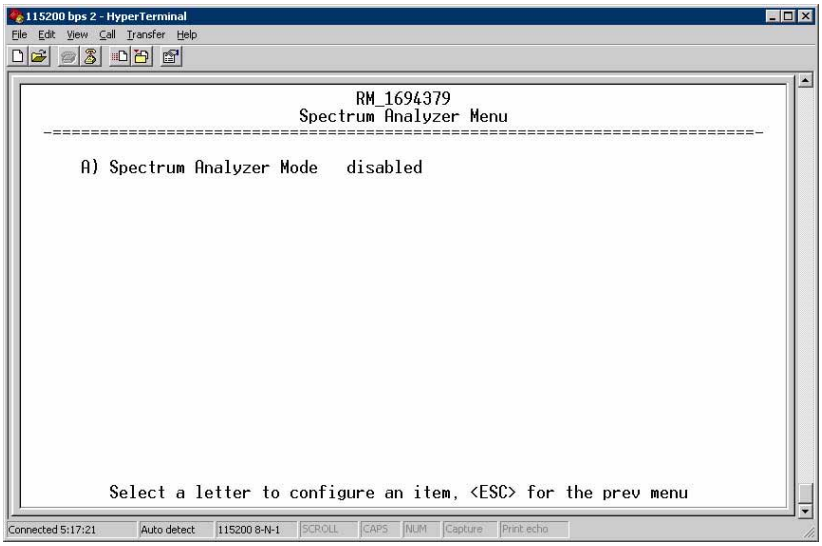

Figure 3-99. Spectrum Analyzer Menu

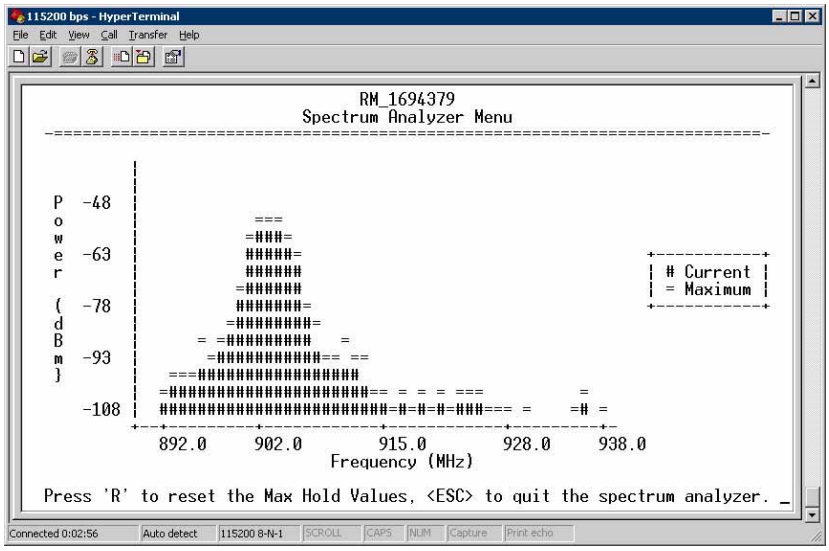

Figure 3-100. Spectrum Analyzer Display

3.13 PERFORMANCE OPTIMIZATION

After checking basic radio operation, you can optimize the network's performance. The effectiveness of these techniques varies with the design of your system and the format of the data being sent.

There are two major areas for possible improvement—the radio and the data network. These sections provide a variety of items to check in both categories, and in many cases, ways to improve performance.

NOTE: *As with any wireless system, the antennas are one of the most important portions of the system. A properly installed antenna with an unobstructed path to associated stations is the optimal configuration, and should be among the first items checked when searching for performance gains.*

Stronger signals allow the use of wider bandwidths and higher data speeds with fewer retries of data transmissions. Time spent optimizing the antenna systems on both AP and Remote stations will often pay huge dividends in system performance. Refer to INSTALLATION PLANNING on Page 149 for additional recommendations on antenna systems.

Table 3-11 on Page 128 provides suggested settings for typical installation scenarios. These settings provide a starting point for configuration of AP and Remote units. Changes might be required to achieve the desired results in a particular situation.

Table 3-11. Recommended Settings for Common Scenarios

For Fixed Locations, where best combination of range and throughput is desired.						
			AP	**Remote**	**Units**	**Notes**
Radio Configuration		**Network Name**	User discretion	User discretion		AP and Remote must match.
		Transmit Power (AP)/ Max Transmit Power (RM)	30	30	dBm	In most cases, power can be set to +30 dBm and left alone. Setting it lower helps control cell overlap.
		Receive Power	-70	N/A	dBm	Sets AP receiver for medium gain. Typical range: -60, -80 dBm.
	Frequency Control	**Frequency Mode**	Static Hopping	Static Hopping		
		Frame Duration	20	20	ms	Changing to 10 ms lowers latency. 5 and 8 ms selections not functional for this release.
		Hop Pattern	A, B, C, D	A, B, C, D		AP and RM must match.
		Hop Pattern Offset	0-13 or 0-6	0-13 or 0-6		AP and RM must match.
		Channel Selection	User discretion	User discretion		Disable channels with interference. AP and RM must match.
		TDD Sync Mode	GPS Required	N/A		GPS Antennas must be connected to both AP and RM.
	Advanced Configuration	**Adaptive Modulation**	Enabled	Enabled		
		Protection Margin	3	3	dB	
		Hysteresis Margin	3	3	dB	
		Data Compression	Enabled	Enabled		Gives best throughput numbers, but may hide true performance if only tested with PING or Text File FTP.
		Max Modulation	QAM/16-3-4	QAM16-3/4		Best combination of range and throughput.
		Cyclic Prefix	1/16	N/A		Best throughput setting.
		Channel Type	Static	N/A		Less periodic ranging when channel type is Static.
		ARQ	Enabled	N/A		
		ARQ Block Size	256	N/A	bytes	
		ARQ Block Lifetime	655	N/A	ms	These 3 settings make the max. no. of ARQ retries =9. (655 ms)/(35 ms + 35 ms = 9.35=>9
		ARQ TX Delay	35	N/A	ms	
		ARQ RX Delay	35	N/A	ms	
		Adaptive Split	Enabled	N/A		Maximizes one-way burst throughput.
		Downlink%	50	N/A	%	If Adaptive Split is disabled, can set downlink% to 15%—75%.

For Optimal Sensitivity (Trades off throughput for best possible sensitivity. AP more susceptible to interference)					
		AP	**Remote**	**Units**	**Notes**
Radio Configuration	**Receive Power**	-80	N/A	dBm	Sets AP receiver for highest gain.

When Heavy Interference Exists at AP (Trades off range for robustness in the face of interference)					
		AP	**Remote**	**Units**	**Notes**
Radio Configuration	**Receive Power**	-60	N/A	dBm	Sets AP receiver for low gain, which forces Remote transmit power to be high.

For Nomadic Systems (Where hand-offs between APs are required)						
			AP	**Remote**	**Units**	**Notes**
Radio Configuration	**Frequency Control**	**Frequency Mode**	Static Hopping	Hopping w/Hand-offs		
	Advanced Configuration	**Protection Margin**	6	6	dB	More channel variation, so use more robust modulation with greater SNRs.
		Channel Type	Static	N/A		Less periodic ranging when Channel Type = Static.
Network Configuration	**AP Location Info Config**	**Retrieve Text File**	N/A	AP Locations file		AP locations file with coordinates and key attributes of APs to which Remote can associate.

3.13.1Proper Operation□What to Look For

Table 3-12 and Table 3-13 on Page 130 show target performance values for AP and Remote transceivers. View these values using the built-in menu system by navigating the path shown under each table title.

Table 3-12. Mercury Remote Transceiver
(Performance Information>>Internal Radio Status Menu)

Name	Target Value	Notes
Connection Status	Associated	Remote must be associated for network operation.
Transmit Power	Varies	Adjusts automatically as requested by AP.
RSSI (Received Signal Strength Indication)	Varies	The less negative an RSSI reading, the stronger the signal (i.e., -75 dBm is stronger than -85 dBm).

Table 3-12. Mercury Remote Transceiver *(Continued)*
(Performance Information>>Internal Radio Status Menu)

Name	Target Value	Notes
SNR (Signal-to-Noise Ratio)	Strong signal (bench setting): 25-28 dB Operational: 3-30 dB Typ. System: 10-20 dB	A low SNR may be caused by noise or interfering signals.
TX Freq. Offset	0-22,875 Hz	Adjusts to accommodate what is expected by the AP.
RX Freq. Offset	0-22,875 Hz	Adjusts to accommodate what is expected by the AP.
Total FEC Count	Varies	
Corrected FEC Count	Varies	
Uncorrected FEC Count	Varies	
Current AP Name	Device name of associated AP	Typically set to reflect the application or system the radio is used in.

Table 3-13. Mercury Access Point
**(Performance Information>>Wireless Network Status>>
Remote Performance Database)**

Name	Target Value	Notes
MAC ADDR	MAC Address of associated Remote	Must match Remote□s MAC address exactly
RSSI (Received Signal Strength Indication)	Varies	The less negative an RSSI reading, the stronger the signal (i.e., -75 dBm is stronger than -85 dBm).
SNR Signal-to-Noise Ratio	Strong signal (bench): 25-28 dB Operational: 3-30 dB Typ. System:10-20 dB	A low SNR may be caused by noise or interfering signals.
Downlink	Varies	QPSK/FEC-3/4 Preferred
Uplink	Varies	QPSK/FEC-3/4 Preferred
FEC Total	Varies	
Corrected FEC Count	Varies	
Uncorrected FEC Count	Varies	

4 TROUBLESHOOTING & RADIO MEASUREMENTS

Contents

4.1 TROUBLESHOOTING

Successful troubleshooting of a wireless system is not difficult, but requires a logical approach. It is best to begin troubleshooting at the Access Point unit, as the rest of the system depends on the Access Point for synchronization data. If the Access Point has problems, the operation of the entire wireless network is affected.

When you find communication problems, it is good practice to begin by checking the simple causes. Applying basic troubleshooting techniques in a logical progression identifies many problems.

Multiple Communication Layers

It is important to remember that the operation of the network is built on a radio communications link. On top of that are two data levels wireless MAC, and the data layer. It is essential that the wireless aspect of the Access Point and the Remotes units to be associated operates properly before data-layer traffic will function.

Unit Configuration

There are numerous user-configurable parameters in the Management System. Do not overlook the possibility that human error is the cause of the problem. With so many parameters to view and change, a parameter might be incorrectly set, and then that change is forgotten.

To help avoid these problems, GE MDS recommends creating an archive of the transceiver s profile in a Configuration File when your installation is complete. You can reload this file into the transceiver to restore the unit to the factory defaults or your unique profile. For details on creating and archiving Configuration Files, see *Configuration Scripts Menu* on Page 119.

Factory Assistance

If problems cannot be resolved using the guidance provided here, review the GE MDS web site s technical support area for recent software/firmware updates, general troubleshooting help, and service information. Additional help is available through our Technical Support Department. (See TECHNICAL ASSISTANCE on the inside of the rear cover.)

4.1.1 Interpreting the Front Panel LEDs

An important set of troubleshooting tools are the LED status indicators on the front panel of the radio case. You should check them first whenever a problem is suspected. Table 2-2 on Page 26 describes the function of each status LED. Table 4-1 on Page 136 provides suggestions for

resolving common system difficulties using the LEDs, and Table 4-2 on Page 137 provides other simple techniques.

Table 4-1. Troubleshooting Using LEDs—Symptom-Based

Symptom	Problem/Recommended System Checks
PWR LED does not turn on	a. Voltage too low—Check for the proper supply voltage at the power connector. (10—30 Vdc) b. Indefinite Problem—Cycle the power and wait (≈ 30 seconds) for the unit to reboot. Then, recheck for normal operation.
LINK LED does not turn on	a. Network Name of Remote not identical to desired Access Point—Verify that the system has a unique Network Name. b. Not yet associated with an Access Point with the same Network Name. Check the "Status" of the unit's process of associating with the Access Point. Use the Management System. c. Poor Antenna System—Check the antenna, feedline and connectors. Reflected power should be less than 10% of the forward power reading (SWR 2:1 or lower).
PWR LED is blinking	a. Blinking indicates that an alarm condition exists. b. View Current Alarms and Event Log and correct the problem if possible. (See "*Using Logged Operation Events*" on Page 139) c. Blinking continues until the source of the alarm is corrected, for example, a valid IP address is entered, etc.
LAN LED does not turn on	a. Verify the Ethernet cable is connect at both ends. b. Verify that the appropriate type of Ethernet cable is used: straight-through or crossover.
LAN LED lights, but turns off after some time	Verify traffic in LAN. Typically, the radio should not be placed in high traffic enterprise LANs, as it will not pass this level of traffic. If needed, use routers to filter traffic.
GPS LED not lit	No satellite fix has been obtained. A fix is required for all operation except single-frequency channel (non-hopping) configurations. The lack of a fix may be caused by an obstructed "view" of the satellites, or a GPS antenna problem. The GPS LED blinks slowly on the AP while it synchronizes its internal clock to the GPS signal. When in this condition, the AP does not transmit.

4.1.2 Troubleshooting Using the Embedded Management System

If you have reviewed and tried the items listed in Table 4-1 and still have not resolved the problem, there are additional tools and techniques you can use. The embedded Management System is a good source of information that you can use remotely to provide preliminary diagnostic information, or may even provide a path to correcting the problem. Refer to Table 4-2 on Page 137 for more information on using the Management System as a troubleshooting tool.

Table 4-2. Basic Troubleshooting Using the Management System

Symptom	Problem/Recommended System Checks
Cannot access the MS through COM1	a. Connect to unit via Telnet or Web browser. b. Disable the serial mode for COM1 (Serial Gateway Configuration>>Com1 Serial Data Port>>Status>>Disabled). Or, if you know the unit□s data configuration: a. Connect to COM 1 via a terminal set to VT100 and the port□s data baud rate. b. Type **+++**. c. Change the terminal□s baud rate to match the transceiver□s Console Baud Rate. d. Type **+++**.
Display on terminal/Telnet screen garbled	Verify the terminal/terminal emulator or Telnet application is set to VT100.
Password forgotten	a. Connect to the transceiver using a terminal through the COM1 Port. b. Obtain a password-resetting Authorization Key from your factory representative. c. At the login prompt, try the user name *authcode*, and enter the Authorization Key for the password.
Remote only gets to **Connecting**	a. Check Network Name, encryption, and Device Auth Mode settings. b. Verify that the correct MAC address is listed in the Approved Remotes List of the Security Configuration Menu.
Remote only gets to **Authenticating**	Check encryption settings and security mode settings.
Cannot pass IP data to WAN	a. Verify your IP settings. b. Use the PING command to test communication with the transceivers in the local radio system. c. If successful with local PING, attempt to PING an IP unit attached to a transceiver. d. If successful with the LAN PINGs, try connecting to a known good unit in the WAN.
Wireless Retries too high	Possible Radio Frequency Interference: a. If omnidirectional antennas are used, consider changing to directional antennas. This usually limits interference to and from other stations. b. Try disabling channels where persistent interference is known or suspected. c. The installation of a filter in the antenna feedline may be necessary. Consult the factory for further assistance. d. Try using an antenna with a downward tilt.

The following is a summary of how you can use several screens in the Management System as diagnostic tools. For information on how to

connect to the Management System, see *STEP 3 CONNECT PC TO THE TRANSCEIVER* on Page 23.

Starting Information Screen

(See Starting Information Screen on Page 40)

The Management System s home page provides some valuable bits of data. One of the most important is the **Device Status** field. This item tells you if the unit is operational.

If the **Device Status** field says **Associated**, then look in the network areas beginning with network data statistics. If it displays some other message, such as **Scanning**, **Connecting**, or **Alarmed**, you must determine why it is in this state.

The *Scanning* state indicates a Remote unit is looking for an Access Point beacon signal to lock onto. It should move to the *Connecting* state and finally to the *Associated* state within less than a minute. If this Remote unit is not providing reliable service, look at the *Event Logs* for signs of lost association with the Access Point, or low signal alarms. Table 4-3 provides a description of the Device Status messages.

Table 4-3. Device Status[1]

Scanning	The unit is looking for an Access Point beacon signal.
Ranging	Remote has detected AP and is synchronizing to it.
Connecting	The Remote has established a radio (RF) connection with the Access Point and is negotiating the network layer connectivity.
Authenticating[2]	The Remote is authenticating itself to the network to obtain cyber-security clearance in order to pass data.
Associated	This unit has successfully synchronized and is associated with an Access Point. This is the normal operating state.
Alarmed	The unit has detected one or more alarms that have not been cleared.

1. Device Status is available in the *Startup Information Screen* or the *Wireless Status Screen* at Remotes.
2. If Device Authentication is enabled.

If the Remote is in an *Alarmed* state, the unit might still be operational and associated. Look for the association state in the *Wireless Network Status* screen to determine if the unit is associated. If it is, look at the *Error Log* for possible clues.

If the unit is in an *Alarmed* state and is not associated with an Access Point, then there might be a problem with the wireless network layer. Call a radio technician to deal with wireless issues. Refer the technician to the *RADIO (RF) MEASUREMENTS* on Page 143 for information on antenna system checks.

Packet Statistics Menu

(See Packet Statistics Menu on Page 105)

This screen provides detailed information on data exchanges between the unit being viewed and the network through the wireless and the Ethernet (data) layers. These include:

Wireless Packet Statistics

- ¥ Packets received
- ¥ Packets sent
- ¥ Bytes received
- ¥ Bytes sent
- ¥ Packets dropped
- ¥ Receive errors
- ¥ Retries
- ¥ Retry errors

Ethernet Packet Statistics

- ¥ Packets received
- ¥ Packets sent
- ¥ Bytes received
- ¥ Bytes sent
- ¥ Lost carrier detected
- ¥ Packets dropped
- ¥ Receive errors
- ¥ Retries
- ¥ Retry errors

The most significant fields are the *Packets Dropped*, *Retries*, *Retry Errors*, *Receive Errors* and *Lost Carrier Detected*. If the data values are more than 10% of their sent and received counterparts, or the *Lost Carrier Detected* value is greater than a few dozen, there might be trouble with radio-frequency interference or a radio link of marginal strength.

If errors are excessive, check the aiming of the antenna system, and check for a satisfactory SWR. Refer to *RADIO (RF) MEASUREMENTS on Page 143* for information on antenna system checks.

Diagnostic Tools

(See MAINTENANCE/TOOLS MENU on Page 113)

The radio□s Maintenance menu contains two tools that are especially useful to network technicians□the *Radio Test Menu* and the *Ping Utility*. Use the Radio Test selection for testing RF operation. Use the Ping Utility to verify communications access to pieces of equipment connected to the radio network. This includes transceivers and user-supplied Ethernet devices.

4.1.3 Using Logged Operation Events

(See PERFORMANCE INFORMATION MENU on Page 101)

The transceiver□s microprocessor monitors many operational parameters and logs them as various classes of *events*. If the event is one that affects performance, it is an *alarm*. There are also normal or routine events such as those marking the rebooting of the system, implementation of parameter changes, and external access to the Management System. Informational events are stored in temporary (RAM) memory that is lost in the absence of primary power, and Alarms are stored in

permanent memory (Flash memory) until cleared by user request. Table 4-4 summarizes these classifications.

Table 4-4. Event Classifications

Level	Description/Impact	Storage
Alarms	Transceiver has detected one or more alarm conditions	Flash Memory
Informational	Normal operating activities	Flash Memory
Temporary Informational	Transient conditions or events	RAM
Minor	Does not affect unit operation	RAM
Major	Degraded unit performance but still capable of operation	RAM
Critical	Prevents the unit from operating	RAM

These events are stored in the transceiver's *Event Log* and can be a valuable aid in troubleshooting unit problems or detecting attempts at breaching network security.

4.1.4 Alarm Conditions

(See Event Log Menu on Page 104)

Most events, classified as "critical" will cause the PWR LED to blink, and will inhibit normal operation of the transceiver. The LED blinks until the corrective action is completed.

Table 4-5. Alarm Conditions (Alphabetical Order)

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_BRIDGE	Network Interface /Error	networkInterface(17)
EVENT_FREQ_CAL	Frequency Not Calibrated	frequencyCal(7)
EVENT_INIT_ERR	Initialization Error	initializationError(18)
EVENT_IPADDR*	IP Address Invalid	ipAddressNotSet(4)
EVENT_IPMASK*	IP Mask Invalid	ipNetmaskNotSet(5)
EVENT_LAN_PORT		lanPortStatus(78)
EVENT_MAC	MAC communication Failed	macCommunication(1)
EVENT_MACADDR	MAC Address Invalid	noMacAddress(6)
EVENT_NETNAME*	Netname Invalid	invalidNetname(12)
EVENT_POWER_CAL	Power Calibrated/Not Calibrated	powerCal(8)
EVENT_REMOTE	Remote Added/ Removed (AP Only)	eventRemote(66)
EVENT_RSSI*	RSSI Exceeds threshold	rssi(11)

Table 4-5. Alarm Conditions (Alphabetical Order) *(Continued)*

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_RSSI_CAL	RSSI Not Calibrated	rssiCal(9)
EVENT_SYSTEM_ERROR*	System Error Cleared; Please Reboot	systemError(16)
EVENT_TFTP_CONN	TFTP connectivity achieved	tftpConnection(73)
EVENT_TFTP_ERR	Attempted TFTP connection failed	tftpConnFailed(79)

* User can correct condition, clearing the alarm.

4.1.5 Correcting Alarm Conditions

(See Event Log Menu on Page 104)

Table 4-6 provides likely causes of events that inhibit the unit from operating, and possible corrective actions. The Event Description column appears on the **Event Log** screen.

Table 4-6. Correcting Alarm Conditions Alphabetical Order

Event Log Entry	Generating Condition	Clearing Condition or Action
Bridge Down	The Bridge fails to be initialized.	Contact factory Technical Services for assistance.
General System Error	Internal checks suggest unit is not functioning properly.	Reboot the transceiver.
Initialization Error	Unit fails to complete boot cycle.	Contact factory Technical Services for assistance.
Invalid IP Address	The IP address is either 0.0.0.0 or 127.0.0.1.	Program IP address to something other than 0.0.0.0 or 127.0.0.1.
Network Interface Error	Unit does not recognize the LAN interface.	Contact factory Technical Services for assistance.
RSSI Exceeds Threshold	The running-average RSSI level is weaker (more negative) than the user-defined value.	Check the aiming of the directional antenna at the Remote; raise the threshold level to a stronger (less-negative) value.

4.1.6 Logged Events

(See Event Log Menu on Page 104)

The following events allow the transceiver to continue operation and do not make the PWR LED blink. Each is reported through an SNMP trap. The left hand column, *Event Log Entry*, is what shows in the Event Log.

Table 4-7. Non-Critical Events Alphabetical Order

Event Log Entry	Severity	Description
Association Attempt Success/Failed	MAJOR	Self explanatory
Association Lost - Local IP Address Changed	MAJOR	Self explanatory
Association Lost - Local Network Name Changed	MAJOR	Self explanatory
Association Lost/Established	MAJOR	Self explanatory
Auth Demo Mode Expired -- Rebooted Radio/Enabled	MAJOR	Self explanatory
Auth Key Entered - Key Valid/Key Invalid	MAJOR	Self explanatory
Console Access Locked for 5 Min	MAJOR	Self explanatory
Console User Logged Out/Logged In	MAJOR	Self explanatory
Current AP No Longer Approved	MAJOR	May occur during the Scanning process at a Remote. Indicates that the received beacon came from an AP which is not in the Approved AP list. This might be caused by some Remotes hearing multiple AP's. This event is expected behavior.
Decryption Error/Decryption OK	MAJOR	A decryption error is logged when an encryption phrase mismatch has occurred. A mismatch is declared after five consecutive errors over a 40-second window. When the error has cleared, **DECRYPT OK** appears.
Ethernet Port Enabled/Disabled	INFORM	Self explanatory
Ranging Lost/Established	INFORM	Self explanatory
Connecting Lost/Established	INFORM	Self explanatory
HTTP Access Locked for 5 Min	MAJOR	Self explanatory
HTTP User Logged Out/Logged In	MAJOR	httpLogin(49)
Log Cleared	INFORM	Self explanatory
Reprogramming Complete	INFORM	Self explanatory
Reprogramming Failed	MAJOR	Self explanatory
Reprogramming Started	INFORM	Self explanatory
Scanning Started	INFORM	Self explanatory

Table 4-7. Non-Critical Events Alphabetical Order *(Continued)*

Event Log Entry	Severity	Description
SNR Within threshold/Below threshold	INFORM	Self explanatory
System Bootup (power on)	INFORM	Self explanatory
Telnet Access Locked for 5 Min	MAJOR	Self explanatory
Telnet User Logged Out/Logged In	MAJOR	Self explanatory
User Selected Reboot	MAJOR	Self explanatory

4.2 RADIO (RF) MEASUREMENTS

There are several measurements that should be performed during the initial installation. These measurements confirm proper operation of the unit and, if they are recorded, serve as a benchmark in troubleshooting should difficulties appear in the future. These measurements are:

- Transmitter Power Output
- Antenna System SWR (Standing-Wave Ratio)
- Antenna Direction Optimization

These procedures might interrupt traffic through an established network and should only be performed by a skilled radio-technician in cooperation with the Network Administrator.

4.2.1 Antenna System SWR and Transmitter Power Output

Introduction

A proper impedance match between the transceiver and the antenna system is important. It ensures the maximum signal transfer between the radio and antenna. You can check the impedance match indirectly by measuring the SWR (standing-wave ratio) of the antenna system. If the results are normal, record them for comparison during future routine preventive maintenance. Abnormal readings indicate possible trouble with the antenna or the transmission line, and should be corrected.

Check the SWR of the antenna system before putting the radio into regular service. For accurate readings, a wattmeter suited to the frequency of operation is required. One unit meeting this criteria is the Bird Model 43" directional wattmeter with the appropriate element installed.

The reflected power should be less than 10% of the forward power (≈2:1 SWR). Higher readings indicate problems with the antenna, feedline or coaxial connectors.

Record the current transmitter power output level, then set it to 30 dBm for the duration of the test to provide an adequate signal level for the directional wattmeter.

Procedure

1. Place a directional wattmeter between the TX antenna connector and the antenna system.

2. Place the transceiver into the Radio Test Mode using the menu sequence below:
   (Maintenance/Tools Menu>>Radio Test>>Radio Mode>>Test)

3. Set the transmit power to 30 dBm. (This setting does not affect the output level during normal operation—only during Test Mode.)
   (Maintenance/Tools Menu>>Radio Test >>Test Mode>>Test>>Test Transmit Power)

4. Key the transmitter.
   (Maintenance/Tools Menu>>Radio Test>>Test Mode>>Test>>Test Key>> enabled)

   Use the PC's spacebar to key and unkey the transmitter. (Enable/Disable)

NOTE: The Transmit Key has a 10-minute timer, after which it unkeys the radio. Manually unkey the transmitter by selecting **Test Key>>disabled** on the menu, or temporarily disconnecting the radio's DC power.

---

5. Measure the forward and reflected power into the antenna system and calculate the SWR and power output level. The output should agree with the programmed value set in the Radio Configuration Menu. **(Radio Configuration>>Transmit Power)**

6. Turn off Radio Test Mode.
   (Maintenance/Tools Menu>>Radio Test>>Test Key>>disabled)

End of procedure.

4.2.2 Antenna Aiming—For Directional Antennas

Introduction

The radio network integrity depends, in a large part, on stable radio signal levels at each end of a data link. In general, signal levels stronger than —80 dBm provide the basis for reliable communication that includes a 15 dB fade margin. As the distance between the Access Point and Remotes increases, the influence of terrain, foliage, and man-made obstructions become more influential, and the use of directional antennas at Remote locations becomes necessary. Directional antennas require fine-tuning of their bearing to optimize the received signal

strength. The transceiver has a built-in received signal strength indicator (RSSI) that can tell you when the antenna is in a position that provides the optimum received signal.

RSSI measurements and Wireless Packet Statistics are based on multiple samples over a period of several seconds. The average of these measurements is displayed by the Management System.

The measurement and antenna alignment process usually takes 10 or more minutes at each radio unit.

The path to the Management System menu item is shown in bold text below each step of the procedure.

Procedure

1. Verify the Remote transceiver is associated with an Access Point unit by observing the condition of the LINK LED (**LINK LED = On** or **Blinking**). This indicates that you have an adequate signal level for the measurements and it is safe to proceed.

2. Record the *Wireless Packets Dropped* and *Received Error* rates.
   (Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

   This information will be used later.

3. Clear the *Wireless Packets Statistics* history.

   (Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics>>Clear Wireless Stats)

4. Read the RSSI level at the Remote.
   (Main Menu>>Performance Information>>Internal Radio Status)

5. Optimize RSSI (less negative is better) by slowly adjusting the direction of the antenna.

   Watch the RSSI indication for several seconds after making each adjustment so that the RSSI accurately reflects any change in the link signal strength.

6. View the *Wireless Packets Dropped* and *Received Error* rates at the point of maximum RSSI level. They should be the same or lower than the previous reading.

   (Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

7. If the RSSI peak results in an increase in the *Wireless Packets Dropped* and *Received Error*, the antenna may be aimed at an undesired signal source. Try a different antenna orientation.

End of procedure.

5 PLANNING A RADIO NETWORK

Contents

5.1 INSTALLATION PLANNING

This section provides tips for selecting an appropriate site, choosing an antenna system, and reducing the chance of harmful interference.

5.1.1 General Requirements

There are three main requirements for installing a transceiver□ adequate and stable primary power, a good antenna system, and the correct interface between the transceiver and the data device. Figure 5-1 shows a typical Remote installation.

NOTE: The transceiver□s network port supports 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

To prevent excessive Ethernet traffic from degrading performance, place the transceiver in a segment, or behind routers.

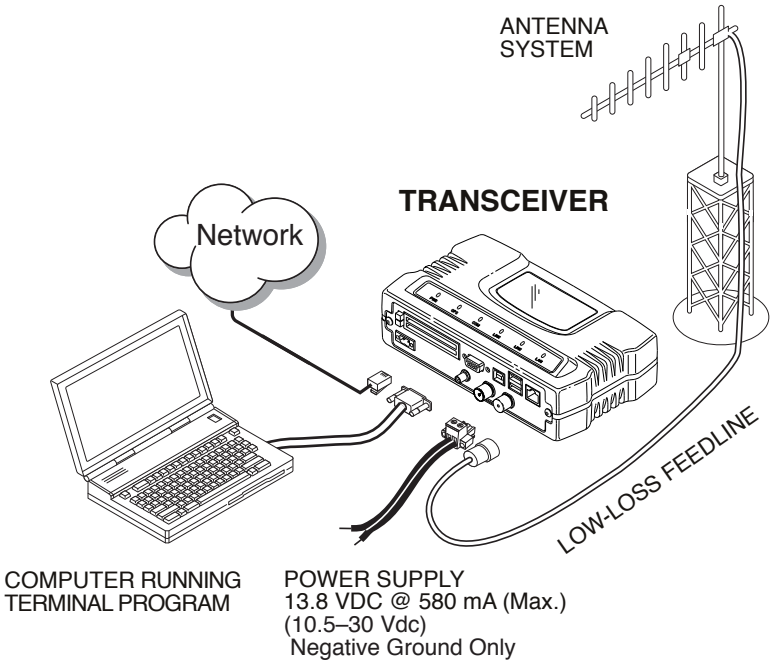

Figure 5-1. Typical Fixed Remote Installation With a Directional Antenna
(Connect user data equipment to any compatible LAN Port)

Unit Dimensions

Figure 5-2 on Page 150 shows the dimensions of the transceiver case and its mounting holes, and Figure 5-3 on Page 150 shows the dimensions for mounting with factory-supplied brackets. If possible, choose a

mounting location that provides easy access to the connectors on the end of the radio and an unobstructed view of the LED status indicators.

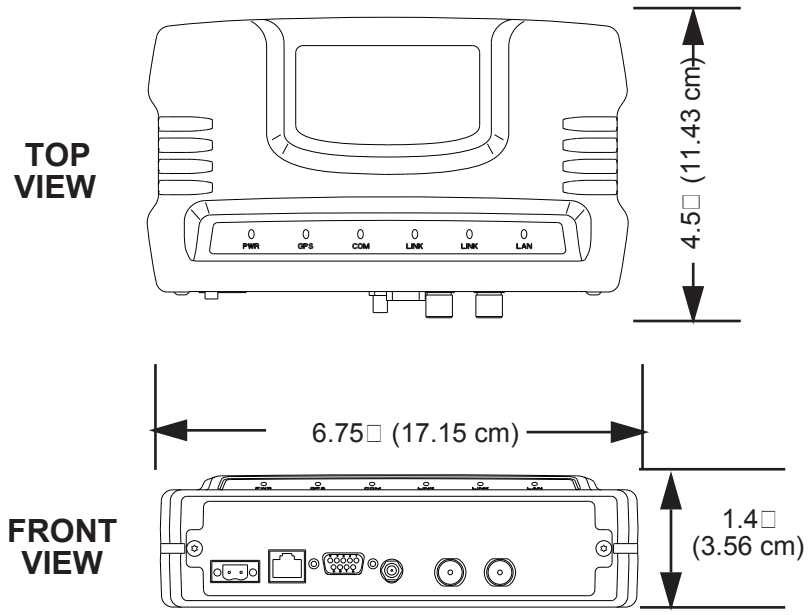

Figure 5-2. Transceiver Dimensions

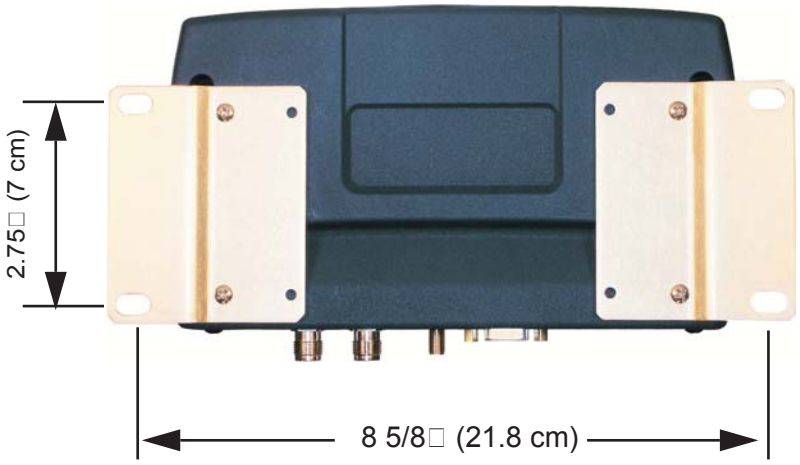

Figure 5-3. Mounting Bracket Dimensions (center to center)

NOTE: To prevent moisture from entering the radio, do not mount the radio with the cable connectors pointing up. Also, dress all cables to prevent moisture from running along the cables and into the radio.

5.1.2 Site Selection

Suitable sites should provide:

- Protection from direct weather exposure
- A source of adequate and stable primary power
- Suitable entrances for antenna, interface, or other required cabling
- An antenna location that provides a transmission path that is as unobstructed as possible in the direction of the associated station(s)

With the exception of the transmission path, you can quickly determine these requirements. Radio signals travel primarily by line-of-sight, and obstructions between the sending and receiving stations will affect system performance. If you are not familiar with the effects of terrain and other obstructions on radio transmission, the discussion below will provide helpful background.

5.1.3 Terrain and Signal Strength

While the license-free 3650 MHz band offers many advantages for data transmission services, signal propagation is attenuated by obstructions such as terrain, foliage, or buildings in the transmission path. A line-of-sight transmission path between the central transceiver and its associated remote site(s) is highly desirable and provides the most reliable communications link.

Much depends on the minimum signal strength that can be tolerated in a given system. Although the exact figure will differ from one system to another, a Received Signal Strength Indication (RSSI) of —80 dBm or stronger will provide acceptable performance in most systems. While the equipment will work at lower-strength signals, signals stronger than — 77 dBm provide a *fade margin* of 15 dB to account for variations in signal strength that might occur. You can measure RSSI with a terminal connected to the COM1 port, or with an HTTP browser connected to the LAN (Ethernet) connector. (See *Antenna Aiming For Directional Antennas* on Page 144 for details.)

5.1.4 Antenna & Feedline Selection

NOTE: The transceiver must be installed by trained professional installers, or factory trained technicians.

The following text will help the professional installer in the proper methods of maintaining compliance with FCC Part 15 limits and the +36 dBm or 4 watts peak E.I.R.P limit.

Antennas

The radio equipment can be installed with a number of antennas. The exact style used depends on the physical size and layout of a system. Contact your factory representative for specific recommendations on antenna types and hardware sources.

In general, an omnidirectional antenna (Figure 5-4) is used at the Access Points. This provides equal signal coverage in all directions.

NOTE: Antenna polarization is important. If the wrong polarization is used, a signal reduction of 20 dB or more will result. Most systems using a gain-type omnidirectional antenna at Access Point stations employ vertical polarization of the signal; therefore, the Remote antenna(s) must also be vertically polarized (elements oriented perpendicular to the horizon).

When required, horizontally polarized omnidirectional antennas are also available. Contact your factory representative for details.

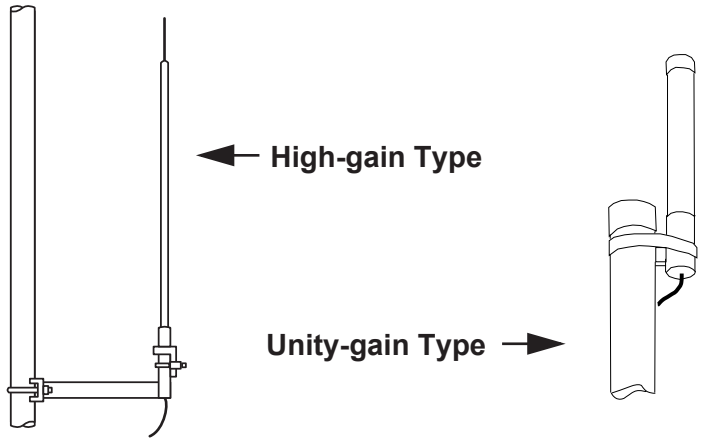

Figure 5-4. Typical Omnidirectional Antennas

At fixed Remote sites, a directional Yagi antenna (Figure 5-5 on Page 153) minimizes interference to and from other users. Antennas are available from a number of manufacturers.

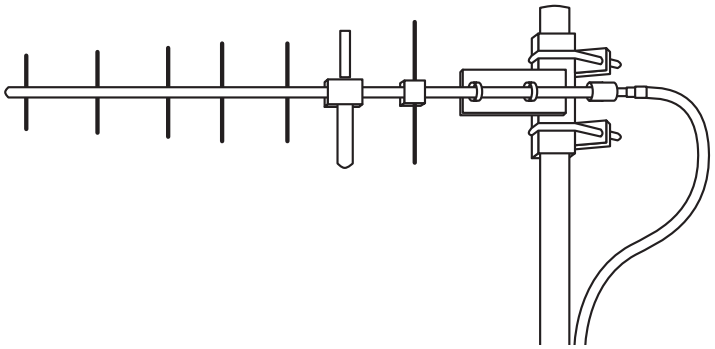

Figure 5-5. Typical Yagi Antenna (mounted to mast)

Diversity Reception (RX2) Antenna Port

Reserved for future functionality. Future releases of the product will allow you to connect a second antenna to the transceiver for space diversity reception.

GPS Antennas

A number of GPS antennas (both active and passive) are available for use with the transceivers. Consult your factory representative for more information.

Feedlines

Carefully consider the choice of feedline used with the antenna. Avoid poor-quality coaxial cables, as they degrade system performance for both transmission and reception. Keep the cable as short as possible to minimize signal loss.

For cable runs of less than 20 feet (6 meters), or for short range transmission, an inexpensive cable such as Type RG-214 might be acceptable. Otherwise, we recommend using a low-loss cable type suited for 3650 MHz, such as Heliax¤ .

Table 5-1 on Page 154 lists several types of popular feedlines and indicates the signal losses (in dB) that result when using various lengths of

cable at 3650 MHz. The choice of cable depends on the required length, cost considerations, and the acceptable amount of signal loss.

Table 5-1. Length vs. Loss in Coaxial Cables at 3650 MHz

Cable Type	10 Feet (3.05 m)	50 Feet (15.24 m)	100 Feet (30.48 m)	500 Feet (152.4 m)
RG-214	.76 dB	3.8 dB	7.6 dB	Unacceptable Loss
LMR-400	0.39 dB	1.95 dB	3.90 dB	Unacceptable Loss
1/2 inch HELIAX	0.23 dB	1.15 dB	2.29 dB	11.45 dB
7/8 inch HELIAX	0.13 dB	0.64 dB	1.28 dB	6.40 dB
1-1/4 inch HELIAX	0.10 dB	0.48 dB	0.95 dB	4.75 dB
1-5/8 inch HELIAX	0.08 dB	0.40 dB	0.80 dB	4.00 dB

The tables below outline the minimum lengths of RG-214 coaxial cable that must be used with common GE MDS omnidirectional antennas in order to maintain compliance with FCC maximum limit of +36 dBi. If other coaxial cable is used, make the appropriate changes in loss figures.

NOTE: The authority to operate the transceiver in the USA may be void if antennas other than those approved by the FCC are used. Contact your factory representative for additional antenna information.

5.1.5 Conducting a Site Survey

If you are in doubt about the suitability of the radio sites in your system, it is best to evaluate them before a permanent installation is underway. You can do this with an on-the-air test (preferred method), or indirectly, using path-study software.

An on-the-air test is preferred because it allows you to see firsthand the factors involved at an installation site, and to directly observe the quality of system operation. Even if a computer path study was conducted earlier, perform this test to verify the predicted results.

Perform the test by first installing a radio and antenna at the proposed Access Point (AP) station site (one-per-system). Then visit the Remote site(s) with another transceiver (programmed as a remote) and a hand-held antenna. (A PC with a network adapter can be connected to each radio in the network to simulate data during this test, using the PING command.)

With the hand-held antenna positioned near the proposed mounting spot, a technician can check for synchronization with the Access Point station (shown by a lit LINK LED on the front panel), then measure the reported RSSI value. (See *Antenna Aiming For Directional Antennas* on Page 144 for details.) If you cannot obtain adequate signal

strength, it might be necessary to mount the station antennas higher, use higher gain antennas, select a different site, or install a repeater station. To prepare the equipment for an on-the-air test, follow the general installation procedures given in this guide and become familiar with the operating instructions found in the *CHAPTER-2 TABLETOP EVALUATION AND TEST SETUP* on Page 19.

5.1.6 A Word About Radio Interference

The transceiver shares the radio-frequency spectrum with other 3650 MHz services and other Part 15 (unlicensed) devices in the USA. Completely error-free communications might not be achievable in a given location, and some level of interference should be expected. However, the radio□s flexible design and hopping techniques should allow adequate performance as long as you carefully choose the station location, configuration of radio parameters, and software/protocol techniques.

In general, keep the following points in mind when setting up your communications network:

- ¥ Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.
- ¥ Use a directional antenna at remote sites whenever possible. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, minimizing interference to (and from) stations located outside the pattern.
- ¥ If interference is suspected from a nearby licensed system (such as a paging transmitter), it might be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in this band, you can achieve an additional 20 dB of attenuation to interference by using horizontal polarization. Another approach is to use a bandpass filter to attenuate all signals outside the 3650 MHz band.
- ¥ Multiple Access Point units can co-exist in proximity to each other with no interference. The APs should be configured to operate in TDD Sync Mode, where their transmissions are synchronized to GPS timing. See □*Protected Network Operation using Multiple Access Points*□on Page 14. For additional isolation, separate directional antennas with as much vertical or horizontal separation as is practical.
- ¥ The power output of all radios in a system should be set for the lowest level necessary for reliable communications. This lessens the chance of causing unnecessary interference to nearby systems.

If you are not familiar with these interference-control techniques, contact your factory representative for more information.

Configuring Mercury 3650 for Shared Spectrum Use (Contention-Based Protocol)

While the Mercury 3650 has been designed to reduce the effects of interferers outside of the RF channel, cases may arrive where interferers may cause undesired operation. In the case of WiMAX interferers, proper configuration of the radio may reduce these effects.

The radio employs a WiMAX contention protocol that effectively reduces the amount of interference the network may cause to other co-located WiMAX networks using the same channel. In addition, proper configuration of the radio will help to reduce the effects of other WiMAX hardware attempting to do the same.

Remote radios receive scheduling information from a central base station (AP). This scheduling information destined for a given remote includes when to transmit, the duration of transmission, and modulation selection. In the event the intended Remote unit is unable to receive or interpret this information from the AP, the Remote will persist in receive mode only.

The radio allows the installer to configure an Approved Access Point list that contains the MAC addresses of desired AP radios in the network. When an Access Point sends scheduling data to the Remote unit, the Remote compares the MAC Address of the AP to this approved MAC address list, and discards the scheduling information if it has originated from a □foreign□ network.

In order to maximize the performance of a shared network, the following configuration is recommended:

1. The Mercury 3650 network should be set to operate on the same channel frequency as the network the channel is shared with. Slight offsets in frequency between two collocated systems will cause on-channel interference that is not decodable by either system. Having both systems operate on the same frequency allows the radio to decode WiMAX scheduling information from the interfering AP.

2. Configure the approved AP list using the AP Locations file as specified in the *AP Location Push Config Menu* on Page 55. After the Remote unit has received scheduling information from the interfering network, it will compare the MAC address of this radio to its AP Locations File. When the MAC address does not match, the radio will ignore this information from the interfering AP and continue to wait for valid scheduling information from an AP in the desired network.

5.2 dBm-WATTS-VOLTS CONVERSION CHART

Table 5-4 is provided as a convenience for determining the equivalent voltage or wattage of an RF power expressed in dBm.

Table 5-2. dBm-Watts-Volts conversion for 50 ohm systems

dBm	V	Po
+53	100.0	200W
+50	70.7	100W
+49	64.0	80W
+48	58.0	64W
+47	50.0	50W
+46	44.5	40W
+45	40.0	32W
+44	32.5	25W
+43	32.0	20W
+42	28.0	16W
+41	26.2	12.5W
+40	22.5	10W
+39	20.0	8W
+38	18.0	6.4W
+37	16.0	5W
+36	14.1	4W
+35	12.5	3.2W
+34	11.5	2.5W
+33	10.0	2W
+32	9.0	1.6W
+31	8.0	1.25W
+30	7.10	1.0W
+29	6.40	800mW
+28	5.80	640mW
+27	5.00	500mW
+26	4.45	400mW
+25	4.00	320mW
+24	3.55	250mW
+23	3.20	200mW
+22	2.80	160mW
+21	2.52	125mW
+20	2.25	100mW
+19	2.00	80mW
+18	1.80	64mW
+17	1.60	50mW
+16	1.41	40mW
+15	1.25	32mW
+14	1.15	25mW
+13	1.00	20mW
+12	.90	16mW
+11	.80	12.5mW
+10	.71	10mW
+9	.64	8mW
+8	.58	6.4mW
+7	.500	5mW
+6	.445	4mW
+5	.400	3.2mW
+4	.355	2.5mW
+3	.320	2.0mW
+2	.280	1.6mW
+1	.252	1.25mW

dBm	V	Po
0	.225	1.0mW
-1	.200	.80mW
-2	.180	.64mW
-3	.160	.50mW
-4	.141	.40mW
-5	.125	.32mW
-6	.115	.25mW
-7	.100	.20mW
-8	.090	.16mW
-9	.080	.125mW
-10	.071	.10mW
-11	.064	
-12	.058	
-13	.050	
-14	.045	
-15	.040	
-16	.0355	

dBm	mV	Po
-17	31.5	
-18	28.5	
-19	25.1	
-20	22.5	.01mW
-21	20.0	
-22	17.9	
-23	15.9	
-24	14.1	
-25	12.8	
-26	11.5	
-27	10.0	
-28	8.9	
-29	8.0	
-30	7.1	.001mW
-31	6.25	
-32	5.8	
-33	5.0	
-34	4.5	
-35	4.0	
-36	3.5	
-37	3.2	
-38	2.85	
-39	2.5	
-40	2.25	.1 W
-41	2.0	
-42	1.8	
-43	1.6	
-44	1.4	
-45	1.25	
-46	1.18	
-47	1.00	
-48	0.90	

dBm	mV	Po
-49	0.80	
-50	0.71	.01 W
-51	0.64	
-52	0.57	
-53	0.50	
-54	0.45	
-55	0.40	
-56	0.351	
-57	0.32	
-58	0.286	
-59	0.251	
-60	0.225	.001 W
-61	0.200	
-62	0.180	
-63	0.160	
-64	0.141	

dBm	V	Po
-65	128	
-66	115	
-67	100	
-68	90	
-69	80	
-70	71	.1nW
-71	65	
-72	58	
-73	50	
-74	45	
-75	40	
-76	35	
-77	32	
-78	29	
-79	25	
-80	22.5	.01nW
-81	20.0	
-82	18.0	
-83	16.0	
-84	11.1	
-85	12.9	
-86	11.5	
-87	10.0	
-88	9.0	
-89	8.0	
-90	7.1	.001nW
-91	6.1	
-92	5.75	
-93	5.0	
-94	4.5	
-95	4.0	
-96	3.51	
-97	3.2	

dBm	V	Po
-98	2.9	
-99	2.51	
-100	2.25	.1pW
-101	2.0	
-102	1.8	
-103	1.6	
-104	1.41	
-105	1.27	
-106	1.18	

dBm	nV	Po
-107	1000	
-108	900	
-109	800	
-110	710	.01pW
-111	640	
-112	580	
-113	500	
-114	450	
-115	400	
-116	355	
-117	325	
-118	285	
-119	251	
-120	225	.001pW
-121	200	
-122	180	
-123	160	
-124	141	
-125	128	
-126	117	
-127	100	
-128	90	
-129	80	.1˜W
-130	71	
-131	61	
-132	58	
-133	50	
-134	45	
-135	40	
-136	35	
-137	33	
-138	29	
-139	25	
-140	23	.01˜W

6 TECHNICAL REFERENCE

Contents

6.1 DATA INTERFACE CONNECTORS

Two types of data interface connectors are provided on the front panel of the transceiver—an RJ-45 LAN port, and a DB-9 serial port (COM1), which uses the RS-232 (EIA-232) signaling standard.

CAUTION
RADIO FREQUENCY INTERFERENCE POTENTIAL

The transceiver meets U.S.A.'s FCC Part 15, Class A limits when used with shielded data cables.

6.1.1 LAN Port

Use the transceiver's LAN port to connect the radio to an Ethernet network. The transceiver provides a data link to an Internet Protocol-based (IP) network via the Access Point station. Each radio in the network must have a unique IP address for the network to function properly.

- To connect a PC directly to the radio's LAN port, an RJ-45 to RJ-45 cross-over cable is required.
- To connect the radio to a Ethernet hub or bridge, use a straight-through cable.

The connector uses the standard Ethernet RJ-45 cables and wiring. For custom-made cables, use the pinout information in Figure 6-1 and Table 6-1.

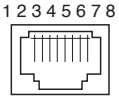

Figure 6-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

Table 6-1. LAN Port (IP/Ethernet)

Pin	Functions	Ref.
1	Transmit Data (TX)	High
2	Transmit Data (TX)	Low
3	Receive Data (RX)	High
4	Unused	
5	Unused	
6	Receive Data (RX)	Low
7	Unused	
8	Unused	

6.1.2 COM1 Port

The COM1 serial port is a DB-9 female connector. Connect a PC to the transceiver via this port with a DB-9M to DB-9F straight-through cable. These cables are available commercially, or may be constructed using the pinout information in Figure 6-2 and Table 6-2.

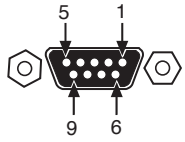

Figure 6-2. COM1 Port (DCE)
(Viewed from the outside of the unit.)

Table 6-2. COM1 Port Pinout, DB-9F/RS-232 Interface

Pin	Functions	DCE
1	Unused	
2	Receive Data (RXD)	< [Out
3	Transmit Data (TXD)	> [In
4	Unused	
5	Signal Ground (GND)	
6—9	Unused	

6.2 SPECIFICATIONS

General

- Raw Bit Rate: from 600 kbps to 12.7 Mbps (see chart below)
- Frequency Band: 902-928 MHz ISM band
- Orthogonal Frequency Division Multiplexing (OFDM)
  - 200 Carriers per Channel
- Available Configurations:
  - Access Point: Ethernet, Serial, GPS
  - Remote: Ethernet, Serial, GPS

Radio

- System Gain: 140 dB for 1.75 MHz channel, 137 dB for 3.5 MHz channel
- Carrier Power AP: -30 to +30 dBm, RM: 0 to +30 dBm (1 watt max.)
- RF Output Impedance: 50 Ohms

¥ Sensitivity and Data Rate (see chart below):

Modulation (CP=1/16)	3.5 MHz Channel			1.75 MHz Channel		
	Sensitivity	Signaling Rate	Max. User Throughput (Aggregate)*	Sensitivity	Signaling Rate	Max. User Throughput (Aggregate)*
64 QAM 3/4 FEC	-77 dBm	12.7 Mbps	7.2 Mbps	-80 dBm	6.35 Mbps	3.6 Mbps
16 QAM 3/4 FEC	-86 dBm	8.4 Mbps	4.8 Mbps	-89.5 dBm	4.2 Mbps	2.4 Mbps
QPSK 3/4 FEC	-92 dBm	4.2 Mbps	2.4 Mbps	-95 dBm	2.1 Mbps	1.2 Mbps
BPSK 1/2 FEC	-95 dBm	1.4 Mbps	500 Kbps	-98 dBm	706 Kbps	250 Kbps

* The transceiver is a half-duplex radio, so maximum user throughput is based on a configured or dynamic duty cycle, which is typically 50/50 indicating that half of the maximum throughput would be available one way. The maximum user throughput is also based on high protocol overhead from TCP/IP applications. For UDP applications, these throughput numbers will increase.

Physical Interface

¥ Ethernet: 10/100BaseT, RJ-45
¥ Serial: 1,200 — 115,200 bps
  ¥ COM1: RS-232, DB-9F
¥ Antennas: TX/RX—TNC connector, GPS□SMA connector
¥ LED Indicators: PWR, COM1, LINK, LAN

Protocols (Pending□contact factory for details)

¥ Ethernet: IEEE 802.3, Spanning Tree (Bridging), VLAN, IGMP
¥ TCP/IP: DHCP, ICMP, UDP, TCP, ARP, Multicast, SNTP, TFTP
¥ Serial: Encapsulation over IP (tunneling) for serial async multi-drop protocols including MODBUS“, DNP.3, DF1, BSAP

GE MDS Cyber Security Suite, Level 1

¥ Encryption: AES-128.
¥ Authentication: 802.1x, RADIUS, EAP/TLS, PKI, PAP, CHAP
¥ Management: SSL, SSH, HTTPS

Management

¥ HTTP, HTTPS, TELNET, SSH, local console
¥ SNMPv1/v2/v3, MIB-II, Enterprise MIB
¥ SYSLOG
¥ MDS NETview MS“ compatible

Environmental

¥ Temperature: -40¡C to +70¡C (-40¡F to +158¡F)
¥ Humidity: 95% at 40¡C (104¡F) non-condensing

Electrical

- Input Power: 10-30 Vdc
- Current Consumption (nominal):

Mode	Power	13.8 Vdc	24 Vdc
AP Transmit	25 W	1.8 A	1.0 A
AP Receive	8 W	579 mA	333 mA
RM Transmit	25W	1.8 mA	1.0 A
RM Receive	6.5W	471 mA	270 mA

Mechanical

- Case: Die Cast Aluminum
- Dimensions: 5.715 H x 20 W x 12.382 D cm. (2.25 H x 7.875 W x 4.875 D in.)
- Weight: 1kg (2.2 lb.)
- Mounting options: Flat surface mount brackets, DIN rail, 19□ rack tray

External GPS PPS Option

Parameter	Minimum	Maximum
Pulse Voltage (logic low)	0 V	1 V
Pulse Voltage (logic high)	1.7 V	10 V
Source Impedance (ohms)	—	200 Ω
Duty Cycle (ton)	0.0001% (1μsec)	50% (0.5 sec)
Operating Frequency	0.99999999 Hz (-0.1 ppm error)	1.00000001 Hz (+0.1 ppm error)
Module Clamping Voltage	2.7 V	3.3 V
Module Imput Resistance	150 Ω (Vin >2.6 V)	10 kΩ (Vin < 2 V)
Input Hysteresis	7 mV	N/A

Agency Approvals

- FCC Part 15.247 (DTS)
- CSA Class 1 Div. 2, (CSA C22.2-213-M1987 & CSA C22.2-142-M1987) (UL1604 & UL916)
- IC RSS-210 □Issue 7□

NOTE: GE MDS products are manufactured under a quality system certified to ISO 9001. GE MDS reserves the right to make changes to specifications of products described in this manual at any time without notice and without obligation to notify any person of such changes.

6.3 NOTES ON SNMP

6.3.1 Overview

The firmware release described in this manual contains changes to the transceiver□s SNMP Agent, several new MIB variables, and new Agent configuration options. This guide reviews the changes and shows how to properly configure the Agent to take advantage of these new features.

SNMPv3 Support

The updated SNMP Agent now supports SNMP version 3 (SNMPv3). The SNMPv3 protocol introduces Authentication (MD5/SHA-1), Encryption (DES), the USM User Table, and View-Based Access (refer to RFC2574 for full details). The SNMP Agent has limited SNMPv3 support in the following areas:

- ¥ Only MD5 Authentication is supported (no SHA-1). SNMPv3 provides support for MD5 and SHA-1.
- ¥ Limited USM User Table Manipulation. The SNMP Agent starts with 5 default accounts. New accounts can be added (SNMPv3 adds new accounts by cloning existing ones), but they will be volatile (will not survive a power-cycle).

  New views cannot be configured on the SNMP Agent. Views are inherited for new accounts from the account that was cloned.

  The SNMP Agent uses one password pair (Authentication/Privacy) for all accounts. This means that when the passwords change for one user, they change for all users.

SNMPv3 Accounts

The following default accounts are available for the SNMP Agent:

enc_mdsadmin□Read/write account using Authentication and Encryption.

auth_mdsadmin□Read/write account using Authentication.

enc_mdsviewer□Read only account using Authentication and Encryption.

auth_mdsviewer□Read only account using Authentication.

def_mdsviewer□Read only account with no Authentication or Encryption.

Context Names

The following Context Names are used (refer to RFC2574 for full details):

Admin accounts: **context_a**/Viewer accounts: **context_v**.

All accounts share the same default passwords:

Authentication default password: **MDSAuthPwd**/Privacy default password: **MDSPrivPwd**.

Passwords can be changed either locally (via the console) or from an SNMP Manager, depending on how the Agent is configured. If passwords are configured and managed locally, they are non-volatile and will survive a power-cycle. If passwords are configured from an SNMP manager, they will be reset to whatever has been stored for local management on power-cycle.

This behavior was chosen based on RFC specifications. The SNMP Manager and Agent do not exchange passwords, but actually exchange *keys* based on passwords. If the Manager changes the Agent□s password, the Agent does not know the new password. The Agent only knows the new key. In this case, only the Manager knows the new password. This could cause problems if the Manager loses the password. If that happens, the Agent becomes unmanageable. Resetting the Agent□s passwords (and therefore keys) to what is stored in flash memory upon power-cycle prevents the serious problem of losing the Agent□s passwords.

If passwords are managed locally, they can be changed on the Agent (via the console). Any attempts to change the passwords for the Agent via an SNMP Manager will fail when the Agent is in this mode. Locally defined passwords will survive a power-cycle.

In either case, the SNMP Manager needs to know the initial passwords being used in order to talk to the Agent. If the Agent□s passwords are configured via the Manager, they can be changed from the Manager. If the passwords are managed locally, then the Manager must be re-configured with any password changes in order to continue talking to the Agent.

Password-Mode Management Changes

When the password management mode is changed, the active passwords used by the Agent may also change. Some common scenarios are discussed below:

Common Scenarios

¥ Passwords are currently being handled by the Manager. The assigned passwords are **Microwave** (Auth), and **Rochester** (Priv). Configuration is changed to manage the passwords locally. The passwords stored on the radio were Fairport (Auth), and Churchville (Priv) (if local passwords have *never* been used, then MDSAuthPwd and MDSPrivPwd are used). These passwords will now be used by the Agent to re-generate keys. The Manager must know these passwords to talk to the Agent.

- Passwords are currently managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The same passwords will continue to be used, but now the Manager can change them.
- Passwords are currently managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Passwords are changed to **Brighton** (Auth) and **Perinton** (Priv). The Agent will immediately generate new keys based on these passwords and start using them. The Manager will have to be re-configured to use these new passwords.
- Passwords are currently managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The Manager changes the passwords to **Brighton** (Auth) and **Perinton** (Priv). The radio is then rebooted. After a power-cycle, the radio will use the passwords stored in flash memory, which are **Fairport** (Auth) and **Churchville** (Priv). The Manager must be re-configured to use these new passwords.

Table 6-3. SNMP Traps *(Sorted by Code)*

SNMP Trap	Severity	Description
bootup(34)	CRITICAL	System Bootup
reboot(35)	MAJOR	User Selected Reboot
reprogStarted(36)	INFORM	Reprogramming Started
reprogCompleted(37)	INFORM	Reprogramming Completed
reprogFailed(38)	MAJOR	Reprogramming Failed
telnetLogin(39)	MAJOR	Telnet/SSH User login/logout
httpLogin(40)	MAJOR	HTTP User login/logout
logClear(41)	INFORM	Event Log Cleared
dhcpServer(42)	INFORM	DHCP server enabled/disabled
dhcpClient(43)	INFORM	DHCP client enabled/disabled
dhcpAddr(44)	MINOR	Obtained DHCP address
timeNotSet(45)	INFORM	Date/time not set
timeByUser(46)	INFORM	Date/time changed by user
timeFromServer(47)	INFORM	Date/time from server
consoleLogin(48)	MAJOR	Console user login/logout
httpLockdown(49)	MAJOR	HTTP Access locked down
parmChanged(50)	INFORM	Parameter changed
cfgscript(51)	INFORM	Configuration script generated/received
authKey(52)	MAJOR	Authorization key entered - valid/invalid
authDemo(53)	MAJOR	Demo authorization enabled/expired
maxDemos(54)	CRITICAL	Max demos reset/reached

Table 6-3. SNMP Traps *(Sorted by Code)* ***(Continued)***

SNMP Trap	Severity	Description
modemRestart(55)	MAJOR	Modem restarted
internalError(56)	MAJOR	Internal error
gpsRestarted(57)	MAJOR	GPS Restarted
remoteConnection(58)	INFORM	Remote associated/disassociated
imageCopyStarted(59)	INFORM	Firmware image copy started
imageCopyComplete(60)	INFORM	Firmware image copy complete
imageCopyFailed(61)	MAJOR	Firmware image copy failed
connectionStatus(64)	INFORM	Connection status change
connAbort(65)	MAJOR	Connection aborted
authenticating(66)	INFORM	Authenticating to Access Point
association(67)	MAJOR	Associated to Access Point established/lost
redundLackRem(72)	MAJOR	Lack of associated remotes exceeded threshold for P21 AP
redundRecvErr(73)	MAJOR	Packet receive errors exceeded threshold for P21 AP
redundForced(74)	MAJOR	P21 AP forced switchover
redundancySwitch(75)	MAJOR	P21 AP auto switchover
radioError(76)	CRITICAL	Radio error
procopen(77)	MAJOR	Proc filesystem access failed
procformat(78)	MAJOR	Unexpected proc filesystem format
csropen(79)	MAJOR	Failed to open CSR device
csrstatus(80)	MAJOR	CSR read failed
csrctrlsignal(81)	MAJOR	CSR write failed
bandwidthMismatch(83)	INFORM	Bandwidth of AP in Locations file does not match this unit
gpsSync(84)	INFORM	GPS synchronized/lost sync
gpsTddSync(85)	INFORM	TDD synchronized/lost sync
tftpClientConn(86)	INFORM	TFTP Connection to Client Opened/Closed
tftpClientError(87)	MAJOR	Error in TFTP Transfer to Client
autoUpgrade(88)	MAJOR	Auto Firmware Upgrade Retry Scheduled/Starting
autoReboot(89)	MAJOR	Auto Firmware Boot Failed/Starting
certVerify(90)	CRITICAL	X.509 certificates loaded/failed
certChainVerify(91)	CRITICAL	Certificate chain verified/invalid
paTemp(92)	MAJOR	PowerAmp temperature Normal/Too hot

7 GLOSSARY OF TERMS AND ABBREVIATIONS

If you are new to wireless IP/Ethernet systems, some of the terms used in this manual might be unfamiliar. The following glossary explains many of these terms and will prove helpful in understanding the operation of your radio network. Some of these terms do not appear in the manual, but are often encountered in the wireless industry, and are therefore provided for completeness.

Access Point (AP)—The transceiver in the network that provides synchronization information to one or more associated Remote units. See *Network Configuration Menu* on Page 43.

AGC—Automatic Gain Control

Antenna System Gain— A figure, normally expressed in dB, representing the power increase resulting from the use of a gain-type antenna. System losses (from the feedline and coaxial connectors, for example) are subtracted from this figure to calculate the total antenna system gain.

AP—See *Access Point*

Association—Condition in which the frequency hopping pattern of the Remote is synchronized with the Access Point station, and the Remote is ready to pass traffic.

Authorization Key—Alphanumeric string (code) that is used to enable additional capabilities in the transceiver.

Bit—The smallest unit of digital data, often represented by a one or a zero. Eight bits usually comprise a byte.

Bits-per-second—See *BPS*.

BPDU—Bridge Protocol Data Units

BPS—Bits-per-second (bps). A measure of the information transfer rate of digital data across a communication channel.

Byte—A string of digital data made up of eight data bits.

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

Cyclic Redundancy Check (CRC)—A technique used to verify data integrity. It is based on an algorithm which generates a value derived

from the number and order of bits in a data string. This value is compared with a locally-generated value and a match indicates that the message is unchanged, and therefore valid.

Data Circuit-terminating Equipment—See *DCE*.

Data Communications Equipment—See *DCE*.

Datagram—A data string consisting of an IP header and the IP message within.

Data Terminal Equipment—See *DTE*.

dBd—Decibels (dipole antenna).

dBi—Decibels referenced to an "ideal" isotropic radiator in free space. Frequently used to express antenna gain.

dBm—Decibels referenced to one milliwatt. An absolute unit used to measure signal power, as in transmitter power output, or received signal strength.

DCE—Data Circuit-terminating Equipment (or Data Communications Equipment). In data communications terminology, this is the "modem" side of a computer-to-modem connection. COM1 Port of the transceiver is set as DCE.

Decibel (dB)—A measure of the ratio between two signal levels. Frequently used to express the gain (or loss) of a system.

Delimiter—A flag that marks the beginning and end of a data packet.

Device Mode—The operating mode/role of a transceiver (Access Point or Remote) in a wireless network.

DHCP (Dynamic Host Configuration Protocol)—An Internet standard that allows a client (i.e. any computer or network device) to obtain an IP address from a server on the network. This allows network administrators to avoid the tedious process of manually configuring and managing IP addresses for a large number of users and devices. When a network device powers on, if it is configured to use DHCP, it will contact a DHCP server on the network and request an IP address.

The DHCP server will provide an address from a pool of addresses allocated by the network administrator. The network device may use this address on a "time lease" basis or indefinitely depending on the policy set by the network administrator. The DHCP server can restrict allocation of IP addresses based on security policies. An Access Point may be configured by the system administrator to act as a DHCP server if one is not available on the wired network.

Digital Signal Processing—See *DSP*.

DSP—Digital Signal Processing. DSP circuitry is responsible for the most critical real-time tasks; primarily modulation, demodulation, and servicing of the data port.

DTE—Data Terminal Equipment. A device that provides data in the form of digital signals at its output. Connects to the DCE device.

Encapsulation—Process in by which, a complete data packet, such as MODBUS“ frame or any other polled asynchronous protocol frame, is placed in the data portion of another protocol frame (in this case IP) to be transported over a network. Typically this action is done at the transmitting end, before being sent as an IP packet to a network. A similar reversed process is applied at the other end of the network extracting the data from the IP envelope, resulting in the original packet in the original protocol.

Endpoint—Data equipment connected to the Ethernet port of the radio.

Equalization—The process of reducing the effects of amplitude, frequency or phase distortion with compensating networks.

Fade Margin—The greatest tolerable reduction in average received signal strength that will be anticipated under most conditions. Provides an allowance for reduced signal strength due to multipath, slight antenna movement or changing atmospheric losses. A fade margin of 15 to 20 dB is usually sufficient in most systems.

Fragmentation—A technique used for breaking a large message down into smaller parts so it can be accommodated by a less capable media.

Frame—A segment of data that adheres to a specific data protocol and contains definite start and end points. It provides a method of synchronizing transmissions.

Frequency Hopping—The spread spectrum technique used by the transceiver, where two or more associated radios change their operating frequencies many times per second using a set pattern. Since the pattern appears to jump around, it is said to “hop” from one frequency to another.

GPS—Global Positioning System. A constellation of orbiting satellites used for navigation and timing data. Although 24 satellites are normally active, a number of spares are also available in case of malfunction. Originally designed for military applications by the U.S. Department of Defense, GPS was released for civilian use in the 1980s. GPS satellites operate in the vicinity of the “L” frequency band (1500 MHz).

Hardware Flow Control—A transceiver feature used to prevent data buffer overruns when handling high-speed data from the connected data

communications device. When the buffer approaches overflow, the radio drops the clear-to-send (CTS) line, that instructs the connected device to delay further transmission until CTS again returns to the high state.

Host Computer—The computer installed at the master station site, that controls the collection of data from one or more remote sites.

HTTP—Hypertext Transfer Protocol

ICMP—Internet Control Message Protocol

IGMP (Internet Gateway Management Protocol)—Ethernet level protocol used by routers and similar devices to manage the distribution of multicast addresses in a network.

IEEE—Institute of Electrical and Electronic Engineers

IEEE 802.1Q—A standard for Ethernet framing which adds a four-byte tag after the Ethernet header. The four-byte tag contains a VLAN ID and a IEEE 802.1P priority value.

IEEE 802.1X—A standard for performing authentication and port blocking. The 802.1X port/device denies access to the network until the client device has authenticated itself.

Image (File)—Data file that contains the operating system and other essential resources for the basic operation of the radio's CPU.

LAN—Local Area Network

Latency—The delay (usually expressed in milliseconds) between when data is applied at the transmit port at one radio, until it appears at the receive port at the other radio.

MAC—Media Access Controller

MD5—A highly secure data encoding scheme. MD5 is a one-way hash algorithm that takes any length of data and produces a 128 bit "fingerprint." This fingerprint is "non-reversible," it is computationally infeasible to determine the file based on the fingerprint. For more details review "RFC 1321" available on the Internet.

MIB—Management Information Base

Microcontroller Unit—See *MCU*.

Mode—*See Device Mode.*

MTBF—Mean-Time Between Failures

Multiple Address System (MAS)—See *Point-Multipoint System.*

NMEA National Marine Electronics Association**.** National body that established a protocol for interfacing GPS data between electronic equipment.

Network Name User-selectable alphanumeric string that is used to identify a group of radio units that form a communications network. The Access Point and all Remotes within a given system should have the same network address.

Network-Wide Diagnostics An advanced method of controlling and interrogating GE MDS radios in a radio network.

NTP Network Time Protocol

Packet The basic unit of data carried on a link layer. On an IP network, this refers to an entire IP datagram or a fragment thereof.

PING Packet INternet Groper. Diagnostic message generally used to test reachability of a network device, either over a wired or wireless network.

PKI Private Key Infrastructure. A set of policies and technologies needed to create, store, and distribute Public Key Certificates used to protect the security of network communications.

Point-to-Multipoint System A radio communications network or system designed with a central control station that exchanges data with a number of remote locations equipped with terminal equipment.

Poll A request for data issued from the host computer (or master PLC) to a remote device.

Portability A station is considered connected when it has successfully authenticated and associated with an access point. A station is considered authenticated when it has agreed with the access point on the type of encryption that will be used for data packets traveling between them. The process of association causes a station to be bound to an access point and allows it to receive and transmit packets to and from the access point. In order for a station to be associated it must first authenticate with the access point. The authentication and association processes occur automatically without user intervention.

Portability refers to the ability of a station to connect to an access point from multiple locations without the need to reconfigure the network settings. For example, a remote transceiver that is connected to an access point may be turned off, moved to new site, turned back on, and, assuming the right information is entered, can immediately reconnect to the access point without user intervention.

PLC—Programmable Logic Controller. A dedicated microprocessor configured for a specific application with discrete inputs and outputs. It can serve as a host or as an RTU.

PuTTY—A free implementation of Telnet and SSH for Win32 and Unix platforms. It is written and maintained primarily by Simon Tatham. Refer to **http://www.pobox.com/~anakin/** for more information.

RADIUS—Remote Authentication Dial In User Service. An authentication, authorization, and accounting protocol used to secure remote access to a device or network.

Remote—A transceiver in a network that communicates with an associated Access Point.

Remote Terminal Unit—See *RTU*.

RFI—Radio Frequency Interference

Roaming—A station's ability to automatically switch its wireless connection between various access points (APs) as the need arises. A station may roam from one AP to another because the signal strength or quality of the current AP has degraded below what another AP can provide. Roaming may also be employed in conjunction with Portability where the station has been moved beyond the range of the original AP to which it was connected. As the station comes in range of a new AP, it will switch its connection to the stronger signal. Roaming refers to a station's logical, not necessarily physical, move between access points within a specific network and IP subnet.

RSSI—Received Signal Strength Indicator

RTU—Remote Terminal Unit. A data collection device installed at a remote radio site.

SCADA—Supervisory Control And Data Acquisition. An overall term for the functions commonly provided through an MAS radio system.

SNMP—Simple Network Management Protocol

SNR—Signal-to-Noise Ratio. A measurement of the desired signal to ambient noise levels.This measurement provides a relative indication of signal quality. Because this is a relative number, higher signal-to-noise ratios indicate improved performance.

SNTP—Simple Network Time Protocol

SSL—Secure Socket Layer

SSH—Secure Shell

STP—Spanning Tree Protocol

Standing-Wave Ratio – See *SWR*.

SWR – Standing-Wave Ratio. A parameter related to the ratio between forward transmitter power and the reflected power from the antenna system. As a general guideline, reflected power should not exceed 10% of the forward power (≈ 2:1 SWR).

TCP – Transmission Control Protocol

TFTP – Trivial File Transfer Protocol

Trap Manager – Software that collects SNMP traps for display or logging of events.

UDP – User Datagram Protocol

UTP – Unshielded Twisted Pair

VLAN – Virtual Local Area Network. A network configuration employing IEEE 802.1Q tagging, which allows multiple groups of devices to share the same physical medium while on separate broadcast domains.

IN CASE OF DIFFICULTY...

GE MDS products are designed for long life and trouble-free operation. However, this equipment, as with all electronic equipment, may have an occasional component failure. The following information will assist you in the event that servicing becomes necessary.

TECHNICAL ASSISTANCE

Technical assistance for GE MDS products is available from our Technical Support Department during business hours (8:00 A.M.—5:30 P.M. Eastern Time). When calling, please give the complete model number of the radio, along with a description of the trouble/symptom(s) that you are experiencing. In many cases, problems can be resolved over the telephone, without the need for returning the unit to the factory. Please use one of the following means for product assistance:

Phone: 585 241-5510	E-Mail: TechSupport@GEmds.com
FAX: 585 242-8369	Web: www.GEmds.com

FACTORY SERVICE

Component level repair of this equipment is not recommended in the field. Many components are installed using surface mount technology, which requires specialized training and equipment for proper servicing. For this reason, the equipment should be returned to the factory for any PC board repairs. The factory is best equipped to diagnose, repair and align your radio to its proper operating specifications.

If return of the equipment is necessary, you must obtain a Service Request Order (SRO) number. This number helps expedite the repair so that the equipment can be repaired and returned to you as quickly as possible. Please be sure to include the SRO number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an SRO number.

SRO numbers are issued online at **www.GEmds.com/support/product/sro/**. Your number will be issued immediately after the required information is entered. Please be sure to have the model number(s), serial number(s), detailed reason for return, "ship to" address, "bill to" address, and contact name, phone number, and fax number available when requesting an SRO number. A purchase order number or pre-payment will be required for any units that are out of warranty, or for product conversion.

If you prefer, you may contact our Product Services department to obtain an SRO number:

Phone Number: 585-241-5540
Fax Number: 585-242-8400
E-mail Address: productservices@GEmds.com

The radio must be properly packed for return to the factory. The original shipping container and packaging materials should be used whenever possible. All factory returns should be addressed to:

GE MDS, LLC
Product Services Department
(SRO No. XXXX)
175 Science Parkway
Rochester, NY 14620 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements. To inquire about an in-process repair, you may contact our Product Services Group using the telephone, Fax, or E-mail information given above.

GE MDS, LLC
175 Science Parkway
Rochester, NY 14620
General Business: +1 585 242-9600
FAX: +1 585 242-9620
Web: www.GEmds.com