Microwave Data Systems Inc.

MDS Mercury 900™

Wireless IP/Ethernet Transceiver
Covering AP and Remote Units

MDS 05-4446A01, Rev. A
APRIL 2007

GE MDS
industrial wireless networks

TABLE OF CONTENTS

3 EMBEDDED MANAGEMENT SYSTEM................... 27

GE MDS

Copyright Notice

ISO 9001 Registration

Microwave Data Systems adheres to the internationally-accepted ISO 9001 quality system standard.

To our Customers

We appreciate your patronage. You are our business. We promise to serve and anticipate your needs. We will strive to give you solutions that are cost effective, innovative, reliable and of the highest quality possible. We promise to build a relationship that is forthright and ethical, one that builds confidence and trust.

Related Materials on the Internet   Data sheets, frequently asked questions, case studies, application notes, firmware upgrades and other updated information is available on the GE MDS Web site at www.GEmds.com.

About GE MDS

Over two decades ago, GE MDS began building radios for business-critical applications. Since then, we have installed thousands of radios in over 110 countries. To succeed, we overcame impassable terrain, brutal operating conditions and disparate, complex network configurations. We also became experts in wireless communication standards and system applications worldwide. The result of our efforts is that today, thousands of utilities around the world rely on GE MDS-based wireless networks to manage their most critical assets.

The majority of GE MDS radios deployed since 1985 are still installed and performing within our customers' wireless networks. That   s because we design and manufacture our products in-house, according to ISO 9001 which allows us to control and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, GE MDS is the wireless leader in industrial automation   including oil and gas production and transportation, water/wastewater treatment, supply and transportation, electric transmission and distribution and many other utility applications. GE MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for GE MDS and our customers as we look forward to further demonstrating our abilities in new and emerging markets.

As your wireless needs change you can continue to expect more from GE MDS. We'll always put the performance of your network above all. Visit us at www.microwavedata.com for more information.

OPERATIONAL & SAFETY NOTICES

RF Exposure

Professional installation required. The radio equipment described in this guide emits radio frequency energy. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard. Do not allow people to come closer than 23 cm (9 inches) to the antenna when the transmitter is operating in indoor or outdoor environments. More information on RF exposure is on the Internet at www.fcc.gov/oet/info/documents/bulletins.

CSA/us Notice (Remote Transceiver Only)

This product is approved for use in Class 1, Division 2, Groups A, B, C & D Hazardous Locations. Such locations are defined in Article 500 of the National Fire Protection Association (NFPA) publication *NFPA 70*, otherwise known as the National Electrical Code.

The transceiver has been recognized for use in these hazardous locations by the Canadian Standards Association (CSA) which also issues the US mark of approval (CSA/US). The CSA Certification is in accordance with CSA STD C22.2 No. 213-M1987.

CSA Conditions of Approval: The transceiver is not acceptable as a stand-alone unit for use in the hazardous locations described above. It must either be mounted within another piece of equipment which is certified for hazardous locations, or installed within guidelines, or conditions of approval, as set forth by the approving agencies. These conditions of approval are as follows:

The transceiver must be mounted within a separate enclosure which is suitable for the intended application.

The antenna feedline, DC power cable and interface cable must be routed through conduit in accordance with the National Electrical Code.

Installation, operation and maintenance of the transceiver should be in accordance with the transceiver's installation manual, and the National Electrical Code.

Tampering or replacement with non-factory components may adversely affect the safe use of the transceiver in hazardous locations, and may void the approval.

A power connector with screw-type retaining screws as supplied by GE MDS must be used.

⚠ WARNING

EXPLOSION HAZARD!

Do not disconnect equipment unless power has been switched off or the area is known to be non-hazardous.

Refer to Articles 500 through 502 of the National Electrical Code (NFPA 70) for further information on hazardous locations and approved Division 2 wiring methods.

FCC Part 15 Notices

The transceiver series complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This device is specifically designed to be used under Section 15.247 of the FCC Rules and Regulations. Any unauthorized modification or changes to this device without the express approval of Microwave Data Systems may void the user   s authority to operate this device. Furthermore, the Mercury Series is intended to be used only when installed in accordance with the instructions outlined in this manual. Failure to comply with these instructions may also void the user   s authority to operate this device.

Part 15 rules also require that the Effective Isotropic Radiated Power (EIRP) from a Mercury Series installation not exceed 36 dBm. Refer to *Antenna & Feedline Selection* on Page 111 for more information.

Industry Canada RSS Notices

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the Equivalent Isotropic Radiated Power (EIRP) is not more than that permitted for successful communication.

GE MDS

This device as been designed to operate with the antennas listed below, and having a maximum gain of 12 dB. Antennas not included in this list or having a gain greater than 12 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. Refer to Table 5-3 on Page 117 for a list of antennas acceptable for use with this transceiver.

Manual Revision and Accuracy

This manual was prepared to cover a specific version of firmware code. Accordingly, some screens and features may differ from the actual unit you are working with. While every reasonable effort has been made to ensure the accuracy of this publication, product improvements may also result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the GE MDS Web site at www.GEmds.com.

Environmental Information

The manufacture of this equipment has required the extraction and use of natural resources. Improper disposal may contaminate the environment and present a health risk due to hazardous substances contained within. To avoid dissemination of these substances into our environment, and to limit the demand on natural resources, we encourage you to use the appropriate recycling systems for disposal. These systems will reuse or recycle most of the materials found in this equipment in a sound way. Please contact GE MDS or your supplier for more information on the proper disposal of this equipment.

1 PRODUCT OVERVIEW AND APPLICATIONS

Contents

1.1   ABOUT THIS MANUAL

This *Reference Manual* is one of two publications provided for users of the Mercury 900™ transceiver system. It contains detailed product information, an overview of common applications, a screen-by-screen review of the menu system, technical specifications, suggested settings for various scenarios, and detailed troubleshooting information. This manual should be available to all personnel who are responsible for network design, setup, commissioning and troubleshooting.

1.1.1 Start-Up Guide

The Mercury 900 *Start-Up Guide* (Part No. 05-4558A01) is a companion publication to the Reference Manual. It is a much smaller book, with a specific purpose—to guide an Installer in the basic steps for getting a transceiver on the air and communicating with other units in a network. It eliminates non-essential information so that installers can focus on the immediate goal of getting their equipment up and running in the shortest time possible.

1.1.2 Online Access to Manuals

In addition to printed manuals, many users value the ability to access documents electronically. This can be especially useful when you need to access documentation while traveling, or want to share a document with another user in the field. Electronic documents also make it easy to search for a specific term or subject, especially in larger manuals.

User manuals for our equipment can be accessed anytime from our website at **www.GEmds.com**. Simply click the **Downloads** tab at the top of the home page and select **Product Manuals** from the drop-down list. A search window then appears to help you locate the manual you need.

Online manuals are provided as PDF files in the Adobe® Acrobat® standard. A reader for PDF files may be downloaded free of charge from **www.adobe.com**.

1.1.3 Conventions Used in This Manual

On-Screen Menu Items

On-screen menu items or command entries are presented in a distinctive typeface to set them apart from regular text (for example: **Network Name, IP Address, Password**). This typeface will be found most often in Chapter 3, where the menu system is discussed in detail. When variable settings or a range of options are available for a menu option, the items are presented inside brackets, with the default setting (if any) shown last, following a semicolon.

Here is an example: [**available settings or range; default setting**]

Menu Strings

To help show the path to a menu selection, navigation strings are used in several places in this manual. For example, suppose you wished to view or set the Network Name assigned to your system. This item is located in the Network Configuration Menu, so the navigation string in the text would appear as follows:

Main Menu>>Network Configuration>>Network Name

By following this order of menus, you will be able to quickly reach the desired menu.

1.2 PRODUCT DESCRIPTION

The GE MDS Mercury 900™ transceiver is an easy-to-install wireless solution offering extended range, secure operation, and at multi-megabit performance in a compact and rugged package. The transceiver is ideally suited for demanding applications in fixed or mobile environments, where reliability and range are paramount.

The transceivers are commonly used to convey text documents, graphics, email, video, voice over IP (VoIP), and a variety of other application data between mobile, fixed-point, and WAN/LAN-based entities.

Based on multi-carrier Orthogonal Frequency Division Multiplexing (OFDM), the transceiver features high speed/low latency, basic Quality of Service (QoS) for prioritizing traffic, Ethernet and serial encapsulation, and network roaming. It also provides enhanced security features including AES encryption and RADIUS authentication, making the Mercury system the best combination of security, range and speed of any industrial wireless solution on the market today.

Figure 1-1. The GE MDS Mercury 900™ Transceiver
(Remote unit shown, AP is similar in appearance)

Rugged Packaging The transceivers are housed in a compact and rugged die cast-aluminum case that need only be protected from direct exposure to the weather. This one enclosure contains all necessary components for radio opera-

tion and data communications. The only user-serviceable component inside the case is a fuse for the DC power input line.

Simple Installation   Mercury Transceivers are designed for rapid and trouble-free installation. For basic services, you simply connect the antennas (900 MHz and GPS, as required), connect your data equipment, apply primary power, set a few operating parameters, and you are done. No license is required for operation in the U.S.A., Canada, and many other countries. Check requirements for your region before placing the equipment in service.

Most installations employ an omni-directional antenna at the Access Point (AP) location and mobile stations. Fixed Remote stations often employ a directional antenna aimed at the AP. Regardless of the type used, antennas are a vital part of the system and must be chosen and installed correctly. Refer to *INSTALLATION PLANNING* on Page 111 for guidance on choosing suitable antennas and installation sites.

Secure Operation   Data network security is a vital issue in today's wireless world. The transceivers provide multiple tools to help you build a network that minimizes the risk of eavesdropping and unauthorized access. Some are inherent in the radio's operation, such as the use of 900 MHz spread-spectrum transmissions; others include data encryption, enabling/disabling remote access channels, and password protection.

Remember, security is not a one-step process that can simply be turned on and forgotten. It must be practiced and enforced at multiple levels, 24 hours-a-day and 7 days-a-week. See *"GE MDS CYBER SECURITY SUITE"* on Page 16 for more information about the transceiver's security tools.

Robust Radio Operation   The transceivers are designed for operation in the license-free 900 MHz Industrial, Scientific, and Medical (ISM) band. They can provide reliable communications over long distances, even in the presence of weak signals or interference.

Mobile range depends on many factors, including terrain, building density, antenna gain, and speed of travel. The unit is designed for successful application in a variety of mobile environments, and offers the best combination of range, speed and robustness available in an industrial wireless package today. By using multiple Access Points, a network can be created that provides consistent, reliable coverage over a large metropolitan area. See *"SPECIFICATIONS"* on Page 125 for more information on transmission range.

Flexible Services   Users with a mix of equipment having Ethernet and serial data interfaces can accommodate this equipment through the use of a Remote Dual Gateway. This flexibility allows the transceiver to provide services in data networks that are being migrated from legacy serial/EIA-232-based hardware to the faster and more easily interfaced Ethernet world.

Flexible Management

Configuration, commissioning, troubleshooting and other maintenance activities can be done locally or remotely. Four different modes of access are available: local RS-232 console terminal, local or remote IP access (via Telnet or SSH), web browser (HTTP, HTTPS), and SNMP (v1/v2/v3).

The text-based interfaces (RS-232 console, Telnet, and SSH) are implemented in the form of easy-to-follow menus, and the terminal server configuration includes a wizard to help you set up the units correctly.

Transceiver Features

The transceiver's design makes the installation and configuration easy, while allowing for future changes.

- Industrial-Grade Product—Extended temperature range for trouble-free operation in extreme environments
- Robust Radio Communications—Designed to operate over long distances in dense, high-interference environments
- Robust Network Security—Prevents common attack schemes and hardware from gaining access or control of network. Common attack events are logged and reported by alarms.
- High Speed—1.5 Mbps is over 100-times faster than 9.6 kbps radios.
- Plug-and-Play Connectivity—AP or Remote configuration requires minimal setup
- Built-in GPS Receiver—GPS technology is used for timing and location data. The only external equipment needed for this functionality is a GPS antenna (several types are available from GE MDS).

1.2.1 Model Offerings

The transceiver comes in two primary models—Access Point and Remote. Unique hardware is used for each of these models. Of the Remote radios, there are two sub-types available—**Standard Remote** and **Max Remote**, both of which support Ethernet and serial services. Table 1-1 summarizes the different interface abilities for each type of radio.

Table 1-1. Transceiver Models and Data Interface Services

Model	Sub-Type	Ethernet/LAN[1]	COM1[1]	USB
Access Point	N/A	Yes	Yes	No
Remote	Ethernet Bridge	Yes	Yes	No
	Max Remote	Yes	Yes	Yes

NOTES
1. COM1 provides access to the embedded Management System on all units.

Access Point or Remote?—Quick ID Tip

The outward appearance of AP and Remote radios is nearly identical, however, the hardware for each type is different and they are *not* inter-cahngeable. An quick way to identify them is to look at the gasket seal in the center of the radio case. **Remote units have yellow gaskets while APs have a black gasket.** In addition, a label on the top each radio identifies it as an AP or Remote unit.

1.2.2 MDS P23 Protected Network (Redundant) Configuration

For mission-critical applications, a Protected Network Station is also offered. This unit incorporates two transceivers, two power supplies, and a switchover logic board that automatically selects between Transceiver A and Transceiver B as the active radio. Figure 1-2 shows a view of the protected chassis. For system-level information on this product, see MDS publication 05-4161A01.
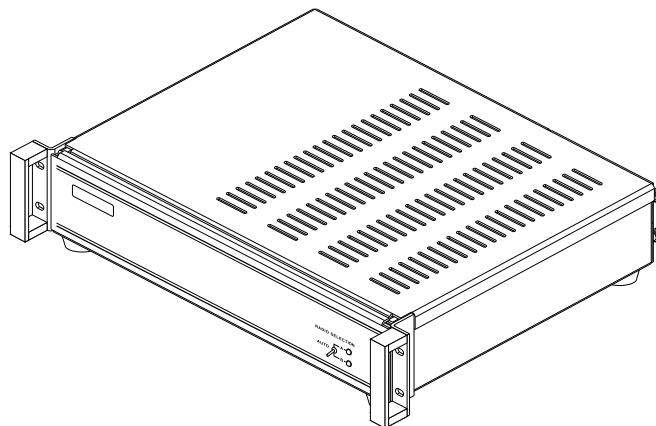
Figure 1-2. MDS P23 Protected Network Station
(incorporates two Transceivers, with Automatic Switchover)

1.3   APPLICATIONS

The following sections provide illustrations of typical transceiver installations. This is meant as an overview only. It is recommended that a network manager be involved in all installation planning activities.

1.3.1 Mobile/Fixed Data System

Mercury transceivers support high-speed data communications in a mobile environment. In this application, Remote radios "roam" between different Access Points, providing seamless transitions and continuous coverage throughout a municipal area. Figure 1-3 shows an example of an integrated system employing both mobile and fixed Mercury transceivers.
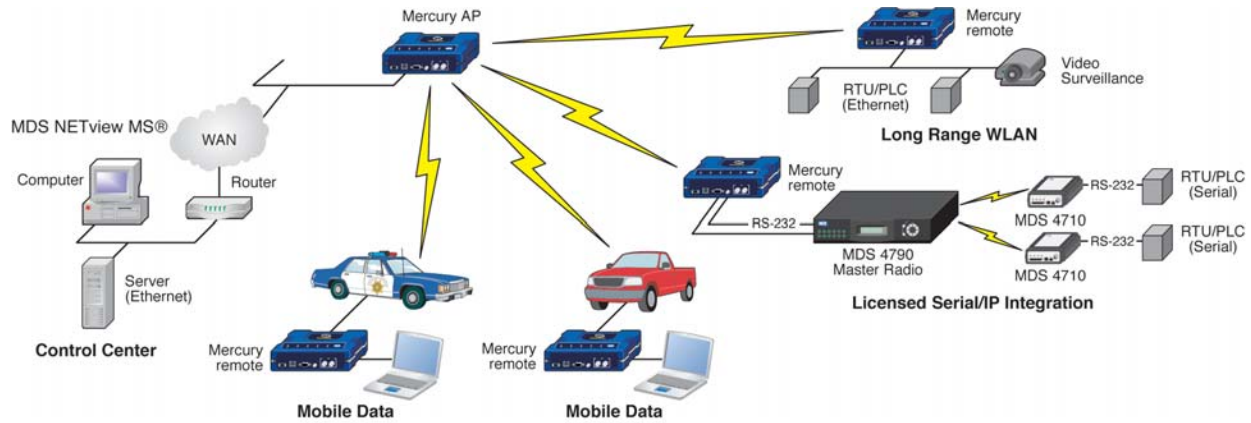
Figure 1-3. Integrated Mobile/Fixed Application

1.3.2 Wireless LAN

The wireless LAN is a common application of the transceiver. It consists of a central control station (Access Point) and one or more associated Remote units, as shown in Figure 1-4 on Page 8. A LAN provides communications between a central WAN/LAN and remote Ethernet segments. The operation of the radio system is transparent to the computer equipment connected to the transceiver.

The Access Point is positioned at a location from which it can communicate with all of the Remote units in the system. Commonly, this is a high location on top of a building or communications tower. Messages are exchanged at the Ethernet level. This includes all types of IP traffic.

A Remote transceiver can only talk over-the-air to an Access Point unit (AP). Peer-to-peer communications between Remotes can only take place indirectly via the AP. In the same fashion, an AP can only talk over-the-air to associated Remote units. Exception: Two APs can communicate with each other "off-the-air" through their Ethernet connectors using a common LAN/WAN.
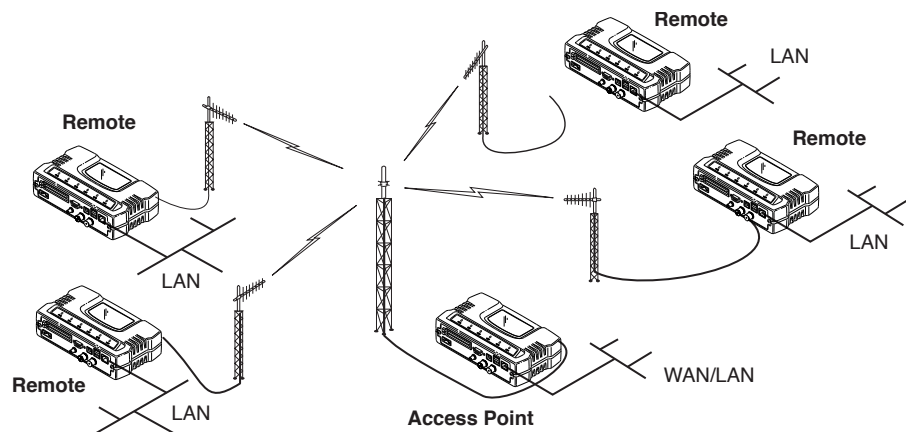
Figure 1-4. Typical Wireless LAN

1.3.3 Point-to-Point LAN Extension

A point-to-point configuration (Figure 1-5) is a simple arrangement consisting of an Access Point and a Remote unit. This provides a communications link for the transfer of data between two locations.
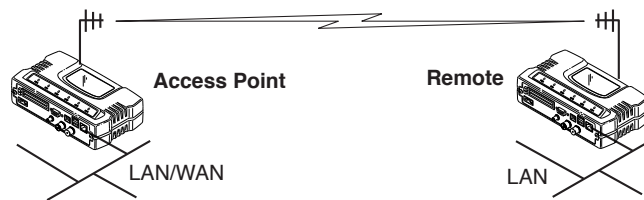
Figure 1-5. Typical Point-to-Point Link

1.3.4 Serial Radio Network Connectivity *(Future Functionality)*

An important design feature of the transceiver is to provide a path for serial devices to migrate to IP/Ethernet systems. Many radio networks in operation today still rely on serial networks at data rates of 9600 bps or less. These networks can use the transceiver as a means to continue using the serial service, while allowing the infrastructure to migrate to an IP format.

A Remote transceiver with its serial port connected to a GE MDS serial-based radio, such as MDS x790/x710, MDS TransNET and others, provides a path for bringing the data from the older radio into the IP/Ethernet environment of a Mercury-based system.
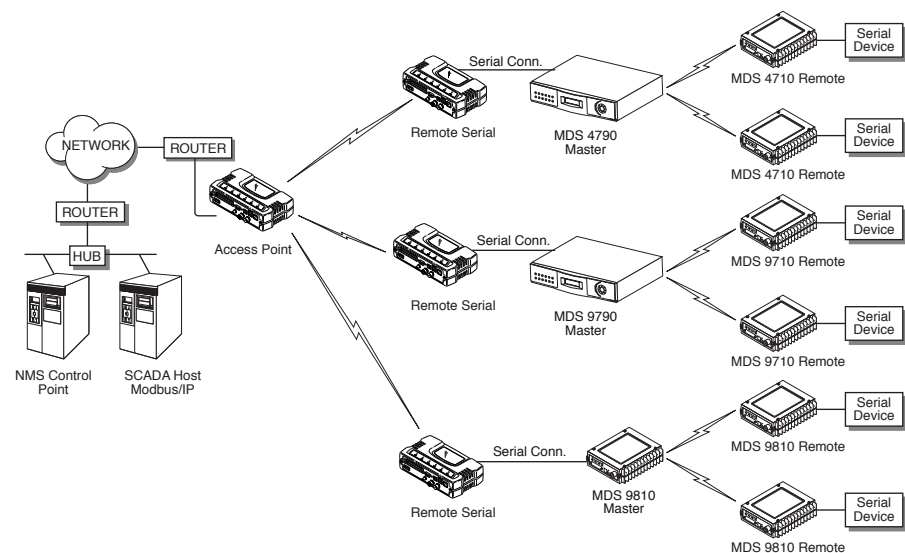
Figure 1-6. Backhaul Network

1.3.5 Multiple Protocols and/or Services *(Future Functionality)*

Prior to the introduction of Ethernet/IP-based radios, two radios were often used to service two different types of devices (typically connected to different SCADA hosts). A Mercury radio provides this functionality using a single remote unit. The unit's serial port can be connected via IP to different SCADA hosts, transporting different (or the same) protocols. Both data streams are completely independent and the transceiver provides seamless simultaneous operation as shown in Figure 1-7.
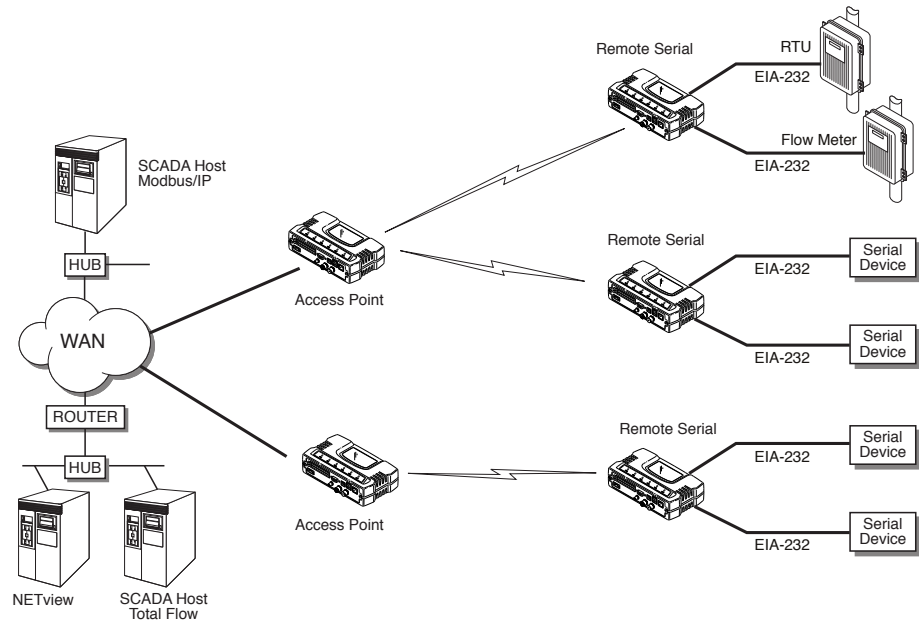
Figure 1-7. Multiple Protocol Network

By using a single radio, the cost of deployment is cut in half. Beyond requiring only one radio instead of two, the biggest cost reduction comes from using half of the required infrastructure at the remote site: one antenna, one feedline, one lightning protector and ancillary hardware. Other cost reductions come from the system as a whole, such as reduced management requirements. And above all, the potential for future applications that run over Ethernet and IP, such as video for remote surveillance.

1.3.6 Wireless LAN with Mixed Services

The transceiver is an excellent solution for a long-range industrial wireless LAN. It offers several advantages over commercial solutions — primarily improved performance over extended distances. The rugged construction of the radio and its extended temperature range make it an ideal solution even in harsh locations. In extreme environments, a simple NEMA enclosure is sufficient to house the unit.

The transceiver trades higher speed for longer range. Commercial 802.11a/b/g solutions are designed to provide service to relatively small areas such as offices, warehouses and homes. They provide high data rates but have limited range. The Mercury transmits at a higher power level, uses a different frequency band, has higher sensitivity, and a narrower channel to concentrate the radio energy and reach farther distances. It is designed for industrial operation from the ground up.

IP-based devices that may be used with the transceiver include a new breed of more powerful Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). These, as well as other devices, may be used in applications ranging from SCADA/telemetry monitoring, web-based video, security monitoring, and voice over IP. Figure 1-8 shows a typical wireless IP network.
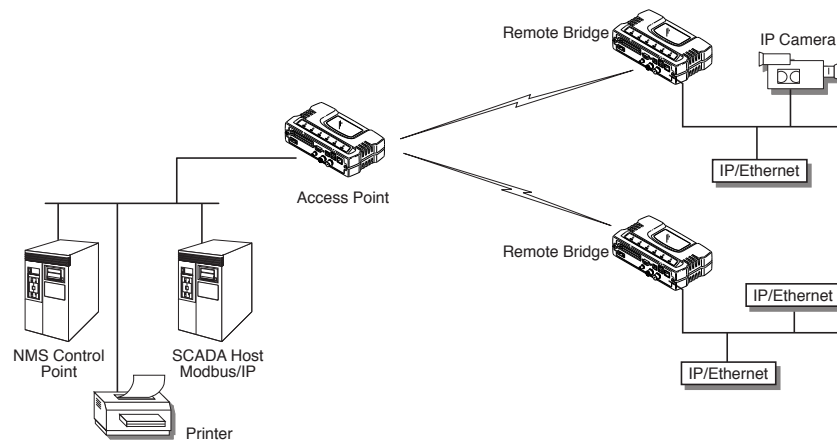
Figure 1-8. Extended-Range LAN with Mixed Applications

1.3.7 Upgrading Older Wireless Network with Serial Interfaces *(Future Functionality)*

Millions of wireless data products have been installed in the last two decades for licensed and license-free operation, many of them manufactured by GE MDS. There are several ways that these systems can benefit from incorporating Mercury equipment. The chief advantages are interface flexibility (serial and Ethernet in one unit), and higher data throughput. By taking advantage of its built-in serial and Ethernet interfaces, the transceiver is well suited to replace leased lines, dial-up lines, or existing 900 MHz "multiple address" data transceivers.

Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with Mercury transceivers. Legacy equipment can be connected to the transceiver through the COM1 port with a DB-25 to DB-9 cable wired for EIA-232 signaling. The COM1 port supports all standard EIA-232 signaling and acts as a data-terminal equipment device (DTE).

> **NOTE:** Several previous GE MDS-brand products had non-standard
> signal lines on their interface connectors (for example, to
> control sleep functions and alarm lines). These special func-
> tions are not provided nor supported by the transceiver.
> Consult equipment manuals for complete pinout information.

1.4 NETWORK DESIGN CONSIDERATIONS

1.4.1 Extending Network Coverage with Repeaters

What is a Repeater System?

A repeater works by re-transmitting data from outlying remote sites to
the Access Point and vice-versa. It introduces some additional
end-to-end transmission delay but provides longer-range connectivity.

In some geographical areas, obstacles can make communications diffi-
cult. These obstacles are commonly large buildings, hills, or dense
foliage. These obstacles can often be overcome with a repeater station.

Option 1—Using two transceivers to form a repeater station (back-to-back repeater)

Although the range between fixed transceivers can be up to 40 km (25
miles) over favorable terrain, it is possible to extend the range consider-
ably by connecting two units together at one site in a "back-to-back"
fashion to form a repeater, as shown in . This arrangement
should be used whenever the objective is to utilize the maximum range
between stations. In this case, using high-gain Yagi antennas at each
location will provide more reliable communications than their counter-
parts—omnidirectional antennas.
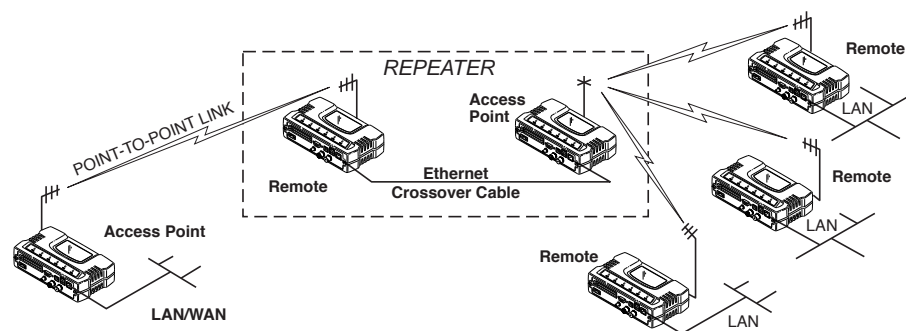
Figure 1-9. Typical LAN with a Repeater Link

Overview

Two transceivers may be connected "back-to-back" through the LAN
Ports to form a repeater station. (The cable must be a "cross-over"
Ethernet cable for this to work). This configuration is sometimes
required in a network that includes a distant Remote that would other-

wise be unable to communicate directly with the Access Point station due to distance or terrain.

The geographic location of a repeater station is especially important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This is often on top of a hill, building, or other elevated terrain from which both sites can be "seen" by the repeater station antennas. A detailed discussion on the effects of terrain is given in Section 5.1.2, *Site Selection* (beginning on Page 112).

The following paragraphs contain specific requirements for repeater systems.

Antennas   Two antennas are required at this type of repeater station—one for each radio. Measures must be taken to minimize the chance of interference between these antennas. One effective technique for limiting interference is to employ *vertical separation*. In this arrangement, assuming both are vertically polarized, one antenna is mounted *directly* over the other, separated by at least 10 feet (3 Meters). This takes advantage of the minimal radiation exhibited by most antennas directly above and below their driven elements.

Another interference reduction technique is to cross-polarize the repeater antennas. If one antenna is mounted for polarization in the vertical plane, and the other in the horizontal plane, an additional 20 dB of attenuation can be achieved. (Remember that the corresponding stations should use the same antenna orientation when cross-polarization is used.)

Network Name   The two radios that are wired together at the repeater site *must* have different network names. To set or view the network names, see *"STEP 3—CONNECT PC TO THE TRANSCEIVER"* on Page 25 for details.

Option 2—Using the AP as a Store-and-Forward Packet Repeater

A wireless network can be extended through the use of an alternate arrangement using the Access Point as a repeater to re-transmit the signals of all stations in the network. The repeater is a standard transceiver configured as an Access Point, and operating in Store and Forward mode. (See Figure 1-10.)
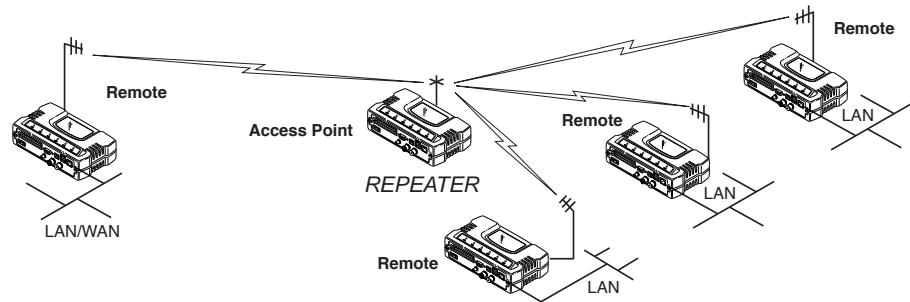
Figure 1-10. Typical Store-and-Forward Repeater Arrangement

As with the conventional repeater described in Option 1 above, the location of a store and forward repeater is also important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This can be on the top of a hill, building, or other elevated terrain from which all sites can be "seen" by the repeater station antenna. A detailed discussion on the effects of terrain is given in Section 5.1.2, *Site Selection* (beginning on Page 112)

1.4.2 Protected Network Operation using Multiple Access Points

Although GE MDS transceivers have a very robust design and have undergone intensive testing before being shipped, it is possible for isolated failures to occur. In mission-critical applications, down time can be virtually eliminated by using some, or all, of the following configurations:

In a point-to-multipoint scenario, the Access Point services multiple remotes. A problem in the Access Point will have an effect on all remotes, since none will have access to the network. When operation of the network does not tolerate any down time, it is possible to set up a protected configuration for the Access Point to greatly reduce the possibility of this occurrence.

Two or more Access Points can be configured with the same Network Name and kept active simultaneously, each with its own independent antenna. In this scenario, Remotes will associate with either one of the available Access Points. In case of a failure of one of the AP's the Remotes will quickly associate with another of the remaining Access Points re-establishing connectivity to the end devices.

The Access Points are unaware of the existence of the other AP's. Because the hopping algorithm uses *both* the Network Name *and* the Wireless MAC address of the AP to generate the hopping pattern, multiple AP's can coexist—even if they use the same network name. The collocated AP's will be using different hopping patterns and frequencies the great majority of the time. Although some data collisions will occur, the wireless-MAC is built to tolerate and recover from such occurrences with minimal degradation.

1.4.3 Collocating Multiple Radio Networks

Many networks can operate in relatively close physical proximity to one another provided reasonable measures are taken to assure the radio signal of one Access Point is not directed at the antenna of the second Access Point.

The Network Name and the association process

The Network Name is the foundation for building individual radio networks. It is part of a beacon signal broadcast by the Access Point (AP) to any Remote units with the same Network Name. Remotes that join the network are referred to as being "associated" with the Access Point unit.

Multiple APs with the same Network Name should be used with care. Using the same Network Name in multiple APs may result in Remotes associating with undesired APs and preventing data exchange from occurring as planned.

The use of a different Network Name does not guarantee an interference-free system. It does however, assure that only data destined for a unique network is passed through to that network.

Co-Location for Multiple Networks

It may be desirable to co-locate Access Points at one location to take advantage of an excellent or premium location that can serve two independent networks. Each network should have unique Network Name and each AP unit's antenna should be provided as much vertical separation as is practical to minimize RFI.

NOTE: All transceivers are shipped with the Network Name set to "Not Programmed." The Network Name must be programmed in order to pass data and begin normal operations.

Can radio frequency interference (RFI) disrupt my wireless network?

When multiple radio networks operate in close physical proximity to other wireless networks, individual units may not operate reliably under weak signal conditions and may be influenced by strong radio signals in adjacent bands. This radio frequency interference cannot be predicted with certainty, and can only be determined by experimentation. If you need to co-locate two units, start by using the largest possible vertical antenna separation between the two AP antennas on the same support structure. If that does not work, consult with your factory representative about other techniques for controlling radio frequency interference between the radios. (See *"A Word About Radio Interference"* on Page 117 for more details.)

1.5   GE MDS CYBER SECURITY SUITE

Today, the operation and management of an enterprise is becoming increasing dependent on electronic information flow. An accompanying concern becomes the cyber security of the communication infrastructure and the security of the data itself.

The transceiver is capable of dealing with many common security issues. Table 1-2 profiles security risks and how the transceiver provides a solution for minimizing vulnerability.

Table 1-2. Security Risk Management

Security Vulnerability	GE MDS Cyber Security Solution
Unauthorized access to the backbone network through a foreign remote radio	• 802.1x RADIUS authentication • Approved Remotes List (local) Only those remotes included in the AP list will associate
"Rogue" AP, where a foreign AP takes control of some or all remote radios and thus remote devices	• 802.1x RADIUS authentication • Approved AP List A remote will only associate to those AP included in its local authorized list of AP
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	• Failed-login lockdown After 3 tries, the transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.
Denial of service, where Remote radios could be reconfigured with bad parameters bringing the network down.	•Remote login with SSH or HTTPS •Local console login •Disabled HTTP & Telnet to allow only local management services
Airsnort and other war-driving hackers in parking lots, etc.	•900 MHz operation is not interoperable with standard 802.11b wireless cards •The transceiver cannot be put in a promiscuous mode •Proprietary data framing
Eavesdropping, intercepting messages	•AES-128 encryption
Key cracking software	• Automatic Rotating Key algorithm
Replaying messages	• Automatic Rotating Key algorithm

Table 1-2. Security Risk Management

Security Vulnerability	GE MDS Cyber Security Solution
Unprotected access to configuration via SNMPv1	• Implement SNMPv3 secure operation
Intrusion detection	• Provides early warning via SNMP through critical event reports (unauthorized, logging attempts, etc.)
	• Unauthorized AP MAC address detected at Remote
	• Unauthorized Remote MAC address detected at AP
	• Login attempt limit exceeded (Accessed via: Telnet, HTTP, or local)
	• Successful login/logout (Accessed via: Telnet, HTTP, or local)

1.6 ACCESSORIES

The transceiver can be used with one or more of the accessories listed in Table 1-3. Contact the factory for ordering details.

Table 1-3. Accessories

Accessory	Description	GE MDS Part No.
AC Power Adapter Kit	A small power supply module designed for continuous service. UL approved. Input: 120/220; Output: 13.8 Vdc @ 2.5 A	01-3682A02
Omni-Directional Antennas	Rugged antennas well suited for use at Access Point installations. Consult with your factory Sales Representative for details	--
Yagi Antenna (Directional)	Rugged antennas well suited for use at fixed Remote sites. Consult with your factory Sales Representative for details.	--
GPS Receiving Antennas	A variety of fixed and mobile GPS antennas (active and passive) are available. Consult with your factory Sales Representative for details.	--
TNC Male-to-N Female Adapter	One-piece RF adaptor plug.	97-1677A161
TNC Male-to-N Female Adapter Cable	Short length of coaxial cable used to connect the radio's TNC antenna connector to a Type N commonly used on large diameter coaxial cables.	97-1677A159 (3 ft./1m) 97-1677A160 (6 ft./1.8m)
Ethernet RJ-45 Crossover Cable (CAT5)	Cable assembly used to cross-connect the Ethernet ports of two transceivers used in a repeater configuration. (Cable length ≈ 3 ft./1M)	97-1870A21

Table 1-3. Accessories *(Continued)*

Accessory	Description	GE MDS Part No.
2-Pin Power Plug	Mates with power connector on transceiver. Screw terminals provided for wires, threaded locking screws to prevent accidental disconnect.	73-1194A39
Ethernet RJ-45 Straight-thru Cable (CAT5)	Cable assembly used to connect an Ethernet device to the transceiver. Both ends of the cable are wired identically. (Cable length ≈ 3 ft./1M)	97-1870A20
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-25 male connector on one end, and a DB-9 female on the other end. Two lengths available (see part numbers at right).	97-3035L06 (6 ft./1.8m) 97-3035L15 (15 ft./4.6m)
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-9 male connector on one end, and a DB-9 female on the other end, 6 ft./1.8m long.	97-1971A03
Fuse	Small, board-mounted fuse used to protect against over-current conditions.	29-1784A03
Flat-Surface Mounting Brackets & Screws	Brackets: 2˝ x 3˝ plates designed to be screwed onto the bottom of the unit for surface-mounting the radio.	82-1753-A01
	Screws: 6-32/1/4˝ with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
DIN Rail Mounting Bracket	Bracket used to mount the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4022A02
COM1 Interface Adapter	DB-25(F) to DB-9(M) shielded cable assembly (6 ft./1.8 m) for connection of equipment or other EIA-232 serial devices previously connected to "legacy" units. (Consult factory for other lengths and variations.)	97-3035A06
Bandpass Filter	Antenna system filter that helps eliminate interference from nearby paging transmitters.	20-2822A02
Ethernet Surge Suppressor	Surge suppressor for protection of Ethernet port against lightning.	29-4018A01

2 TABLETOP EVALUATION AND TEST SETUP

Contents

2.1 OVERVIEW

It is recommended that a "tabletop network" be set up to verify the basic operation of the transceivers. This allows experimenting with network designs, configurations or network equipment in a convenient location. This test can be performed with any number of radios.

When you are satisfied that the network is functioning properly in a benchtop setting, field installation can be performed. Complete information for field installation, including mounting dimensions and antenna selection, is provided in *INSTALLATION PLANNING* on Page 111.

NOTE: It is important to use a "Network Name" that is different from any currently in use in your area during the testing period.

To simulate data traffic over the radio network, connect a PC or LAN to the Ethernet port of the Access Point and PING each *transceiver* several times.

2.2 STEP 1—CONNECT THE ANTENNA PORTS

Figure 2-1 is a drawing of the tabletop arrangement. Connect the antenna ports of each transceiver as shown. This provides stable radio communications between each unit and prevents interference to nearby electronic equipment.
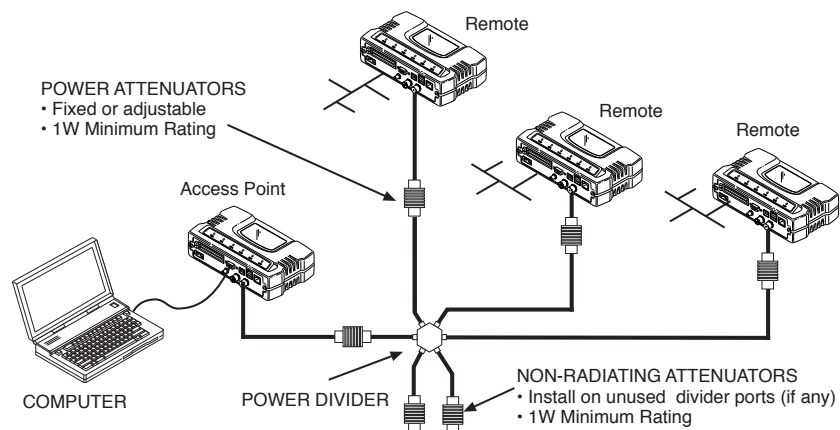
Figure 2-1. Typical setup for tabletop-testing of radios

NOTE: It is important to use attenuation between all units in the test setup. The amount of attenuation required will depend on the number of units being tested and the desired signal strength (RSSI) at each transceiver during the test. In no case should a signal greater than –50 dBm be applied to any transceiver in the test setup. An RF power output level of +20 dBm is recommended from the AP. Remote power is not settable. (See *"Radio Configuration Menu"* on Page 54.)

2.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER

The primary power at the transceiver's power connector must be within 10.5–30 Vdc and be capable of continuously providing 30 Watts. Typical power consumption for 13.8 and 24 Vdc operation are listed in *SPECIFICATIONS* on Page 125.

A Phoenix two-pole power connector with screw-terminals is provided with each unit. Strip the wire leads to 6 mm (0.25"). Be sure to observe proper polarity with the positive lead (**+**) on the left and negative (**–**) on the right.

NOTE: It typically requires about 30 seconds for the transceiver to power up, and may take several minutes to associate with another unit, if GPS is required for time synchronization.

GPS is required for all configurations except when "Free Run" single-channel (non-frequency hopping) operation is used, which may be possible in some low-interference environments.

CAUTION POSSIBLE EQUIPMENT DAMAGE	The transceiver must only be used with negative-ground power systems. Make sure the polarity of the power source is correct.

Figure 2-2. Power Connector
(Polarity: Left +, Right –)

2.4   STEP 3—CONNECT PC TO THE TRANSCEIVER

Connect a PC's Ethernet port to the LAN port using an Ethernet crossover cable. The LAN LED should light. Alternatively, you can use a serial cable to connect to the COM1 port. (Figure 2-3 on Page 26)

2.5   STEP 4—REVIEW TRANSCEIVER CONFIGURATION

2.5.1 Getting Started

Start by logging into the Access Point radio. This is done first because the Remotes are dependent on the AP's beacon signal to achieve an "associated" state.

Once the Access Point is up and running, move the computer connection to each of the Remote units, log-in at each unit, review their configuration, set their IP addresses and Network Name and wait for each to achieve an associated state.

With all units associated, you will be ready to connect and test your data services.

2.5.2 Procedure

The following is a summary of the configuration procedure that must be done on each unit in the system. Key parameters are shown on the Embedded Management System overview (Figure 3-1 on Page 31). A lists of parameters can found in two tables—Table 4-5 on Page 100 and Table 4-7 on Page 103. Detailed information on using the Management System can be found in *MS INTRODUCTION* on Page 30.

NOTE: The Management System supports the use of "configuration files" to aid in uniformly configuring multiple units. These are explained in *Configuration Scripts Menu* on Page 81.

2.5.3 Basic Configuration Defaults

Table 2-1 provides a selection of key operating parameters, their range, and default values. All of these are accessible through a terminal emulator connected to the COM1 serial port or through a Web browser connected to the LAN Port. (See Figure 5-1 on Page 111 for hookup.)

NOTE: Access to the transceiver's Management System and changes to some parameters, require the entry of a password to maintain security.

Table 2-1. Basic Configuration Defaults

Item	Menu Location	Default	Values/Range
Network Name	Main Menu>> Network Configuration>> Network Name	"Not Programmed"	• 1–15 alphanumeric characters • Case-sensitive; can be mixed case
IP Address	Main Menu>> Network Configuration>> IP Address	192.168.1.1	Contact your network administrator
RF Output Power *(adjustable only at AP)*	Main Menu>> Radio Configuration>> RF Output Power	30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watts)
Unit Password	Main Menu>> Device Information>> User Password	admin (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case

A unique IP address and subnet are required to access the browser-based Management System either through the LAN port, or remotely over-the-air.

2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT

Connect a local area network to the LAN port or a serial device to the COM1 (DCE) port. The LAN port will support any Ethernet-compatible equipment. This includes devices that use Internet Protocol (IP).

Figure 2-3 shows the interface connectors on the front panel of the transceiver.
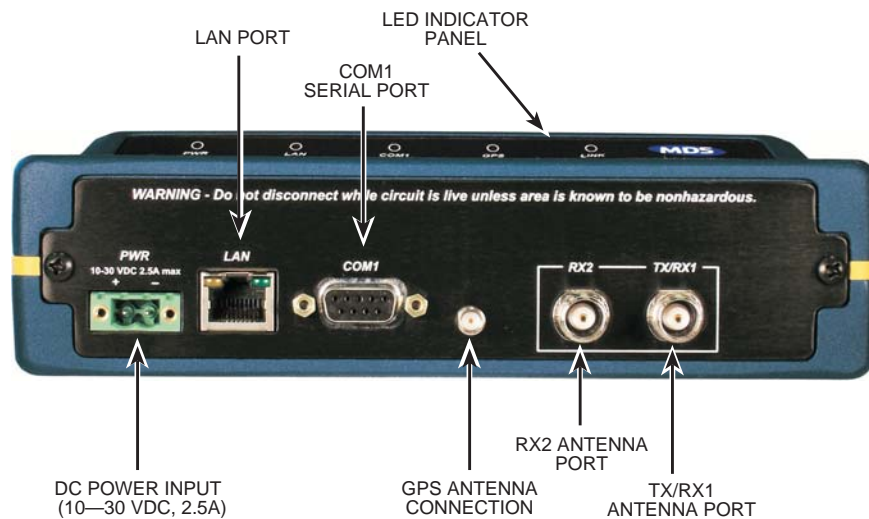
Figure 2-3. Transceiver Interface Connectors

- **LED INDICATOR PANEL**—Displays the basic operating status of the transceiver. Section 2.7 contains detailed information.
- **COM1 SERIAL PORT**— DB-9 connector used for management of the transceiver via a connected PC. *MS INTRODUCTION* on Page 30 provides complete connection details.
- **LAN PORT**—Connection point for Ethernet Local Area Network. An integrated LED on this port glows yellow for 10 mbps, green for 100 mbps.
- **PWR**— DC power connection for the transceiver. Power source must be 10–30 Vdc, negative ground, and capable of furnishing at least 10 watts.
- **GPS ANTENNA PORT**— Coaxial connector (SMA-type) for connection of a Global Positioning System receiving antenna. Provides 3.5 Vdc output for compatibility with powered (active) GPS antennas.

NOTE: GPS functionality is required on all Access Points and Remotes except when "Free Run" single-channel (non-frequency hopping) operation is used, which may be possible in some low-interference environments.

- **RX2 ANTENNA PORT**— Coaxial connector (TNC-type) for attachment of a second 900 MHz receiving antenna used in space diversity arrangements.
- **TX/RX1 ANTENNA PORT**— Coaxial connector (TNC-type) for attachment of the main station antenna (transmit and receive).

2.7 STEP 6—CHECK FOR NORMAL OPERATION

Once the data equipment is connected, you are ready to check the transceiver for normal operation.

Observe the LEDs on the top cover for the proper indications. In a normally operating system, the following LED indications will be seen within 45seconds of start-up:

- PWR—Lit continuously
- LINK—On, or blinking intermittently to indicate traffic flow
- LAN—On, or blinking intermittently to indicate traffic flow

Figure 2-4 shows a close-up view of the transceiver's LED Indicator panel. Table 2-2 provides details on each LED function.

Figure 2-4. LED Indicator Panel

If the radio network seems to be operating properly based on observation of the unit's LEDs, you can use the **PING** command to verify the link integrity with the Access Point. This command can also be used to point your browser to another Remote unit's IP address in the same network.

Table 2-2. Transceiver LED Functions

LED Label	Activity	Indication
PWR	ON	Primary power (DC) present
	Blinking	Unit in "Alarmed" state
	OFF	Primary power (DC) absent
LAN*	ON	LAN detected
	Blinking	Data TX/RX
	OFF	LAN not detected, or excessive traffic present
COM1 (MGT System)	Blinking	Data TX/RX
	OFF	No data activity
GPS	ON	Internal GPS receiver is synchronized with the satellite network.
	OFF	Internal GPS receiver is not synchronized with the satellite network.
LINK (Access Point)	ON	Default state
	Blinking	Data Tx/Rx
	OFF	Traffic exceeds the capacity of the radio network
LINK (Remote)	ON	Associated to AP
	Blinking	Data Tx/Rx
	OFF	Not associated with AP

* The LAN connector itself has an integrated LED which glows yellow for 10 mbps operation, and green for 100 mbps.

3 EMBEDDED MANAGEMENT SYSTEM

Contents

3.1 MS INTRODUCTION

The transceiver's embedded management system is accessible through various data interfaces. These include the COM1 (serial) port, LAN (Ethernet) port, and via SNMP. Essentially the same capabilities are available through any of these paths.

For support of SNMP software, a set of MIB files is available for download from the GE MDS Web site at **www.GEmds.com**. An overview of SNMP commands can be found at *SNMP Agent Configuration* section on Page 48 of this manual.

The transceiver's Management System and its functions are divided into seven functional groups as listed below.

- Section 3.3, *BASIC DEVICE INFORMATION* (beginning on Page 38)
- Section 3.4, *CONFIGURING NETWORK PARAMETERS* (beginning on Page 43)
- Section 3.5, *RADIO CONFIGURATION* (beginning on Page 53)
- Section 3.5.4, *Security Configuration* (beginning on Page 57)
- Section 3.6, *PERFORMANCE OPTIMIZATION* (beginning on Page 87)
- Section 3.5.8, *Maintenance/Tools Menu* (beginning on Page 76)

Each of these sections has a focus that is reflected in its heading. The section you are now reading provides information on connecting to the Management System, how to navigate through it, how it is structured, and how to perform top-level configuration tasks. Figure 3-1 on the following page shows a top-level view of the Management System (MS).

3.1.1 Differences in the User Interfaces

Although there are slight differences in navigation among the user interfaces, the content is very similar. You will notice a few differences in capabilities as the communications tool is driven by limitations of the access channel. Figure 3-2 and Figure 3-3 show examples of the Starting Information Screen as seen through a console terminal and a web-browser, respectively.

Starting Information Screen (Read-Only Status)

MAIN MENU

Network Configuration
- IP Configuration
- Ethernet Port Config
- Bridge Configuration
- VLAN Configuration
- SNMP Agent Config. (AP)
- SMTP Agent Config. (RM)
- Wireless Ntwk Config. (AP)
- AP Location Info (RM)
- DHCP Server Config.
- SNTP Server Config.

Radio Configuration
- Network Name
- Transmit Pwr (AP)
- Freq. Control
- Receive Pwr (AP)
- Freq. Control
- Adv. Config.

Security Configuration
- Device Security
- Wireless Security
- RADIUS Configuration
- Manage Certif.

Redundancy Configuration (AP)
- Redundancy Config.
- Ntwk Event Triggers
- Radio Event Triggers
- Hdwr Event Triggers
- Red. Config. Options
- Force Switchover

GPS Configuration (RM)
- Stream GPS
- Send GPS via UDP
- GPS IP Address
- GPS Server Port

Device Information
- Model
- Serial Number
- Uptime
- Date
- Time
- Date Format
- Console Bd. Rt.
- UTC Time Offset
- Device Names

Performance Information
- Event Log
- Packet Statistics
- GPS Status
- Wireless Ntwk Stat.
- Intl. Radio Stat. (RM)

Maintenance/Tools
- Reprogramming
- Config. Scripts
- Ping Utility
- Auth. Codes
- Reset to Defaults
- Radio Test

NOTES
• Chart shows top-level view only. See *Reference Manual* for details.
• Not all menu items are-user configurable
• Spacebar is used to make some menu selections
• AP = Access Point Only
• RM = Remote Only

Figure 3-1. Embedded Management System—Top-Level Flowchart
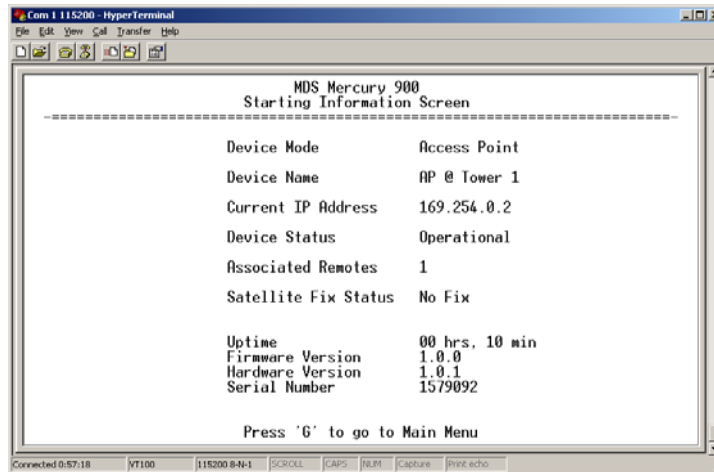
Figure 3-2. View of MS with a text-based program—
(Console Terminal shown—Telnet has similar appearance)
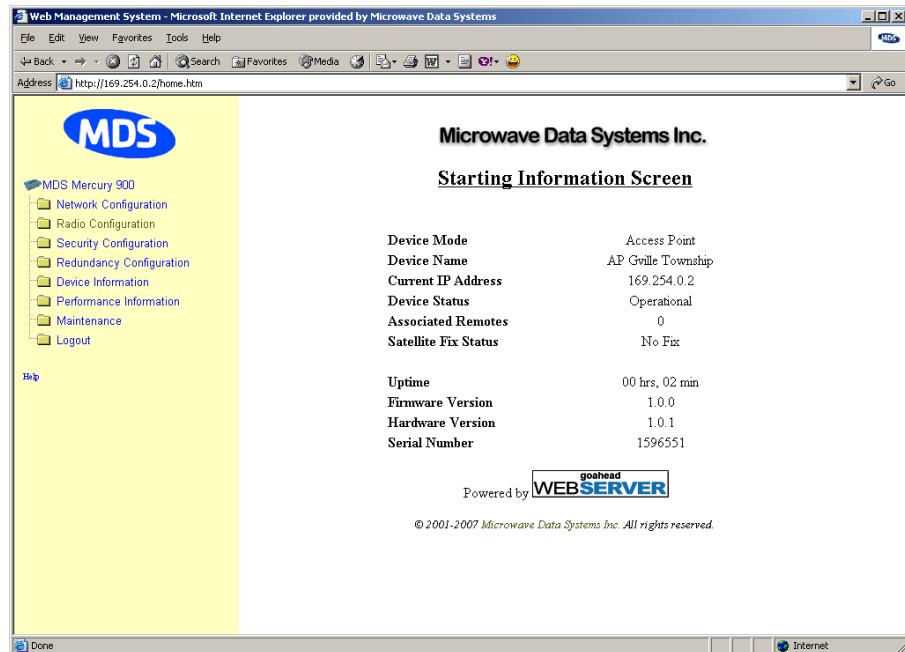
Figure 3-3. View of the MS with a Browser
(Selections at left provide links to the various menus)

3.2   ACCESSING THE MENU SYSTEM

The radio has no external controls or adjustments. All configuration, diagnostics and control is performed electronically using a connected PC. This section explains how to connect a PC, log into the unit, and gain access to the built-in menus.

3.2.1 Methods of Control

The unit's configuration menus may be accessed in one of several ways:

- **Local Console**—*This is the primary method used for the examples in this manual*. Connect a PC directly to the COM 1 port using a serial communications cable and launch a terminal communications program such as HyperTerminal (found on most PCs by selecting **Start>>Programs>>Accessories>>Communications>>HyperTerminal**). This method provides text-based access to the unit's menu screens. Console control is a hardware-based technique, and is intended for local use only (maximum recommended cable length of 50 ft./15 m).
- **Telnet or SSH***—Connect a PC to the unit's LAN port, either directly or via a network, and launch a Telnet session. This method provides text-based access to the unit's menu screens in a manner similar to a Local Console session. Telnet sessions may be run locally or remotely through an IP connection.
- **Web Browser***—Connect a PC to the unit's LAN port, either directly or via a network, and launch a web browser session (*i.e.,* Internet Explorer, Netscape, etc.) This method provides a graphical representation of each screen, just as you would see when viewing an Internet website. The appearance of menu screens differs slightly from other methods of control, but the content and organization of screen items is similar. Web browser sessions may be run locally or remotely via the Internet.

*   Telnet, SSH and Web Browser sessions require the use of a *straight-through* cable to connect the radio with a PC.

3.2.2 PC Connection & Log In Procedures

The following steps describe how to access the radio's menu system. These steps require a PC to be connected to the unit's COM 1 or LAN port as shown in Figure 3-4.
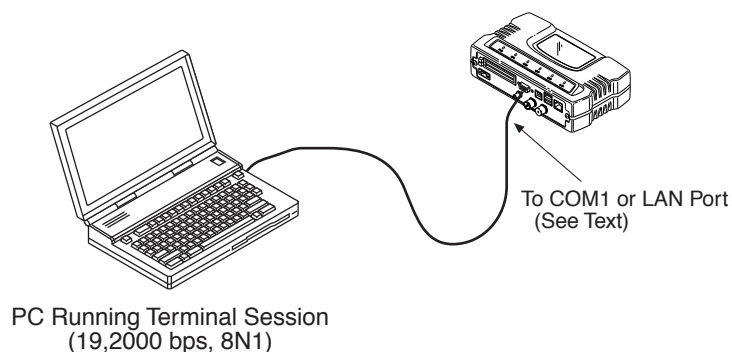

To COM1 or LAN Port
(See Text)

PC Running Terminal Session
(19,2000 bps, 8N1)

Figure 3-4. PC Configuration Setup

Starting a Local
Console Session
(Recommended for
first-time log-in)

1. Connect a serial communications cable between the PC and the unit's COM 1 port. If necessary, a cable may be constructed for this purpose as shown in Figure 3-5.
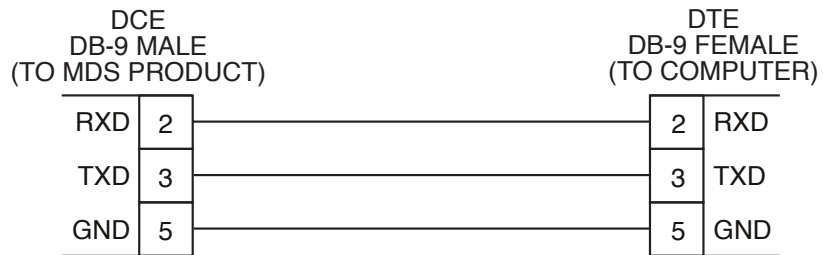
```
        DCE                                          DTE
     DB-9 MALE                                   DB-9 FEMALE
  (TO MDS PRODUCT)                              (TO COMPUTER)

   RXD  | 2 |─────────────────────────────| 2 |  RXD

   TXD  | 3 |─────────────────────────────| 3 |  TXD

   GND  | 5 |─────────────────────────────| 5 |  GND
```

Figure 3-5. Serial Communications Cable (DB-9M to DB-9F)
(Maximum Recommended Cable Length 50 Feet/15 meters)

2. Launch a terminal emulation program such as HyperTerminal and configure the program with the following settings:

   - 115,200 bps data rate
   - 8 data bits, no parity
   - One stop bit, and no flow-control
   - Use ANSI or VT100 emulation.

TIP: The HyperTerminal communications program can be accessed on most PCs by selecting this menu sequence: **Start>>Programs>>Accesso-ries>>Communications>>HyperTerminal**.

NOTE: Early versions of PuTTY may not operate when using SSH to connect to the transceiver. The latest version (0.58 at the time of publication) does work with the transceiver's internal server. Both the latest released and the latest development snapshot can be downloaded from: **www.chiark.greenend.org.uk/~sgtatham/putty/**.

NOTE: If the unit is powered-up or rebooted while connected to a terminal, you will see a series of pages of text information relating to the booting of the unit's microcomputer. Wait for the log-in screen before proceeding.

---

3. Press the ENTER key to receive the **login:** prompt.

4. Enter the username (default username is **admin**). Press ENTER.

5. Enter your password (default password is **admin**). (For security, your password keystrokes do not appear on the screen.) Press ENTER.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

The unit responds with the Starting Information Screen (Figure 3-6). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.
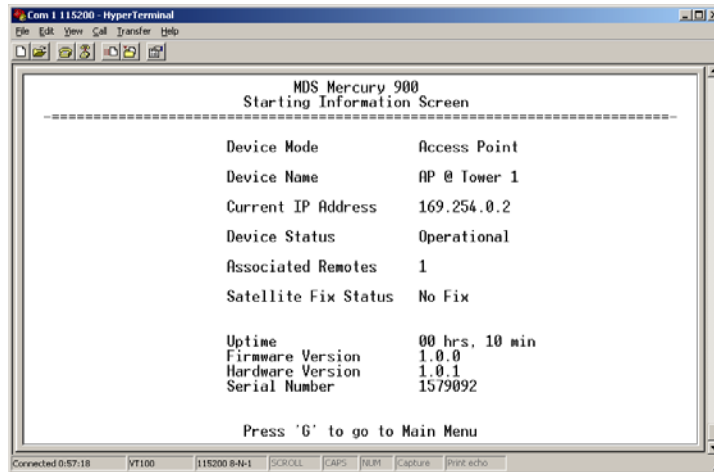
Figure 3-6. Starting Information Screen—Local Console Session

Starting a Telnet Session

NOTE: This method requires that you know the IP address of the unit beforehand. If you do not know the address, use the Local Console method (above) and access the *Starting Information Screen*. The address is displayed on this screen.

1. Connect a PC to the unit's LAN port, either directly or via a network with a *straight-through* cable. The LAN LED lights to indicate an active connection.

NOTE: When using Ethernet to access the unit, it may be necessary to change your computer's IP access to be compatible with the radio IP address. You can identify or verify the unit's IP address by using a Local Console session to communicate with the radio through its COM 1 Port and viewing the *Starting Information Screen*.

2. Start the Telnet program on your computer targeting the IP address of the unit to which you are connected. and press ENTER.

TIP: A Telnet session can be started on most PCs by selecting: **Start>>Programs>>Accessories>>Command Prompt**. At the command prompt window, type the word **telnet**, followed by the unit's IP address (*e.g.*, **telnet 10.1.1.168**). Press ENTER to receive the Telnet log in screen.

NOTE: Never connect multiple units to a network with the same IP address. Address conflicts will result in improper operation.

3. Enter your username (default username is **admin**). Press ENTER.

Next, the **Password:** prompt appears. Enter your password (default password is **admin**). (For security, your password keystrokes will not appear on the screen.) Press ENTER.

The unit responds with a Starting Information Screen (see Figure 3-6). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

Starting a Web Browser Session

NOTE: Web access requires that you know the IP address of the unit you are connecting to. If you do not know the address, start a Local Console session (see *Starting a Local Console Session (Recommended for first-time log-in)* on Page 34) and access the *Starting Information Screen*. The IP address is displayed on this screen.

1. Connect a PC to the unit's LAN port, either directly or via a network. If connecting directly, use an Ethernet *crossover* cable; if connecting via a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.

2. Launch a Web-browser session on your computer (*i.e.,* Internet Explorer, Netscape Navigator, etc.).

3. Type in the unit's IP address and press ENTER.

4. A log-in screen is displayed (Figure 3-7) where you enter a user name and password to access the unit's menu system. Note that the default entries are made in *lower case*. (Default User Name: **admin**; Default Password: **admin**)
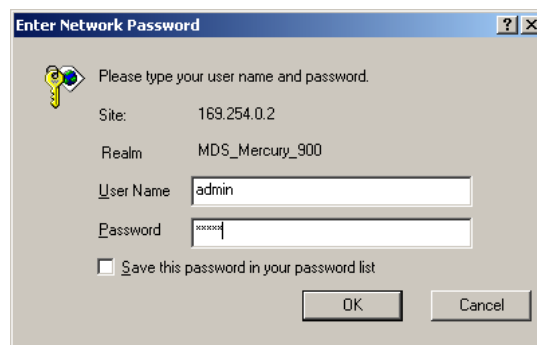

Figure 3-7. Log-in Screen when using a Web Browser

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. You may use up to eight alpha-numeric characters.

5. Click **OK**. The unit responds with a startup menu screen similar to that shown in Figure 3-8. From here, you can review basic information about the unit or click on one of the menu items at the left side of the screen.
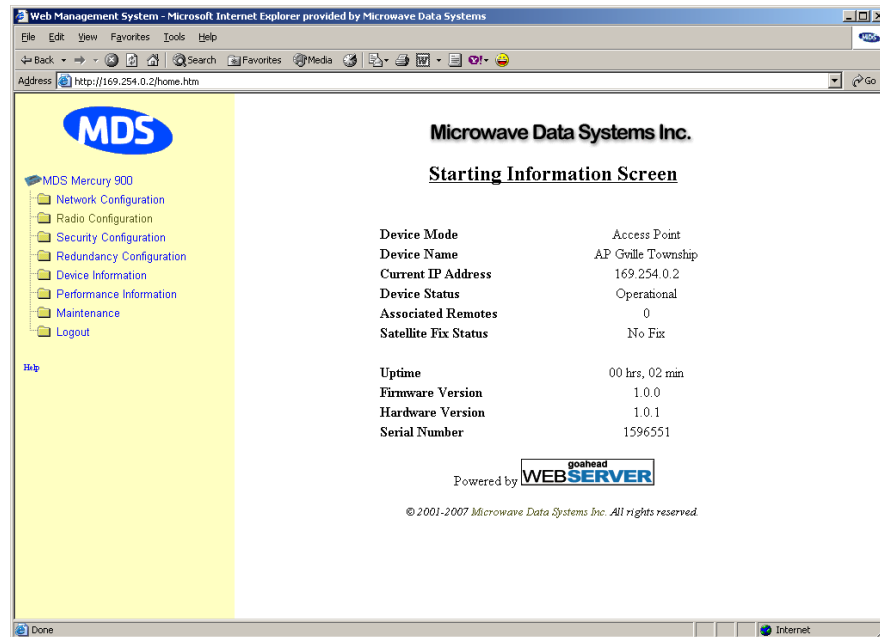

Figure 3-8. Starting Information Screen—Web Browser Example

3.2.3 Navigating the Menus

Via Terminal Telnet or SSH Sessions
Recommended for first-time log-in

Local Console, Telnet, and SSH sessions use multi-layered text menu systems that are nearly identical. To move further down a menu tree, you type the letter assigned to an item of interest. This takes you to an associated screen where settings may be viewed, or changed. In most cases, pressing the ESCAPE key moves the screen back one level in the menu tree.

In general, the top portion of menu screens show *read-only* information (with no user selection letter). The bottom portion of the screen contains parameters that can be selected for further information, alteration of values, or to navigate to other submenus.

When you arrive at a screen with user-controllable parameter fields, you select the menu item by pressing an associated letter on the keyboard. If there is a user definable value, the field will clear to the right of the menu item and you can type in the value you wish to use. Follow this action

by pressing the ENTER key to save the changes. If you make a mistake or change your mind before pressing the ENTER key, simply press ESCAPE to restore the previous value.

In some cases, when you type a letter to select a parameter, you will see a prompt at the bottom of the screen that says **Choose an Option**. In these screens, press the keyboard's SPACEBAR to step through the available selections. When the desired option appears, press the ENTER key to choose that selection. In some cases, several parameters may be changed and then saved by a single keystroke. The ESCAPE key can be used to cancel the action and restore the previous values.

Logging Out Via Terminal Emulator or Telnet

From the Main Menu screen, press **Q** to quit and terminate the session.

Navigating via Web Browser

Navigating with a Web browser is straightforward with a framed "homepage." The primary navigation menu is permanently located on the left-hand side of this page. Simply click on a desired menu item to bring it to the forefront.

NOTE: To maintain security, it is best to log-out of the menu system entirely when you are done working with it. If you do not log out, the session automatically ends after 10 minutes of inactivity.

Logging Out Via Web Browser

Click on **Logout** in the left-hand frame of the browser window. The right-hand frame will change to a logout page. Follow the remaining instructions on this screen.

NOTE: In the menu descriptions that follow, parameter options/range, and any default values are displayed at the end of the text between square brackets. Note that the default setting is always shown after a semicolon:
[**available settings or range; default setting**]

3.3 BASIC DEVICE INFORMATION

This section contains detailed menu screens and settings that you can use to specify the behavior of the unit.

3.3.1 Starting Information Screen

Once you have logged into the Management System, the Starting Information Screen (Figure 3-9) appears with an overview of the transceiver and its current operating conditions.
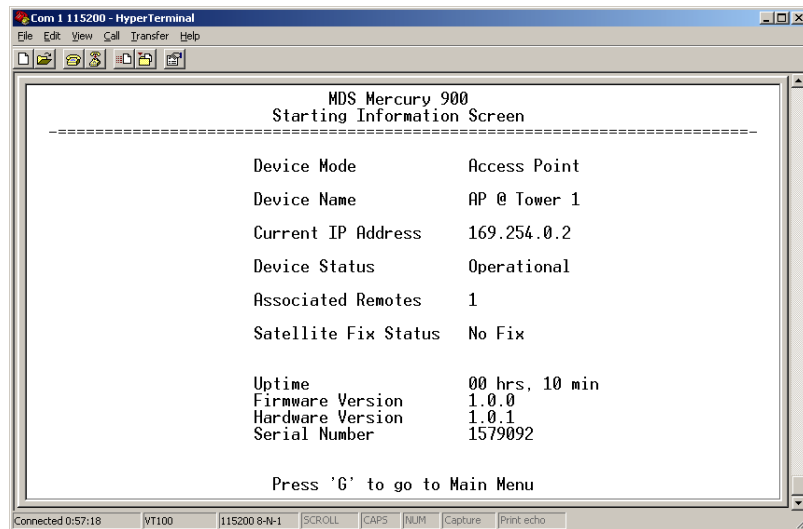
Figure 3-9. Starting Information Screen
(AP screen shown; Remote similar, differences noted below)

- **Device Mode**—Current operating mode of the unit as it relates to the radio network.
- **Device Name**—This is a user-defined parameter that appears in the heading of all pages. (To change it, see *Network Configuration Menu* on Page 43.)
- **Current IP Address**—Unit's IP address [**169.254.0.2**]
- **Device Status**—Condition of the unit's association with an Access Point.

At the Access Point:
- *Operational*—Unit operating normally.
- *Initializing*—This is the first phase after boot-up.
- *Alarmed*—A alarm event has been logged and not cleared.

At a Remote:
- *Scanning*—The unit is looking for an Access Point beacon signal.
- *Connecting*—The unit has found a valid beacon signal for its network.
- *Associated* —This unit has successfully synchronized and associated with an Access Point.
- *Alarmed*—The unit is has detected one or more alarms that have not been cleared.

NOTE: If an alarm is present when this screen is displayed, an "A)" appears to the left of the **Device Status** field. Pressing the "A" key on your keyboard takes you directly to the "Current Alarms" screen.

- **Associated Remotes** (AP Only)—Indicates the number of Remotes that have achieved association with the AP.
- **Connection Status** (Remote Only)—Indicates whether the Remote has an RF connection with an AP.
- **Satellite Fix Status**—Indicates how many satellites.have been detected by the internal GPS receiver. A minimum of five satellites are required to achieve Precise Positioning Service (PPS), and four are needed to maintain service.
- **Uptime**—Elapsed time since the transceiver was powered-up.
- **Firmware Version**—Version of firmware that is currently active in the unit.
- **Hardware Version**— Hardware version of the transceiver's printed circuit board.
- **Serial Number**—Make a record of this number. It must be provided to purchase Authorization Codes to upgrade unit capabilities in the future. (See *"Authorization Codes" on Page 85*.)

3.3.2 Main Menu

The Main Menu is the entry point for all user-controllable features. The transceiver's **Device Name** appears at the top of this and all other screens as a reminder of the unit that is currently being controlled.
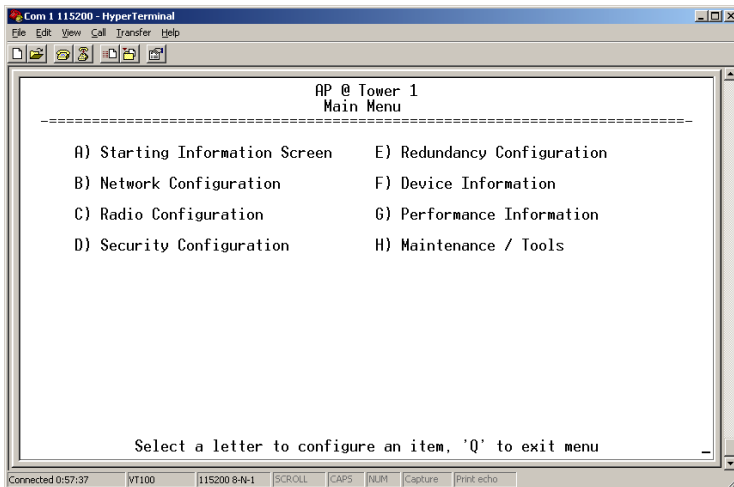
Figure 3-10. Main Menu (AP)
(AP screen shown; Remote similar, differences noted below)

- **Starting Information Screen**—Select this item to return to the Starting Information screen described above.
- **Network Configuration**—Tools for configuring the data network layer of the transceiver. (See *"Network Configuration Menu" on Page 43*)
- **Radio Configuration**—Tools to configure the wireless (radio) layer of the transceiver. (See *"Radio Configuration Menu" on Page 54*)

- **Security Configuration**—Tools to configure the security services available with the transceiver's environment. (See *"GE MDS CYBER SECURITY SUITE" on Page 16*)

- **Redundancy Configuration**—(AP Only) Allows setting of the criteria for switchover in the event of loss of associated Remotes or excessive packet receive errors.

- **GPS Configuration**—(Remote Only) View/set parameters related to GPS timing signals. (See *"GPS Configuration (Remote Only)" on Page 68*)

- **Device Information**—Top level device fields such as model, serial number, date/time, etc. (See *"Device Information" on Page 41*)

- **Performance Information**—Tools to measure the radio and data layer's performance of the radio network. (See *"Performance Information Menu" on Page 68*)

- **Maintenance/Tools**—Tools for upgrading firmware code and testing major unit capabilities. (See *"Authorization Codes" on Page 85*)

3.3.3 Configuring Basic Device Parameters

Device Information

Figure 3-11 shows the menu that displays basic administrative data on the unit to which you are connected. It also provides access to some user- specific parameters such as date/time settings and device names.
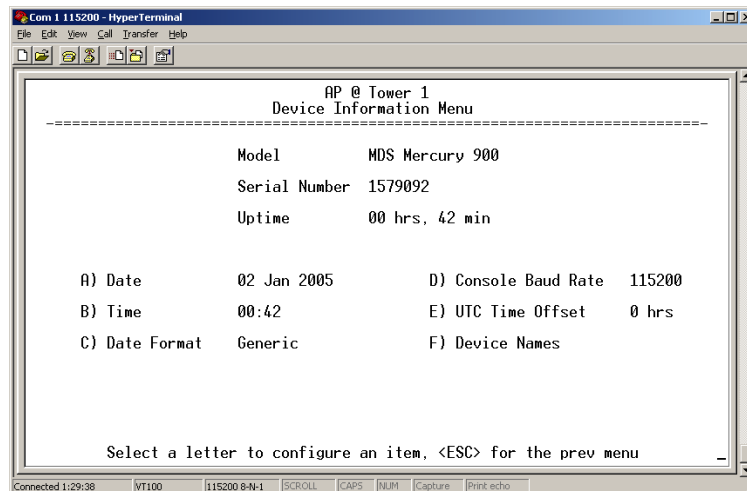

Figure 3-11. Device Information Menu

- **Model** *(Display only)*
- **Serial Number** *(Display only)*
- **Uptime** *(Display only)*—Elapsed time since powering up.
- **Date**—Current date being used for the transceiver logs. User-settable. (Value lost with power failure if SNTP (Simple Network Time Protocol) server not accessible.)

- **Time**—Current time of day. User-setable.
  Setting: HH:MM:SS
  (Value lost with power failure if SNTP server not accessible.)
- **Date Format**—Select presentation format:
  - Generic = dd Mmm yyyy
  - European = dd-mm-yyyy
  - US = mm-dd-yyyy
- **Console Baud Rate**—Used to set/display data communications rate (in bits-per-second) between a connected console terminal and the radio. [**115200**]
- **UTC Time Offset**—Set/view the number of hours difference between your local clock time and Coordinated Universal Time.
- **Device Names**—Fields used at user's discretion for general administrative purposes. The Device Name field is shown on all menu screen headings. (See Figure 3-12 on Page 42)

NOTE: The transceivers do not save time and date information when power is removed.
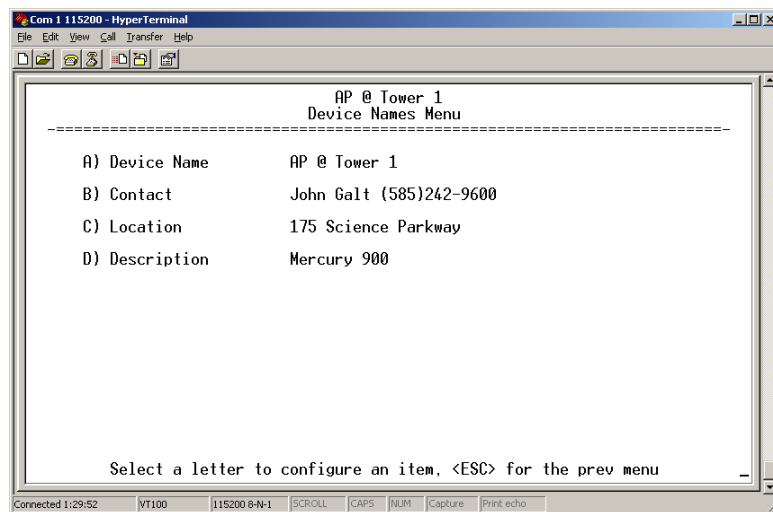

Device Names Menu

Figure 3-12. Device Names Menu

- **Device Name**—Device Name, used by the transceiver as the "Realm" name for network login (web browser only) and menu headings.
- **Contact**—User defined; appears on this screen only.
- **Location**—User defined; appears on this screen only.
- **Description**—User defined; appears on this screen only.

3.4 CONFIGURING NETWORK PARAMETERS

3.4.1 Network Configuration Menu

The *Network Configuration Menu* is the home of several parameters that may need to be reviewed and set as necessary before placing a transceiver in service.
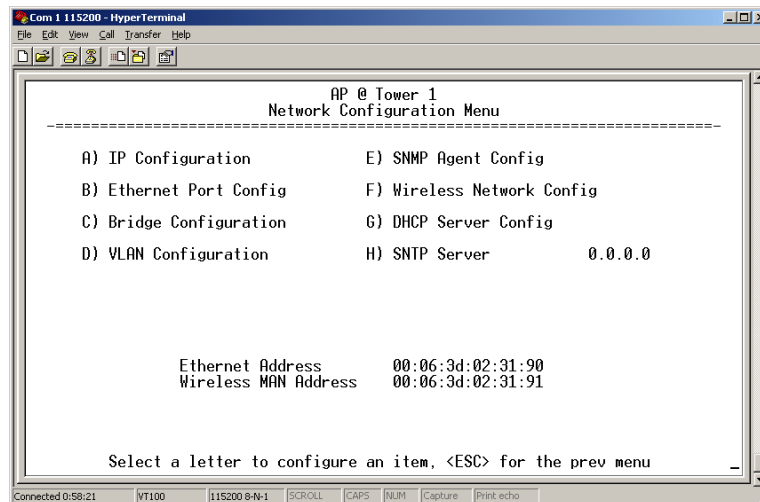

Figure 3-13. Network Configuration Menu

- **IP Configuration**   This selection presents a submenu for configuring the local static IP address of the transceiver. Detailed explanations are provided in the section titled *IP Configuration Menu* on Page 44.

- **Ethernet Port Configuration**—Presents a menu for defining the status of the Ethernet port (enabled or disabled), the Ethernet rate limit, link hardware watch (enabled/disabled), and the Ethernet link poll address. Detailed explanations of this menu are contained in *Ethernet Port Configuration Menu* on Page 45

- **Bridge Configuration**—View/set options for Ethernet Bridge operation.

- **VLAN Configuration**—Presents a menu for configuring the Virtual LAN (VLAN) and IP address of the transceiver. Detailed explanations are provided in the section titled *VLAN Configuration* on Page 47.

- **SNMP Agent Configuration** (AP Only)—View/set SNMP configuration parameters. See *"SNMP Agent Configuration"* on Page 48 for more information.

- **SNTP Agent Configuration** (Remote Only)—View/set SNTP options. See *"SNTP Server Configuration"* on Page 53 for details.

- **Wireless Network Configuration** (AP Only)—Presents a submenu where the device mode may be viewed and the maximum number of Remotes can be set. See *"Wireless Network Configuration (AP Only)" on Page 51* for details.

- **AP Location Info** (Remote Only)—Presents a submenu where many parameters related to the Access Point location can be viewed or set. See *"AP Location Info Config Menu (Remote Only)" on Page 51* for details.

- **DHCP Server Configuration**—Menu for configuration of DHCP services by the Access Point. DHCP provides "on-the-fly" IP address assignments to other LAN devices, including MDS Mercury 900 units. [**Disabled**]

- **SNTP Server Configuration**—Address of SNTP server (RFC 2030) from which the transceiver will automatically get the time-of-day startup time. Without an SNTP server, the date and time must be manually set. An AP will try to get the time and date from the SNTP server only if an IP address is configured. It will continue to retry every minute until it succeeds.

  A remote will get the time and date from the SNTP server if an IP address is configured. Otherwise, it gets it from the AP at authentication time. The transceivers use UTC (Universal Time Constant) with a configurable time offset. [**0.0.0.0**]
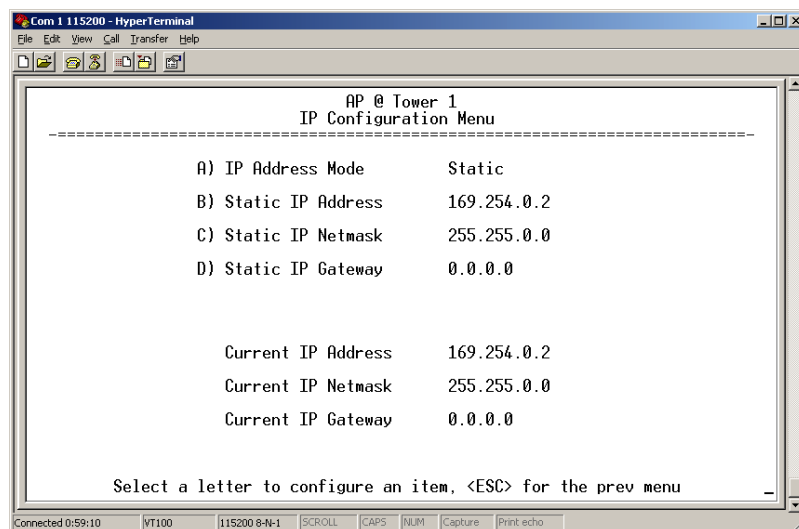
3.4.2 IP Configuration Menu

Figure 3-14. IP Configuration Menu

CAUTION: Changes to the following parameters while communicating over the network (LAN or over-the-air) may cause a loss of communication with the unit being configured. Communication will need to be re-established using the new IP address.

- **IP Address Mode**—Defines the source of the IP address of this device. [**Static, Dynamic**; **Static**]
- **Static IP Address** *(User Review Recommended)*—Essential for connectivity to the transceiver's MS via the LAN port and to send Ethernet data over the network. Enter any valid IP address that will be unique within the network. [**192.168.1.1**]
  This field is unnecessary if DHCP is enabled. [**255.255.0.0**]
- **Static IP Netmask**—The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled. [**255.255.0.0**]
- **Static IP Gateway**—The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled. [**0.0.0.0**]

  The lower three items on the screen (Current IP Address, Netmask and Gateway) show the actual addressing at the transceiver whether it was obtained from static configuration or from a DHCP server.

NOTE: Any change made to the above parameters results in the **Commit Changes** option appearing on screen. This allows all IP settings to be changed at the same time.

3.4.3 Ethernet Port Configuration Menu

The transceiver allows for special control of the Ethernet interface, to allow traffic awareness and availability of the backhaul network for redundancy purposes.

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.
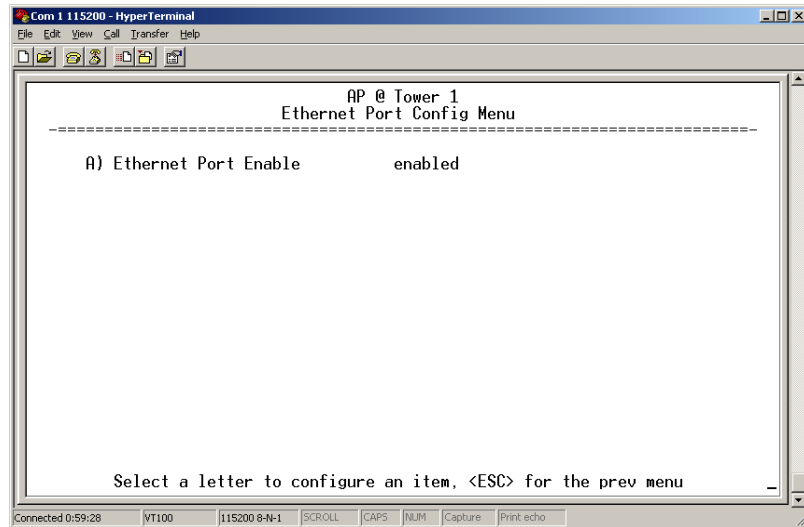
Figure 3-15. Ethernet Port Configuration Menu

- **Ethernet Port Enable**—Allows enabling/disabling Ethernet traffic for security purposes. Setting it to **enabled** enables the port if there is a connection established with the AP, but disables it otherwise. [AP: **enabled, disabled; enabled**]
  [Remote: **Always On, Follow Radio Link, Disabled; Always On**]

3.4.4 Bridge Configuration

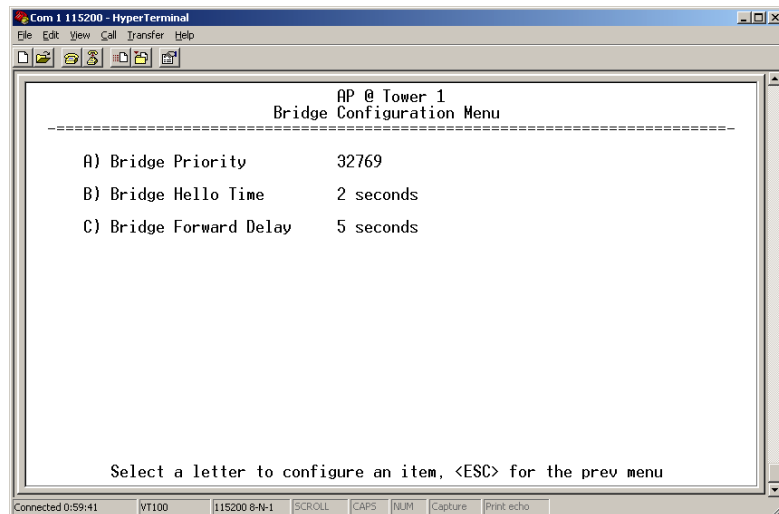**Figure 3-16. Bridge Configuration Menu**

- **Bridge Priority**—View/set the priority of the bridge in the spanning tree. [**0-65535; 32769**]
- **Bridge Hello Time**—View/set spanning tree hello time.
  [**1-10 seconds; 2 seconds**]
- **Bridge Forward Delay**—View/set spanning tree forwarding delay. Affects how long the bridge spends listening and learning after initialization. [**4-30 seconds; 5 seconds**].

3.4.5 VLAN Configuration

CAUTION: The VLAN Status parameter must be consistent at both the Access Point and Remote radios in order for data to flow correctly. Failure to do so may result in data not being transported correctly even when the radios are in an associated state and able to communicate over-the-air.

Virtual LAN in Mercury

A VLAN is essentially a limited broadcast domain, meaning that all members of a VLAN receive broadcast frames sent by members of the same VLAN but *not* frames sent by members of a different VLAN. Additional details can be found in the IEEE 802.1Q standard.

The transceiver supports port-based VLAN at the Ethernet interface and over the air, according to the IEEE 802.1Q standard. When VLAN Status is enabled, the wireless port of both AP and remote radios act as a trunk port.

The Ethernet port of an Access Point radio is normally configured as a trunk port. This type of port expects incoming frames to have a **VLAN ID** and sends outgoing frames with a VLAN structure as well.

The Ethernet port of a remote radio can be configured as an access port or as a trunk port.

When the Ethernet port of a Remote radio is configured as VLAN Access Port, the radio will tag incoming traffic with a VLAN ID, and will strip the tag before sending out traffic. This VLAN is known as the DATA VLAN. Additionally, a second VLAN is assigned for other traffic that is terminated at the radio, such as SNMP, TFTP, ICMP, Telnet, etc. This is known as the MANAGEMENT VLAN. Traffic directed to the integrated terminal server that handles the serial ports is assigned to the DATA VLAN.

When the Ethernet port of a remote radio is configured as a VLAN trunk the radio expects all incoming Ethernet frames to be tagged, and passes through all outgoing frames as received from the wireless link, with the unchanged VLAN tag.

NOTE: The Ethernet port is 10BaseT. Some Ethernet switches allow a VLAN trunk port only on a 100BaseT interface and may not be able to communicate with the radio.
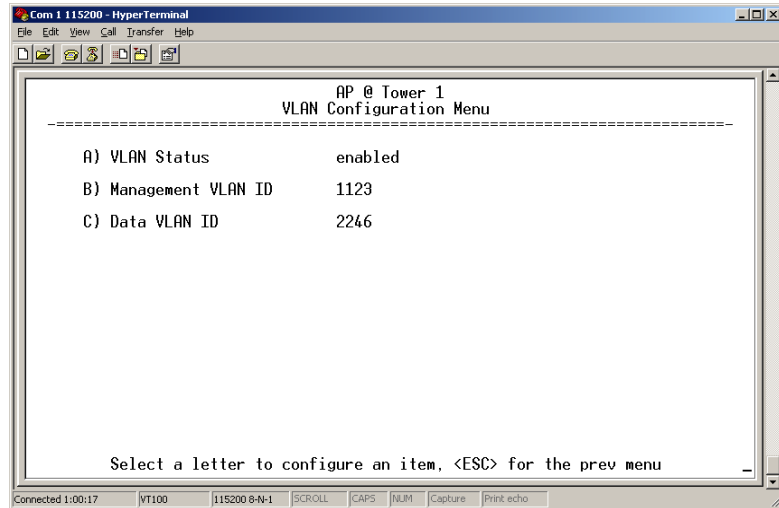
VLAN Configuration Menu

Figure 3-17. VLAN Configuration Menu

- **VLAN Status**—Defines whether the radio handles Ethernet frames in "extended" 802.1Q mode or in "normal" mode in the Ethernet port. Ethernet frames intended for the radio, but with a VLAN ID not configured in the radio are discarded. [**enabled, disabled; disabled**]

- **Management VLAN ID**—Defines the VLAN ID for traffic directed to the radio itself, other than the terminal server process. This VLAN ID is used for filtering and for tagging purposes. [**1-4094; 2**]

- **Data VLAN ID**—Defines the VLAN ID assigned to traffic directed to and from the Ethernet port and the terminal server process in the radio. This VLAN ID is used for filtering and for tagging purposes. [**1-4094; 3**]

3.4.6 SNMP Agent Configuration

The transceiver contains over 100 custom SNMP-manageable objects as well as the IETF standard RFC1213 for protocol statistics, also known as MIB II. Off-the-shelf SNMP managers such as Castle Rock Computing *SNMPc™* and Hewlett Packard HP *OpenView™* may also be used to access the transceiver's SNMP Agent's MIB. The transceiver's SNMP agent supports SNMPv3.

The objects are broken up into nine MIB files for use with your SNMP manager. There are textual conventions, common files and specific files. This allows the flexibility to change areas of the MIB and not affect other existing installations or customers.

- **msdreg.mib**—MDS sub-tree registrations
- **mds_comm.mib**—MDS Common MIB definitions for objects and events which are common to the entire product family

- **mercury_reg.mib**—MDS sub-tree registrations
- **mercurytrv1.mib**—SNMPv1 enterprise-specific traps
- **mercurytrv2.mib**—SNMPv2 enterprise-specific traps
- **mercury_comm.mib**— MIB definitions for objects and events which are common to the entire Mercury Series
- **mercury_ap.mib**—MIB definitions for objects and events for an Access Point transceiver
- **mercury_sta.mib**—Definitions for objects and events for a Remote radio
- **mercury_sec.mib**—For security management of the radio system. SNMPv3 allows read/write operation. SNMPv1/2 allows only for read-only access.

NOTE: SNMP management requires that the proper IP address, network and gateway addresses are configured in each transceiver of the associated network.

In addition, some management systems may require the MIB files to be compiled in the order shown above.

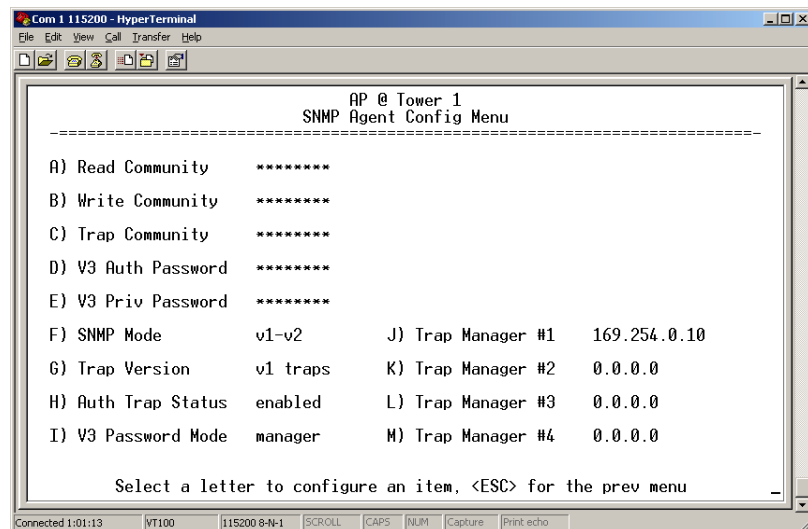---

Figure 3-18. SNMP Server Configuration Menu

This menu provides configuration and control of vital SNMP functions.

- **Read Community String**—SNMP community name with SNMPv1/SNMPv2c read access. This string can be up to 30 alpha-numeric characters.
- **Write Community String**—SNMP community name with SNMPv1/SNMPv2c write access. This string can be up to 30 alpha-numeric characters.

- **Trap Community String**—SNMP community name with SNMPv1/SNMPv2c trap access. This string can be up to 30 alpha-numeric characters.

- **V3 Authentication Password**—Authentication password stored in flash memory. This is used when the Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for Authentication (currently, only MD5 is supported). This string can be up to 30 alpha-numeric characters.

- ¥ **V3 Privacy Password**   Privacy password stored in flash memory. Used when the SNMP Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for privacy (DES encryption). This string can be between 8 and 30 alpha-numeric characters.

- **SNMP Mode**—This specifies the mode of operation of the radio's SNMP Agent. The choices are: disabled, v1_only, v2_only, v3_only. v1-v2, and v1-v2-v3. If the mode is disabled, the Agent does not respond to any SNMP traffic. If the mode is v1_only, v2_only, or v3_only, the Agent responds only to that version of SNMP traffic. If the mode is v1-v2, or v1-v2-v3, the Agent responds to the specified version of SNMP traffic. [**v1-v2-v3**]

- **Trap Version**—This specifies what version of SNMP will be used to encode the outgoing traps. The choices are v1_traps, v2_traps, and v3_traps. When v3_traps are selected, v2-style traps are sent, but with a v3 header. [**v1 Traps, v2 Traps, v3 Traps**]

- **Auth Traps Status**—Indicates whether or not traps will be generated for login events to the transceiver. [**Disabled/Enabled; Disabled**]

- **SNMP V3 Passwords**—Determines whether v3 passwords are managed locally or via an SNMP Manager. The different behaviors of the Agent depending on the mode selected, are described in **SNMP Mode** above.

- **Trap Manager #1–#4**— Table of up to 4 locations on the network that traps are sent to. [**Any standard IP address**]

NOTE: The number in the upper right-hand corner of the screen is the SNMP Agent's SNMPv3 Engine ID. Some SNMP Managers may need to know this ID in order interface with the transceiver's SNMP Agent. The ID only appears on the screen when SNMP Mode is either v1-v2-v3 or v3_only.

3.4.7 Wireless Network Configuration (AP Only)

This menu only available on early firmware versions
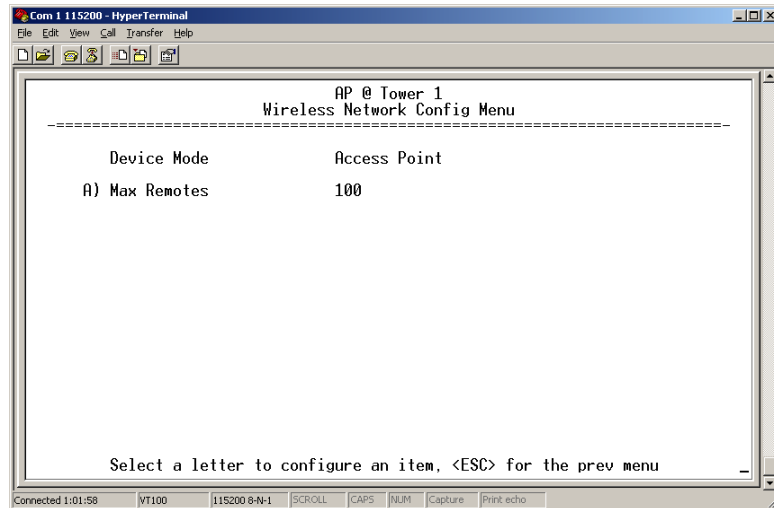
Figure 3-19. Wireless Network Configuration Menu

- **Device Mode** (Read only)—Indicates the operating mode of the radio— **Access Point**, **Remote** or **Remote Repeater**. Mercury employs different hardware for each type of radio, and this parameter may not be changed through software.
- **Max Remotes** (AP Only)—The maximum umber of Remotes that may connect to this Access Point. [**1-1000; 100**]

3.4.8 AP Location Info Config Menu (Remote Only)

This selection shows a menu where parameters related to Access Point location may be viewed or set.

Figure 3-20. AP Location Info Menu

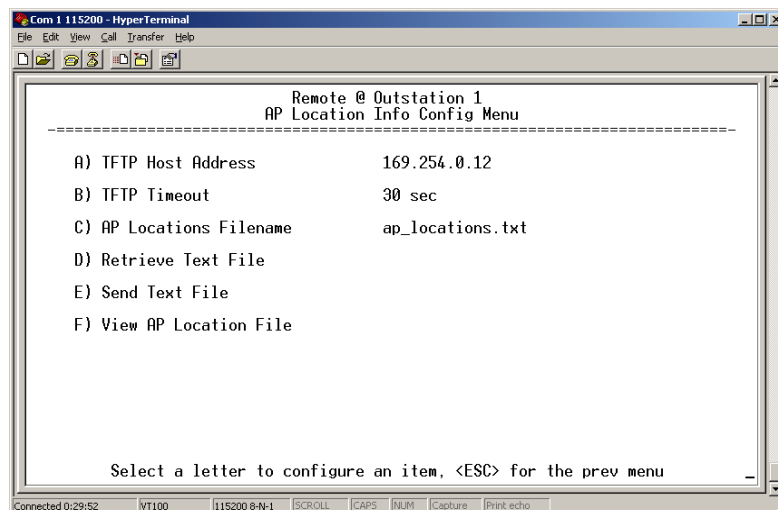- **AP Location Info** (Remote Only)—Launches a submenu **TFTP Host Address**—IP address of TFTP network server that holds the firmware [**any valid IP address; 0.0.0.0**].
- **TFTP Timeout**—View/set timeout seconds for TFTP protocol [**10–60; 10**]
- **AP Locations Filename**—View/set name of text file for AP Locations. [**any valid filename string; ap_locations.txt**]
- **Retrieve Text File**—Locate text file from stored location.
- **Send Text File**—Initiate the file transfer from the transceiver.
- **View AP Location File**—Allows on-screen review of text file.

3.4.9 DHCP Server Configuration (AP Only)

A transceiver can provide automatic IP address assignments to other IP devices in the network by providing DHCP (Dynamic Host Configuration Protocol) services. This service eliminates setting individual device IP address on Remotes in the network, but it requires some planning of the IP address range. One drawback to network-wide automatic IP address assignments is that SNMP services may become inaccessible as they are dependent on fixed IP addresses.

The network can be comprised of radios with the DHCP-provided IP address enabled or with DHCP services disabled. In this way, you can accommodate locations for which a fixed IP address if desired.

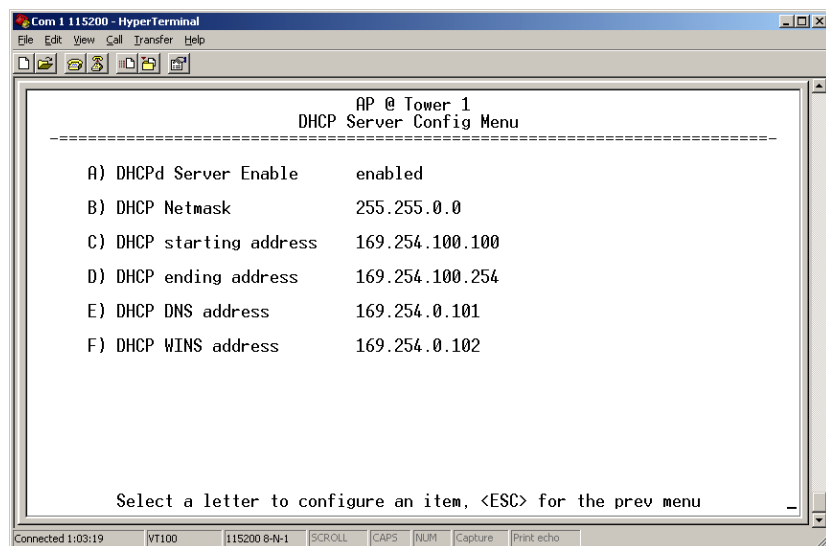**Figure 3-21. DHCP Server Configuration Menu**

NOTE: There should be only one DHCP server active in a network. If more than one DHCP server exists, network devices may randomly get their IP address from different servers every time they request one.

NOTE: Combining DHCP and RADIUS device authentication may result in a non-working radio module if the DHCP server is located at a remote radio. The DHCP server should be placed at the AP location, if possible.

- **DHCP Server Enable**—Enable/Disable responding to DHCP requests to assign an IP address. [**Disabled/Enabled; Disabled**]
- **DHCP Netmask**—IP netmask to be assigned along with the IP address in response to a DHCP request. [**0.0.0.0**]
- **DHCP Starting Address**—Lowest IP address of the range of addresses to be provided by this device. [**0.0.0.0**]
- **DHCP Ending Address**—Highest IP address in the range of addresses to be provided by this device. A maximum of 256 addresses is allowed in this range. [**0.0.0.0**]
- **DHCP DNS Address**—Domain Name Server address to be provided by this service.
- **DHCP WINS Address**—Windows Internet Naming Service server address to be provided by this service.

3.4.10 SNTP Server Configuration
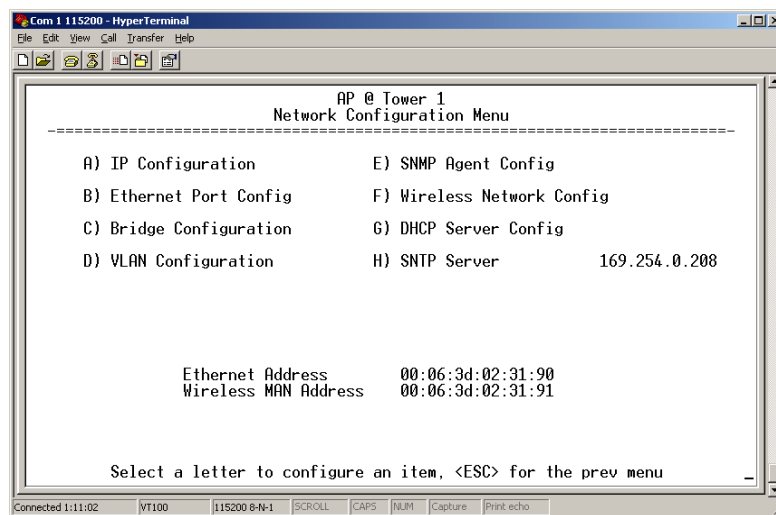
Figure 3-22. SNTP Server Entry (on Network Configuration Menu)

When **SNTP Server** is selected (item H), the area to the right of the parameter becomes active, allowing you to enter a valid SNTP server address. Press the Return key to make the address entry active.

3.5 RADIO CONFIGURATION

There are two primary data layers in the transceiver network—radio and data. Since the data layer is dependent on the radio layer working properly, configuration of the radio items should be reviewed and set before proceeding. This section explains the *Radio Configuration Menu*, (Figure 3-23 for AP, Figure 3-24 for Remote).

3.5.1 Radio Configuration Menu
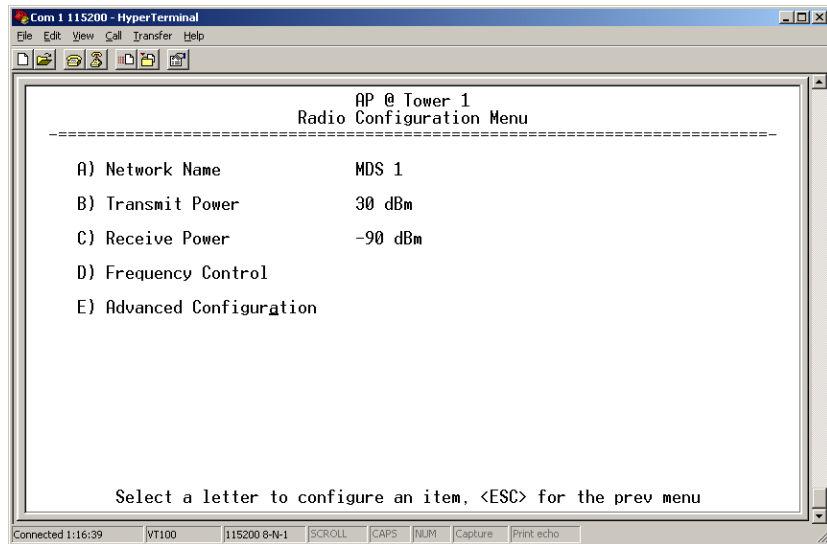
Figure 3-23. Radio Configuration Menu
(From Access Point)
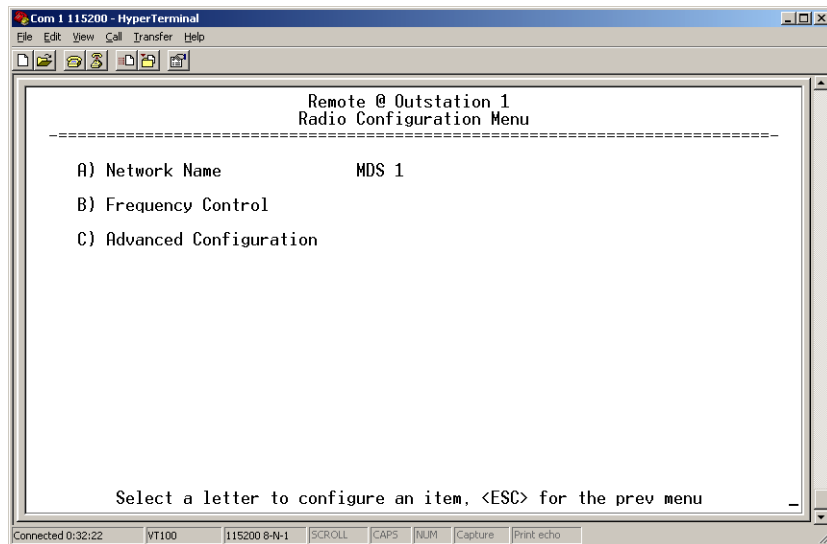
Figure 3-24. Radio Configuration Menu
(From Remote Unit)

- **Network Name**—The user-defined name for the wireless network. [**Any 40 character string; mdsmercuryany**]

- **Transmit Power** (AP Only)—Sets/displays RF power output level in dBm. Setting should reflect local regulatory limitations and losses in antenna transmission line. (See *"How Much Output Power Can be Used?"* on Page 116 for information on how to calculate this value.) [**20–30; 30**]

- **Receive Power** (AP Only)—View/set the receiver's Automatic Gain Control (AGC) setting for the expected strength of incoming signals from Remotes. This setting indicates at what level (in dBm) the AP wants to hear the Remote stations. A setting of -70 would set the AP receiver's gain to a relatively low level, while a setting of -85 would be a comparatively high gain setting. [**-100 to -20; -75**]

- **Frequency Control**—Brings up a submenu where frequency mode bandwidth, channel and other parameters may be viewed or set as described in *Frequency Control Menu* below.

- **Advanced Configuration**—Brings up a submenu where modulation, protection/hysteresis margins, data compression, ARQ settings and other parameters may be viewed or set as described in *Advanced Configuration Menu* on Page 56.

3.5.2 Frequency Control Menu
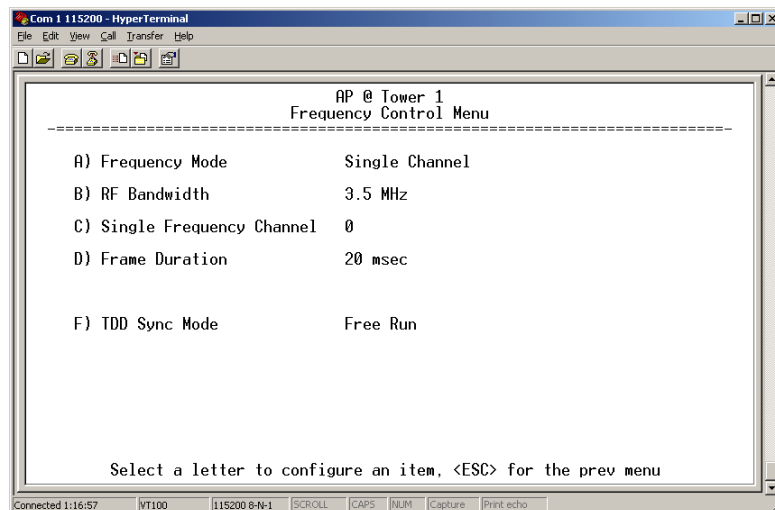
Figure 3-25. Frequency Control Menu

- **Frequency Mode**—The unit can operate on one selected frequency or frequency hop. Remotes have the option of using a static hopping configuration or using the AP locations file to select an AP and perform hand-offs.
  [**Static Hopping, Hopping with Hand-offs, Single Channel; Single channel**]

- **RF Bandwidth**—Selects the RF operating bandwidth of the radio. The setting must match the hardware configuration of the unit, which can be determined by viewing the "CONFIG" number on the label at the bottom of the radio. 1.75 MHz units will have a Configuration string starting with "HGA/R9N1", and 3.5 MHz units will have a string starting with "HGA/R9N3"
  [**1.75MHz, 3.5MHz**]

- **Single Frequency Channel**—The RF frequency that the integrated radio will operate on when in single frequency (non-hopping) mode. [**0 to 6 for 3.5-MHz, 0 to 13 for 1.75-MHz; 0**].

- **Frame Duration**—Defines the over-the-air media access control framing. [**5, 8, 10, or 20 msec; 20 msec**]
- **TDD Sync Mode**—Indicates if the Access Point's transmissions should be synchronized with the GPS timing.
  [**Free Run, GPS Required; Free Run**]
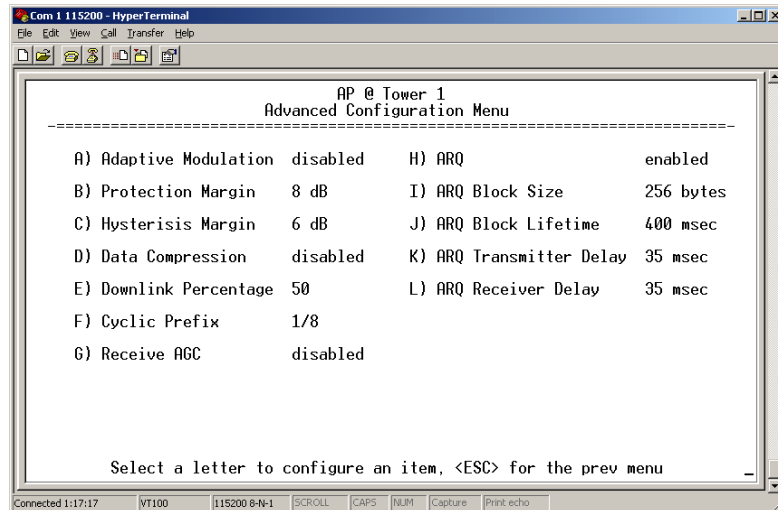
3.5.3 Advanced Configuration Menu

Figure 3-26. Advanced Configuration Menu

- **Adaptive Modulation**—Enables automatic selection of modulation and FEC rate based on SNR. [**enabled, disabled; disabled**]
- **Protection Margin**—A number of decibels of SNR added to the minimum SNR required for a given modulation and FEC rate. [**0-50; 5**]
- **Hysteresis Margin**—A number of decibels of SNR added to the maximum SNR required before shifting to the next higher modulation and FEC rate. [**0-50; 3**]
- **Data Compression**—Enables payload compression. [**enable, disable; disabled**]
- **Downlink Percentage**—The percentage of link time given to downstream traffic [**10-90%; 50%**]
- **Cyclic Prefix**—Amount of additional information added to the over-the-air packets to mitigate the effects of channel interference. [**1/4, 1/8, 1/16,1/32; 1/16**]
- **Receive AGC**—Enables additional Automatic Gain Control (AGC) hardware in the transceiver. [**enable, disable; disabled**]
- **ARQ**—Enables the Automatic Repeat Request function. [**enable, disable; enabled**]
- **ARQ Block Size**—ARQ is applied to payload data in blocks of this size. [**4–2040; 256**]
- **ARQ Block Lifetime**—ARQ blocks are valid for this length of time. [**0–655; 400**]

- **ARQ Transmitter Delay**—The length of time the ARQ transmitter waits before repeating an unacknowledged packet.
[**1–655; 35**]
- **ARQ Receiver Delay**—The length of time the ARQ receiver waits before repeating an unacknowledged packet. [**1–655; 35**]

3.5.4 Security Configuration

The security features of the transceiver are grouped into four major categories and are accessible from the Security Configuration Menu (see Figure 3-27). These categories are:

Device Security—Contains settings for controlling access to the radio itself for configuration and management.

Wireless Security—Controls how and when radios communicate with each other, as well as how data traffic is handled.

RADIUS Configuration—This section deals with authentication and authorization using a central server (RADIUS Configuration)

Manage Certificates—Allows setting of certificate types, download paths and TFTP parameters.
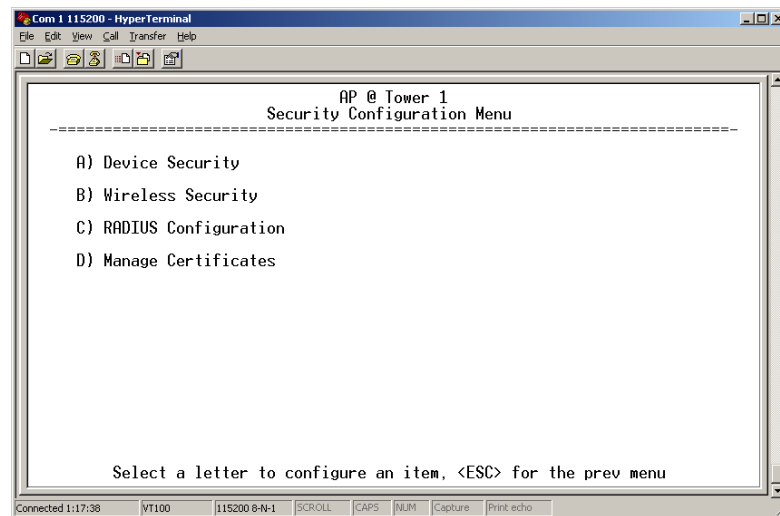

Figure 3-27. Security Configuration Menu

Selecting any of the Security Configuration Menu items causes a submenu to appear where settings may be viewed or changed. Examples of these screens and more detailed descriptions of their contents are provided below.

.

Device Security Menu

The Device Security Menu (Figure 3-28) controls how the radios can be accessed either locally or remotely for configuration and management.
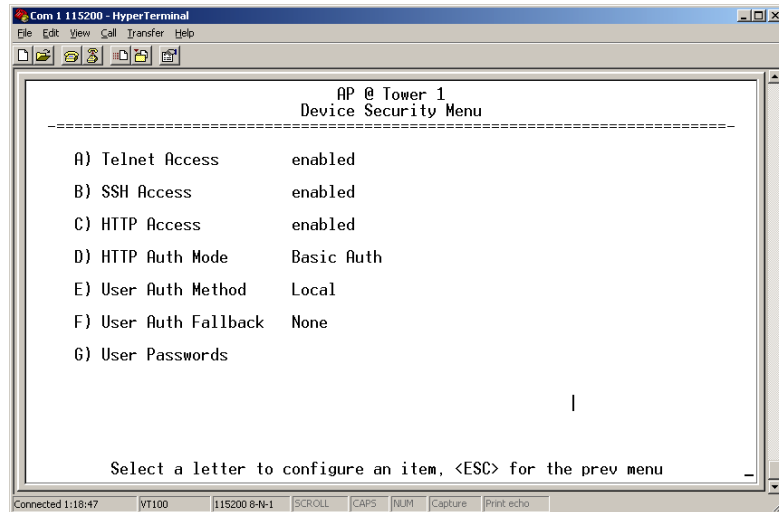
Figure 3-28. Device Security Menu

- **Telnet Access**—Controls telnet access to the transceiver' management system.
  [**enable, disable; disable**]
- **SSH Access**—Controls access to the Secure Shell (SSH) server.
  [**enable, disable; disable**]
- **HTTP Access**—Controls access to the transceiver' management system via the web server. [**enable, disable; enable**]
- **HTTP Auth Mode**—Selects the mode used for authenticating a web user. [**Basic Auth, MD5 Digest; Basic Auth**]
- **User Auth Method**—View/set the method of authentication for users. [**Local, Radius; Local**]
- **User Auth Fallback**—View/set method of authentication to use if RADIUS is unavailable. [**None, Local; None**]
- **User Passwords**—Allows changing of Administrative and Guest passwords. When selected, a new screen appears (Figure 3-29).

User Passwords Menu

Figure 3-29. User Passwords Menu

To change the Administrator or Guest password, select the appropriate menu item (A or B) and a flashing cursor appears to the right. From here, you simply type the new password, which can be any alpha-numeric string up to 8 characters long. The change is asserted when the Return key is pressed.
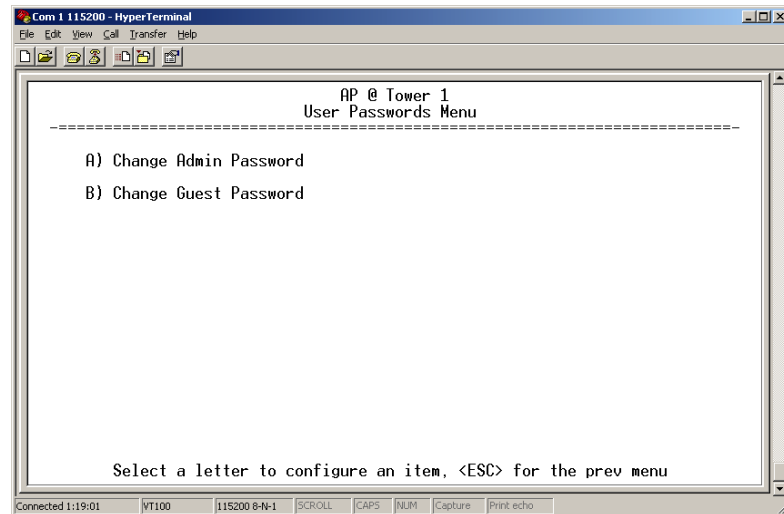
- **Change Admin Password**—Allows a new password to be set
  [**any alpha-numeric string up to 8 characters; admin**]
- **Change Guest Password**—Allows a new password to be set.
  [**any alpha-numeric string up to 8 characters; guest**]

TIP: For enhanced security, consider using misspelled words, a combination of letters and numbers, and a combination of upper and lower case letters. Also, the more characters used (up to eight), the more secure the password will be. These strategies help protect against sophisticated hackers who may use a database of common words (for example, dictionary attacks) to determine a password.

Wireless Security Menu

The features in the Wireless Security menu (Figure 3-30) control the communication of data across the wireless link. The radios can be authenticated locally via a list of authorized radios, or remotely via a centralized RADIUS server. RADIUS is a centralized authentication mechanism based on standards.
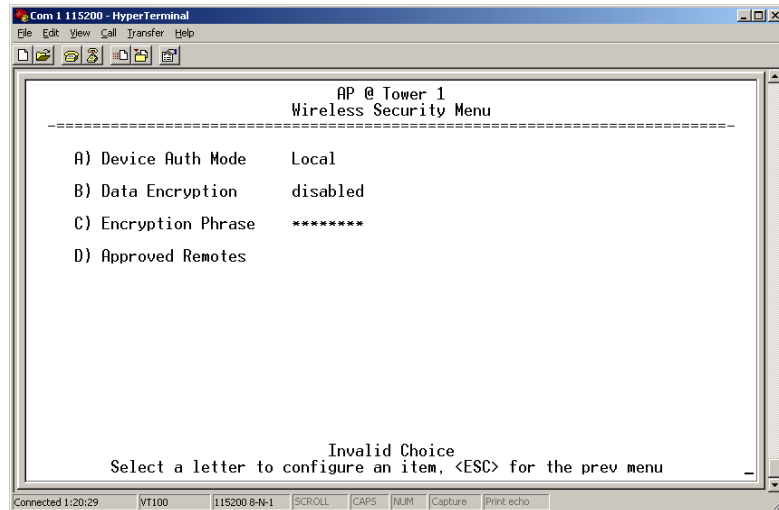
Figure 3-30. Wireless Security Menu

- **Device Auth Mode**—View/set the method of authentication of the device. [**None, Local, IEEE 802.1X; None**]
- **Data Encryption**—Controls AES-128 bit encryption of the over-the-air payload data. [**enable, disable; disabled**]
- **Encryption Phrase**—View/set the phrase used to generate encryption keys. [**any alpha-numeric string of 5 to 40 characters; <empty>**]
- **Approved Remotes**—Launches a submenu where approved Remotes may be viewed, added, or deleted.

Local Authentication—Approved Remotes/Access Points List Submenu

Setting the **Device Auth Mode** to **Local** forces the transceiver to check the *Approved AP List* before a radio link can be established. In the case of a Remote, the AP must be in the *Approved Access Points List* before it accepts the beacon as being valid. In the case of an AP, a Remote must be in the *Approved Remotes List* to be granted authorization. Before enabling this option, at least one entry must already exist in the *Approved AP/Remotes List*.

This menu is the same for both Access Points and Remotes and the names change to reflect their mode.

This section covers the authentication settings needed for the radios to access the RADIUS server, which is used for Device Level Security and for Wireless Access Security. MDS does not provide the RADIUS server software.

Operation of Device Authentication

Device authentication forces the radio to authenticate before allowing user traffic to traverse the wireless network. When Device Security is configured to use RADIUS as the Authentication Method, Remote radios need three types of certificates: public (client), private, and root

(Certificate Authority). These files are unique to each Remote radio and need to first be created at the server and then installed into each unit via TFTP. The certificate files must be in DER format.

Device authentication uses the serial number of each radio as the Common Name (CN) in its certificate and in its RADIUS identity field. Each Access Point *and* Remote radio must be identified/recognized by the RADIUS Server through the Common Name (Serial number) and IP address entries.

NOTE: Consult your RADIUS network administrator for assistance in configuration, or for help with other issues that may arise.

To activate device authentication, select **Device Auth Mode** and set **RADIUS** as the active mode. The behavior of this setting differs depending on whether it is implemented on an Access Point or a Remote transceiver. An explanation of these behaviors is given below:

Access Point: When **Device Auth Mode** is set to **RADIUS**, the AP disassociates all associated Remotes and waits for the RADIUS Server to Authenticate the Remotes before allowing data to be passed from them. When approval is received from the RADIUS Server, data from the Remote is allowed to pass.

Remote: When **Device Auth Mode** is set to **RADIUS**, the Remote halts any data it is passing, and requests Authentication from the RADIUS Server. If accepted, data is allowed to be transmitted.

Operation of User Authentication

When user authentication is set to **Local** or **RADIUS**, you must enter a valid user name and password before being allowed to manage the radio. In **RADIUS** mode both of these fields may be up to 40 characters long. In **Local** mode the user name is **admin** and the password may be up to 8 characters long.

When set to **RADIUS**, *all* logins to the local configuration services are required to be authenticated via the RADIUS Server, including telnet and SSH (Secure Shell) sessions. Authentication must be accepted before access to the radio menu is granted.
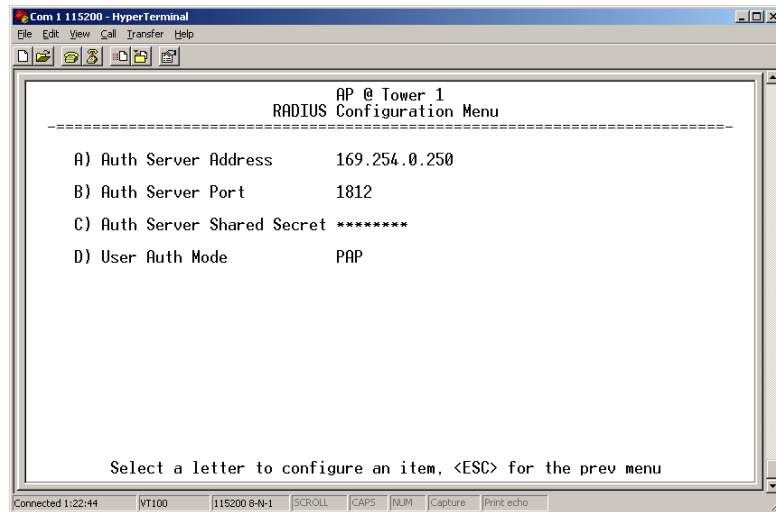
RADIUS Configuration Menu

Figure 3-31. Radius Configuration Menu

- **Auth Server Address**—The IP address of the Authentication (RADIUS) Server. [**any valid IP address; 0.0.0**].
- **Auth Server Port**—The UDP Port of the Authentication (RADIUS) Server. [**1812, 1645, 1812**]
- **Auth Server Shared Secret**—User authentication and Device authentication require a common shared secret to complete a RADIUS transaction. This entry must match the string used to configure the appropriate files on the RADIUS Server. [**<empty>; any alpha-numeric string up to 16 characters**]
- **User Auth Mode**—Authentication algorithm for RADIUS. [**PAP, CHAP, EAP; PAP**]

NOTE: CHAP is more secure than PAP. PAP may display the login password in log files at the RADIUS Server while CHAP will encrypt the login password.

Manage Certificates

Use Certificate generation software to generate certificate files and then install these files into each Remote unit via TFTP. This is done using the Manage Certificates Menu (Figure 3-32).

The certificate files must be in DER format. The Common Name (CN) field in the public certificate file must match the serial number of the unit it will be installed in.
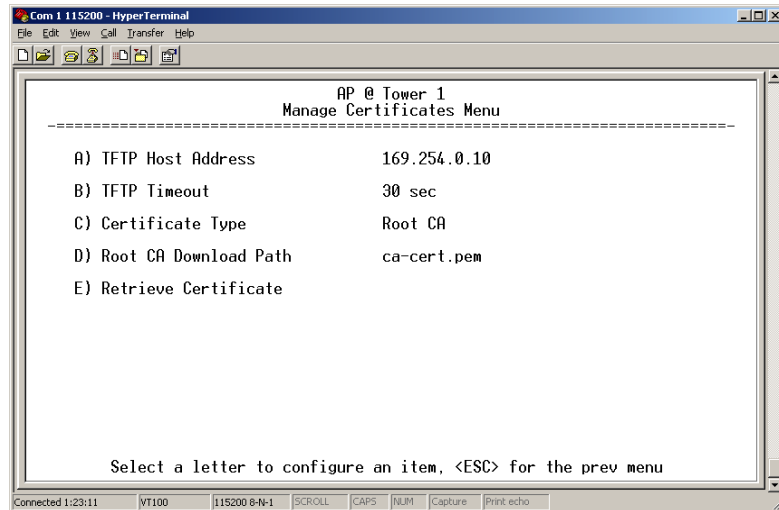
Figure 3-32. Manage Certificates Menu

- **TFTP Host Address**—*(Telnet/Terminal only)*—IP address of the computer on which the TFTP server resides. This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions. [**Any valid IP address; 127.0.0.1**].

- **TFTP Timeout**—should be set appropriately according to the layout of the network.

Three certificate files (Root CA, Client, and Private Key) must be present in *each* of the Remote radios. Use the commands described below to install these files into each Remote radio:

- **Certificate Type**—Selects one the three certificate file types mentioned above. [**Root CA, Client, Private Key; Root CA**]

- **Root CA Download Path**—Specifies the software path for downloading certificates.

- **Retrieve Certificate**—Initiates the retrieval of the certificate file from the storage location. A successful installation issues a **Complete** status message.

NOTE: It is *imperative* that the three certificate files are installed correctly into the Remote radio, in their respective file types. If they are not, it will render the Remote un-authenticated for data traffic. Consult your RADIUS network administrator if issues arise.

3.5.5 Redundancy Configuration (AP Only)

For operation in protected (redundant) mode, an AP must be in a Packaged P23 enclosure with a backup radio. See MDS publication 05-4161A01 for details. This manual is available under the Downloads tab at www.GEmds.com.

The Redundancy Configuration Menu (Figure 3-33) is where you enable/disable redundancy operation and define the triggers that will cause a switchover.
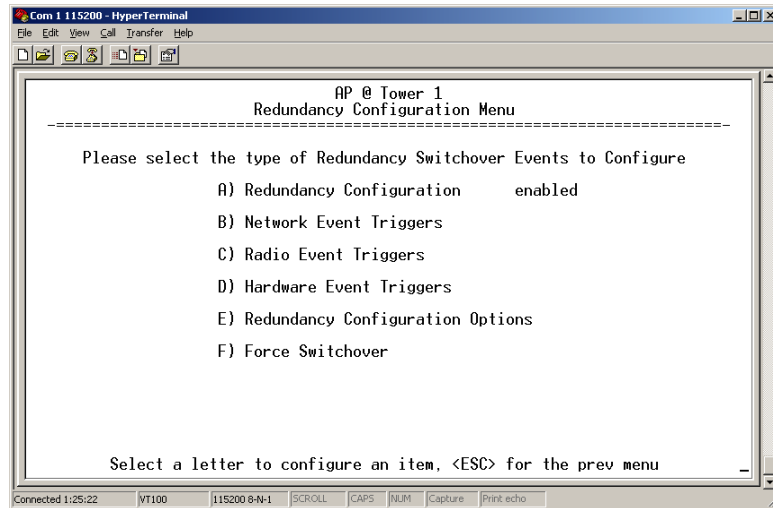

Figure 3-33. Redundancy Configuration Menu (AP Only)

- **Redundancy Configuration**—Enable/disable redundancy switchover for AP. [**enabled, disabled; disabled**]

- **Network Event Triggers**—This selection brings up a submenu (Figure 3-34) where you can set/view the trigger status for Network Events.

- **Radio Event Triggers**—This selection presents a submenu (Figure 3-35) where you can set/view the trigger status for Radio Events, such as a loss of associated Remotes or excessive packet errors.

- **Hardware Event Triggers**—This selection brings up a submenu (Figure 3-36) where you can set/view the trigger status for initialization/hardware errors.

- **Redundancy Configuration Options**—Presents a submenu (Figure 3-37) where you can set the threshold criteria for declaring an error event.

- **Force Switchover**—Selecting this option forces a manual (user initiated) switchover to the backup AP. The "challenge question" **Are you sure? (y/n)** is presented to avoid an unintended switchover. To invoke the change, press the letter **y** followed by the Enter key.

Network Events Triggers Menu
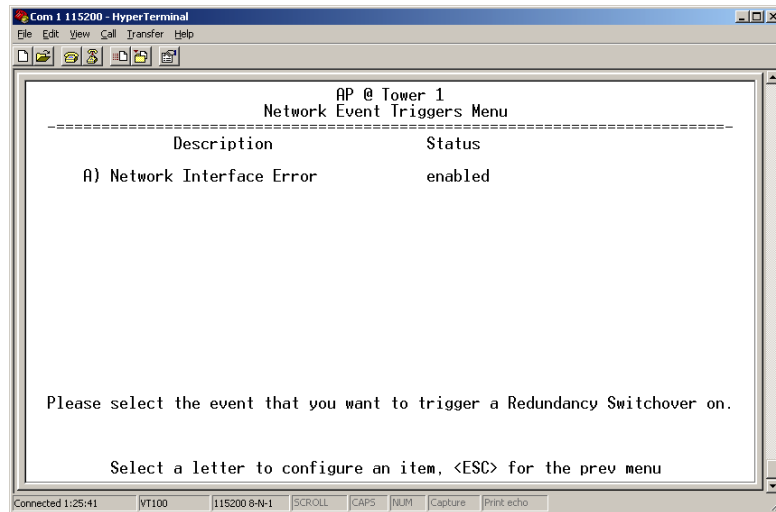
Figure 3-34. Network Events Triggers Menu

- **Network Interface Error**—The setting of this menu item determines whether or not a network interface error will cause redundancy switchover. [**enabled, disabled; disabled**]

Radio Event Triggers
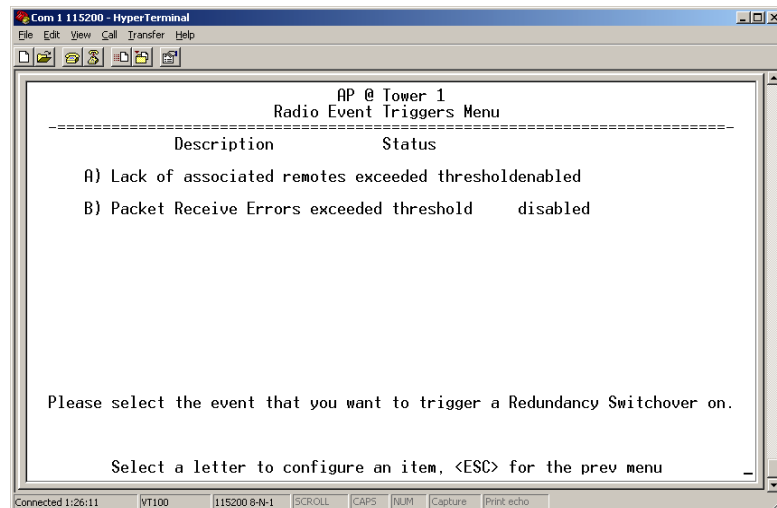
Figure 3-35. Radio Event Triggers

- **Lack of associated remotes exceeded threshold**—This setting determines whether or not a switchover occurs when a lack of associated Remote units exceeds the time period set in Figure 3-38 on Page 67. [**enabled, disabled; disabled**]
- **Packet Receive Errors exceeded threshold**—This setting determines whether or not a switchover occurs when the number of Packet Receive errors exceeds the number set in Figure 3-39 on Page 67. [**enabled, disabled; disabled**]

Hardware Event Triggers
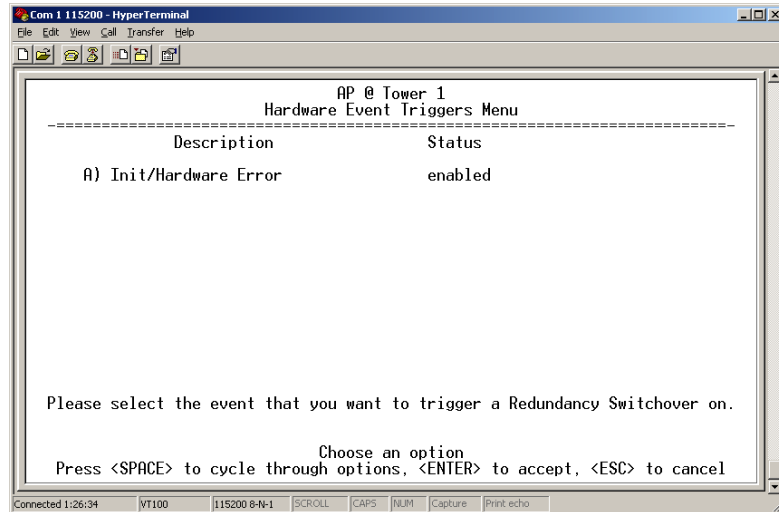
Figure 3-36. Hardware Event Triggers

- **Init/Hardware Error**—This setting determines whether or not an initialization or hardware error will result in a redundancy switchover. [**enabled, disabled; disabled**].

Redundancy Configuration Options Menu

This menu (Figure 3-37) is a gateway for setting the thresholds for the Lack of Associated Remotes and Packet Receive Errors. Selecting either item presents a submenu where settings can be viewed or changed.
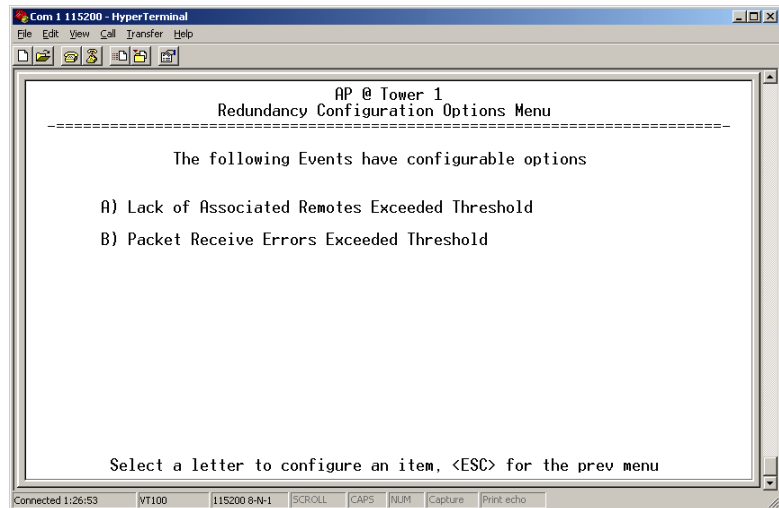
Figure 3-37. Redundancy Configuration Options Menu

- **Lack of Associated Remotes Exceeded Threshold**—This selection presents a submenu (Figure 3-38) where you can view or change the time period allowed for a lack of associated Remotes.

- **Packet Receive Errors Exceeded Threshold**—This selection presents a submenu (Figure 3-39) where you can view or change the maximum allowable number of receive errors.

Lack of Associated Remotes Exceeded Threshold Menu
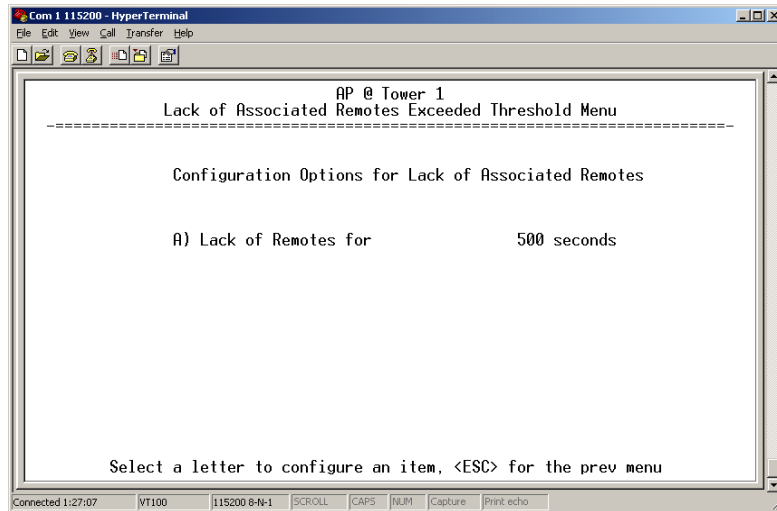
Figure 3-38. Lack of Associated Remotes Exceeded Threshold Menu

- **Lack of Remotes for**—Select this item to change the time setting (in seconds) for a lack of associated Remotes. When there are no associated Remotes for a period exceeding this time, a redundancy switchover occurs. [**60-500; 500**]

Packet Receive Errors Exceeded Threshold Menu
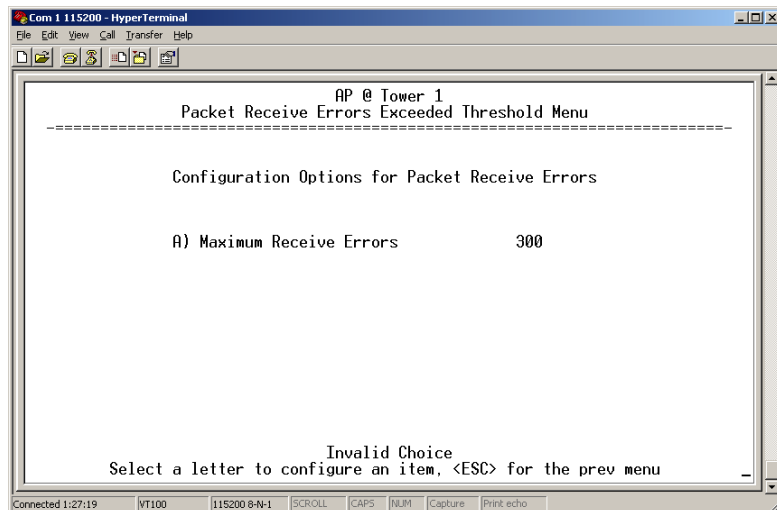
Figure 3-39. Packet Receive Errors Exceeded Threshold Menu

- **Maximum Receive Errors**—Select this item to change the maximum allowable number of receive errors. When the number of errors exceeds this number, a redundancy switchover occurs. [**0-1000; 500**]

3.5.6 GPS Configuration (Remote Only)

This menu allows key settings of the built-in Global Positioning System (GPS) receiver in the Mercury Remote to be viewed or set.
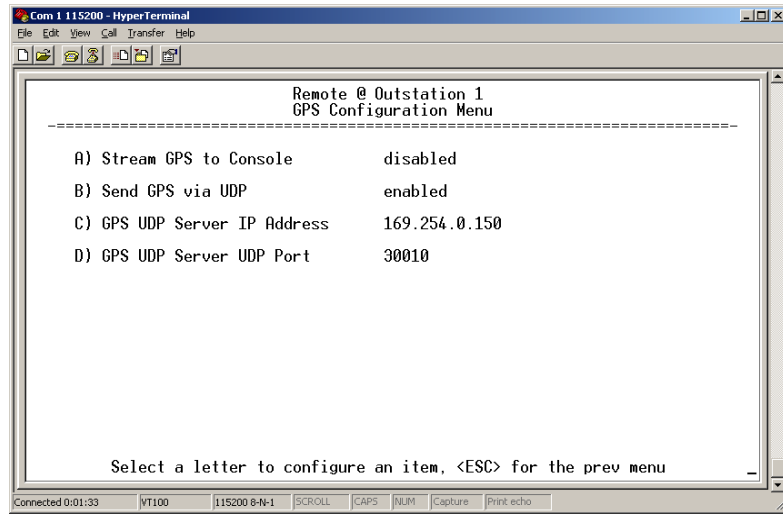
Figure 3-40. GPS Configuration Menu (Remote Only)

- **Stream GPS to Console**—Used to enable/disable streaming of GPS NMEA data to the console port (COM1). [**enabled, disabled; disabled**]
- **Send GPS via UDP**—Used to enable/disable sending GPS NMEA data to a server via UDP. [**enabled, disabled; disabled**]
- **GPS UDP Server IP Address**—Here, the destination address for GPS NMEA UDP packets is specified. [**any valid IP address; 0.0.0.0**].
- **GPS UDP Server UDP Port**—Destination UDP port for GPS NMEA UDP packets. [**valid UDP port number; 0**]

3.5.7 Performance Information Menu

The Performance Information Menu (Figure 3-41) is the entry point for a series of submenus where transceiver operating status and network performance can be evaluated. The menu can be used as an important troubleshooting tool, or for evaluating changes made to the network configuration or equipment.
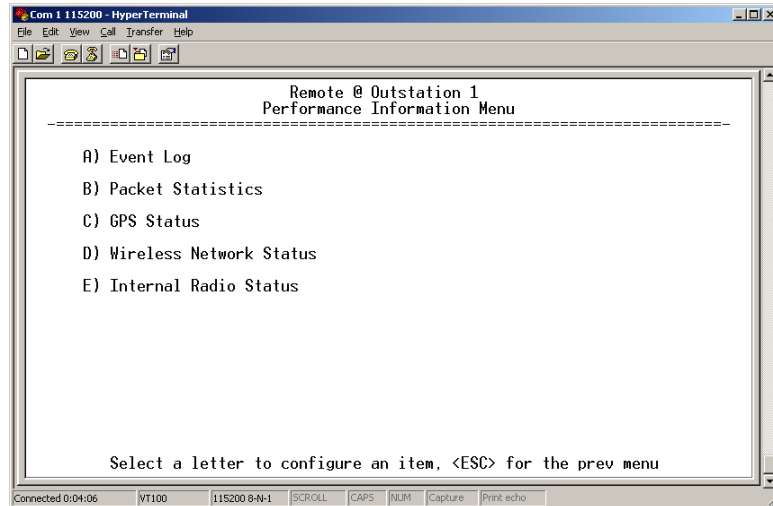
Figure 3-41. Performance Information Menu

- **Event Log**—Access the menu for managing the unit's log of operational activities. (See Figure 3-42 for details.)
- **Packet Statistics**—Multiple radio and network operating statistics. (See Figure 3-44 for details.)
- **GPS Status**—Shows satellite fix status, number of satellites being received, and unit location data. (See Figure 3-45 for details.)
- **Wireless Network Status**—Current association state and MAC address of the Access Point. (See Figure 3-47 for details.)
- **Internal Radio Status** (Remote Only)—Shows connection status, RF parameters, and total FEC count for the unit. (See Figure 3-49 for details.)

Event Log Menu
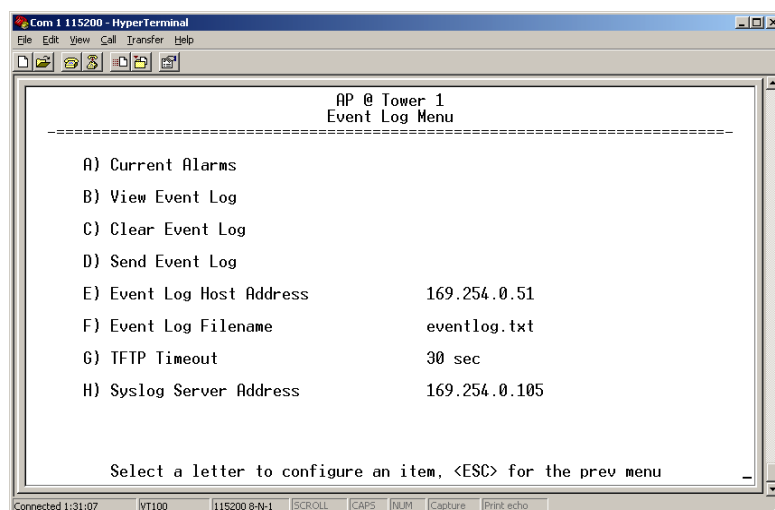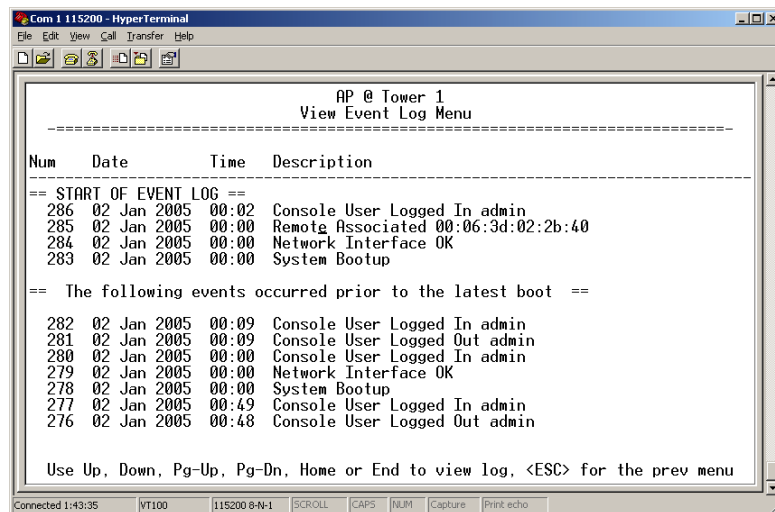
Figure 3-42. Event Log Menu

- **Current Alarms**—Shows active alarms (if any) that are being reported by the transceiver.
- **View Event Log**—Displays a log of radio events arranged by event number, date, and time. (Screen example shown in Figure 3-43).
- **Clear Event Log**—Erases all previously logged events.
- **Send Event Log**—Sends the event log to the server. The challenge question **Send File? y/n** must first be answered before the request proceeds.
- **Event Log Host Address**—Set/display the IP address of the TFTP server. [**any valid IP address; 0.0.0.0**]
- **Event Log Filename**—Set/display the name of the event log file on the TFTP server. [**any valid filename; eventlog.txt**]
- **TFTP Timeout**—Set/display the TFTP timeout setting (in seconds). [**10-120; 30**]
- **Syslog Server Address**—The IP address of the Syslog server. [**any valid IP address; 0.0.0.0**]

View Event Log Menu

Figure 3-43. View Event Log Menu

The transceiver's microprocessor monitors many operational parameters and logs them. Events are classified into four levels of importance, which are described in Table 3-1. Some of these events will result from a condition that prevents the normal of the unit—these are "critical" events. These will cause the unit to enter an "alarmed" state and the PWR

LED to blink until the condition is corrected. All events are stored in the Event Log that can hold up to 8,000 entries**.**

Table 3-1. Event Classifications

Level	Description/Impact
Informational	Normal operating activities
Minor	Does not affect unit operation
Major	Degraded unit performance but still capable of operation
Critical	Prevents the unit from operating

Time and Date   The events stored in the Event Log are time-stamped using the time and date of the locally connected device. Remote units obtain this information from the Access Point when they associate with it. The Access Point obtains the time and date from a Time Server. This server can generally be provided by a standard Windows PC server SNTP application. In the absence of the SNTP services, the user must manually enter it at the Access Point. (See *"Device Information"* on Page 41 for SNTP server identification.) The manually set time and date clock is dependent on the unit's primary power. A loss of power will reset the clock to **02 Jan 2005** but will not affect previously stored error events.

Packet Statistics Menu

The transceivers maintain running counters of different categories of events in the Ethernet protocol. The Packet Statistics refer to each Ethernet interface from the perspective of the *radio*.
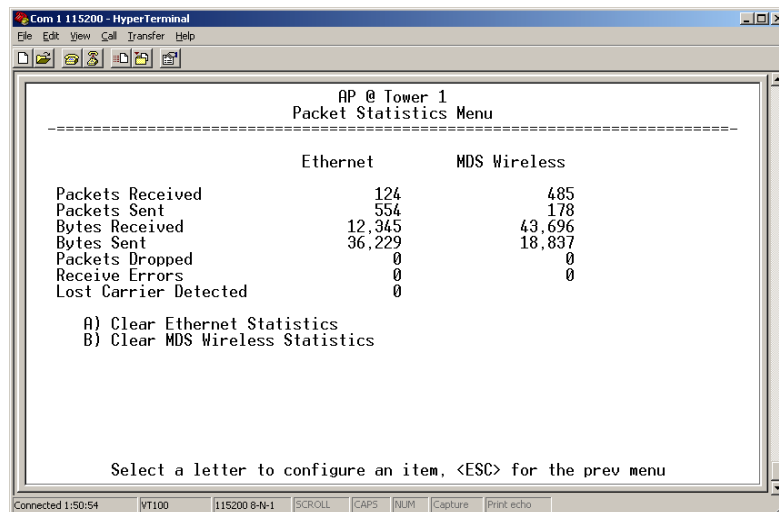
Figure 3-44. Packet Statistics Menu

- **Packets Received**—Over-the-air data packets received by this unit
- **Packets Sent**—Over-the-air data packets sent by this Remote.

- **Bytes Received**—Over-the-air data bytes received by this Remote.
- **Bytes Sent**—Over-the-air data bytes sent by this Remote.
- **Packets Dropped**—To-be-transmitted packets dropped as a result of a lack of buffers in the RF outbound queue.
- **Receive Errors**—Packets that do not pass CRC. This may be due to transmissions corrupted by RF interference.
- **Lost Carrier Detected**—This parameter reports how many times the transceiver has detected a loss of the received RF carrier.
- **Clear Ethernet Statistics**—Resets the statistics counter. The challenge question **Send File? y/n** must first be answered before the request proceeds.
- **Clear MDS Wireless Statistics**—Resets the statistics counter. The challenge question **Send File? y/n** must first be answered before the request proceeds.

GPS Status Menu
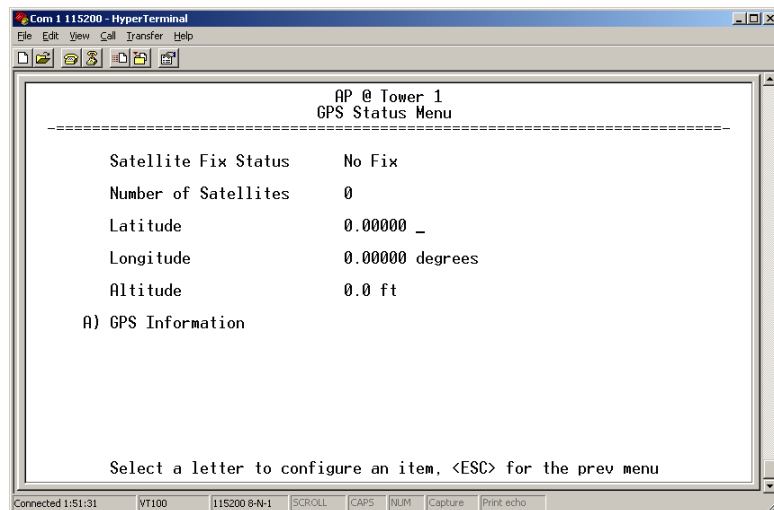
Figure 3-45. GPS Status Menu

- **Satellite Fix Status**—Indicates whether or not the unit has achieved signal lock with the minimum required number of GPS satellites. The transceiver requires a fix on five satellites to achieve Precise Positioning Service (PPS) and four to maintain PPS. [**No Fix, Fix**]
- **Number of Satellites**—Shows the number of GPS satellites being received by the transceiver. Although there are typically 24 active GPS satellites orbiting the Earth twice a day, only a subset of these will be "visible" to a receiver at a given location.
- **Latitude**—Shows the transceiver's latitudinal location (in degrees), based on GPS data received from the satellites.
- **Longitude**—Shows the transceiver's longitudinal location (in degrees), based on GPS data received from the satellites.
- **Altitude**—Shows the transceiver's altitude above sea level (in feet), based on GPS data received from the satellites.

- **GPS Information**—Shows data about the individual satellites being received, including the Pseudo-Random Noise (PRN) code (a unique bit stream for each satellite), the satellite's elevation (in degrees), azimuth (in degrees), and the signal-to-noise ratio of the carrier signal (SNR). Figure 3-46 shows a layout example for this screen.

*GPS Information
Menu*
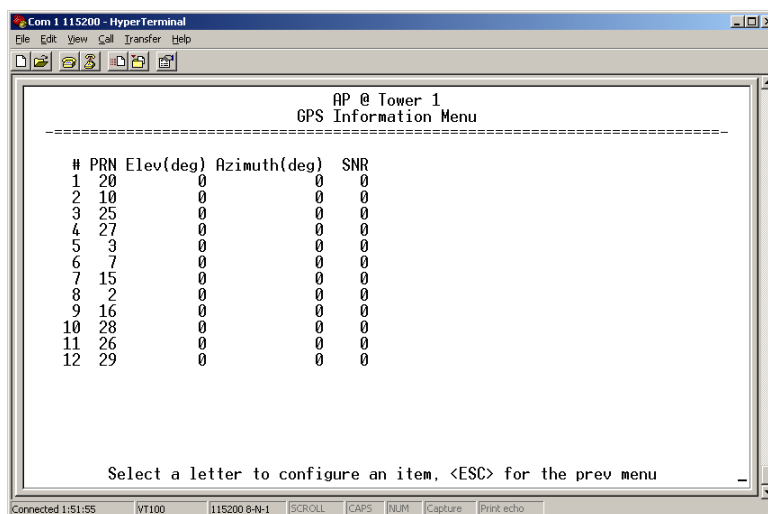
Figure 3-46. GPS Information Menu

Wireless Network Status Menu

The Wireless Network Status screen provides information on a key operating process of the transceiver—the association of the Remote with the Access Point. The following is a description of how this process takes place and as monitored by the menu system.

*The Transceiver's
Association Process*

After the Remote is powered up and finishes its boot cycle, it begins scanning the 900 MHz band for beacon signals being sent out from AP units. If the Remote sees a beacon with a *Network Name* that is the same as its own, the Remote will stop its scanning and temporarily synchronize its frequency-hopping pattern to match the one encoded on the AP's beacon signal. The Remote waits for three identical beacon signals from the AP and then it toggles into a fully synchronized "associated" state. If the Remote does not receive three identical beacons from the Access Point unit within a predetermined time period, it returns to a scanning mode and continues to search for an AP with a matching network name in its beacon.

Under normal circumstances, the association process should be completed within 20 seconds after boot-up. This time can vary depending on the beacon period setting at the AP. See **Beacon Period** description in Section 3.5.1, *Radio Configuration Menu* (beginning on Page 54).

Remote units are always monitoring the beacon signal. If an associated Remote loses the AP's beacon for more than 20 seconds, the association process starts again.
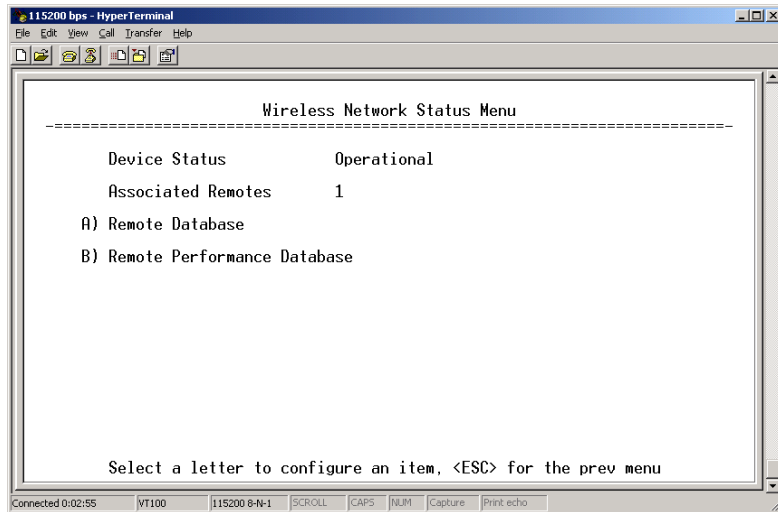
Figure 3-47. Wireless Network Status Menu (AP)
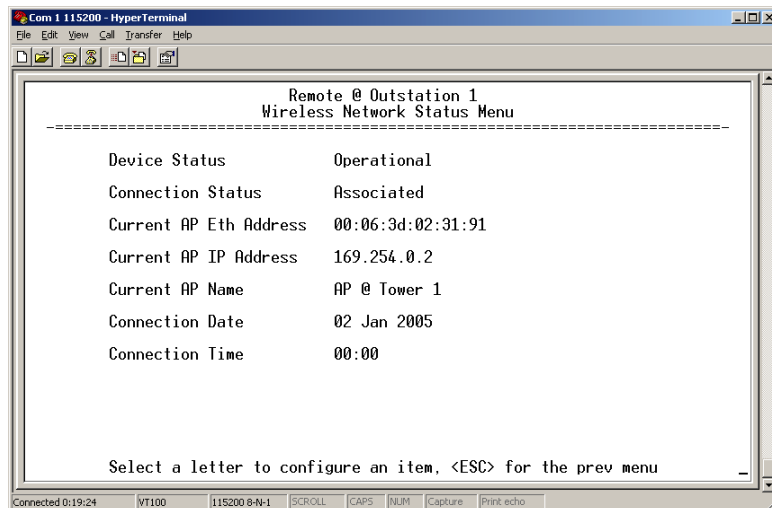
Figure 3-48. Wireless Network Status Menu (Remote)

* **Device Status**—Displays the overall operating condition of the transceiver. [**Operational, Alarmed**]

* **Associated Remotes** (AP Only)—Shows the number of Remote transceivers that have successfully associated with the AP.

* **Remote Database** (AP Only)—Displays a submenu where associated Remotes are listed in table form according to their number, operational state, MAC address, IP address, and name (if assigned).

- **Remote Performance Database** (AP Only)—Displays a submenu where associated Remote performance data is listed in table form. Remotes are presented according to their number, MAC address, RSSI, SNR, downlink type, uplink type and FEC total.
- **Connection Status** (Remote Only)—Displays the current state of the wireless network communication as follows: **Scanning, Ranging, Connecting, Authenticating, Associated,** or **Alarmed**. A complete explanation of these operating states is provided in Table 4-3 on Page 98.
- **Current AP Eth Address**—Displays the Ethernet MAC address of the current AP.
- **Current AP IP Address**—Shows the IP address of the current AP.
- **Current AP Name**—Displays the device name of the current AP.
- **Connection Date**—Shows the date at which the remote connected to the AP. The Remote has been continually connected since this date.
- **Connection Time**—Shows the time at which the remote connected to the AP. The Remote has been continually connected since this time.

Internal Radio Status Menu (Remote Only)
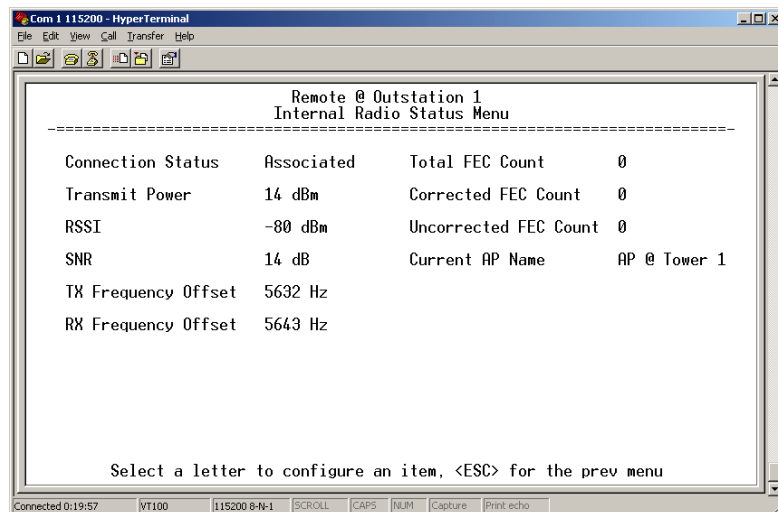
Figure 3-49. Internal Radio Status (Remote Only)

- **Connection Status**—Indicates whether or not the Remote station has associated with an AP. [**Associated, Scanning**]
- **Transmit Power**—Shows the actual RF output (in dBm of the Remote's transmitter. [**0-30 dBm**]
- **RSSI**—Received Signal Strength Indication. This displays the strength of the incoming signal from the AP station (in dBm). The more negative this number, the weaker the signal.

- **SNR**—Signal-to-Noise-Ratio, displayed in dB. This is a measurement of the quality of the incoming signal. It is possible for an incoming signal to be strong, yet be affected by interference or other noise, resulting in a low SNR. This parameter can be used to help determine the actual quality of a signal.

- **TX Frequency Offset**—Shows the RF carrier shift of the Remote's transmitter, measured in Hertz (Hz). The transmitted frequency is continually reviewed and adjusted to agree with what the AP expects to see. This optimization results in more efficient operation, corrects for doppler shift, and results in higher throughput between AP and Remote stations.

- **RX Frequency Offset**—This is a measurement of how far in frequency the Remote's receiver is shifting (in Hz) to accommodate the incoming signal from the AP. Operation

- **Total FEC Count**—This parameter shows the total number of Forward Error Correction (FEC) blocks handled by the radio.

- **Corrected FEC Count**—Displays the number of blocks corrected with FEC by the radio.

- **Uncorrected FEC Count**—Shows the number of blocks uncorrected with FEC by the radio.

- **Current AP Name**—Shows the Device Name of the current AP.

3.5.8 Maintenance/Tools Menu

In the course of operating your network, you may wish to upgrade transceiver firmware to take advantage of product improvements, work with configuration scripts, conduct "ping" tests of your system, or reset operating parameters to factory default settings. All of these tasks are performed using the *Maintenance/Tools Menu* (Figure 3-50). This section explains how to take advantage of these services.

The functions available from this menu are:

- **Reprogramming**— Managing and selecting the unit's operating system firmware resources. *(See "Reprogramming Menu" on Page 77)*

- **Configuration Scripts**—Saving and importing data files containing unit operating parameters/settings. *(See "Configuration Scripts Menu" on Page 81)*

- **Ping Utility**—Diagnostic tool to test network connectivity. (See *"Ping Utility Menu" on Page 84*)

- **Authorization Codes**—Alter the unit's overall capabilities by enabling the built-in resources. *(See "Authorization Codes" on Page 85)*

- **Reset to Factory Defaults**—Configure when remotes retrieve new firmware versions from the associated AP, and whether or not they reboot to the new firmware after receiving the new firmware. (See *"Reset to Factory Defaults" on Page 85*)

* **Radio Test** — A diagnostic tool for testing RF operation. (See *"Radio Test Menu"* on Page 86)
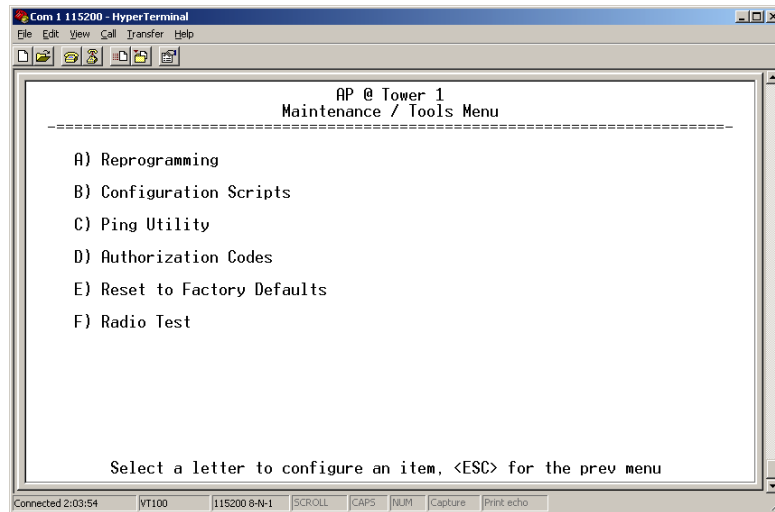
Figure 3-50. Maintenance/Tools Menu

Reprogramming Menu

The transceiver has two copies of the firmware (microprocessor code) used for the operating system and applications. One copy is "active" and the second one is standing by, ready to be used once activated. You can load new firmware into the inactive position and place it in service whenever you desire.

From time-to-time upgrades to the transceiver firmware are offered by the factory. Loading new firmware into the unit will not alter any privileges provided by Authorization Keys and does *not* require the transceiver be taken off-line until you want to operate the unit from the newly installed firmware image.

Firmware images are available free-of-charge at:
www.GEmds.com/service/technical/support

NOTE: Firmware for AP radios is different than for Remotes, and may *not* be interchanged.

NOTE: Always read the release notes for downloaded firmware. These notes contain important information on compatibility and any special steps needed for proper installation.
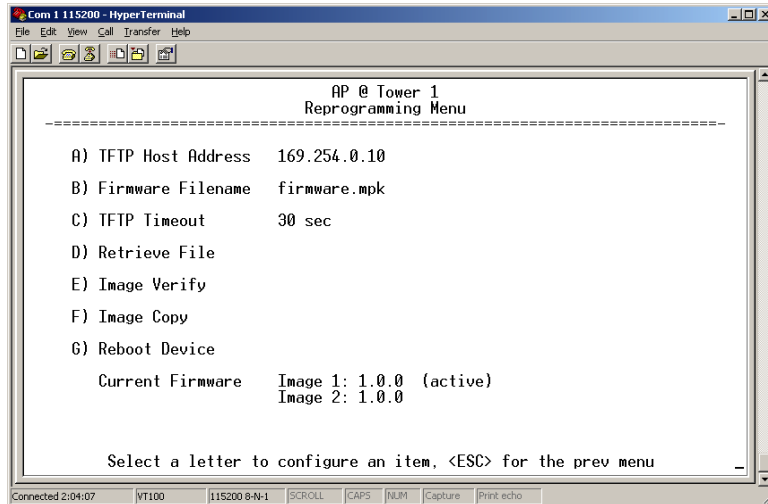
Figure 3-51. Reprogramming Menu

- **TFTP Host Address**—IP address of the host computer from which to get the file. [**Any valid IP address**] This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions.

- **Firmware Filename**—Name of file to be received by the TFTP server. [**Any 40-character alphanumeric string**] Verify that this corresponds to the TFTP directory location. May require sub-directory, for example: **\firmware\mercury\mercury-4_4_0.ipk**.

- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before canceling the file transfer. [**2 to 60 seconds; 10**]

- **Retrieve File**—Initiates the file transfer from the TFTP server. The new file is placed into inactive firmware image. [**Y, N**]

- **Image Verify**—Initiate the verification of the integrity of firmware file held in unit.

- **Image Copy**—Initiate the copying of the active firmware into the inactive image.

- **Reboot Device**—Initiates rebooting of the *transceiver*. This will interrupt data traffic through this unit, and the network if performed on an Access Point. Intended to be used for switching between firmware images 1 and 2.

- **Current Firmware**—Displays the versions of firmware images installed in the transceiver and shows whether Image 1 or Image 2 is currently active.

   NOTE: *Upgrading the Firmware* below for details on setting up the TFTP server.

Upgrading the Firmware

Firmware images are available free-of-charge at:
www.microwavedata.com/service/technical/support

NOTE: AP firmware may *not* be installed in Remote radios, or vice-versa.

To install firmware by TFTP, you will need:

- A PC with a TFTP server running.
- The IP address of the PC running the TFTP server.
- A valid firmware file

The IP address of the radio can be found under the Management Systems' **Starting Information Screen**. (See *"Starting Information Screen"* on Page 38.)

A TFTP server is available on the GE MDS Web site at:
www.GEmds.com/service/technical/support/downloads.asp

TIP: If you do not know your computer's address on a Windows PC, you can use the **RUN** function from the **Start** menu and enter **winipcfg** or **ipconfig** to determine your local PC's IP address.

There are several alternatives to connecting the transceiver for firmware upgrade. Figure 3-52 and Figure 3-53 show two variations. It is essential that all of the equipment be on the same subnet.
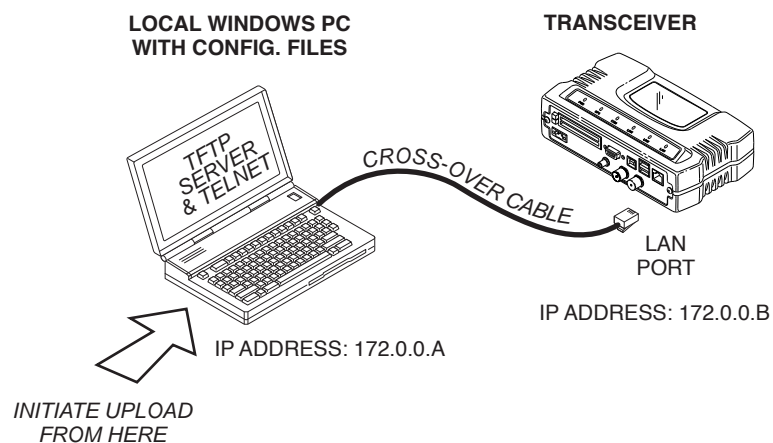
Figure 3-52. Firmware Upgrade Setup—Option 1
(TFTP Server and Firmware File on Same CPU)
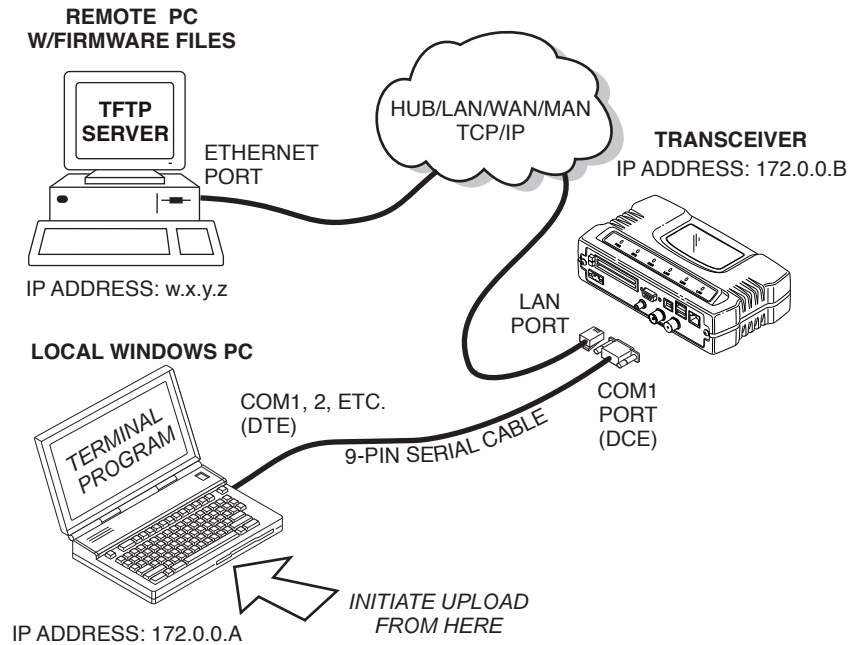
Figure 3-53. Firmware Upgrade Setup—Option 2
(TFTP Server and Firmware File on Remote Server)

NOTE: The LAN and COM1 ports share a common data channel when loading firmware over-the-air. Transferring the radio firmware image file ($\approx$ 3 Mb), may take several minutes depending on traffic between the TFTP server and the transceiver.

Regardless of your connection to the transceiver, loading firmware/configuration files into the unit's flash-RAM is much slower than loading software onto a PC hard drive or RAM.

Upgrade Procedure

To load a new firmware file (**filename.ipk**) into the transceiver, use the following procedure:

1. Launch a TFTP server on a PC connected either directly or via a LAN to the Ethernet port (LAN) of the radio. Point the server towards the directory containing the firmware image file.

2. Connect to the Management System by whichever means is convenient: Browser or Telnet via the LAN, or Terminal emulator via the COM1 port.

3. Go to the MS Reprogramming Menu.
   (**Main Menu>>Maintenance Menu>>Reprogramming Menu**)

4. Fill in the information for the:

   - **TFTP Host Address**—IP Address of server (host computer) running TFTP server.
   - **Retrieve File**—Name of file (**filename.ipk**) to be pulled from the TFTP server holding the firmware file.

---

5. Pull the firmware file through the TFTP server into the transceiver. (**Main Menu>>Maintenance Menu>>Reprogramming Menu>>Retrieve File**)

Status messages on the transfer are posted on the Management System screen.

NOTE: The new firmware image file that replaces the "Inactive Image" file will be automatically verified.

---

6. Reboot the transceiver.
Main Menu>>Maintenance Menu>>Reprogramming Menu>>Reboot Device

7. Test the transceiver for normal operation.

End of Procedure

Error Messages During File Transfers

It is possible to encounter errors during a file transfer. In most cases errors can be quickly corrected by referring to Table 3-2.

Table 3-2. Common Errors During TFTP Transfer

Error Message	Likely Cause/Corrective Action
Invalid File Type	Indicates that the file is not a valid firmware file. Locate proper file and re-load.
File not found	Invalid or non-existent filename on TFTP server
Invalid file path	Invalid or non-existent file path to TFTP server
Timeout	TFTP transfer time expired. Increase the timeout value.
Flash Error	Flash memory error. Contact factory for assistance.
Bad CRC	Cyclic Redundancy Check reporting a corrupted file. Attempt to re-load, or use a different file.
Version String Mismatch	Invalid file detected. Attempt to re-load, or use a different file.
Sending LCP Requests	The PPP server is querying for any clients that may need to connect.
Port not Enabled	The serial port is disabled.

Configuration Scripts Menu

A configuration script file contains all of the settable parameters of a radio that are accessible through the menu interface, with a few exceptions. A configuration script file is in plain text format and can be easily edited in any text program.

Configuration scripts can be helpful in several ways. Three common uses for them are:

- To save "known-good" configuration files from your radios. These can be used for later restoration if a configuration problem occurs, and it is unclear what parameter is causing the issue.
- To facilitate the rapid configuration of a large number of radios.
- To provide troubleshooting information when you contact the factory for technical support. A technician can often spot potential problems by reviewing a configuration file.

How Configuration Files Work

When a configuration script file is downloaded to a radio (**Retrieve File**), the radio executes the parameters as commands and takes the values contained in it. When a configuration script file is uploaded from the radio (**Send**) it contains the current values of the parameters that the radio is configured with. Figure 3-54 below shows the Configuration Scripts Menu.
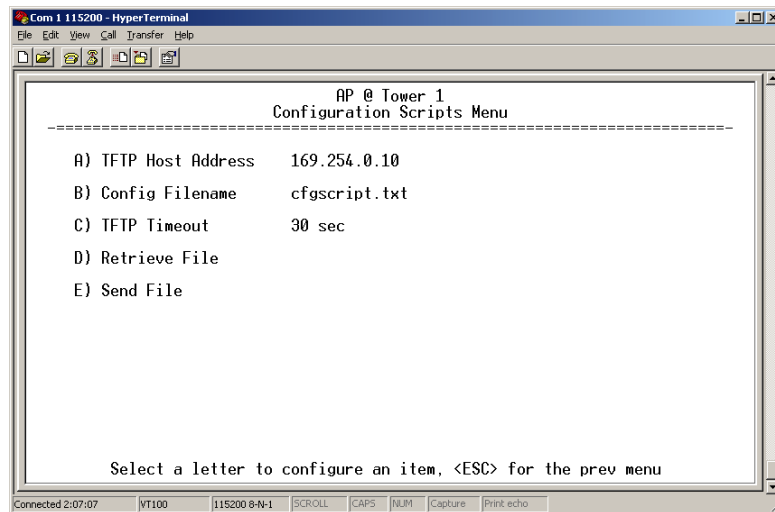
Figure 3-54. Configuration Scripts Menu

- **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 will be in a 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 81* for more information.)

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

- **TFTP Timeout**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer. [**10 to 120 seconds; 10**]
- **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 *Upgrading the Firmware* on Page 78 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.microwavedata.com/service/technical/support**

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 81 to save a copy of the configuration on a PC. Once the file is saved on the PC it can be used as a source to generate modified copies adjusted to match other devices. The configuration files can be modified 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. Other parameters may also be changed as necessary. Each resulting file should be saved with a different name. We recommend using directories and file names that reflect the location of the unit to facilitate later identification.

Table 3-3. 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
Unit 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
- You may include only 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
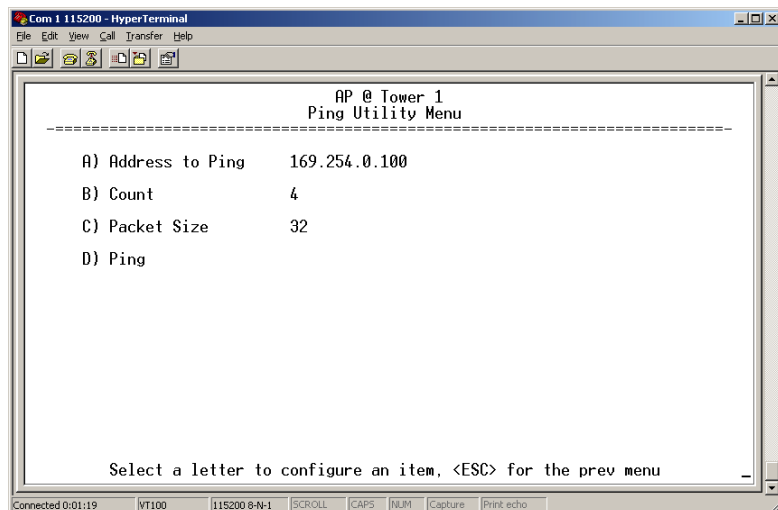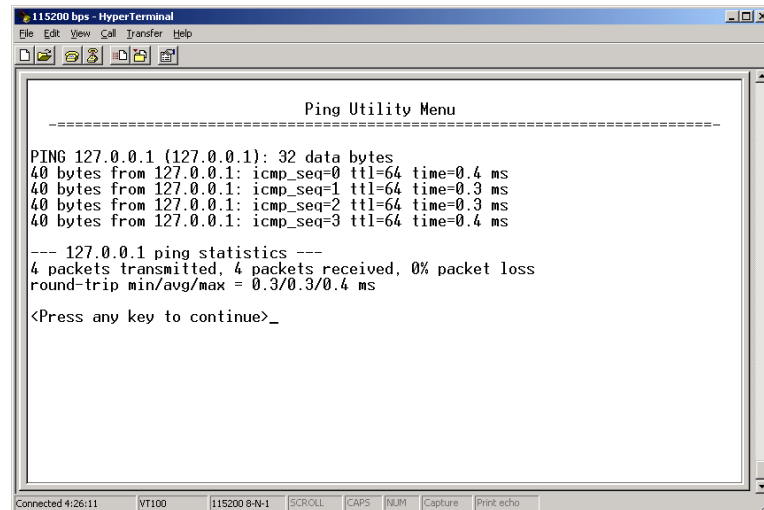
Figure 3-55. Ping Utility Menu

- **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 detailed report of Ping activity (see example in Figure 3-56). Press any key after viewing the results to return to this menu.
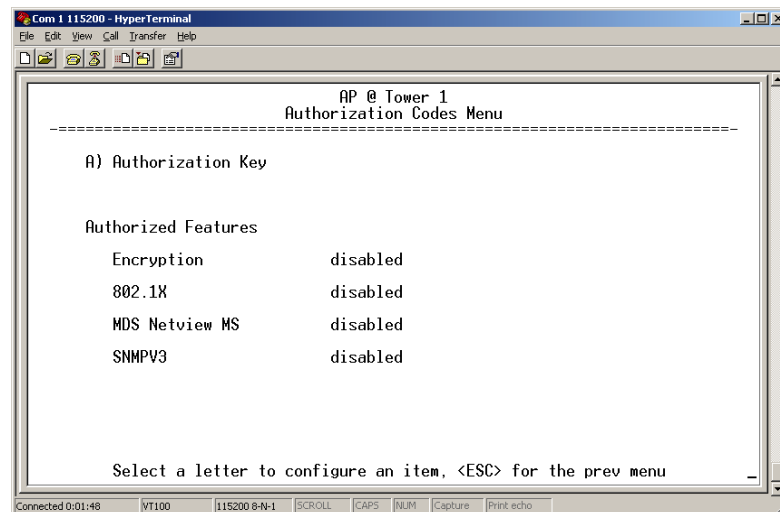
Figure 3-56. Ping Results Screen

Authorization Codes

Figure 3-57. Authorization Codes Menu

- **Authorization Key**—Initiate the entering of an Authorization Key into the transceiver's non-volatile memory.
- **Authorized Features**—List of authorized features available for use with the transceiver. Each item will show **enabled** or **disabled** according to the settings allowed by the Authorization Key that was entered into the radio.

Reset to Factory Defaults

The **Reset to Factory Defaults** selection on the Maintenance/Tools Menu is used to return all configurable settings to those set at the factory prior to shipping. This selection should be used with caution, as any custom settings you have established for your transceiver will be lost and need to be re-entered 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 3-58). 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 any changes being made.)
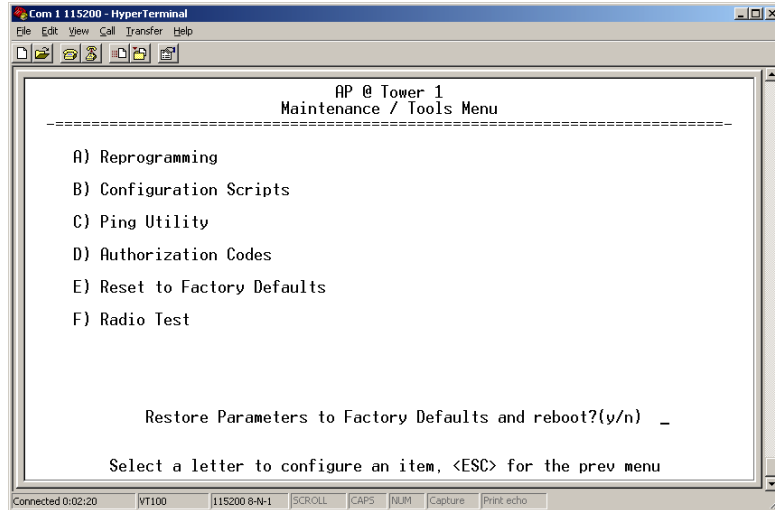
Figure 3-58. Reset to Factory Defaults Action
(Note challenge question at bottom of screen)

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**.
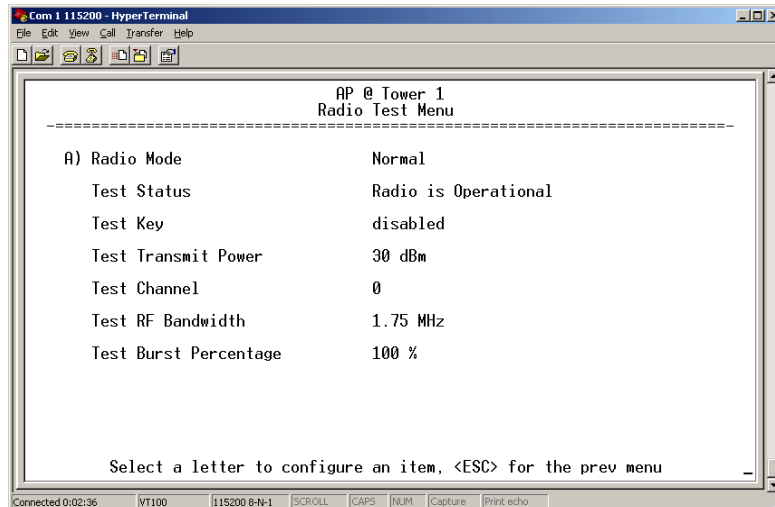
Figure 3-59. Radio Test Menu

NOTE : Use of the 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 and *should only be used for brief measurements.*

- **Radio Mode**—Sets/displays the radio's operating mode. To change the setting, press **A** on the PC's keyboard and use 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 their entries may be set using the Spacebar or with a numeric entry, followed by an Enter keystroke.

- **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. A numerical entry may be made within the allowable range. [**0-30 dBm; 30 dBm**]
- **Test Channel**—Sets/displays the radio's test channel number. A numerical entry may be made 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. A numerical entry may be made within the allowable range.[**0-100%; 100**]

3.6   PERFORMANCE OPTIMIZATION

After the basic operation of the radio has been checked, you may wish to optimize the network's performance using some of the suggestions given in this section. The effectiveness of these techniques will vary 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 correct or improve performance.

As with any wireless system, one of the most important things to check is the antenna system. A properly installed antenna with an unobstructed path to associated stations is highly desirable 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 111 for additional recommendations on antenna systems.

Table 3-4 provides some suggested settings for typical installation scenarios. These settings provide a "starting point" for configuration of AP and Remote units and may require changes to achieve the desired results in a particular situation.

, .

Table 3-4. Standard Recommended Settings for Common Scenarios

For Fixed Locations, where best combination of range and throughput is desired.			AP	Remote	Units	Notes
Radio Configuration	Frequency Control	Network Name	User discretion	User discretion		AP and Remote must match
		Transmit Power	30	N/A	dBm	In most cases, power can be set to +30 dBm and left alone. Setting it lower may help control cell overlap.
		Receive Power	-85	N/A	dBm	Sets AP receiver for high gain.
		Frequency Mode	Static Hopping	Static Hopping		
		Frame Duration	20	20	ms	
		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
		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.
		Downlink%	50	N/A	%	Keep at 50%. Other selections are for future releases.
		Cyclic Prefix	1/16	N/A		Best throughput setting
		Receive AGC				Keep disabled. Reserved for future releases.
		ARQ	Disabled	N/A		
		ARQ Block Size	Enabled	N/A	bytes	
		ARQ Block Lifetime	256	N/A	ms	
		ARQ TX Delay	655	N/A	ms	
		ARQ RX Delay	35	N/A	ms	

For optimum sensitivity (trades off throughput for best possible sensitivity).		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 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 and forces Remote transmit power to be high.

For a mobile system, where hand-offs between APs are required.						
			AP	**Remote**	**Units**	**Notes**
Radio Configuration	**Frequency Control**	**Frequency Mode**	Static Hopping	Hopping w/Handoffs		
Network Configuration	**AP Location Info Config**	**Retrieve Text File**	N/A	AP locations file		AP and Remote must match

3.6.1 Proper Operation—What to Look For

Table 3-5 and Table 3-6 show target performance values for AP and Remote transceivers that are operating properly. These values may be viewed using the built-in menu system by navigating the path shown under each table title.

Table 3-5. 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).
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	200-10,000 Hz	Adjusts to accommodate what is expected by the AP.
RX Freq. Offset	200-10,000 Hz	Adjusts to accommodate what is expected by the AP.
Total FEC Count	Varies	
Corrected FEC Count	Varies	

Table 3-5. Mercury Remote *(Continued)* **Transceiver**
(Performance Information>>Internal Radio Status Menu)

Name	Target Value	Notes
Uncorrected FEC Count	Varies	
Current AP Name	Set as desired	Typically set to reflect the application or system the radio is used in.

Table 3-6. 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	
CoU	Varies	

Additional Considerations for Mobile Operation

The following key points should be considered for all mobile installations:

- Use middleware—The use of middleware in the mobile laptops is highly recommended for better operation of a mobile data system. GE MDS provides middleware from one of the vendors in this market. Contact your factory representative for details.

- Plan your network coverage accordingly—Deploy Access Points so that they provide overlapping coverage to each other. Access Points must use the same network name to enable roaming service.

- Set the RSSI Threshold to -85 dBm—This level is typically used for mobile systems with good performance. Make sure there is overlapping coverage of more than one AP to provide a good user experience and continuous coverage.

- At Every AP Radio, the following settings should be reviewed when providing service to mobile remotes:

  - **TDD Sync**—Must be set to **GPS Required**.
  - **Pattern Offset**—Each AP should be different. Cell planning is required if there are overlaps.
  - **Hop Pattern**—Setting should be the same on all APs.
  - **Compression** [**disabled**]—Disable radio compression. Data compression is best performed by the middleware running on the mobile laptop PC. Gains in efficiency are made because middleware compresses data at a higher stack level, and it aggregates multiple data frames and streams into a single packet. Compression at the radio level, although highly efficient, works only at the individual packet level.

- Use of space diversity antennas often improves signal reception in mobile applications. See *"Diversity Reception (RX2 Antenna Port)" on Page 115* for more information.

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 will be affected.

When communication problems are found, it is good practice to begin by checking the simple things. Applying basic troubleshooting techniques in a logical progression can identify many problems.

Multiple Communication Layers It is important to remember the operation of the network is built upon 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 are operating 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 may be the cause of the problem. With so many possible parameters to look at and change, a parameter may be incorrectly set, and then what was changed is forgotten.

To help avoid these problems, we recommend creating an archive of the transceiver's profile when your installation is complete in a Configuration File. This file can be reloaded 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 81.

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 case. You should check them first whenever a problem is suspected. Table 2-2 on Page 28 describes the function of each status LED. Table 4-1 below provides suggestions for resolving

common system difficulties using the LEDs, and Table 4-2 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 an alarm condition exists. b. View Current Alarms and Event Log and correct the problem if possible. (See *"Using Logged Operation Events"* on Page 100) c. Blinking will continue 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 the it will not be able to 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 for single-frequency channel (non-hopping) configurations. The lack of a fix may be caused by an obstructed "view" of the satellites or 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 RF at all.

4.1.2 Troubleshooting Using the Embedded Management System

If you have reviewed and tried the items mentioned in Table 4-1 and still have not resolved the problem, there are some additional tools and techniques that can be used. The embedded Management System is a good source of information that may be used remotely to provide preliminary diagnostic information, or may even provide a path to correcting the problem.

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. Enter the Authorization Key at the login prompt as a password.
Remote does not associate; stays in HOPSYNC	a. Verify the AP has sufficiently large number in the "Max Remotes" parameter of the Network Configuration Menu.
	b. Verify the correct MAC address is listed in the "Approved Remotes List" or "Approved Access Points List" of the Security Configuration menu.
Remote only gets to **Connecting**.	Check Network Name and encryption settings
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 unit in the WAN.
Wireless Retries too high.	Possible Radio Frequency Interference—
	a. If omnidirectional antennas are used, consider changing to directional antennas. This will often limit interference to and from other stations.
	b. Try skipping some zones 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.

The following is a summary of how several screens in the Management System can be used as diagnostic tools. For information on how to con-

nect to the Management System See *"STEP 3—CONNECT PC TO THE TRANSCEIVER"* on Page 25.

Starting Information Screen
*(*See *Starting Information Screen* on Page 38*)*

The Management System's "homepage" provides some valuable bits of data. One of the most important is the "Device Status" field. This item tells you if the unit is showing signs of life.

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 will need to 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. If this is a Remote radio, *Associated* means that this unit is associated with an Access Point
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 is 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 may 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, then look at the *Error Log* for possible clues.

If the unit is in an "Alarmed" state and not able to associate with an Access Point unit, then there may be problem with the wireless network layer. Call in a radio technician to deal with wireless issues. Refer the technician to the *RADIO (RF) MEASUREMENTS* on Page 105 for information on antenna system checks.

Packet Statistics Menu
(See Packet Statistics Menu on Page 71)

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 dropped
• Packets sent	• Receive errors
• Bytes received	• Retries
• Bytes sent	• Retry errors

Ethernet Packet Statistics

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

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 may be trouble with radio-frequency interference or a radio link of marginal strength. Review the *RSSI by Zone Screen's* values (Page 86) for zones that are more than 2 dB (decibels) below the average level, and for signal level values that are likely to provide marginal service. For example, an average level is less than –85 dBm during normal conditions with a data rate of 256 kbps.

If the RSSI levels in each zone are within a few dB of each other, but less than –85 dBm, then a check should be made of the aiming of the antenna system and for a satisfactory SWR. Refer to *RADIO (RF) MEASUREMENTS* on Page 105 for information on antenna system checks.

NOTE: For a data rate of 1 Mbps the average signal level should be –77 dBm or stronger with no interference.

Diagnostic Tools
(See Maintenance/Tools Menu on Page 76)

The radio's Maintenance menu contains two tools that are especially useful to network technicians—the Radio Test Menu and the Ping Utility. The Radio Test selection allows for testing RF operation, while the Ping Utility can be used to verify reachability 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 68)

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 "alarmed". 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 will be lost in the absence of primary power, and Alarms will be 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
Informational	Normal operating activities	Flash Memory
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 various 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 69)

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_50_LIMIT	Crossed 50% of Eth Port Rate Limit	rateLimit50(20)
EVENT_75_LIMIT	Crossed 75% of Eth Port Rate Limit	rateLimit75(21)
EVENT_100_LIMIT	Crossed 100% of Eth Port Rate Limit	rateLimit100(22)
EVENT_ADC	ADC output Railed	adcInput(3)
EVENT_AP_NN_CHANGED	Network Name changed at the AP	apNetNameChanged(74)
EVENT_BRIDGE	Network Interface /Error	networkInterface(17)
EVENT_NO_CHAN_CNT	Mismatch in Channel count at AP/REM	ChanCnt(71)

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

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_NO_CHAN	Using Channel hopping but no channels selected	NoChan(23)
EVENT_COMPRESS	Compression setting changed	compressionChanged(76)
EVENT_ENDPOINT	Endpoint Added/Removed (AP Only)	eventEndpoint(67)
EVENT_ETH_LINK_AP*	AP Ethernet Link Disconnected	apEthLinkLost(19)
EVENT_FLASH_TEST	Flash Test Failed	-
EVENT_FPGA	FPGA communication Failed	fpgaCommunication(2)
EVENT_FREQ_CAL	Frequency Not Calibrated	frequencyCal(7)
EVENT_INIT_ERR	Initialization Error	initializationError(18)
EVENT_IPADDR*	IP Address Invalid	ipAddressNotSet(4)
EVENT_IP_CONN(OK)		ipConnectivityOK(75)
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_PLL_LOCK	PLL Not locked	pllLock(10)
EVENT_POWER_CAL	Power Calibrated/Not Calibrated	powerCal(8)
EVENT_POWER_HIGH	RF Power Control Saturated High	rfPowerHigh(13)
EVENT_POWER_LOW	RF Power Control Saturated Low	rfPowerLow(14)
EVENT_REMOTE	Remote Added/ Removed (AP Only)	eventRemote(66)
EVENT_REPETITIVE	The previous event is occurring repetitively	
EVENT_ROUTE_ADD	Manual entry added to Routing table	routeAdded(68)
EVENT_ROUTE_DEL	Manual entry deleted from Routing table	routeDeleted(69)
EVENT_RSSI*	RSSI Exceeds threshold	rssi(11)
EVENT_RSSI_CAL	RSSI Not Calibrated	rssiCal(9)
EVENT_SDB_ERR	Internal Remote/Endpoint database error (AP Only)	sdbError(80)

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

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_SINREM_SWITCH	Eth/Serial mode switch in a Single Remote	sinRemSwitch(70)
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)

* Condition may be corrected by user and alarm cleared.

4.1.5 Correcting Alarm Conditions

Table 4-6 provides insight on the 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
ADC Failure	The ADC always reads the same value (either high or low limit)	Contact factory Technical Services for assistance
AP Ethernet Link	Monitor will check state of Ethernet link and set alarm if it finds the link down	Ethernet link is re-established
Bridge Down	When the Bridge fails to be initialized	Contact factory Technical Services for assistance
Flash Test Failed	Internal check indicates corruption of Flash memory	Contact factory Technical Services for assistance
FPGA Failure	Communication lost to the FPGA	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
MAC Failure	The monitor task reads the LinkStatus from the MAC every second. If the MAC does not reply 10 consecutive times (regardless of what the result is) the CPU assumes the transceiver has lost communication to the MAC.	Contact factory Technical Services for assistance
Network Interface Error	Unit does not recognize the LAN interface	Contact factory Technical Services for assistance

Table 4-6. Correcting Alarm Conditions—Alphabetical Order

Event Log Entry	Generating Condition	Clearing Condition or Action
Network Name Not Programmed	Network name is "Not Programmed"	Change Network Name to something other than "Not Programmed"
PLL Out-of-Lock	The FPGA reports a synthesizer out-of-lock condition when monitored by the CPU.	Contact factory Technical Services for assistance.
Power Control Railed High	Power control can no longer compensate and reaches the high rail	Contact factory Technical Services for assistance
Power Control Railed Low	Power control can no longer compensate and reaches the low rail	Contact factory Technical Services for assistance
RSSI Exceeds Threshold	The running-average RSSI level is weaker (more negative) than the user-defined value.	Check aiming of the directional antenna used at the Remote; or raise the threshold level to a stronger (less-negative) value.

4.1.6 Logged Events
(See Event Log Menu on Page 69)

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 will be shown 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 - AP Hop Parameter Changed	MINOR	Self explanatory
Association Lost - AP's Ethernet Link Down	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
Bit Error Rate Below threshold/Above threshold	INFORM	Self explanatory
Console Access Locked for 5 Min	MAJOR	Self explanatory

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

Event Log Entry	Severity	Description
Console User Logged Out/Logged In	MAJOR	Self explanatory
Country/SkipZone Mismatch	INFORM	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 may be caused by some remotes hearing multiple AP's. This event is expected behavior.
Decryption Error/Decryption OK		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** will appear.
Desired AP IP Addr Mismatch	INFORM	Self explanatory
ETH Rate		Indicates heavy bursts of traffic on the unit's Ethernet port (LAN). This is expected behavior, resulting from the network configuration.
Ethernet Port Enabled/Disabled	INFORM	Self explanatory
Ranging Lost/Established	INFORM	Self explanatory
Connecting Lost/Established	INFORM	Self explanatory
Hop Table Generated/Generation Failed	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
MAC Param Changed		Caused by remotes running in auto data rate mode. Every time the link conditions cause a data rate change, the remote's MAC changes to the new rate and forwards a signal to the AP. This indicates link quality is changing and causing the data rate to adjust accordingly.
Max Beacon Wait Time Exceeded	MAJOR	Self explanatory
Received Beacon - AP is Blacklisted	INFORM	Self explanatory
Received Beacon - Netname Does Not Match	INFORM	Self explanatory
Received Beacon - Valid/Errored	INFORM	Self explanatory

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

Event Log Entry	Severity	Description
Rem Ethernet Link Connected/Disconnected	MAJOR	Self explanatory
Reprograming Complete	INFORM	Self explanatory
Reprograming Failed	MAJOR	Self explanatory
Reprograming Started	INFORM	Self explanatory
Scanning Started	INFORM	Self explanatory
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 are a good practice to perform during the initial installation. The will 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 may interrupt traffic through an established network and should only be performed by a skilled radio-technician in cooperation with the network manager.

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. The impedance match can be checked indirectly by measuring the SWR (standing-wave ratio) of the antenna system. If the results are normal, record them for comparison for use during future routine preventative maintenance. Abnormal readings indicate possible trouble with the antenna or the transmission line that will need to be corrected.

The SWR of the antenna system should be checked before the radio is put into regular service. For accurate readings, a wattmeter suited to

1000 MHz measurements is required. One unit meeting this criteria is the Bird Model 43™ directional wattmeter with a 5J element installed.

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

If the reflected power is more than 10%, check the feedline, antenna and its connectors for damage.

Record the current transmitter power output level, and 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)

NOTE: The Test Mode has a 10-minute timer, after which it will return the radio to normal operation. The Radio Test Mode can be terminated manually by selecting **Test Key>>disabled** on the menu or temporarily disconnecting the radio's DC power.

---

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 ON and OFF. (Enable/Disable)

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 being received 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 usually require some fine-tuning of their bearing to optimize the received signal strength. The transceiver has a built-in received signal strength indicator (RSSI) that can be used to 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 will be displayed by the Management System.

The measurement and antenna alignment process will usually take 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. View and 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>>RSSI by Zone)

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)

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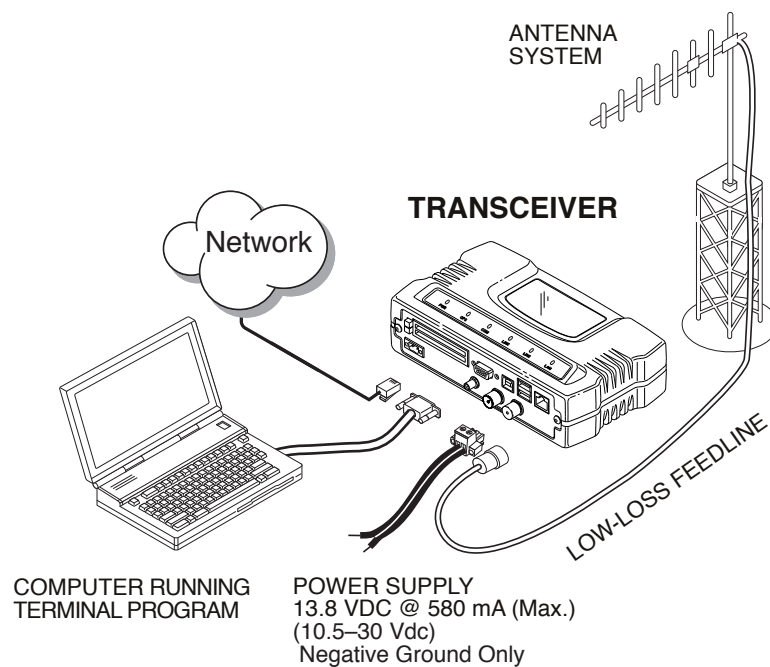
**Figure 5-1. Typical Fixed Remote Installation
With a Directional Antenna**
(Connect user data equipment to any compatible LAN Port)

Unit Dimensions

Figure 5-2 shows the dimensions of the transceiver case and its mounting holes, and Figure 5-3 on Page 112, 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.
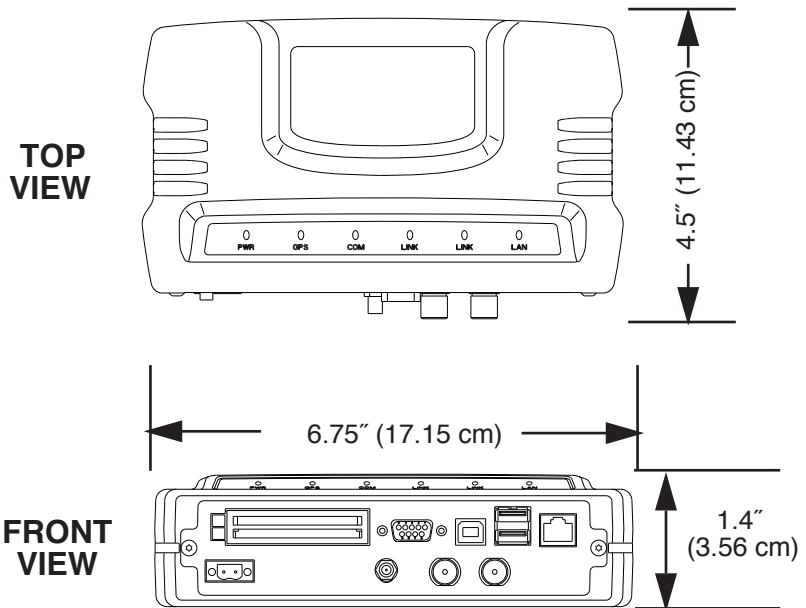
TOP VIEW

4.5″ (11.43 cm)

6.75″ (17.15 cm)

FRONT VIEW

1.4″ (3.56 cm)

Figure 5-2. Transceiver Dimensions
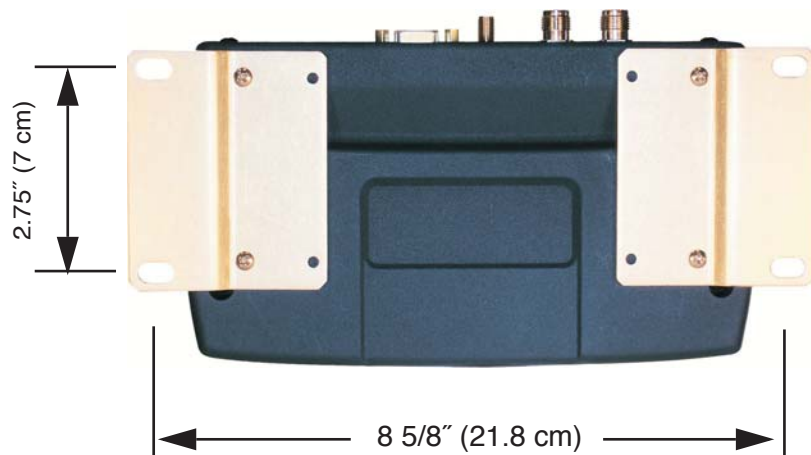
2.75″ (7 cm)

8 5/8″ (21.8 cm)

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

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

- Antenna location that provides as unobstructed a transmission path as possible in the direction of the associated station(s)

These requirements can be quickly determined in most cases. A possible exception is the last item—verifying that an unobstructed transmission path exists. 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 900 MHz band offers many advantages for data transmission services, signal propagation is affected by attenuation from 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 for or stronger will provide acceptable performance in many 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 may occur from time-to-time. RSSI can be measured with a terminal connected to the COM1 Port or with a HTTP browser to the LAN (Ethernet) connector. (See *"Antenna Aiming—For Directional Antennas"* on Page 107 for details.)

5.1.4 Antenna & Feedline Selection

NOTE: The transceiver is a Professional Installation radio system and must be installed by trained professional installers, or factory trained technicians.

This text that follows is designed to aid 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 equipment can be used 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 and mobile Remote stations. 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.
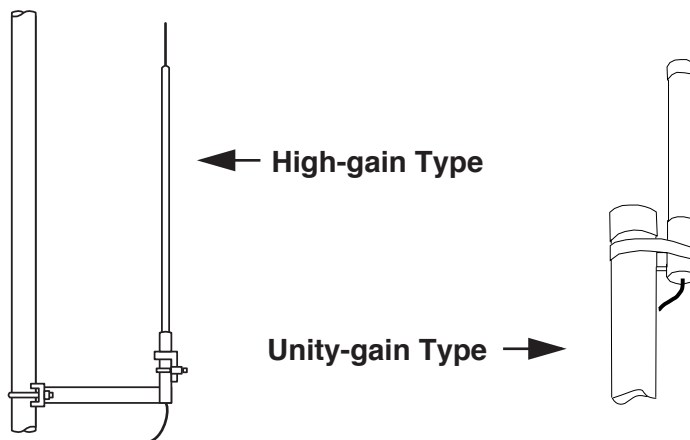
Figure 5-4. Typical Omnidirectional Antennas

At fixed Remote sites a directional Yagi (Figure 5-5) antenna is often used to minimize interference to and from other users. Antennas are available from a number of manufacturers.
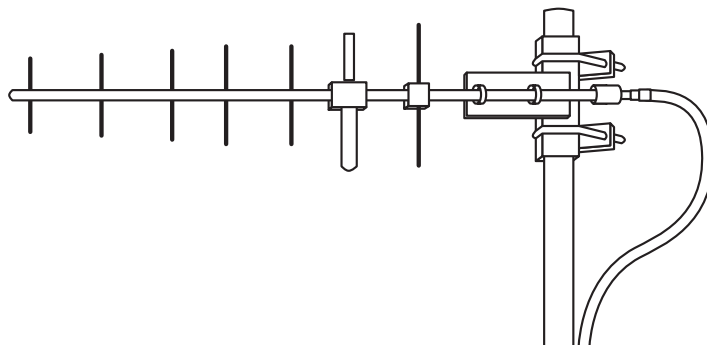

Figure 5-5. Typical Yagi Antenna (mounted to mast)

Diversity Reception (RX2 Antenna Port)

A second 900 MHz antenna may optionally be attached to the transceiver for space diversity reception. Space diversity improves reception of weak or fading signals, such as those that are encountered during mobile operation. This second antenna is connected to the RX2 connector on the radio's front panel. It is for reception only and does not affect the transmitting capabilities of the unit.

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

The choice of feedline used with the antenna should be carefully considered. Poor-quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception. The cable should be kept 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 type such as Type RG-8A/U may be acceptable. Otherwise, we recommend using a low-loss cable type suited for 900 MHz, such as Heliax®.

Table 5-1 lists several types of popular feedlines and indicates the signal losses (in dB) that result when using various lengths of cable at 900 MHz. The choice of cable will depend on the required length, cost considerations, and the amount of signal loss that can be tolerated.

Table 5-1. Length vs. Loss in Coaxial Cables at 900 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, the appropriate changes in loss figures must be made.

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.

Table 5-2. Feedline Length vs. Antenna Gain*
(Required for Regulatory compliance)

Antenna Gain (dBd)	Antenna Gain (dBi)	Minimum Feedline Length (Loss in dB)	EIRP Level @ Min. Length	Maxrad Antenna Part No.
Unity (0 dB)	2.15 dBi	No minimum length	+32.15 dBm	Omni #MFB900
3 dBd	5.15 dBi	No minimum length	+35.15 dBm	Omni # MFB900
5 dBd	7.15 dBi	3.1 meters (1.2 dB)	+35.95 dBm	Omni # MFB900
6 dBd	8.15 dBi	9.1 meters (2.2 dB)	+35.95 dBm	Yagi # BMOY8903
10 dBd	12.15 dBi	24.7 meters (6.15 dB)	+35.25 dBm	Yagi # Z941

*Refer to Table 5-3 for allowable power settings of the transceiver for each antenna type.

NOTE: There is no minimum feedline length required when a 6 dBi gain or less antenna is used, as the EIRP will never exceed 36 dBm which is the maximum allowed, per FCC rules. The transceiver's RF output power may only be adjusted by the manufacturer or its sub-contracted Professional Installer.

The Transceiver's power output is factory set to maintain compliance with the FCC's Digital Transmission System (DTS) Part 15 rules. These rules limit power to a maximum of 8 dBm/3 kHz, thus the Transceiver is factory set to +30 dBm. When calculating maximum transceiver power output, use +30 dBm if the antenna gain is 6 dBi or less (36 dBm ERP). See *How Much Output Power Can be Used?* below for power control of higher gain antennas.

5.1.5 How Much Output Power Can be Used?

The transceiver is normally supplied from the factory set for a nominal +30 dBm RF power output setting; this is the maximum transmitter output power allowed under FCC rules. The power must be *decreased* from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

NOTE: In some countries, the maximum allowable RF output may be limited to less than the figures referenced here. Be sure to check for and comply with the requirements for your area.

5.1.6 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. This can be done 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, this test should be done to verify the predicted results.

The test can be performed 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) and measure the reported RSSI value. (See *"Antenna Aiming—For Directional Antennas"* on Page 107 for details.) If adequate signal strength cannot be obtained, it may be necessary to mount the station antennas higher, use higher gain antennas, select a different site or consider installing 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* section Page 21.

5.1.7 A Word About Radio Interference

The transceiver shares the radio-frequency spectrum with other 900 MHz services and other Part 15 (unlicensed) devices in the USA. As such, near 100% error-free communications may not be achieved 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 care is taken in choosing 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, that minimizes interference to (and from) stations located outside the pattern.

- If interference is suspected from a nearby licensed system (such as a paging transmitter), it may be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in this band, an additional 20 dB of attenuation to interference can be achieved by using horizontal polarization. Another approach is to use a bandpass filter to attenuate all signals outside the 900 MHz band.

- Multiple Access Point units can co-exist in proximity to each other with only very minor interference. Each network name has a different hop pattern. (See *"Protected Network Operation using Multiple Access Points"* on Page 14.) Additional isolation can be achieved by using 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.

Calculating System Gain

To determine the maximum allowable power setting of the radio, perform the following steps:

1. Determine the antenna system gain by subtracting the feedline loss (in dB) from the antenna gain (in dBi). For example, if the antenna gain is 9.5 dBi, and the feedline loss is 1.5 dB, the antenna system gain would be 8 dB. (If the antenna system gain is 6 dB or less, no power adjustment is required.)

2. Subtract the antenna system gain from 36 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 28 dBm.

3. If the maximum transmitter power allowed is less than 30 dBm, set the power to the desired level using the Management System. (**Main Menu>>Radio Configuration>>Transmit Power**)

For convenience, Table 5-3 lists several antenna system gains and shows the maximum allowable power setting of the radio. Note that a gain of 6 dB or less entitles you to operate the radio at full power output –30 dBm.

For assistance in the conversion of dBm to Watts, please see *dBm-WATTS-VOLTS CONVERSION CHART* on Page 120.

Table 5-3. Antenna System Gain vs. Power Output Setting

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (PWR command)	EIRP (in dBm)
Omni 6 (or less)	30	36
Omni 9	27	36
Yagi 12	24	36
Yagi 14	22	36
Yagi 16	20	36

* Most antenna manufacturers rate antenna gain in dBd in their literature. To convert to dBi, add 2.15 dB.

† Feedline loss varies by cable type and length. To determine the loss for common lengths of feedline, see Table 5-1 on Page 115.

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 5-4. dBm-Watts-Volts conversion—for 50 ohm systems

dBm	V	Po	dBm	V	Po	dBm	mV	Po	dBm	µV	Po
+53	100.0	200W	0	.225	1.0mW	-49	0.80		-98	2.9	
+50	70.7	100W	-1	.200	.80mW	-50	0.71	.01µW	-99	2.51	
+49	64.0	80W	-2	.180	.64mW	-51	0.64		-100	2.25	.1pW
+48	58.0	64W	-3	.160	.50mW	-52	0.57		-101	2.0	
+47	50.0	50W	-4	.141	.40mW	-53	0.50		-102	1.8	
+46	44.5	40W	-5	.125	.32mW	-54	0.45		-103	1.6	
+45	40.0	32W	-6	.115	.25mW	-55	0.40		-104	1.41	
+44	32.5	25W	-7	.100	.20mW	-56	0.351		-105	1.27	
+43	32.0	20W	-8	.090	.16mW	-57	0.32		-106	1.18	
+42	28.0	16W	-9	.080	.125mW	-58	0.286				
+41	26.2	12.5W	-10	.071	.10mW	-59	0.251		**dBm**	**nV**	**Po**
+40	22.5	10W	-11	.064		-60	0.225	.001µW	-107	1000	
+39	20.0	8W	-12	.058		-61	0.200		-108	900	
+38	18.0	6.4W	-13	.050		-62	0.180		-109	800	
+37	16.0	5W	-14	.045		-63	0.160		-110	710	.01pW
+36	14.1	4W	-15	.040		-64	0.141		-111	640	
+35	12.5	3.2W	-16	.0355					-112	580	
+34	11.5	2.5W				**dBm**	**µV**	**Po**	-113	500	
+33	10.0	2W	**dBm**	**mV**	**Po**	-65	128		-114	450	
+32	9.0	1.6W	-17	31.5		-66	115		-115	400	
+31	8.0	1.25W	-18	28.5		-67	100		-116	355	
+30	7.10	1.0W	-19	25.1		-68	90		-117	325	
+29	6.40	800mW	-20	22.5	.01mW	-69	80		-118	285	
+28	5.80	640mW	-21	20.0		-70	71	.1nW	-119	251	
+27	5.00	500mW	-22	17.9		-71	65		-120	225	.001pW
+26	4.45	400mW	-23	15.9		-72	58		-121	200	
+25	4.00	320mW	-24	14.1		-73	50		-122	180	
+24	3.55	250mW	-25	12.8		-74	45		-123	160	
+23	3.20	200mW	-26	11.5		-75	40		-124	141	
+22	2.80	160mW	-27	10.0		-76	35		-125	128	
+21	2.52	125mW	-28	8.9		-77	32		-126	117	
+20	2.25	100mW	-29	8.0		-78	29		-127	100	
+19	2.00	80mW	-30	7.1	.001mW	-79	25		-128	90	
+18	1.80	64mW	-31	6.25		-80	22.5	.01nW	-129	80	.1ƒW
+17	1.60	50mW	-32	5.8		-81	20.0		-130	71	
+16	1.41	40mW	-33	5.0		-82	18.0		-131	61	
+15	1.25	32mW	-34	4.5		-83	16.0		-132	58	
+14	1.15	25mW	-35	4.0		-84	11.1		-133	50	
+13	1.00	20mW	-36	3.5		-85	12.9		-134	45	
+12	.90	16mW	-37	3.2		-86	11.5		-135	40	
+11	.80	12.5mW	-38	2.85		-87	10.0		-136	35	
+10	.71	10mW	-39	2.5		-88	9.0		-137	33	
+9	.64	8mW	-40	2.25	.1µW	-89	8.0		-138	29	
+8	.58	6.4mW	-41	2.0		-90	7.1	.001nW	-139	25	
+7	.500	5mW	-42	1.8		-91	6.1		-140	23	.01ƒW
+6	.445	4mW	-43	1.6		-92	5.75				
+5	.400	3.2mW	-44	1.4		-93	5.0				
+4	.355	2.5mW	-45	1.25		-94	4.5				
+3	.320	2.0mW	-46	1.18		-95	4.0				
+2	.280	1.6mW	-47	1.00		-96	3.51				
+1	.252	1.25mW	-48	0.90		-97	3.2				

6 *TECHNICAL REFERENCE*

Contents

6.1 DATA INTERFACE CONNECTORS

Three types of data interface connectors are provided on the face of the transceiver. The first, the LAN Port, is an RJ-45 connector. The second are USB connectors, of which there are two Type-A and one Type-B provided. Finally, COM1 is a DB-9 female interface connector that 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

The transceiver's LAN Port is used 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 below.
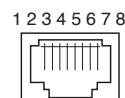
Figure 6-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

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

To connect a PC to the transceiver's COM1 port use 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.
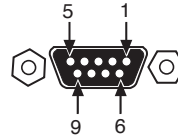
Figure 6-2. COM1 Port (DCE)
(Viewed from the outside of the unit.)

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 FUSE REPLACEMENT PROCEDURE

An internal fuse protects the transceiver from over-current conditions or an internal component failure. It should not be replaced until you are certain you are in a safe (non-flammable) environment.

1. Disconnect the primary power source and all other connections to the unit.

2. Place the radio on its back and remove the four Phillips screws on the bottom cover.

3. Carefully separate the top and bottom covers. There is a flat ribbon cable between the top cover's LEDs and the unit motherboard. You do not need to disconnect the ribbon cable.

4. Locate the fuse and fuse holder on the transceiver's PC board. See Figure 6-3 for details.

5. Loosen the fuse from the holder using a very small screwdriver. Use a small pair of needle-nose pliers to pull the fuse straight up and remove it.

6. Using an Ohmmeter, or other continuity tester, verify the fuse is blown.

7. Install a new fuse by reversing the process.

   Littelfuse P/N: 0454002; 452 Series, 2 Amp SMF Slo-Blo
   GE MDS P/N: 29-1784A03

8. Install the covers and check the transceiver for proper operation.
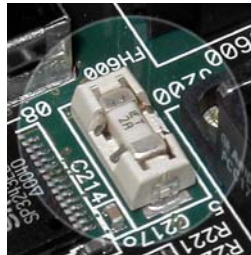
**Figure 6-3.
Internal Fuse and Holder
Assembly**

6.3   SPECIFICATIONS

General

- Raw Bit Rate: from 600 kHz to 12.7 Mbps (see chart below)
- Frequency Band: 902-928 MHz ISM band
- Orthogonal Frequency Division Multiplexing (OFDM)
  - 200 Carriers per Channel
- Range (BPSK/1.75 MHz channel)[1]
  - Typical Fixed Range: 12-15 miles
  - Maximum Fixed Range: 25-30 miles
  - Typical Mobile Range (parked): 3-5 miles, depending on terrain
  - Typical Mobile Range (moving): 2-4 miles, depending on terrain
- 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: 0.1 to 1 watt
- RF Output Impedance: 50 Ohms

- Sensitivity and Data Rate (see chart below):[2]

Modulation (CP=1/16)	3.5 MHz Channel Max. User Throughput (Aggregate)*		1.75 MHz Channel Max. User Throughput (Aggregate)*	
	Sensitivity	Signaling Rate	Sensitivity	Signaling Rate
64 QAM	-77 dBm	12.7 Mbps	-80 dBm	6.35 Mbps
16 QAM	-86 dBm	4.8 Mbps	-89.5 dBm	2.4 Mbps
QPSK	-92 dBm	2.4 Mbps	-95 dBm	1.2 Mbps
BPSK	-95 dBm	1.2 Mbps	-98 dBm	600 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.

Physical Interface

- Ethernet: 10/100BaseT, RJ-45
- Serial: 1,200 – 115,200 bps
  - COM1: RS-232, DB-9F
- Antennas: TX/RX and RX (diversity mode)–TNC connectors, GPS—SMA connector
- LED Indicators: PWR, COM1, LINK, LAN

Protocols

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

GE MDS Cyber Security Suite, Level 1

- Encryption: AES-128 with automatic key rotation.
- 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: 10.5-30 Vdc
- Current Consumption (nominal):

Mode	Power	13.8 Vdc	24 Vdc
Transmit	25 W	1.8 A	1.0 A
Receive	4 W	240 mA	170 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

Agency Approvals

- FCC Part 15.247 (DTS)
- CSA Class 1 Div. 2 Pending (UL 916, UL 1604, CSA C22.2-213-M1987, CSA C22.2-142-M1987)
- IC RSS-210 "Issue 6" (Pending)

1. Typical fixed range calculation assumes a 6 dBd gain Omni-directional antenna on a 100 ft tower at the AP, a 10 dBd gain Yagi on a 25 ft mast at the remote with output power decreased to yield maximum allowable EIRP (36 dBm), a 10 dB fade margin, and a mix of agricultural and commercial terrain with line of sight.

   Typical mobile range calculation assumes a 6 dBd gain Omni on a 100 ft tower at the AP, a 5 dBd gain Omni with 1 watt output power at 6 ft height, a 10 dB fade margin, and 90% reliability with near line-of-sight in a mix of agricultural and commercial terrain. Maximum range achieved with a clear line-of-sight path, and fresnel zone clearance. Actual performance is dependent on many factors including antenna height, blocked paths and terrain.

2. Please note that for best range and performance, mobile data is limited to using a 1.75 MHz channel and BPSK and QPSK modulation schemes.

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.

6.4   NOTES ON SNMP

6.4.1 Overview

The firmware release described in this manual contains major 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. Currently, only MD5 Authentication is supported in the SNMP Agent.
- 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 will be 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 (please 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 don't exchange passwords, but actually exchange *keys* based on passwords. If the Manager changes the Agent's password the Agent doesn't know the new password; just 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 that are being used in order to talk to the Agent. If the Agent's passwords are configured via the Manager, then 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 to talk 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 will be used). These passwords will now be used by the Agent to re-generate keys. The Manager will need to know these passwords in order to talk to the Agent.

- Passwords are currently being 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 being 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 being 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, which are **Fairport** (Auth) and **Churchville** (Priv). The Manager will have to be re-configured to use these new passwords.

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

SNMP Trap	Severity	Description
systemBoot(32)	INFORM	SNR Within threshold/Below threshold
systemReboot(33)	MAJOR	Telnet User Logged Out/Logged In
startScan(34)	INFORM	Reprogramming Started
rxBeaconErrored(35)	INFORM	Received Beacon - Netname Does Not Match
rxBeaconWrongNetworkName (36)	INFORM	Received Beacon - AP is Blacklisted
rxBeaconFromBlacklistAP(37)	MAJOR	Max Beacon Wait Time Exceeded
expectedSync(38)	INFORM	Ranging Lost/Established
hopSync(39)	INFORM	Connecting Lost/Established
snr(41)	INFORM	Scanning Started
ber(42)	INFORM	Bit Error Rate Below threshold/Above threshold
associated(43)	MAJOR	Association Lost/Established
apParmChange(44)	MINOR	Association Lost - AP Hop Parameter Changed
reprogStarted(45)	MAJOR	Reprogramming Failed
reprogComplete(46)	MAJOR	Rem Ethernet Link Connected/Disconnected
reprogFailed(47)	INFORM	Reprogramming Complete
telnetLogin(48)	MAJOR	Telnet Access Locked for 5 Min
httpLogin(49)	MAJOR	HTTP User Logged Out/Logged In
countrySkipZoneMismatch(50)	INFORM	Country/SkipZone Mismatch
desiredAPIPMismatch(51)	INFORM	Desired AP IP Addr Mismatch
eventLogCleared(52)	INFORM	Log Cleared

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

SNMP Trap	Severity	Description
authDemoMode(53)	MAJOR	Auth Demo Mode Expired -- Rebooted Radio/Enabled
keyEntered(54)	MAJOR	Auth Key Entered - Key Valid/Key Invalid
apEthLinkDown(55)	MAJOR	Association Lost - AP's Ethernet Link Down
noBeacons(56)	MAJOR	MAC Param Changed
apNotApproved(57)	MAJOR	Current AP No Longer Approved
netnameChanged(58)	MAJOR	Association Lost - Local Network Name Changed
ipAddrChanged(59)	MAJOR	Association Lost - Local IP Address Changed
assocTryFail(60)	MAJOR	Association Attempt Success/Failed
remEthLinkLost(61)	INFORM	Received Beacon - Valid/Errored
consoleLogin(62)	MAJOR	Console User Logged Out/Logged In
consoleLockdown(63)	MAJOR	Console Access Locked for 5 Min
telnetLockdown(64)	INFORM	System Bootup (power on)
httpLockdown(65)	MAJOR	HTTP Access Locked for 5 Min
eventRemote(66)	INFORM	Remote added/removed from internal database
eventEndpoint(67)	INFORM	Endpoint added/removed from internal database
routeAdded(68)	INFORM	Radio attempted but failed to add a route to its internal routing table
routeDeleted(69)	INFORM	Radio attempted but failed to delete a route from its internal routing table
sinRemSwitch(70)	INFORM	Remote mode was switched (serial to ethernet, ethernet to serial)
ChanCnt(71)	INFORM	Number of channels defined does not match (Channel 130 only)
tftpConnection(73)	INFORM	TFTP Server on AP started or finished a transfer
apNetNameChanged(74)	MAJOR	Remote lost association due to a change in the AP's netname
ipConnectivityOK(75)	INFORM	Radio is associated AND 1) has an IP address statically defined, OR 2) received an IP address via DHCP
compressionChanged(76)	INFORM	Compression state has changed (enabled, disabled)
macDecryptError(77)	INFORM	MAC has received a packet that it could not decrypt
lanPortStatus(78)	INFORM	Ethernet port has changed (enabled, disabled)
tftpConnFailed(79)	INFORM	TFTP server on AP failed to transfer
sdbError(80)	INFORM	AP encountered an internal database error

7 *GLOSSARY OF TERMS AND ABBREVIATIONS*

If you are new to wireless IP/Ethernet systems, some of the terms used in this manual may 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. AP units may be configured for either the Access Point (master) or Remote services. (See *"Network Configuration Menu"* on Page 43.)

Active Scanning—See *Passive Scanning*

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 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 (plus start, stop, and parity 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 usually made up of eight data bits and start, stop and parity 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*.

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 receiving 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—IP address of data equipment connected to the ports 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 several 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.

Hop Pattern Seed—A user-selectable value to be added to the hop pattern formula in an unlikely event of nearly identical hop patterns of two collocated or nearby radio networks to eliminate adjacent-network interference.

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

IAPP (inter-Access Point Protocol)—A protocol by which access points share information about the stations that are connected to them. When a station connects to an access point, the access point updates its database. When a station leaves one access point and roams to another access point, the new access point tells the old access point, using IAPP, that the station has left and is now located on the new access point.

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

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*.

Mobile IP—An emerging standard by which access points and stations maintain network connectivity as the stations move between various IP networks. Through the use of Mobile IP a station can move from its home IP network to a foreign network while still sending and receiving data using it's original IP address. Other hosts on the network will not need to know that the station is no longer in its home network and can continue to send data to the IP address that was assigned to the station. Mobile IP also uses DHCP when the station moves into a foreign network.

Mobility—Refers to a station that moves about while maintaining active connections with the network. Mobility generally implies physical motion. The movement of the station is not limited to a specific network and IP subnet. In order for a station to be mobile it must establish and tear down connections with various access points as it moves through the access points' territory. To do this, the station employs roaming and Mobile IP.

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.

Passive Scanning—Scanning is a process used by stations to detect other access points on network to which it may connect if it needs to roam. Passive scanning is a slower process in which it listens for information offered by the access points on a regular basis. Active scanning is a faster process in which the station sends out probe message to which the access points respond. Passive scanning can be done while main-

taining the current network connectivity. Active scanning affects the RF configuration of the radio and therefore, at least temporarily, disconnects the station from the access point.

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

Point-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 radio.

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.

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.

When two access points are co-located for redundancy, roaming allows the stations to switch between them to provide a robust network. 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.

Skip Zone(s)—Groups of operating channels (frequencies) deleted from the radio transmitter and receiver operating range.

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 ($\approx$ 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

INDEX

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.