

# MDS entraNET™ 900

# MDS entraNET™ 2400



Access Point



Remote

## 900 MHz and 2400 MHz

## Extended Range IP Networking Transceivers

Firmware Code 3.0

05-4055A01, Rev. E

JANUARY 2011



Digital Energy  
MDS

# Quick Start Instructions

Listed below are the basic steps for installing GE MDS entraNET transceivers. Refer to the appropriate sections in the manual for detailed information.

## 1. Initial Checkout

---

- Set the equipment up in a tabletop arrangement as described in [2 TABLETOP SETUP AND EVALUATION](#), (beginning on Page 15).
- Follow all steps to ensure proper cable connections and unit configuration. As a minimum, Access Points must have the following programmed: IP Address, IP Network identifier, and Radio Network Address. (RF output power and Password should also be reviewed and set if necessary.) Remote radios normally require only a Radio Network Address to be set. (Note: The Remote Radio Network Address *must* match that of the AP.)
- Connect data equipment to the transceivers. Use LAN/ETH ports for Ethernet systems, or COM2 ports for Serial data systems.
- Verify proper exchange of data communications by viewing the LEDs. The following indications should be seen on the LED panel within 30 seconds of startup:

*PWR*—Lit continuously

*LINK*—Lit continuously

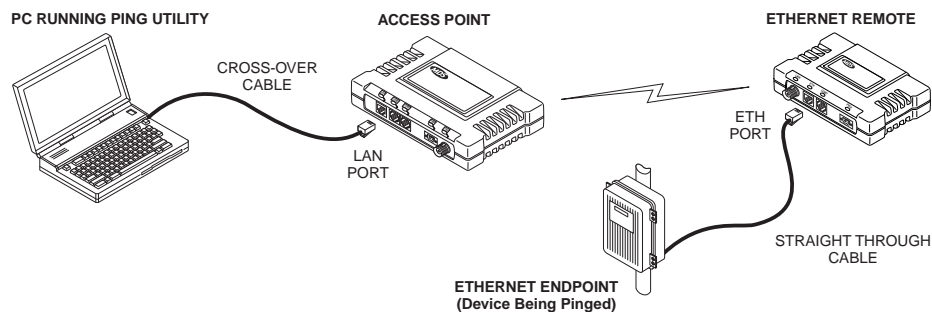
*ETH*—Lit continuously (unless Sleep is activated)

*COM2*—Blinking to indicate exchange of data communications

## 2. Endpoint Connectivity (PING) Test—for Ethernet Systems Only

---

- For Ethernet systems, verify the link integrity between the Access Point and endpoint devices connected to Remotes by issuing a **PING** command from the AP. Below is a basic setup diagram for the PING test. (NOTE: Endpoint devices must have a compatible IP address for this test to work.)



## 3. Set Configuration of AP and Remote Radios

---

- Refer to [3 AP MANAGEMENT beginning on Page 29](#) for details on connecting to the AP and using the built-in menu system. Refer to [4 REMOTE RADIO MANAGEMENT beginning on Page 99](#) for details on programming Remotes.
- If you have a large number of radios to configure, a configuration script may be used to speed the process. See [USING CONFIGURATION SCRIPTS beginning on Page 181](#) for details.

## 4. Install the Equipment in the Field

---

- Refer to [6 INSTALLATION beginning on Page 147](#) for details on site selection, mounting, cabling, and antenna/feedline recommendations.
- After basic installation, optimize the performance of the radio network following the recommendations beginning on Page 160.

---

# TABLE OF CONTENTS

---

<b>1</b>	<b><i>INTRODUCING THE MDS entraNET SYSTEM</i></b> .....	<b>1</b>
1.1	ABOUT THIS MANUAL .....	3
1.1.1	Supplemental Information Online .....	3
1.2	PRODUCT DESCRIPTION.....	3
1.2.1	Model Offerings .....	6
1.3	APPLICATIONS .....	6
1.3.1	Long-Range Wireless LAN .....	6
	Antenna Placement.....	6
	Communication Rules.....	6
1.3.2	Combining Serial and Ethernet Devices .....	7
1.3.3	DNP3 Protocol-Aware Networks .....	8
1.3.4	Upgrading an Older Wireless Network with Serial Interfaces .....	9
	Replacing Legacy Wireless Products .....	9
	Supplementing a Legacy Wireless Network with IP Services.....	9
1.3.5	P22 Protected Network (Redundant) Configuration .....	9
1.4	GE MDS SECURITY SUITE .....	10
1.4.1	Intrusion Detection via SNMP Traps .....	11
1.5	ACCESSORIES.....	12
<b>2</b>	<b><i>TABLETOP SETUP AND EVALUATION</i></b> .....	<b>15</b>
2.1	INTRODUCTION .....	17
2.2	CONNECTOR OVERVIEW .....	17
2.3	TEST SETUP.....	18
	STEP 1—CONNECT THE ANTENNA PORTS .....	19
	STEP 2—MEASURE AND CONNECT DC POWER .....	19
	STEP 3—CONFIGURE THE AP .....	22
	Log-in and Configuration.....	22

Set Key AP Parameters .....	23
STEP 4—CONFIGURE THE REMOTE RADIO .....	24
Log-in and Configuration.....	24
Set or Verify Network Address .....	25
STEP 5—CONNECT TERMINAL EQUIPMENT.....	26
Ethernet Device Connection to Remote.....	26
Serial Device Connection to Remote .....	26
STEP 6—CHECK FOR NORMAL OPERATION .....	26
2.3.1 Verify Connectivity (PING command) .....	27
Serial Connections.....	27

## **3 AP MANAGEMENT ..... 29**

<b>3.1 INTRODUCTION .....</b>	<b>31</b>
3.1.1 PC-Based Configuration Software .....	31
3.1.2 Menu Structure .....	32
3.1.3 Differences in the User Interfaces .....	35
<b>3.2 ACCESSING THE MENU SYSTEM .....</b>	<b>36</b>
3.2.1 Methods of Control .....	36
3.2.2 PC Connection and Log-In Procedures .....	37
3.2.3 Navigating the Menus .....	42
Navigating via Terminal or Telnet Sessions	
Recommended for first-time users.....	42
Navigating via a Web Browser.....	42
<b>3.3 BASIC DEVICE INFORMATION.....</b>	<b>43</b>
3.3.1 Starting Information Screen .....	43
3.3.2 Main Menu .....	44
<b>3.4 CONFIGURING NETWORK PARAMETERS .....</b>	<b>45</b>
3.4.1 Network Configuration Menu .....	45
3.4.2 IP Configuration Menu .....	46
3.4.3 Wireless MAC Configuration Menu .....	48
3.4.4 Mobility Configuration Menu .....	49
3.4.5 SNMP Agent Configuration Menu .....	50
3.4.6 Bridge Configuration Menu .....	51
<b>3.5 CONFIGURING RADIO PARAMETERS .....</b>	<b>52</b>
3.5.1 Radio Configuration Menu .....	52
Skip Zones Menu.....	53
<b>3.6 CONFIGURING THE SERIAL INTERFACES.....</b>	<b>54</b>
3.6.1 Overview .....	54
Serial-to-Serial Services .....	55

IP-to-Serial Services .....	55
Configuration.....	56
Serial Configuration Wizard .....	56
3.6.2 Local Serial Configuration Menu .....	57
View Current Settings Screen—Serial-to-Serial Example .....	59
View Current Settings Screen—Unicast UDP Mode Example.....	61
3.6.3 Remote Serial Gateway Configuration (IP-to-Remote Serial) .....	62
<b>3.7 SECURITY CONFIGURATION.....</b>	<b>64</b>
3.7.1 Security Configuration Menu .....	65
<b>3.8 WIRELESS NETWORK MENU .....</b>	<b>69</b>
3.8.1 Remote Management Submenu .....	70
Manage Selected Remote Submenu .....	71
Broadcast Remote Reprogramming Menu .....	72
Remote Database Menu .....	74
Group Database Menu.....	75
Endpoint Database Menu .....	75
Access Point Database Menu.....	76
<b>3.9 STATISTICS AND EVENT LOG .....</b>	<b>77</b>
3.9.1 COM1 and COM2 Data Statistics Menus .....	78
3.9.2 Remote Serial Gateway Statistics .....	79
3.9.3 Ethernet and Wireless Packet Statistics .....	80
Ethernet Packet Statistics .....	80
Wireless Packet Statistics .....	80
3.9.4 Radio Packet Statistics .....	81
3.9.5 Event Log Menu .....	82
Time and Date Stamping.....	82
<b>3.10 DEVICE INFORMATION MENU .....</b>	<b>84</b>
Device Names Menu.....	85
<b>3.11 MAINTENANCE AND TOOLS .....</b>	<b>85</b>
3.11.1 Reprogramming Menu .....	86
3.11.2 Configuration Scripts Menu .....	87
A Brief Description of Configuration Files .....	87
3.11.3 RSG Configuration Script Menu .....	89
3.11.4 Authorization Codes Menu .....	91
3.11.5 Transmitter Test Menu .....	92
<b>3.12 REDUNDANCY MENU .....</b>	<b>93</b>
Packet Rx Errors Exceeded Threshold Menu.....	96
<b>3.13 DNP3 ROUTING MENU .....</b>	<b>97</b>

## **4 REMOTE RADIO MANAGEMENT . . . . . 99**

4.1 INTRODUCTION .....	101
4.2 Programming Methods.....	101
4.2.1 Terminal Interface Mode .....	101
4.2.2 Remote Management via the AP .....	101
4.3 Log-in Procedure .....	101
4.4 Commands.....	102
4.4.1 Entering Remote Commands .....	102
4.5 Minimum Configuration for Remotes .....	102
4.5.1 Detailed Command Descriptions .....	103
4.6 UPGRADING REMOTE FIRMWARE .....	117

## **5 SAMPLE CONFIGURATIONS . . . . . 119**

5.1 INTRODUCTION .....	121
5.2 IP-to-Local Serial Application Example.....	121
Establishing a Connection .....	121
5.3 IP-to-Remote Serial Application Example.....	122
5.3.1 Endpoint Device Connected to the AP .....	123
5.4 Point-to-Point, Serial-to-Serial Application Example.....	123
5.4.1 Step-by-step Instructions for Configuring a Point-to-Point Serial Connection .....	124
5.5 Point-to-Multipoint, Serial-to-Serial Application Example.....	132
5.5.1 Step-by-Step Instructions for Configuring a Point-to-Multipoint Serial Connection .....	133
5.6 Mixed-Mode Application Example.....	140
5.6.1 Operation and Data Flow .....	140
5.7 Group Broadcast Session Example .....	142

## **6 INSTALLATION ..... 147**

### **6.1 INSTALLATION..... 149**

6.1.1 General Requirements .....	149
6.1.2 Site Selection .....	149
6.1.3 Conducting a Site Survey .....	150
Terrain and Signal Strength.....	150
A Word About Radio Interference .....	150
Mounting Dimensions for Radios.....	152
6.1.4 Antenna and Feedline Selection .....	153
Antennas.....	153
Feedlines .....	154

### **6.2 HOW MUCH OUTPUT POWER CAN BE USED? (U.S.A. and Canada, 900 MHz systems) ..... 156**

6.2.1 Calculating System Gain .....	156
-------------------------------------	-----

### **6.3 HOW MUCH OUTPUT POWER CAN BE USED? (U.S.A. and Canada, 2400 MHz systems) ..... 157**

6.3.1 Calculating System Gain .....	157
-------------------------------------	-----

### **6.4 HOW MUCH OUTPUT POWER CAN BE USED? (ETSI 2400 MHz systems)..... 158**

6.4.1 Calculating System Gain .....	159
-------------------------------------	-----

### **6.5 OPTIMIZING PERFORMANCE ..... 160**

6.5.1 Principles of Wireless Network Operation .....	160
6.5.2 Aiming Directive Antennas for Maximum RSSI .....	162
Procedure .....	162
6.5.3 Tips for Improving Data Throughput .....	163
To Maximize Throughput of Data and Reduce Latency Time .....	163
To Maximize Overall Data Performance .....	164

## **7 TROUBLESHOOTING AND RADIO TESTS ..... 165**

### **7.1 TROUBLESHOOTING..... 167**

7.1.1 Interpreting the Front Panel LEDs .....	167
7.1.2 Troubleshooting Using the Embedded Management System .....	168
Serial Port and Remote Serial Statistics Menu .....	171
Diagnostic Tools.....	171
7.1.3 Using Logged Operation Events .....	172

## 8 TECHNICAL REFERENCE ..... 177

8.1 UPGRADING AP FIRMWARE .....	179
8.2 USING CONFIGURATION SCRIPTS .....	181
Sample of an Exported Configuration File .....	182
Editing Configuration Files .....	186
8.3 DATA INTERFACE CONNECTORS .....	187
8.3.1 LAN/ETH Port .....	187
8.3.2 COM1 Port .....	188
8.3.3 COM2 Port .....	189
8.4 TECHNICAL SPECIFICATIONS .....	189
8.5 dBm-WATTS-VOLTS CONVERSION CHART .....	193

## 9 TERMS AND ABBREVIATIONS ..... 195

### Copyright Notice

This publication is protected by U.S.A. copyright law. Copyright 2011, GE MDS. All rights reserved.

### ISO 9001 Registration

GE MDS adheres to the internationally-accepted ISO 9001 quality system standard.

### Related Materials on the Internet

Data sheets, frequently asked questions, application notes, information on firmware upgrades, and other valuable information can be found on the GE MDS Web site at [www.gemds.com](http://www.gemds.com).

### About GE MDS

Over two decades ago, GE MDS began building radios for business-critical applications. Since then, we've installed more than 500,000 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.gemds.com](http://www.gemds.com) for more information.



## OPERATIONAL & SAFETY NOTICES

### RF Exposure



**U.S. Installations:** 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. For 900 MHz units, do not allow people to come closer than 23 cm (9 inches) to the antenna. For 2.4 GHz units, do not allow people to come closer than 5 cm (2 inches) to the antenna. These distances apply whether the transmitter is operated in indoor or outdoor environments. More information on RF exposure is available on the Internet at [www.fcc.gov/oet/info/documents/bulletins](http://www.fcc.gov/oet/info/documents/bulletins).

**ETSI Installations:** In regions where the European Telecommunications Standards Institute (ETSI) standards apply, 2.4 GHz units with a maximum output power of 100 mW EIRP are supplied. Do not allow people to come closer than 2.2 cm (1 inch) to the antenna.

### CSA/US Notice



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

### FCC Part 15 Notice

The transceiver 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 GE MDS may void the user's authority to operate this device. Furthermore, this device 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.

### Manual Revision and Accuracy

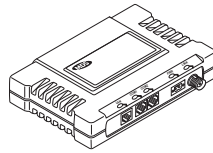
While every reasonable effort has been made to ensure the accuracy of this manual, product improvements may result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service 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](http://www.gemds.com).

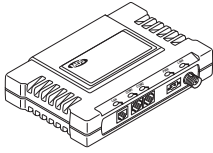
### Environmental Information



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.

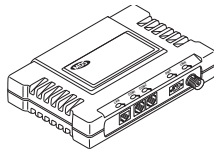
**Battery Disposal**—This product may contain a battery. Batteries must be disposed of properly, and may not be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. Batteries are marked with a symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling return the battery to your supplier or to a designated collection point. For more information see: [www.weeerohsinfo.com](http://www.weeerohsinfo.com).





# 1 INTRODUCING THE MDS entraNET SYSTEM

1.1	ABOUT THIS MANUAL	3
1.1.1	Supplemental Information Online .....	3
1.2	PRODUCT DESCRIPTION	3
1.2.1	Model Offerings .....	6
1.3	APPLICATIONS	6
1.3.1	Long-Range Wireless LAN .....	6
	Antenna Placement .....	6
	Communication Rules .....	6
1.3.2	Combining Serial and Ethernet Devices .....	7
1.3.3	DNP3 Protocol-Aware Networks .....	8
1.3.4	Upgrading an Older Wireless Network with Serial Interfaces .....	9
	Replacing Legacy Wireless Products .....	9
	Supplementing a Legacy Wireless Network with IP Services .....	9
1.3.5	P22 Protected Network (Redundant) Configuration .....	9
1.4	GE MDS SECURITY SUITE	10
1.4.1	Intrusion Detection via SNMP Traps .....	11
1.5	ACCESSORIES	12



## 1.1 ABOUT THIS MANUAL

This guide provides installation and operating instructions for the MDS entraNET 900™ and MDS entraNET 2400™ series radio system. The guide is intended for use by those who install, configure, and operate the entraNET wireless network.

*Quick Start* instructions are provided on the inside front cover of this guide. They provide the basic steps for installing and operating the transceivers, but do not cover all of the configurable parameters. The main section of this guide contains complete information on menu functions, as well as detailed installation, operation, and troubleshooting information. This guide is arranged into the following eight chapters:

- Chapter 1—*Introducing the MDS entraNET System* (Page 1)
- Chapter 2—*Tabletop Setup and Evaluation* (Page 15)
- Chapter 3—*Access Point (AP) Management* (Page 29)
- Chapter 4—*Remote Radio Management* (Page 99)
- Chapter 5—*Sample Configurations* (Page 119)
- Chapter 6—*Installation* (Page 147)
- Chapter 7—*Troubleshooting and Radio Tests* (Page 165)
- Chapter 8—*Technical Reference* (Page 177)
- Chapter 9—*Terms and Abbreviations* (Page 195). Terms defined in Chapter 9 are italicized on first appearance.

### 1.1.1 Supplemental Information Online

Release notes, manual updates, and other supplemental materials are available online for many GE MDS products. For more information, visit us at online at [www.gemds.com](http://www.gemds.com).

## 1.2 PRODUCT DESCRIPTION

The entraNET system is an easy-to-install wireless solution supporting long-range serial and Ethernet data transmission at speeds up to 106 *kbps*. The system includes an *Access Point* (AP) transceiver and a Remote transceiver capable of serial and Ethernet communication. These radios serve a variety of network configurations. [Figure 1-1](#) shows the two radios.



**Figure 1-1. MDS entraNET Transceiver Models**

***Robust Radio Operation***

MDS entraNET transceivers use an advanced Media Access Controller (MAC) to ensure network access for stations with data to send. The MAC permits data to be sent from endpoint devices on an on-demand basis, preventing over-the-air data collisions and ensuring that data gets through as intended. MAC functionality eliminates the need for active polling of Remotes, an important requirement in Report-by-Exception (RBE) applications.

***Rugged Packaging***

MDS entraNET radios are housed in compact and rugged die-cast cases that need only be protected from direct exposure to the weather. The transceivers are supplied with flat surface-mounting brackets or optional 35 mm DIN rail brackets, depending on customer requirements.

***Simple Installation***

Basic installation typically employs an omni-directional antenna at the AP site and a directional antenna at each *associated* Remote site. The antenna is a vital link in the system and must be chosen and installed correctly. [INSTALLATION PLANNING](#) on Page 149 provides guidance on choosing proper antennas and installation sites.

To establish basic service, connect an antenna, connect an Ethernet LAN (Local Area Network) to the AP, connect a serial or Ethernet device to the Remotes, apply power, set a few operating parameters using a personal computer, and you are done. No license is required for operation in the U.S.A., Canada, and many other countries. Check the regulations in your country before placing the radios on the air.

***GE MDS Security Suite***

Network security is a vital issue in today's wireless world. The MDS entraNET system provides multiple tools to help you build a network that minimizes the risk of eavesdropping or unauthorized access. Some security features are inherent to radio operation, such as the use of spread-spectrum transmission. Other techniques are built into

the radio firmware, including data encryption, enabling or disabling remote access channels, and password protection.

Security is not a one-step process that can be simply turned on and forgotten. It must be practiced and enforced at multiple levels, every day. Section 1.4 contains additional information about entraNET security features.

***License-Free Operation***

The transceivers are designed for frequency-hopping spread-spectrum operation in the license-free 900 MHz or 2400 MHz band. They can provide reliable long distance communications over line-of-sight signal paths.

***Multiple Services***

Networks can include a mixture of equipment requiring Ethernet and serial data interfaces on the same cell or AP. This flexibility allows the transceiver to provide services in data networks that are on a migration path from legacy serial or EIA-232-based hardware to faster and more easily interfaced Ethernet systems.

***Flexible Management***

Configuration, troubleshooting and other management activities are performed using a connected PC, locally or remotely. Modes of access include a local RS-232 console, local or remote IP access through Ethernet, Telnet, or a Web browser, and Simple Network Management Protocol (SNMP).

***Feature Summary***

The MDS entraNET design makes installation and configuration an easy task, while allowing for configuration changes in the future.

- Long-range transmission over favorable, unobstructed terrain, with sufficient antenna heights
- Low power consumption—Sleep and Shutdown modes to enable solar-powered operation
- Repeater configurations—A repeater scheme can be established to extend the transmission range or to work around obstructions in a network. This is accomplished by connecting two radios back to back at a single site.
- Industrial-grade product—Extended temperature range for trouble-free operation in extreme environments
- Robust radio communications—Designed to perform in high-interference environments
- GE MDS Security Suite—Blocks common attack schemes and prevents “rogue” hardware from gaining access to or control of a network. Common attack events are logged and reported using alarms.
- Fast, 106 kbps data speed—Ten times faster than 9.6 kbps radios
- Simple setup—Ethernet bridge configuration option requires minimal setup
- Serial ports—Gateway for serial interface equipment to IP or Ethernet networks with an embedded terminal server

## 1.2.1 Model Offerings

The MDS entraNET system includes two primary radio types— APs and Remotes. [Table 1-1](#) summarizes the interface capabilities for each entraNET radio type.

---

**NOTE:** A Remote can serve multiple *endpoint* MAC addresses if the Remote is provided an authorization code.

---

**Table 1-1. MDS entraNET Models and Data Interface Services**

Model	LAN/ETH	COM1*	COM2
AP	LAN	Yes	Yes
Remote	ETH	Yes	Yes

**NOTES**

\*This connector provides access to the radio menu system.

---

## 1.3 APPLICATIONS

The following sections describe typical entraNET installations. All installations should be reviewed by a network manager to ensure proper integration with existing equipment.

### 1.3.1 Long-Range Wireless LAN

The wireless LAN is a common application of the entraNET system. It consists of a central control station (AP) and one or more associated Remote radios, as shown in [Figure 1-2 on Page 7](#). A LAN provides communications between a central LAN/WAN and remote Ethernet endpoints. Remote radios can support multiple Ethernet endpoints if the Remote is provided an authorization code.

The operation of the radio system is transparent to the computer equipment connected to it. As such, the system behaves just as it would in a hardwired arrangement, with respect to data format and integrity. Over-the-air messages are exchanged at the Ethernet level, including all types of IP traffic.

#### Antenna Placement

The AP antenna is positioned at a location from which it can reliably communicate with all of the Remote radios in the system. Commonly, this is a relatively high location on top of a building, communications tower or other elevated point.

#### Communication Rules

- A Remote transceiver can only talk over-the-air to an AP.
- Peer-to-peer communications between Remotes can take place indirectly through the AP.



- An AP can only talk over-the-air to Remote radios; however, two APs can communicate with each other through their Ethernet connectors when a wired LAN/WAN is utilized.

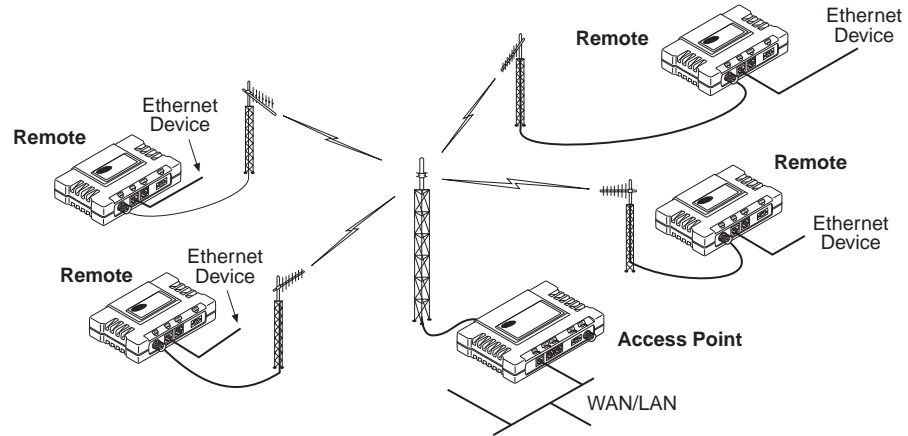


Figure 1-2. Typical Wireless LAN System

### 1.3.2 Combining Serial and Ethernet Devices

Prior to the introduction of the entraNET series, multiple networks were often needed to service different types of communication protocols. An entraNET system provides this functionality through a single AP radio. Each of the Remote radios in a system can be connected via IP to different SCADA or telemetry hosts, transporting different (or the same) protocols. Both data streams are completely independent, and the transceiver provides seamless, simultaneous operation, as shown in Figure 1-3.

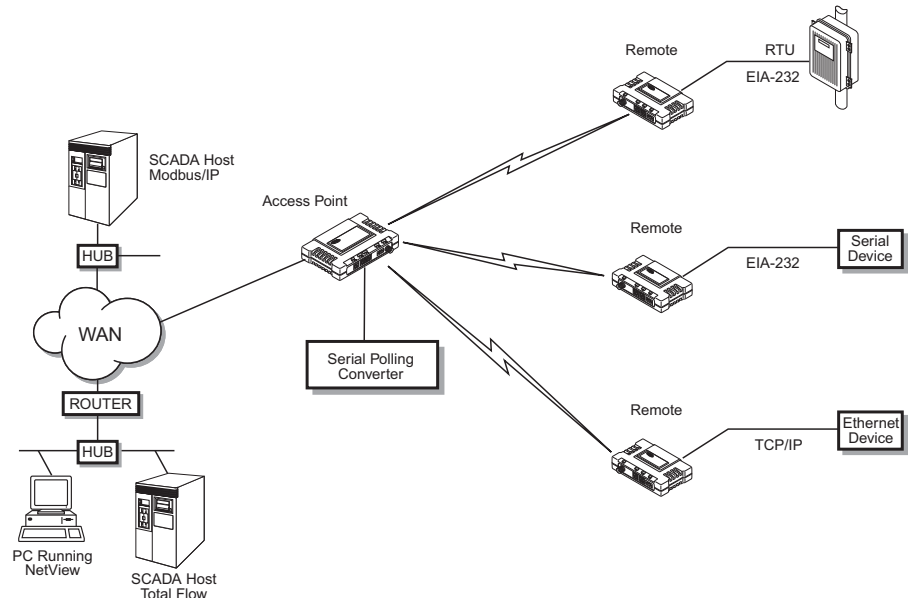


Figure 1-3. Multiple Protocol Network

By using a single AP, the cost of infrastructure deployment is cut in half, with only one antenna, one feedline, and one lightning protector required. Other cost reductions come from the system as a whole, including reduced management requirements when using GE MDS NETview Management System (MS) software. In addition, entraNET offers nearly unlimited potential for future applications that run over IP and Ethernet services.

In an IP-to-serial scenario, every Remote is sent information received by the AP Ethernet port. Likewise, information received at the Remote serial port is transmitted to the AP, and the AP delivers this information through its Ethernet port in the form of an IP packet.

Additionally, the AP serial port can be used as a virtual Remote. This means that encapsulated serial information received by the AP is sent out the serial port of all Remotes as well as the AP serial port. The reverse is also true, meaning that data received by the serial port of any Remote or the AP serial port is encapsulated and sent out the AP Ethernet port.

This arrangement can be used to connect an endpoint device at a Repeater site without the need for an additional Remote radio.

### 1.3.3 DNP3 Protocol-Aware Networks

The GE MDS implementation of Distributed Network Protocol 3 (*DNP3*) allows the transfer and routing of DNP3 messages between serial devices, while also supporting the conversion to an IP Ethernet network. As DNP3 messages are routed through the system, the APs “learn” the locations of all end devices, regardless of whether they are configured for serial or Ethernet communication, eliminating the need to configure their individual locations.

DNP3 devices with an Ethernet or IP interface can be connected to a transceiver in one of two ways:

- To the Ethernet port of an AP radio
- To the Ethernet port of a Remote radio

DNP3 devices with a serial RS-232 interface can be connected to a transceiver in one of two ways:

- To the serial port of an AP radio
- To the serial port of a Remote radio

The capability for DNP3 message routing is optional for the transceiver. An *Authorization Key* is required to enable this functionality, and is available for purchase from GE MDS.

---

**NOTE:** Detailed information on the DNP3 protocol is available on the DNP Users' Group Web site at [www.dnp.org](http://www.dnp.org).

---

### 1.3.4 Upgrading an Older Wireless Network with Serial Interfaces

Millions of wireless data products have been sold 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 employing MDS entraNET wireless equipment, including flexible serial and Ethernet interfaces, higher data throughput, and ease of installation.

MDS entraNET radios are well suited to replace leased lines, dial-up lines, or existing data radios by taking advantage of the built-in serial and Ethernet interfaces on the transceiver. The sections below discuss two common scenarios.

#### Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial interface equipment can be replaced with MDS entraNET radios with little or no special configuration. This equipment can be connected to MDS entraNET radios through the COM1 or COM2 port with a DB-25 to RJ-45 cable wired for EIA-232 signaling. The COM2 port supports standard EIA-232 signaling and acts as a data communications equipment (*DCE*) device.

---

**NOTE:** Several previous GE MDS-brand products contained signal lines on their interface connectors that are not used or required on entraNET radios. Consult the equipment manual(s) for interface pinout information, and connect **only** the required pins.

---

#### Supplementing a Legacy Wireless Network with IP Services

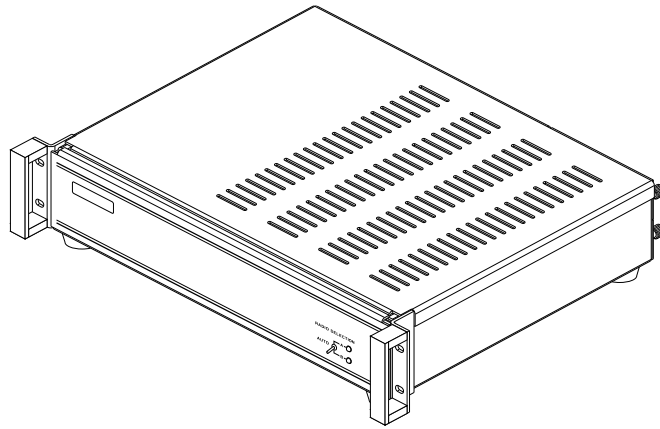
MDS entraNET Remotes support most polled protocols. The serial interfaces encapsulate serial data in two different modes: connectionless (*User Datagram Protocol*, or UDP) and connection-oriented (*Transmission Control Protocol*, or TCP).

For complete details on serial gateway interface modes, see [“CONFIGURING THE SERIAL INTERFACES”](#) on Page 54.

### 1.3.5 P22 Protected Network (Redundant) Configuration

For mission-critical applications, GE MDS offers the Protected Network Station. This radio incorporates two entraNET AP transceivers, two power supplies, and a switchover logic board that automatically selects between Transceiver A and Transceiver B as the active radio. [Figure 1-4](#)

shows a view of the protected chassis. For system-level information on this product, see GE MDS publication 05-4161A01.



**Figure 1-4. GE MDS P22 Protected Network Station**  
*(incorporates two MDS entraNET APs)*

## 1.4 GE MDS SECURITY SUITE

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

The MDS entraNET is capable of dealing with many common security issues. [Table 1-2](#) profiles security risks and how the MDS entraNET provides a solution for minimizing vulnerability.

**Table 1-2. Security Risk Management**

Security Risk	The MDS entraNET Solution
Unauthorized access to the backbone network through a foreign remote radio	✓ Approved Remotes List Only radios on the Approved Remotes list connect
“Rogue” AP, where a foreign AP takes control of some or all Remote radios and thus remote devices	✓ Approved AP List A Remote connects only to APs on its Approved AP List
“Dictionary attacks”, where an intruder runs a program that sequentially tries to break a password	✓ Failed log-in lockdown After three tries, a transceiver ignores log-in requests for 5 min. Critical event reports (traps) are generated as well.

**Table 1-2. Security Risk Management**

Security Risk	The MDS entraNET Solution
Denial of service, where Remote radios could be reconfigured with bad parameters, bringing the network down	<ul style="list-style-type: none"> <li>✓ Remote log-in</li> <li>✓ Local console log-in</li> <li>✓ HTTP (Hypertext Transfer Protocol) and Telnet disabled, enabling only local management services</li> </ul>
Airsnort and other war-driving intruders in parking lots, near buildings, and so on	<ul style="list-style-type: none"> <li>✓ Frequency-hopping spread spectrum (<i>FHSS</i>) does not talk over the air with standard 802.11b cards</li> <li>✓ The transceiver cannot be put in a “promiscuous” mode</li> <li>✓ Proprietary data framing</li> </ul>
Eavesdropping, intercepting messages	<ul style="list-style-type: none"> <li>✓ 128-bit encryption</li> </ul>
Key cracking	<ul style="list-style-type: none"> <li>✓ Automatic Key Rotation algorithm. In addition, a Force Key Rotation command is available to immediately rotate the keys of the AP and synchronize all Remotes with it.</li> </ul>
Replaying messages	<ul style="list-style-type: none"> <li>✓ 128-bit encryption with rotating keys</li> </ul>
Unprotected access to configuration using SNMP	<ul style="list-style-type: none"> <li>✓ Non-secure SNMP versions can be enabled or disabled at will.</li> <li>✓ SNMPv3 password protection</li> </ul>
Potential, ongoing attacks	<ul style="list-style-type: none"> <li>✓ Provides early warning using SNMP through critical event reports of unauthorized log-in attempts and suspicious activities</li> </ul>

### 1.4.1 Intrusion Detection using SNMP Traps

In addition to the operative tools and techniques, the entraNET system provides an SNMP-based network management system with traps (alarms) that report suspicious activities or events. These include:

- Log-in attempt limit exceeded (accessed using HTTP)
- Successful log-in or logout (accessed using HTTP)

## 1.5 ACCESSORIES

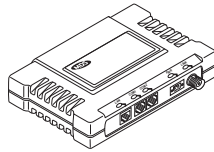
MDS entraNET transceivers may be used with the accessories listed in [Table 1-3](#). Contact GE MDS for ordering details.

**Table 1-3. Accessories**

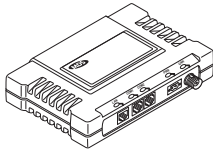
Accessory	Description	GE MDS Part No.
AC Power Adapter Kit	A small power supply module designed for continuous service. UL approved. Input: 120/220; Output: 13.8 Vdc at 2.5 A	01-3682A02
Omni-Directional Antennas	Rugged antennas well suited for use at AP installations. Ask your GE MDS Sales Representative for details.	Contact GE MDS
Yagi Antenna (Directional)	Rugged antennas well suited for use at Remote installations. Ask your GE MDS Sales Representative for details.	Contact GE MDS
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 TNC antenna connector to a Type N connector commonly used on large-diameter coaxial cables.	97-1677A159 (3 ft./1m) 97-1677A160 (6 ft./1.8m)
2-Pin Power Plug	Mates with power connector on the transceiver. Screw terminals are provided for wires; locking screws are threaded to prevent accidental disconnection.	73-1194A39
Ethernet RJ-45 Straight-thru Cable (CAT5)	Cable assembly normally used to connect an Ethernet device or LAN to the transceiver. Both ends of the cable are wired identically. (Cable length $\approx$ 3 ft/1 m)	97-1870A20
Ethernet RJ-45 Crossover Cable (CAT5)	Cable assembly used to connect an AP to an Ethernet endpoint. (Cable length $\approx$ 3 ft/1 m)	97-1870A21
RJ-12 to DB-9 Female Adapter	Allows access to Data Serial port COM1 on Remotes or APs.	73-2434A02
RJ-45 to DB-9 Female Adapter	Allows access to Data Serial port COM2 on Remotes or APs.	73-2434A12
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. (Cable length $\approx$ 6 ft/1.8 m)	97-1971A03
Fuse	Small, board-mounted fuse used to protect against overcurrent conditions.	29-1784A03

**Table 1-3. Accessories**

<b>Accessory</b>	<b>Description</b>	<b>GE MDS Part No.</b>
Flat-Surface Mounting Brackets and Screws	Brackets: 2 in. x 3 in. plates designed to be screwed onto the bottom of the radio for surface-mounting the radio.	82-1753-A01
	Screws: 6-32, 1/4 in. with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
DIN Rail Mounting Bracket	Bracket used to attach the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4124A01 (Remote) 03-4125A02 (AP)
Ethernet Surge Protector	Protects against voltage spikes or surges on Ethernet lines. These conditions may be caused by nearby lightning strikes or transient conditions.	29-4018A01

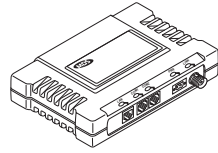






# 2 TABLETOP SETUP AND EVALUATION

2.1	INTRODUCTION	17
2.2	CONNECTOR OVERVIEW	17
2.3	TEST SETUP	18
	STEP 1—CONNECT THE ANTENNA PORTS .....	19
	STEP 2—MEASURE AND CONNECT DC POWER.....	19
	STEP 3—CONFIGURE THE AP .....	22
	Log-in and Configuration .....	22
	Set Key AP Parameters.....	23
	STEP 4—CONFIGURE THE REMOTE RADIO .....	24
	Log-in and Configuration .....	24
	Set or Verify Network Address.....	25
	STEP 5—CONNECT TERMINAL EQUIPMENT .....	26
	Ethernet Device Connection to Remote .....	26
	Serial Device Connection to Remote.....	26
	STEP 6—CHECK FOR NORMAL OPERATION .....	26
2.3.1	Verify Connectivity (PING command) .....	27
	Serial Connections .....	27



## 2.1 INTRODUCTION

Prior to installation in the field, you should set up the radio system in an office or lab and become familiar with its operation and features. This also allows tests of various network designs and configurations prior to arrival at a field site. A tabletop test can be performed with any number of radios.

This section describes the hardware setup and software configuration needed for testing an Ethernet connection. To simulate data traffic flow over the radio network, a PC or LAN is connected to the LAN port of the AP and used to *PING* (Packet INternet Groper) a device connected to the Remote transceiver.

---

**NOTE:** It is important to use a radio system *network address* and device IP address that are different from any radios currently in use in your region or network. This greatly reduces the possibility of disruption to traffic on existing systems during testing.

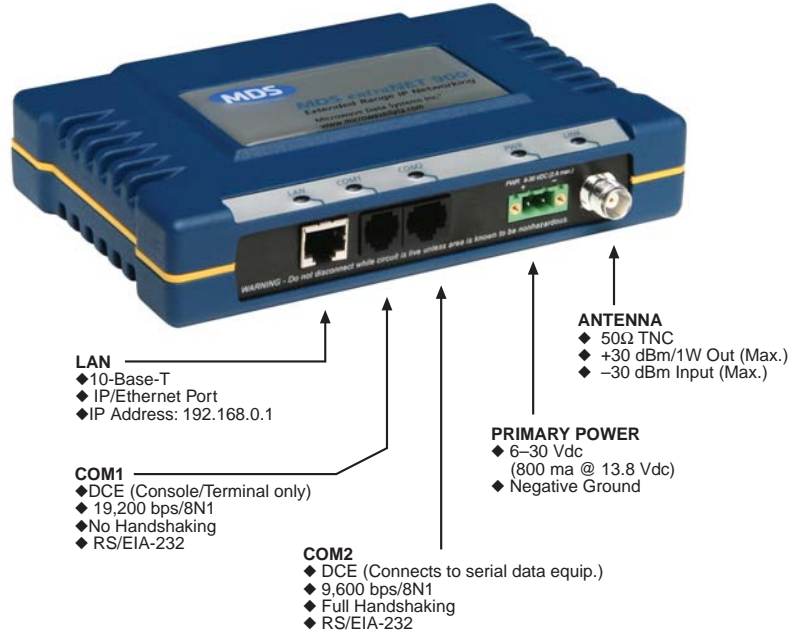
A recommended technique for minimizing the chance of radio network address conflicts is to use the last four digits of the AP serial number.

---

## 2.2 CONNECTOR OVERVIEW

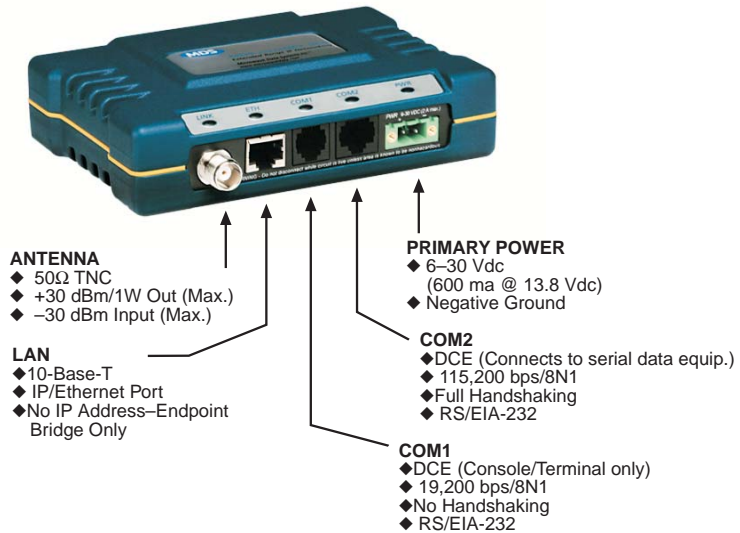
The following illustrations show all of the interface connectors present on entraNET transceivers. Review these items when making the connections described in this section.

[Figure 2-1 on Page 18](#) shows the interface connectors for the AP transceiver.



**Figure 2-1. AP Interface Connectors**

Figure 2-2 shows the interface connectors for the Remote transceiver.



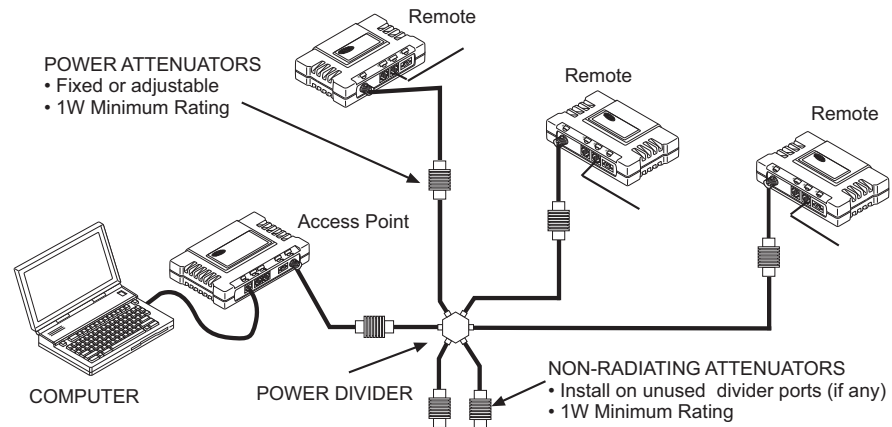
**Figure 2-2. Remote Interface Connectors**

## 2.3 TEST SETUP

The following steps explain how to make connections to the transceiver system, power it up, and set basic configuration. After these steps are complete, the system is ready for field installation.

## STEP 1—CONNECT THE ANTENNA PORTS

Figure 2-3 is a drawing of a tabletop arrangement. Connect the antenna ports of each transceiver as shown through attenuators and an RF power divider. This provides for stable communications between each radio, while preventing interference to nearby electronic equipment.



**Figure 2-3. Typical Setup for Tabletop Radio Testing**

---

**NOTE:** It is very important to use attenuation between radios in the test setup. The amount of attenuation required depends on the number of radios being tested and the desired signal strength (Received Signal Strength Indicator, or RSSI) at each transceiver during the test. In no case should a signal greater than  $-30\text{ dBm}$  be applied to any transceiver in the test setup. A transmit RF power output level of  $+20\text{ dBm}$  (100 mW) is recommended. This can be set via the radio menu (**Main Menu > Radio Configuration > RF Output Power Setpoint**).

---

## STEP 2—MEASURE AND CONNECT DC POWER

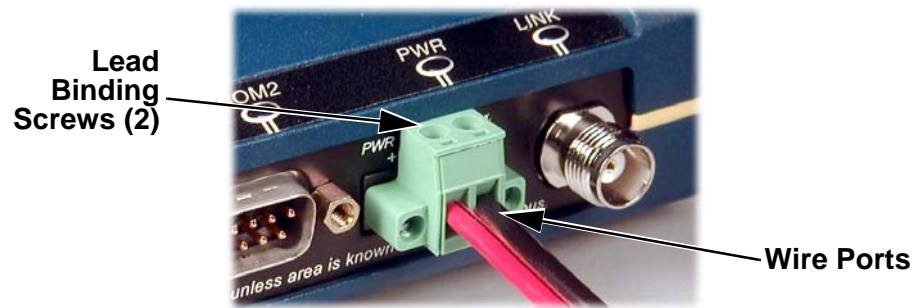
The power applied to transceivers (AP and Remotes) must be within 6–30 Vdc and be capable of continuously providing a minimum of 11 W (typical power consumption is 800 mA at 13.8 Vdc for the AP and 600 mA at 13.8 Vdc for Remotes).

A power connector with screw terminals is provided with each radio. Strip the wire leads to 6 mm (0.25 in.). Observe proper polarity, as shown in Figure 2-4 on Page 20, with the positive lead (+) on the left.

---

**NOTE:** It takes about 30 sec for the AP transceiver to power up and be ready for operation. The Remote requires approximately 5 sec to power up.

---



**Figure 2-4. Power Connector**  
*(polarity: left +, right –)*

**CAUTION**  
 POSSIBLE  
 EQUIPMENT  
 DAMAGE

The transceiver must be used only with negative-ground systems. Make sure the polarity of the power source is correct. The radio is protected from reverse polarity by an internal diode and an on-board fuse.

**Power Supply  
 Connections at  
 28 Vdc**

Common 28 Vdc supplies are often high-current power supplies designed primarily to charge battery banks. The radio can be operated from these supplies, providing there are no transients on the leads as power is applied to the radio. Transients can be created that rise above 30 Vdc to a voltage that exceeds the primary voltage rating of the radio and can destroy its voltage regulators and other components. It is important to keep this potential hazard in mind when designing 28 Vdc power supply connections for the radio.

- Use a two-conductor cable to power to the radio. Then the currents in the positive and negative wires are equal and opposite, causing their magnetic fields to cancel. The result is no net inductance in the connection to cause voltage overshoot.
- Do not connect a radio to a power supply that is already powered up, unless necessary (that is, when connecting a radio to a battery bank and charger). When power is applied by switching on a power supply, the rise time of the supply is too slow to cause overshoot.
- Typically, there are multiple return paths for the negative side of the power supply, through the coaxial cable shield and the chassis, for example. Any imbalance in the currents in the power cable results in voltage overshoot, so this should be minimized during initial power-up if the supply cannot be turned off.
- Add a 1 to 2  $\Omega$ , 2 W resistor in series with the positive lead. This greatly limits voltage overshoot. Since these radios draw very little current in receive mode, and transmit only briefly, there is little loss in power efficiency. In transmit, the voltage drop is minimal and has no effect.

- Minimize the length of the power cabling, within reason.
- When power is applied from a power source having a relatively high (1 or 2  $\Omega$ ) source impedance, or from a power source without a large amount of output capacitance, no overshoot occurs. Therefore, use a power supply that is rated appropriately for the radio if possible—avoid using power supplies that far exceed the radio’s current requirements.

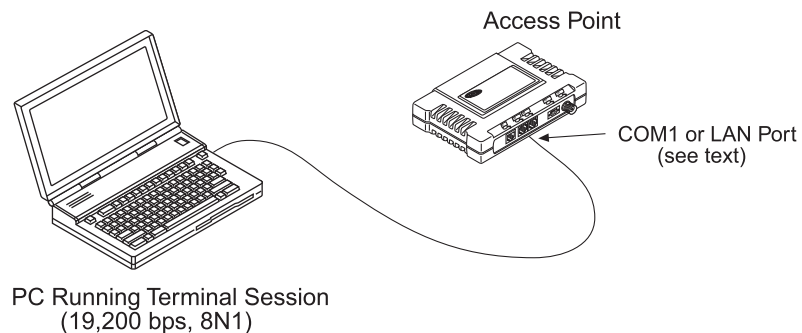
Direct any questions you may have about interfacing to GE MDS radios to GE MDS Technical Services at [gemds.techsupport@ge.com](mailto:gemds.techsupport@ge.com), or telephone +1-585-241-5510.

### STEP 3—CONFIGURE THE AP

The instructions below summarize essential AP settings for tabletop testing. For detailed AP log-in and menu navigation instructions, see [ACCESSING THE MENU SYSTEM](#) on Page 36.

#### Log-in and Configuration

The AP must be configured first, as Remote transceivers depend on the AP beacon signal to achieve a connected (linked) state. [Figure 2-5](#) shows the basic setup for configuring an AP with a personal computer.



**Figure 2-5. AP Configuration Setup**

#### **Console Terminal Connection** (recommended for first-time log-in)

To configure the AP using a console terminal:

1. Connect a PC to the COM1 port on the radio.
2. Establish a terminal session (using HyperTerminal, for example) using the following data parameters:
  - 19200 *bps*
  - 8 *bits*
  - no parity
  - one stop bit (8N1)
  - *hardware flow control* disabled
  - VT100 emulation

---

**NOTE:** The **exact** parameters given above must be used for console terminal communication. Improper settings are a common cause of difficulty.

---

**Telnet Connection  
Using the AP LAN  
Port** (a valid IP  
address must be set)

To configure the AP using its LAN port:

1. Connect a PC Ethernet port to the AP with an Ethernet crossover cable.

---

**NOTE:** The radio must first have a valid IP address programmed—the default IP address is 192.168.1.1.

---

2. Log in to the AP as follows:
  - a. Press the **[ENTER]** key to receive the **login** prompt. The COM1/LAN LED flashes to indicate data communications.
  - a. At the **login** prompt, enter the username (**admin** is the default username). Press **[ENTER]**.
  - b. At the **Password** prompt, enter the password (**admin** is the default password). Press **[ENTER]**. Upon successful log-in, the *Starting Information Screen* appears.
3. Review the current menu settings and make any necessary changes. Refer to [Set Key AP Parameters](#) on Page 22 for configuration guidance.
4. Repeat Steps 1 through 3 for any other AP radios in your system.

---

**NOTE:** You can save time by using configuration scripts to uniformly configure multiple transceivers. This technique is discussed in the [Configuration Scripts Menu](#) on Page 87.

---

### Set Key AP Parameters

[Table 2-1](#) provides a listing of key AP operating parameters, their default settings, and their values or range. Typically, these are the only settings that need to be set or reviewed for a basic check of the radio system. A complete list of AP commands appears in [CHAPTER 3 AP MANAGEMENT](#), beginning on Page 29.



**Table 2-1. Key AP Parameters and Defaults**

Menu Item	Management System Location	Default	Values or Range
<b>IP Address</b>	Main Menu >> Network Configuration > IP Configuration	192.168.1.1	Contact your Network Administrator.  If <b>IP Address Mode</b> (below) is set to Dynamic, <b>IP Address</b> is configured automatically.
<b>IP Address Mode</b>	Main Menu >> Network Configuration > IP Configuration	Static	Static   Dynamic
<b>IP Netmask</b>	Main Menu >> Network Configuration > IP Configuration	255.255.0.0	Settable per customer requirements
<b>Net Address</b>	Main Menu >> Network Configuration > Wireless MAC Configuration	9999	1-15 alphanumeric characters*
<b>RF Output Power (non-ETSI)</b>	Main Menu >> Radio Configuration >	900 MHz: 30 dBm 2.4 GHz: 27 dBm	900 MHz: 20–30 dBm 2.4 GHz: 17-27 dBm
<b>RF Output Power (ETSI)</b>	Main Menu >> Radio Configuration >	2.4 GHz: 20 dBm	2.4 GHz: 10-20 dBm
<b>Password Changes</b>	Main Menu >> Security Configuration > User Passwords	Administrator Password: <b>admin</b> (lower case)  Guest Password: <b>guest</b> (lower case)	<ul style="list-style-type: none"> <li>• 1–8 alphanumeric characters</li> <li>• Passwords are case sensitive; can be mixed case</li> </ul>

\* We recommend setting Net Address to the last four digits of the AP serial number to reduce the chance of conflict with other nearby entraNET systems.

## STEP 4—CONFIGURE THE REMOTE RADIO

The instructions below summarize essential Remote settings for tabletop testing. For detailed log-in and menu navigation instructions, see [CHAPTER 4 REMOTE RADIO MANAGEMENT](#), beginning on Page 99.

### Log-in and Configuration

Prepare the Remote for configuration as follows:

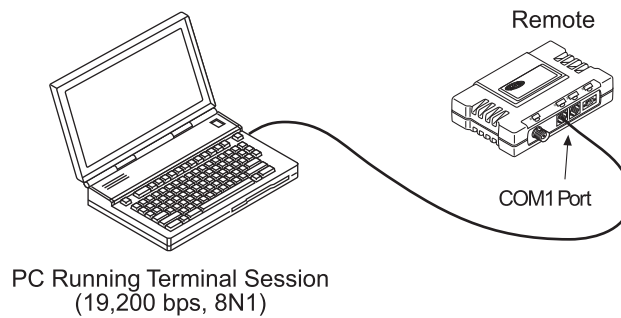
1. Connect a PC to the COM1 port on the radio.
2. Establish a terminal session (using HyperTerminal, for example) using the following data parameters:
  - 19200 bps
  - 8 bits
  - no parity
  - one stop bit (8N1)

- hardware flow control disabled
- VT100 emulation

---

**NOTE:** The **exact** parameters given above must be used for console terminal communication. Improper settings are a common cause of difficulty.

---



**Figure 2-6. Remote Configuration Setup**

3. Press **[ENTER]** several times to receive the **entranet>** prompt (the COM1/ETH LED blinks to indicate data communication).
4. At the **entranet>** prompt, enter **login**. Press **[ENTER]**.
5. At the next prompt, enter the username (the default username is **admin**). Press **[ENTER]**.
6. At the next prompt, enter the password (the default password is **admin**). Press **[ENTER]**. The radio is now ready to accept commands.

### Set or Verify Network Address

The only setting normally required for initial checkout of a Remote radio is the network address. All radios in a given network **must** be programmed with the same network address as the AP, or communication is impossible. Follow the steps below to check the address, and program a new one if necessary.

1. Enter the **RADIO NETADDR=** command. This displays the currently programmed network address.
2. If changes are required, enter the **RADIO NETADDR=<netaddr>** command, where **<netaddr>** is 1 to 15 alphanumeric characters (the network address of the Remote radio **must** match that of the AP).
3. Verify that the LINK LED lights to indicate successful connection with the AP (it might take several seconds for the LED to light).

4. Repeat Steps 1 through 3 for each Remote radio to be installed in the network.

This concludes the basic setup of a Remote radio. A full listing of Remote programming commands is given in *CHAPTER 4 REMOTE RADIO MANAGEMENT*, beginning on Page 99.

With all radios connected, you are ready to connect data devices to the transceivers so that their operation can be tested over the wireless network. This is discussed in the next step.

## STEP 5—CONNECT TERMINAL EQUIPMENT

This step describes connection of external data equipment to the Remote radio. Verify that your transceiver is capable of supporting your devices. See *Table 1-1 on Page 6* for a summary of model capabilities.

Be sure not to overload the radio network with high-bandwidth LAN traffic during this test. Refer to the *Bridge Configuration Menu* on Page 51 for more information.

### Ethernet Device Connection to Remote

---

**NOTE:** Verify that the Remote ETH port is enabled (on) using the **ETH** command. If it is not, use the **ETH=ON** command to enable the port.

---

Connect an Ethernet endpoint to the Remote ETH port. The ETH port supports any Ethernet-compatible device. This includes a device that uses Internet Protocol (IP).

### Serial Device Connection to Remote

Connect a serial device to the Remote COM2 port and verify that the port settings are compatible with the connected device (baud rate, data format, and so on).

## STEP 6—CHECK FOR NORMAL OPERATION

With data equipment connected, you are ready to check the transceivers for normal operation.

Observe the transceiver LEDs on the top cover for the proper indications. In a normally operating system, the following LED indications should be seen within 30 sec of start-up:

- PWR—Lit continuously
- LINK—Lit continuously (unless Sleep is enabled)
- ETH—On, or blinks intermittently
- COM1/COM2—Blinks to indicate data communications

Table 2-2 provides details on the LED functions for Remotes and AP radios.

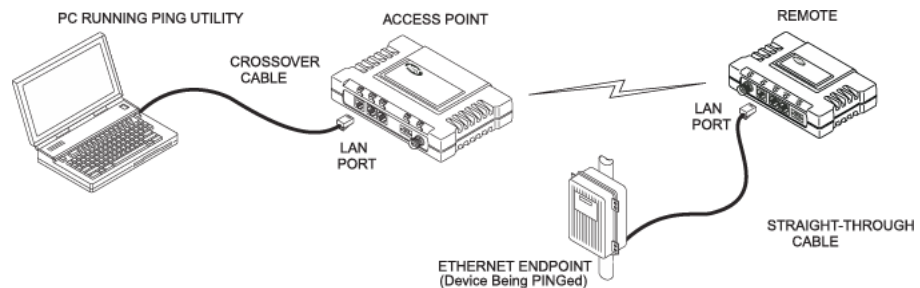
**Table 2-2. Transceiver LED Functions**

LED Label	Activity	Indication
LAN/ETH	ON	LAN or endpoint detected
	Blinking	Data TX or RX
	OFF	LAN or endpoint not detected
COM1 (MGT System)	Blinking	Data TX or RX
	OFF	No data activity
COM2	Blinking	Data TX or RX
	OFF	No data activity
PWR	ON	Primary power (DC) present
	Blinking	Radio in "Alarmed" state
	OFF	Primary power (DC) absent
LINK (AP)	ON	Lights when radio has finished its startup cycle. Remains lit.
LINK (Remote)	ON	Connected to an AP
	OFF	Not connected to an AP

### 2.3.1 Verify Connectivity (PING command)

If the radio LEDs indicate that the radio network is operating properly, you can use the **PING** command from the AP to verify the link integrity between the AP and an endpoint device connected to the Remote radio. Figure 2-7 shows the typical arrangement for this test.

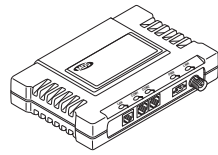
**NOTE:** To conduct a **PING** test, an Ethernet-enabled device must be connected to the Remote, and it must have a compatible IP address. Remote radios do not have an IP address and cannot be verified directly using this method.

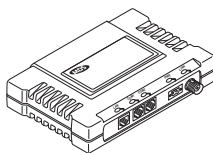


**Figure 2-7. PING Test Setup**  
*(to test connectivity between an AP and an Ethernet endpoint)*

## Serial Connections

To check a serial connection, refer to *Local Serial Configuration Menu* on Page 57. This section contains details on establishing an IP-to-serial or serial-to-serial connection.





# 3 AP MANAGEMENT

<b>3.1 INTRODUCTION</b>	<b>31</b>
3.1.1 PC-Based Configuration Software .....	31
3.1.2 Menu Structure .....	32
3.1.3 Differences in the User Interfaces .....	35
<b>3.2 ACCESSING THE MENU SYSTEM</b>	<b>36</b>
3.2.1 Methods of Control .....	36
3.2.2 PC Connection and Log-In Procedures .....	37
3.2.3 Navigating the Menus .....	42
Navigating via Terminal or Telnet Sessions	
Recommended for first-time users .....	42
Navigating via a Web Browser.....	42
<b>3.3 BASIC DEVICE INFORMATION</b>	<b>43</b>
3.3.1 Starting Information Screen .....	43
3.3.2 Main Menu .....	44
<b>3.4 CONFIGURING NETWORK PARAMETERS</b>	<b>45</b>
3.4.1 Network Configuration Menu .....	45
3.4.2 IP Configuration Menu .....	46
3.4.3 Wireless MAC Configuration Menu .....	48
3.4.4 Mobility Configuration Menu .....	49
3.4.5 SNMP Agent Configuration Menu .....	50
3.4.6 Bridge Configuration Menu .....	51
<b>3.5 CONFIGURING RADIO PARAMETERS</b>	<b>52</b>
3.5.1 Radio Configuration Menu .....	52
Skip Zones Menu.....	53
<b>3.6 CONFIGURING THE SERIAL INTERFACES</b>	<b>54</b>
3.6.1 Overview .....	54
Serial-to-Serial Services .....	55
IP-to-Serial Services .....	55
Configuration .....	56
Serial Configuration Wizard .....	56
3.6.2 Local Serial Configuration Menu .....	57
View Current Settings Screen—Serial-to-Serial Example .....	59
View Current Settings Screen—Unicast UDP Mode Example .....	61
3.6.3 Remote Serial Gateway Configuration (IP-to-Remote Serial) .....	62

<b>3.7 SECURITY CONFIGURATION</b>	<b>64</b>
3.7.1 Security Configuration Menu .....	65
<b>3.8 WIRELESS NETWORK MENU</b>	<b>69</b>
3.8.1 Remote Management Submenu .....	70
Manage Selected Remote Submenu .....	71
Broadcast Remote Reprogramming Menu .....	72
Remote Database Menu.....	74
Group Database Menu .....	75
Endpoint Database Menu .....	75
Access Point Database Menu .....	76
<b>3.9 STATISTICS AND EVENT LOG</b>	<b>77</b>
3.9.1 COM1 and COM2 Data Statistics Menus .....	78
3.9.2 Remote Serial Gateway Statistics .....	79
3.9.3 Ethernet and Wireless Packet Statistics .....	80
Ethernet Packet Statistics .....	80
Wireless Packet Statistics.....	80
3.9.4 Radio Packet Statistics .....	81
3.9.5 Event Log Menu .....	82
Time and Date Stamping .....	82
<b>3.10 DEVICE INFORMATION MENU</b>	<b>84</b>
Device Names Menu .....	85
<b>3.11 MAINTENANCE AND TOOLS</b>	<b>85</b>
3.11.1 Reprogramming Menu .....	86
3.11.2 Configuration Scripts Menu .....	87
A Brief Description of Configuration Files.....	87
3.11.3 RSG Configuration Script Menu .....	89
3.11.4 Authorization Codes Menu .....	91
3.11.5 Transmitter Test Menu .....	92
<b>3.12 REDUNDANCY MENU</b>	<b>93</b>
Packet Rx Errors Exceeded Threshold Menu .....	96
<b>3.13 DNP3 ROUTING MENU</b>	<b>97</b>



## 3.1 INTRODUCTION

The GE MDS entraNET AP embedded Management System (MS) is accessible through various data interfaces. These include the COM1 (serial) port, LAN (Ethernet) port, and SNMP. Essentially the same capabilities are available through any of these paths.

For SNMP management, the transceiver is compatible with GE MDS NETview MS™ software. Refer to GE MDS publication 05-2973A01 for more information on this product. For support of other SNMP software, a set of MIB files is available for download from the GE MDS Web site at [www.gemds.com](http://www.gemds.com).

The entraNET MS has the following functions:

- [3.4 CONFIGURING NETWORK PARAMETERS](#) (beginning on page 45)
- [3.5 CONFIGURING RADIO PARAMETERS](#) (beginning on page 52)
- [3.6 CONFIGURING THE SERIAL INTERFACES](#) (beginning on page 54)
- [3.7 SECURITY CONFIGURATION](#) (beginning on page 64)
- [3.8 WIRELESS NETWORK MENU](#) (beginning on page 69)
- [3.9 STATISTICS AND EVENT LOG](#) (beginning on page 77)
- [3.10 DEVICE INFORMATION MENU](#) (beginning on page 84)
- [3.11 MAINTENANCE AND TOOLS](#) (beginning on page 85)
- [3.12 REDUNDANCY MENU](#) (beginning on page 93)
- [3.13 DNP3 ROUTING MENU](#) (beginning on page 97)

Each of these sections has a focus that is reflected in its heading. The section you are now reading provides you with information on connecting to the AP, how to navigate through its menus, and how to perform some top-level configuration tasks.

### 3.1.1 PC-Based Configuration Software

The *GE MDS Remote Access Manager Application* (Part Number 06-4490A01) makes it possible to authenticate all Access Points and associated Remotes from a PC, without having to update individual radios. The software maintains a Master Approved Remotes List, and all participating access points are synchronized with this list. Contact GE MDS for more information.

---

**NOTE:** If a PC is connected to a Remote radio while the Remote is asleep, the PC does not enable its Ethernet adapter, as it believes the port is disconnected. Also, if a PC is connected to a Remote and the radio goes to sleep, the PC goes into a “port disconnected” state. The PC must be properly configured to avoid these scenarios.

---

The commands for Remote radios are presented separately in [CHAPTER 4 REMOTE RADIO MANAGEMENT](#), beginning on Page 99.

---

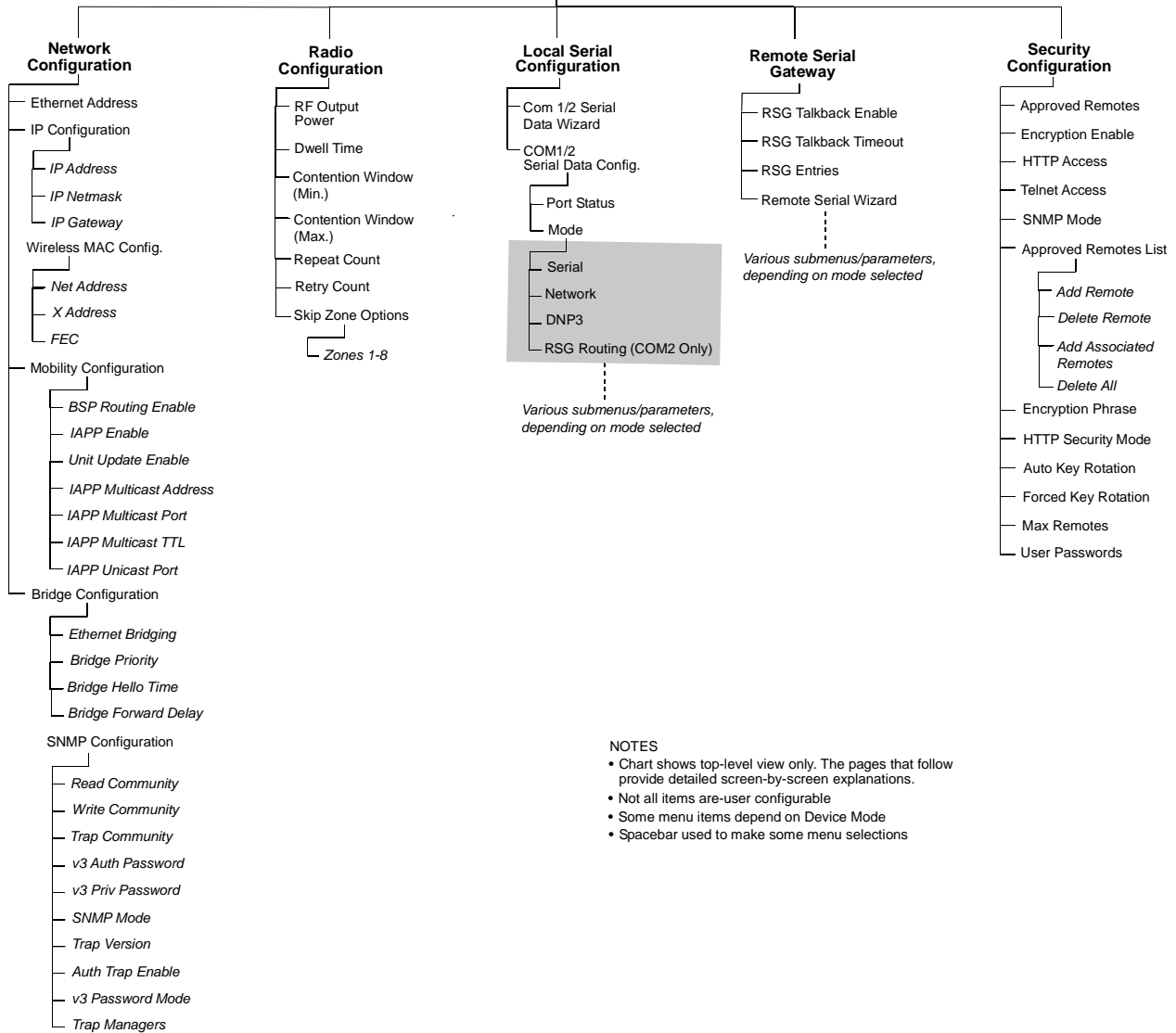
**NOTE:** Any parameter options, ranges, or default values are displayed at the end of the field description between square brackets. The default value is always shown last in a series of items. For example:  
[Range, Options or Description; Default]

---

### 3.1.2 Menu Structure

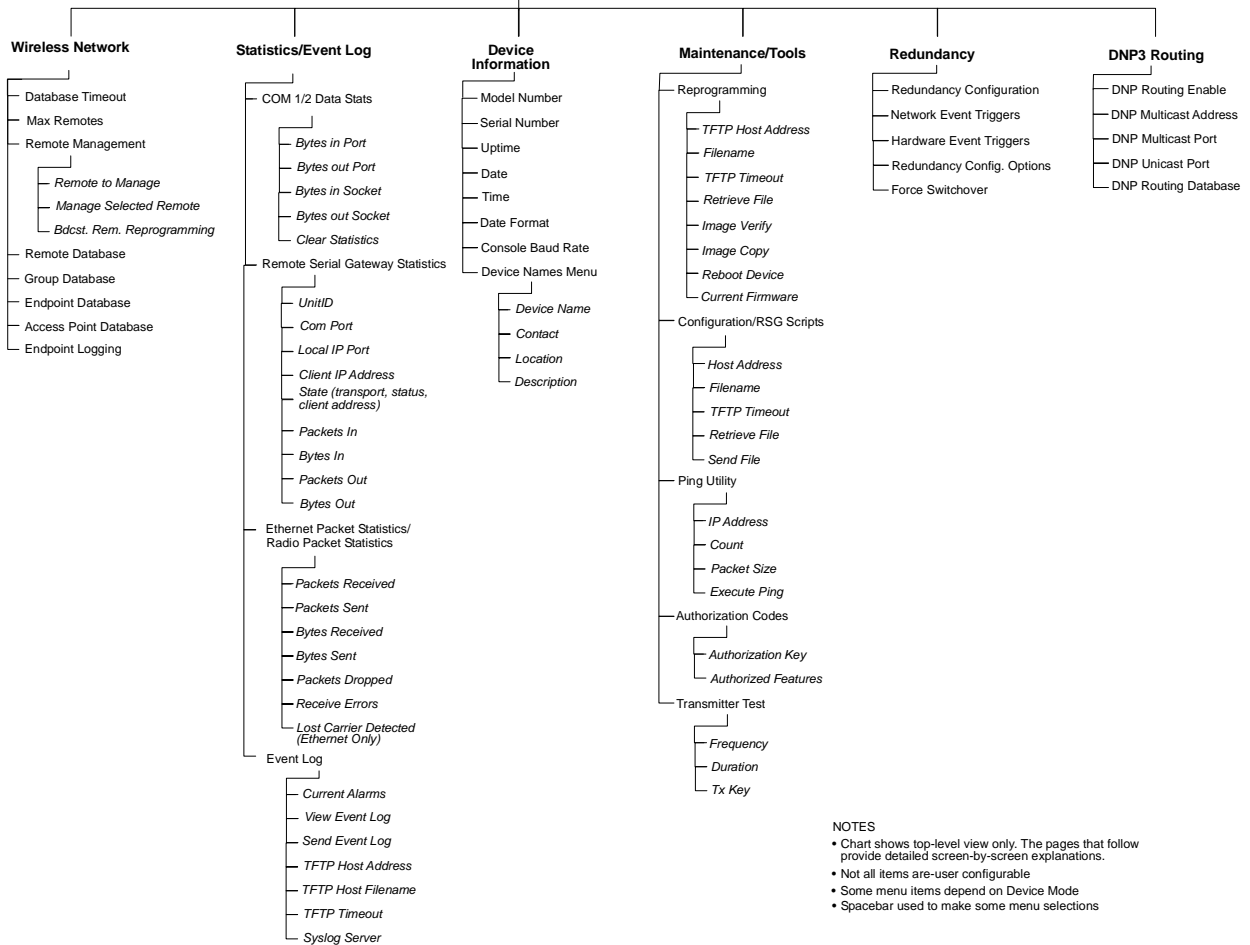
The following illustrations ([Figure 3-1](#) and [Figure 3-2](#)) show an overall view of the entraNET MS. Detailed information for screens and menu items is provided on the pages that follow.

**MAIN MENU—Diagram 1 of 2**  
Starting Information Screen (read-only items)



**Figure 3-1. entraNET MS Menu Flowchart**  
(diagram 1 of 2)

**MAIN MENU—Chart 2 of 2**  
**Starting Information Screen (read-only items)**

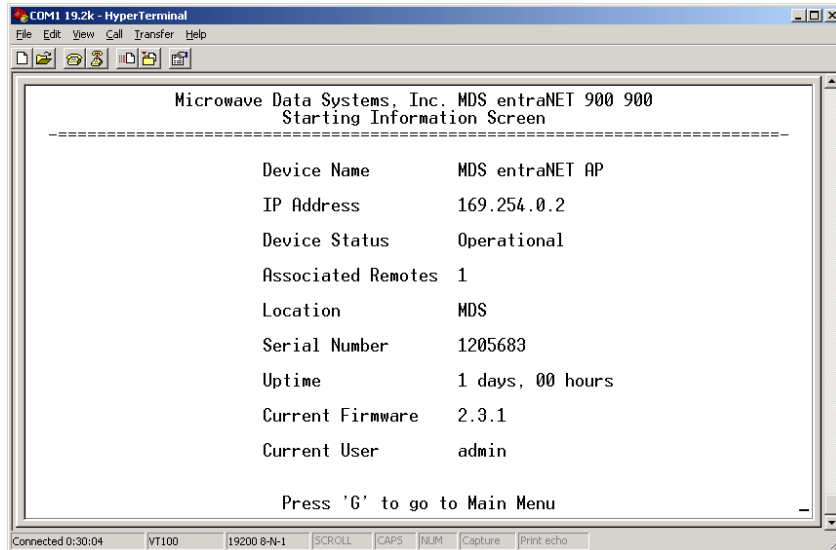


**NOTES**  
 • Chart shows top-level view only. The pages that follow provide detailed screen-by-screen explanations.  
 • Not all items are user configurable  
 • Some menu items depend on Device Mode  
 • Spacebar used to make some menu selections

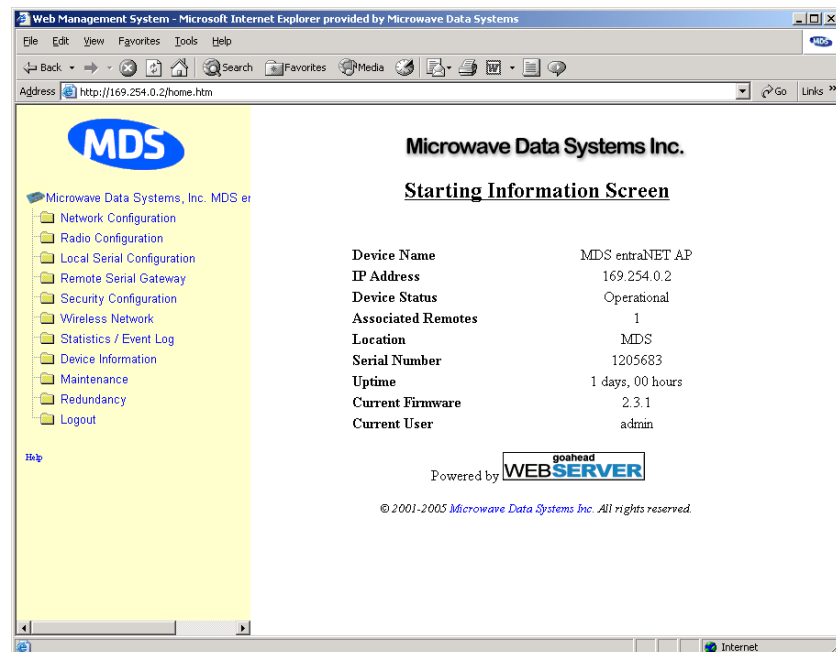
**Figure 3-2. entranET MS Menu Flowchart**  
*(diagram 2 of 2)*

### 3.1.3 Differences in the User Interfaces

There are slight differences in navigation between Telnet, terminal, and Web interfaces. Generally, the screen content is the same. There are minor differences in capabilities from limitations of the access channel. Below are samples of the *Starting Information Screen* as seen through a terminal session and a Web browser.



**Figure 3-3. View of entraNET MS Using a Terminal Session**  
(a Telnet session is similar)



**Figure 3-4. View of the entraNET MS from a Web Browser**

## 3.2 ACCESSING THE MENU SYSTEM

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

### 3.2.1 Methods of Control

The radio configuration menus may be accessed in several ways:

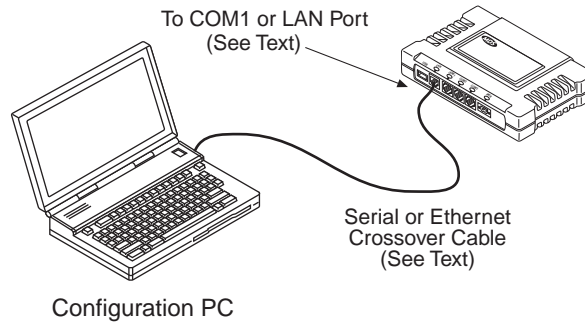
- **Local Console**—*This is the primary method used for the examples in this manual.* Connect a PC directly to the COM 1 port on the radio using a serial communications cable and launch a terminal communications program such as HyperTerminal. This method provides text-based access to the radio menu. Console control is a hardware-based technique, and is intended for local use only.
- **Telnet\***—Connect a PC to the LAN port on the radio, either directly or over a network, and launch a Telnet session. This method provides text-based access to the radio menu, 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 LAN port on the radio, either directly or over a network, and open a Web browser (Internet Explorer, Netscape, and so on). This method provides a graphical representation of each screen, just as you see when viewing an Internet Web site. The menu screens look a little different from other methods of control, but the content and organization of screen items is similar. Web browser sessions may be run locally or remotely over the Internet.

\* Telnet and Web browser sessions require the use of a straight-through or Ethernet crossover cable, depending on the whether the PC-to-radio connection is made directly or through an Ethernet switch or hub. For direct connection, a **crossover** cable is required; for connection via a switch or hub, a **straight-through** cable is needed.

To identify the cable type, hold the two cable ends side by side and in the same plug orientation (that is, both locking tabs are up or down). Now look at the individual wire colors on each plug. If the wires on both plugs are ordered in the same sequence from left to right, the cable is a straight-through type. If they are not in the same order, it **may** be a crossover cable, or it may be wired for some other application. Refer to [DATA INTERFACE CONNECTORS](#) on Page 187 for detailed pinout information.

### 3.2.2 PC Connection and Log-In Procedures

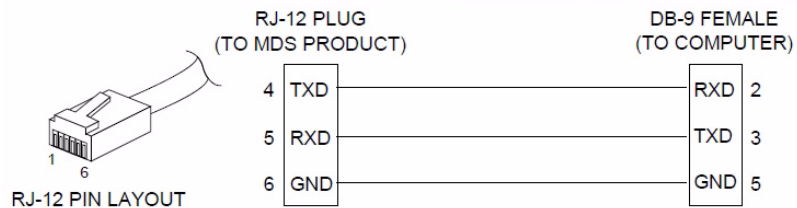
The following steps describe how to access the radio menu. These steps require a PC to be connected to the COM 1 or LAN port on the radio, as shown in [Figure 3-5](#).



**Figure 3-5. PC Configuration Setup**

#### **Starting a Local Console Session** (recommended for first-time users)

1. Connect a serial communications cable between the PC and the COM 1 port on the radio. If necessary, a cable may be constructed for this purpose, as shown in [Figure 3-6](#).



**Figure 3-6. Serial Communications Cable (RJ-12 to DB-9)**  
(maximum recommended cable length is 50 ft/15m)

2. Launch a terminal emulation program such as HyperTerminal.
 

**TIP:** The HyperTerminal program can be accessed on most PCs by selecting **Start > Programs > Accessories > Communications > HyperTerminal**.
3. Configure the connection with the following settings:
  - 19200 bps
  - 8 bits
  - no parity
  - one stop bit (8N1)
  - hardware flow control disabled
  - VT100 emulation

The **exact** parameters given above must be used for console terminal communication. Improper settings are a common cause of difficulty.

---

**NOTE:** If the radio is powered up or restarted while connected to a terminal, a series of pages of text relating to the startup of the internal microcomputer is displayed. Wait for the log-in screen before proceeding.

---

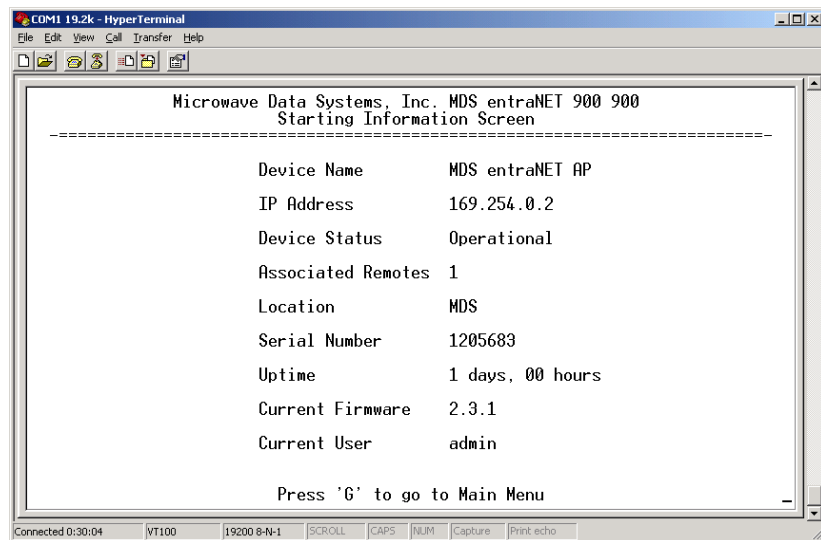
4. Press **[ENTER]** to receive the **login** prompt.
5. Enter the username (the default username is **admin**). Press **[ENTER]**.
6. Enter your password (the default password is **admin**). For security, your password keystrokes do not appear on the screen. Press **[ENTER]**.

---

**NOTE:** Passwords are case sensitive. Do not use punctuation marks. You may use up to eight alphanumeric characters.

---

The *Starting Information Screen* is displayed (Figure 3-7). From here, you can review basic information about the radio, or press **G** to proceed to the *Main Menu*.



**Figure 3-7. Starting Information Screen—Local Console Session**

### **Starting a Telnet Session**

---

**NOTE:** This method requires that you know the IP address of the radio 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 LAN port on the radio, either directly or over a network. If connecting directly, use an Ethernet **crossover** cable; if connecting over a network, use a **straight-through** cable. The LAN LED lights to indicate an active connection.



---

**NOTE:** When using a Local Area Network (LAN) to access the radio, it may be necessary to change the computer IP access to the LAN in order to be compatible with the entraNET radio (compatible subnets). You can identify or verify the radio IP address by using a Local Console session to communicate with the entraNET 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 radio 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, enter the word **telnet**, followed by the radio IP address (for example, **telnet 10.1.1.168**). Press **[ENTER]** to display the Telnet log-in screen.

---

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

---

3. Enter the username (the username default is **admin**). Press **[ENTER]**.

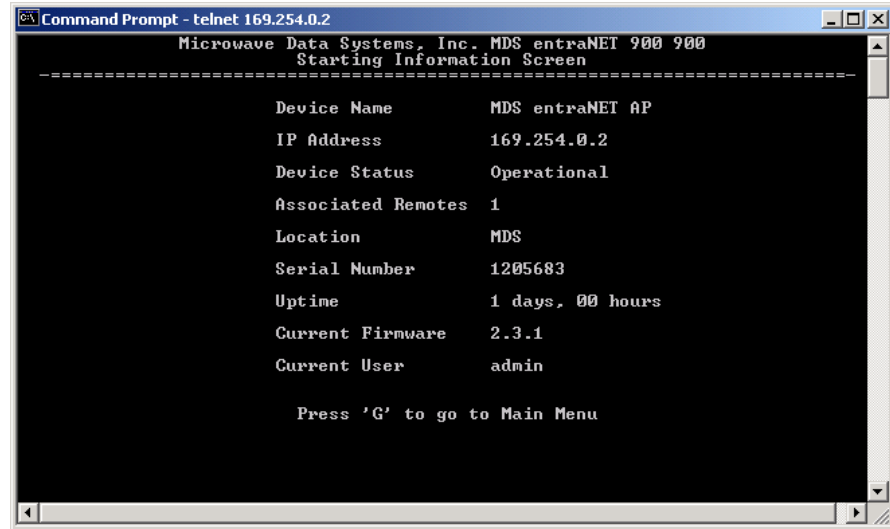
Next, the **Password** prompt appears. Enter your password (the default password is **admin**). For security, your password keystrokes do not appear on the screen. Press **[ENTER]**.

The *Starting Information Screen* is displayed ([Figure 3-8](#)). From here, you can review basic information about the radio, or press **G** to proceed to the *Main Menu*.

---

**NOTE:** Passwords are case sensitive. Do not use punctuation marks. You may use up to eight alphanumeric characters.

---

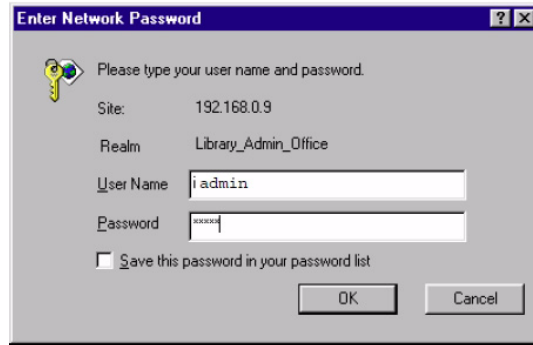


**Figure 3-8. Starting Information Screen—Telnet Example**

### Starting a Web Browser Session

**NOTE:** This method requires that you know the IP address of the radio to which you are connecting. If you do not know the address, start a Local Console session (see [Starting a Local Console Session \(recommended for first-time users\)](#) on Page 37) and access the *Starting Information Screen*. The IP address is displayed on this screen.

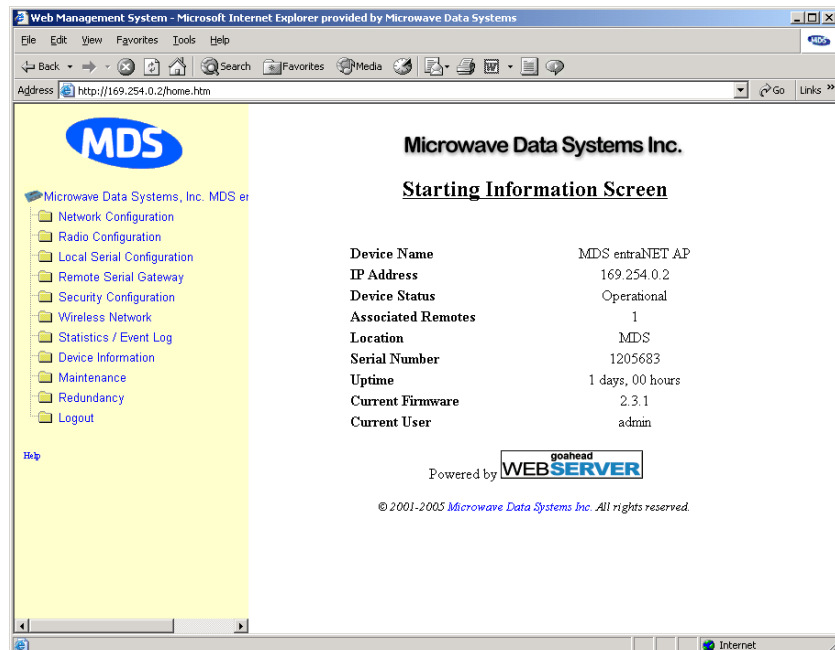
1. Connect a PC to the LAN port on the radio, either directly or over a network. If connecting directly, use an Ethernet **crossover** cable; if connecting over a network, use a **straight-through** cable. The LAN LED lights to indicate an active connection.
2. Open a Web browser on your computer (for example, Internet Explorer or Netscape Navigator).
3. Enter the radio IP address and press **[ENTER]**.
4. A log-in page is displayed ([Figure 3-1](#)) where you enter a user name and password to access the radio menu. The default entries are made in **lower case** (default username: **admin**; default password: **admin**).



**Figure 3-9. Log-in Page when using a Web Browser**

**NOTE:** Passwords are case sensitive. Do not use punctuation marks. You may use up to eight alphanumeric characters.

5. Click **OK**. The radio responds with a startup menu (Figure 3-10). From here, you can review basic information about the radio, or click one of the menu items on the left side of the page.



**Figure 3-10. Starting Information Page—Web Browser Example**

## 3.2.3 Navigating the Menus

### Navigating Using Terminal or Telnet Sessions

*Recommended for first-time users*

Local console and Telnet sessions use multi-layered text menu systems that are nearly identical.

- To select a menu item, press the letter shown at the beginning of that item. This takes you to an associated screen where you can view or change settings.
- To return to the previous menu (in most cases), press `[ESCAPE]`.

In general, the top portion of menu screens show **read-only** information (with no menu 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-definable parameter fields:

- Press the letter shown at the beginning of the user-definable parameter.

If there is a user-definable value, the field clears to the right of the menu item, and you can enter the value you wish to use.

In some cases, when you select a parameter, you see a prompt at the bottom of the screen that says **Choose an Option**. Press `[SPACE]` to step through the available selections.

- Press `[ENTER]` to accept the displayed parameter (the one you entered, or the one you chose by pressing `[SPACE]`). In some cases, several parameters may be changed and then saved with a single keystroke.
- To cancel the parameter change, simply press `[ESCAPE]` to restore the previous value.

#### **Log Out Using Terminal Emulator or Telnet**

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

### Navigating Using a Web Browser

Navigating with a Web browser is straightforward, with a scrollable, clickable “page” instead of a command-line interface. The primary navigation menu is permanently located on the left side of this page. Click a desired menu item to display it.

---

**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 min of inactivity.

---

## Log Out Using a Web Browser

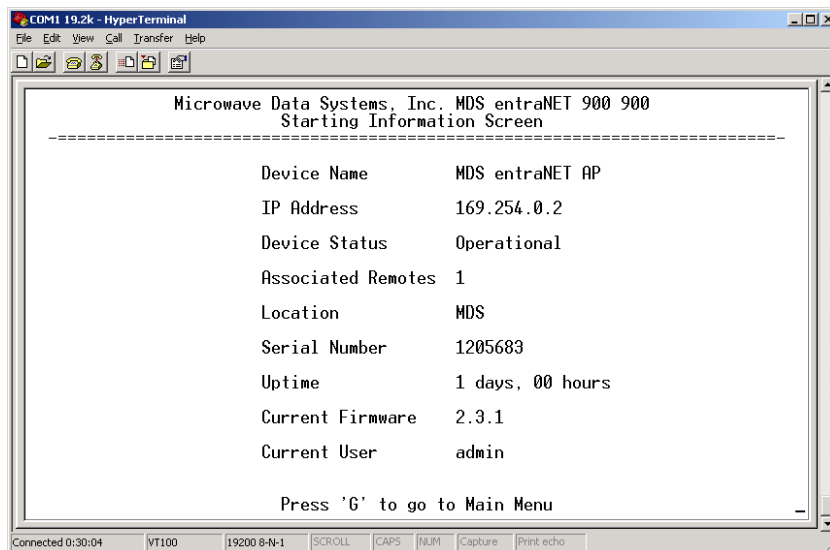
Click **Logout** in the left-hand frame of the browser window. The right-hand frame changes to a log-out page. Follow the remaining instructions on this screen.

This completes the instructions for connecting to the entraNET radio for PC configuration and control. The next section contains detailed menu screens and settings you can use to specify the behavior of the radio.

## 3.3 BASIC DEVICE INFORMATION

### 3.3.1 Starting Information Screen

Upon successful log-in to the menu system, the *Starting Information Screen* appears. This screen provides a read-only overview of the current operating conditions on the transceiver ([Figure 3-11](#)), although some items can be changed using the *Device Information Screen* described on Page 84.



**Figure 3-11. Starting Information Screen**

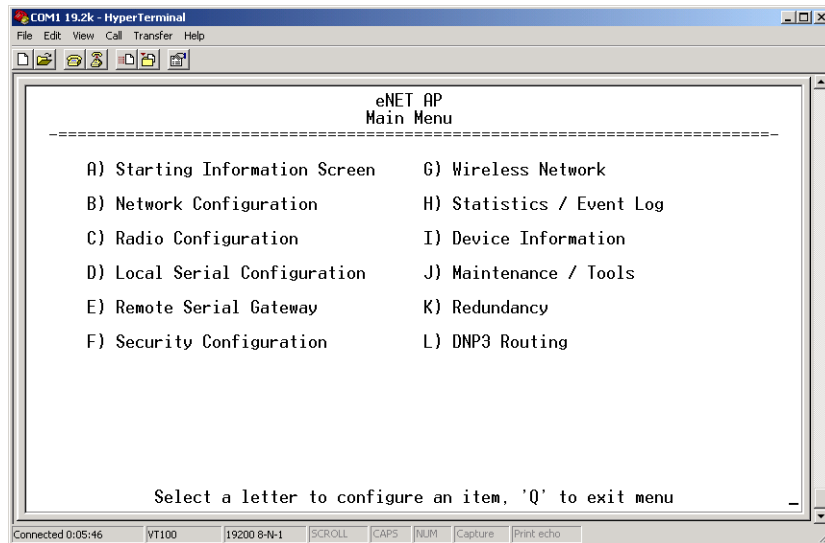
- **Device Name**—This is a user-defined name for the radio that appears on every screen (40 characters maximum).
- **IP Address**—Shows the radio Internet Protocol (IP) address.
- **Device Status**—Shows the transceiver condition:
  - *Operational*—The radio is operating normally
  - *Alarmed*—An alarm event has been logged and not cleared.

**NOTE:** If an alarm is present when this screen is displayed, an “A” appears to the left of the **Device Status** field. (The PWR LED also flashes.) Typing “A” on your keyboard takes you directly to the *Current Alarms Screen*.

- **Associated Remotes**— Shows current number of Remote radios associated with the AP.
- **Location**—User-definable string that you can use to identify the radio location (40 characters maximum).
- **Serial Number**—Unique identifier for this device. It must be provided to GE MDS when purchasing Authorization Keys to upgrade radio capabilities. See “*Authorization Codes Menu*” on Page 91.
- **Uptime**—Elapsed time since the transceiver was powered up.
- **Current Firmware**—Version of firmware that is currently active in the radio.
- **Current User**—Privilege level of the currently logged in user.

### 3.3.2 Main Menu

The *Main Menu* (Figure 3-12) is the entryway to all customer-definable features. The radio **Device Name** appears at the top of this and all other screens as a reminder of the radio that is being interrogated.



**Figure 3-12. Main Menu**

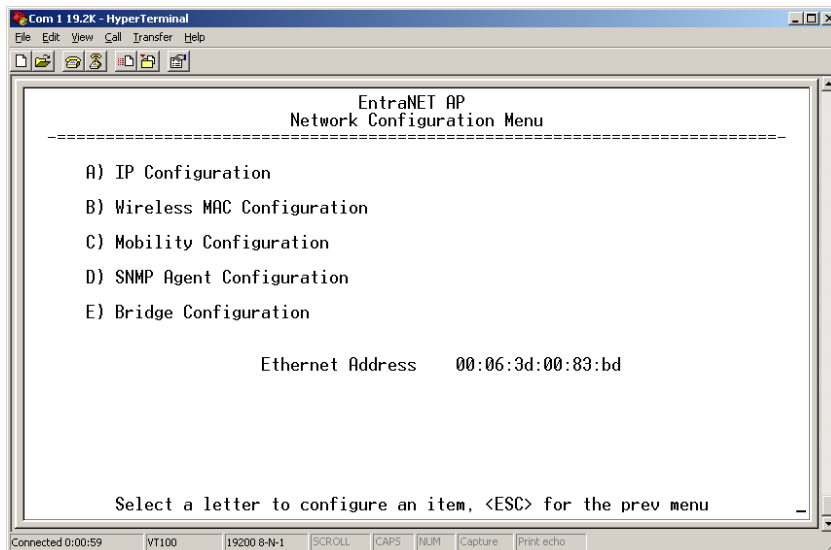
- **Starting Information Screen**—Select this item to return to the *Starting Information Screen*. See “*Starting Information Screen*” on Page 43.
- **Network Configuration**—Tools to configure the transceiver data network settings. See “*Network Configuration Menu*” on Page 45.
- **Radio Configuration**—Tools to configure the transceiver wireless (radio) functions. See “*Radio Configuration Menu*” on Page 52.
- **Local Serial Configuration**—Tools to configure the AP COM1 and COM2 serial ports. See “*Local Serial Configuration Menu*” on Page 57.

- **Remote Serial Gateway**—Tools to configure the data connections to the Remote transceiver serial ports. See *“Remote Serial Gateway Configuration (IP-to-Remote Serial)”* on Page 62.
- **Security Configuration**—Tools to configure the transceiver security services. See *“SECURITY CONFIGURATION”* on Page 64.
- **Wireless Network**—Tools to manage Remote and AP databases, and manage Remote radios. See *“WIRELESS NETWORK MENU”* on Page 69.
- **Statistics/Event Log**—Tools to measure the radio and data layer network performance. See *“STATISTICS AND EVENT LOG”* on Page 77.
- **Device Information**—Top-level customer-specific and definable parameters, such as the date, time, console baud rate, and device name information. See *“DEVICE INFORMATION MENU”* on Page 84.
- **Maintenance/Tools**—Tools for upgrading and selecting firmware images and configuration files, and applying Authorization Keys to change radio capabilities. See *“MAINTENANCE AND TOOLS”* on Page 85.
- **Redundancy**—Places the radio in a “1+1” redundancy-compatible mode. This mode is specifically for use with GE MDS P22 packaged model chassis. Check with your GE MDS sales representative for available configurations. See *“REDUNDANCY MENU”* on Page 93.
- **DNP3 Routing**—This selection provides access to a submenu where you can manage DNP3 routing attributes. See *“DNP3 ROUTING MENU”* on Page 97.

## 3.4 CONFIGURING NETWORK PARAMETERS

### 3.4.1 Network Configuration Menu

The *Network Configuration Menu* (Figure 3-13) is the home of all IP- and Ethernet-level parameters.



**Figure 3-13. Network Configuration Menu**  
(From Access Point)

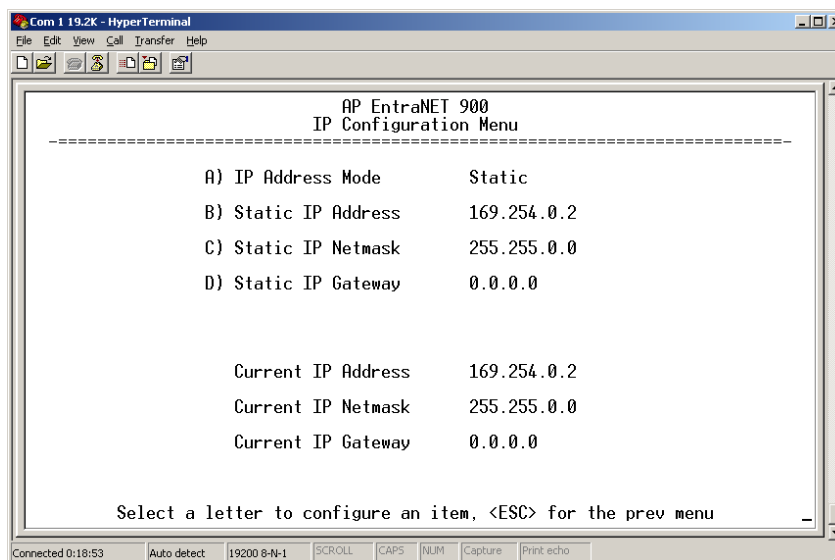
This menu is subdivided into the following sections:

- **IP Configuration**—The transceiver IP address, netmask, and gateway addresses.
- **Wireless MAC Configuration**—Parameters for the Media Access Control (MAC) wireless protocol.
- **Mobility Configuration**—Parameters that control handoffs.
- **SNMP Configuration**—Details that control the operation of the Simple Network Management Protocol (SNMP). SNMP is used in conjunction with GE MDS NETview MS software. See publication 05-2973A01 for details.
- **Bridge Configuration**—Specialized parameters for the operation of Ethernet bridging, including priority and forward delay settings.

### 3.4.2 IP Configuration Menu

The radios use a local IP address to support remote management and serial device services. You can set the IP address of a radio as a static IP address or as a dynamic IP address using the *IP Configuration Menu* (Figure 3-14).





**Figure 3-14. IP Configuration Menu**

When static IP addressing is used, the user must manually configure the IP address and other parameters. When dynamic addressing is used, the radio uses a *Dynamic Host Configuration Protocol* (DHCP) Client process to obtain an IP address from a DHCP Server, along with other parameters such as a net mask and a default gateway.

---

**CAUTION:** Changing any of the following parameters while communicating over the network (LAN or over-the-air) might cause a loss of communication with the unit being configured. You will need to reestablish communication using the new IP address.

---

- **IP Address Mode**—Defines how the IP address of this device is obtained: either statically configured, or dynamically assigned from a DHCP server. [**Static, Dynamic; Static**]
- **Static IP Address**—(*We recommend that you review this setting.*) Essential for connectivity to the transceiver MS using the LAN port, and to encapsulate serial data over an IP. Enter any valid IP address that is unique within the network. [**192.168.1.1**]

This field is unnecessary if you enable DHCP.

- **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, or if all devices are on the same subnet. [**0.0.0.0**]
- **Current IP Address**—(*We recommend that you review this setting.*) Displays the IP address.
- **Current IP Netmask**—Displays the IPv4 local subnet mask.

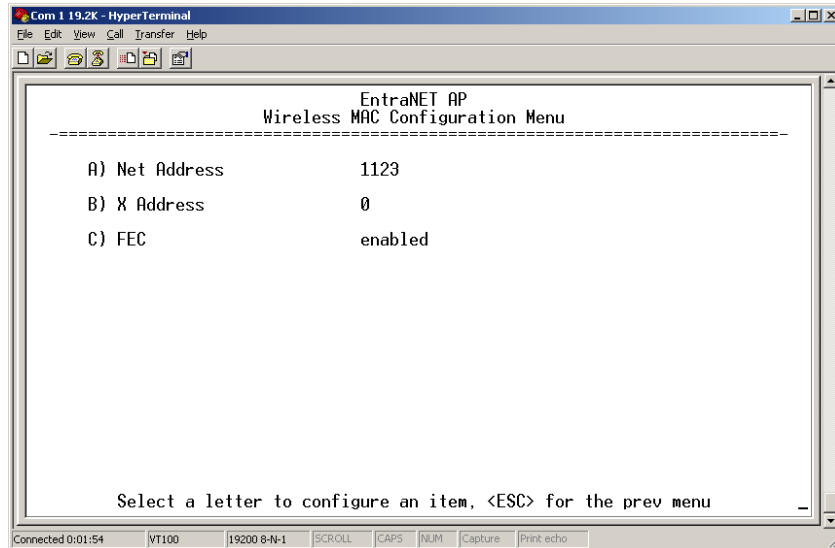
- **Current IP Gateway**—Displays the IPv4 address of the default gateway device, typically a router.

---

**NOTE:** The radio is not a router, so all IP parameters access local management only and have no effect on the routing of system data.

---

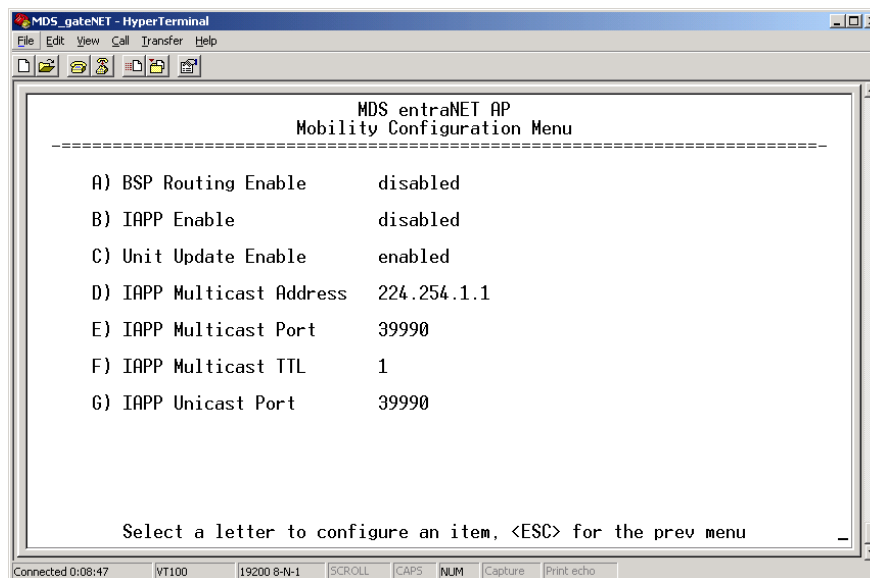
### 3.4.3 Wireless MAC Configuration Menu



**Figure 3-15. Wireless Mac Configuration Menu**

- **Net(work) Address**—(You must review this setting.) ID of the network to which this radio belongs (1-15 alphanumeric characters). An address is essential for connection of Remotes to the AP in the entraNET network. The radio network address is not programmed at the factory. [9999]
- **X Address**—Extended Address, used for installations with multiple APs supporting mobility. This address must be a unique value for each AP. This parameter has no effect in single AP networks. [0]
- **FEC**—Forward Error Correction status (enabled or disabled). The FEC setting has a significant effect on the throughput or speed of the radio network. For a discussion of this and other issues affecting throughput, see *“OPTIMIZING PERFORMANCE”* on Page 160. In particular, Table 6-7 on Page 163 of this section shows the FEC settings and how they relate to hop times and the *bytes-per-packet* rate. [Enabled, Disabled; Disabled]

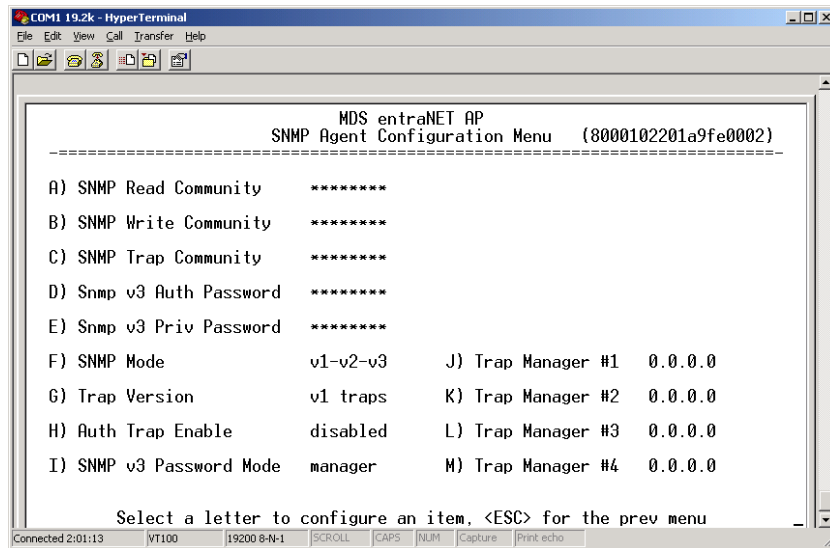
### 3.4.4 Mobility Configuration Menu



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

- **BSP Routing Enable**—This parameter controls intra-cell transmission and routing of Basic Serial Protocol packets. [Enabled, Disabled; Disabled]
- **IAPP Enable**—This parameter enables the Inter-Access Point Protocol (*IAPP*), which allows APs to pass payload data over the Ethernet LAN. [Enabled, Disabled; Disabled]
- **Unit Update Enable**—This parameter allows the AP to immediately send out an IAPP update when a Remote connects or disconnects. [Enabled, Disabled; Disabled]
- **IAPP Multicast Address**—An address that allows multicast messaging to reach all radios in a subnetwork (all radios with a common network address). [224.254.1.1]
- **IAPP Multicast Port**—An assigned software port that allows multicast messaging to reach all radios in a subnetwork (all radios with a common network address). [39990]
- **IAPP Multicast TTL**—Multicast “time to live” number. This is the number of hops that a message is allowed to make before it is no longer transportable. This feature prevents “infinite life” packets that degrade system performance. [1-15; 1]
- **IAPP Unicast Port**—An address that allows messaging to travel to a specific radio when that message has originated from another subnetwork. [39990]

### 3.4.5 SNMP Agent Configuration Menu



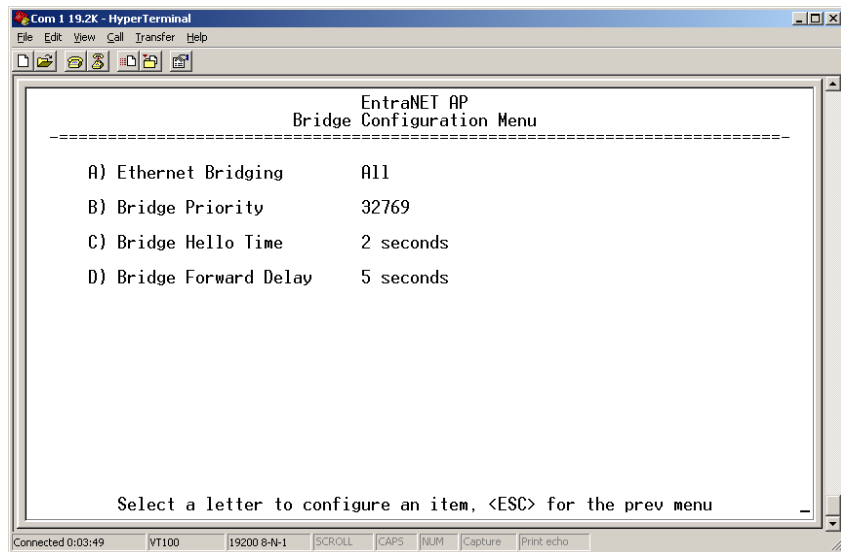
**Figure 3-17. SNMP Agent Configuration Menu**

This menu provides configuration and control of SNMP functionality.

- **SNMP V3 Agent ID**—The alphanumeric string that appears in the upper right-hand corner of the screen. The entry of this string is required in non-GE MDS SNMP manager programs (for example, SNMPc). Refer to program documentation for details.
- **SNMP Read Community**—Community name with SNMP read-level access. Any eight-character alphanumeric string.
- **SNMP Write Community**—Community name with SNMP write-level access. Any eight-character alphanumeric string.
- **Snmp Trap Community**—Community name with SNMP access to receive traps. Any eight-character alphanumeric string.
- **Snmp v3 Auth Password**—The password used in an MD5 (Message-Digest algorithm 5) hash along with the message data to create a message digest. The digest is used by the SNMP entities to validate the source of the packet. The password can be any alphanumeric string between eight and 30 characters in length.
- **Snmp v3 Priv Password**—The privacy password stored in the transceiver flash memory. The password is used in DES (*Data Encryption Standard*) encryption, and can be any alphanumeric string between eight and 30 characters in length. It is used when the SNMP Agent is managing passwords locally (or initially for all cases on restart).
- **SNMP Mode**—Set or display current state of the SNMP agent. [Disabled, v1 only, v2 only, v3 only, v1-v2, v1-v2-v3; v1-v2-v3]
- **Trap Version**—Set the SNMP version for traps. [v1 Traps, v2 Traps, v3 Traps; v1 Traps]

- **Auth Trap Enable**—Current state of the authentication traps. [Disabled/Enabled; Disabled]
- **SNMP v3 Password Mode**—Determines whether v3 passwords are managed locally or using an SNMP Manager. The different behaviors of the Agent, depending on the mode selected, are described in **SNMP Mode** above. [Manager, Local; Manager]
- **Trap Manager (#1–#4)**— Table of up to four locations to which traps are sent. [Any valid IP address]

### 3.4.6 Bridge Configuration Menu



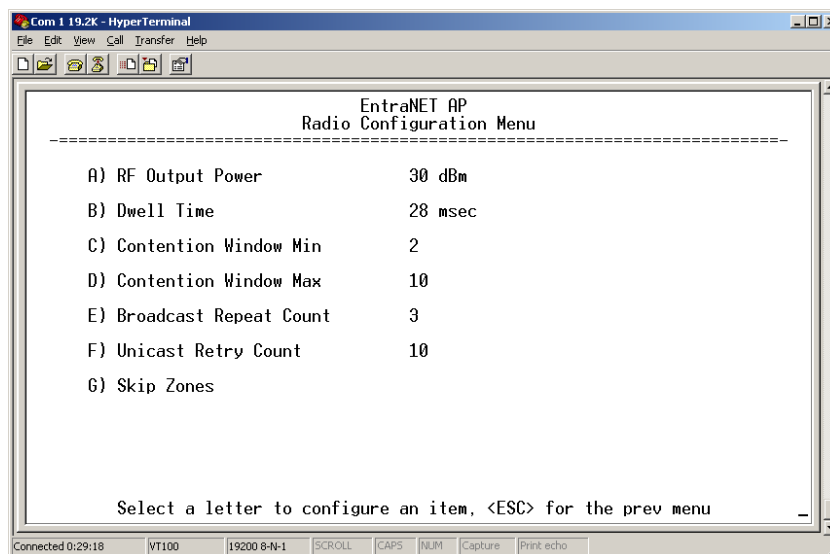
**Figure 3-18. Bridge Configuration Menu**

- **Ethernet Bridging**—Select the type of Ethernet frames sent over the air to Remote radios. [All, Disabled, No Broadcast/Multicast, IP/ARP Only; All]
- **Bridge Priority**—This value is used along with the MAC address to define the bridge ID. The Bridge ID is used by the Spanning Tree protocol to determine the root bridge in the network. This value is useful for forcing a certain bridge to always be the root.
- **Bridge Hello Time**—Defines how often Spanning Tree protocol Bridge Protocol Data Units (BPDU) are sent out by the AP. Each bridge in the network should have the same hello time. [Number of seconds; 2]
- **Bridge Forward Delay**—This value decides how long a bridge is in the “learning” and “listening” states. Traffic begins forwarding through the bridge after twice the Forward Delay time. [Number of seconds; 5]

## 3.5 CONFIGURING RADIO PARAMETERS

There are two primary data layers in the MDS entraNET network—radio (RF) and data. The data layer is dependent on the radio layer to work properly. The *Radio Configuration Menu* is the primary menu used to set radio parameters. This screen includes the *Skip Zone Options Submenu*.

### 3.5.1 Radio Configuration Menu

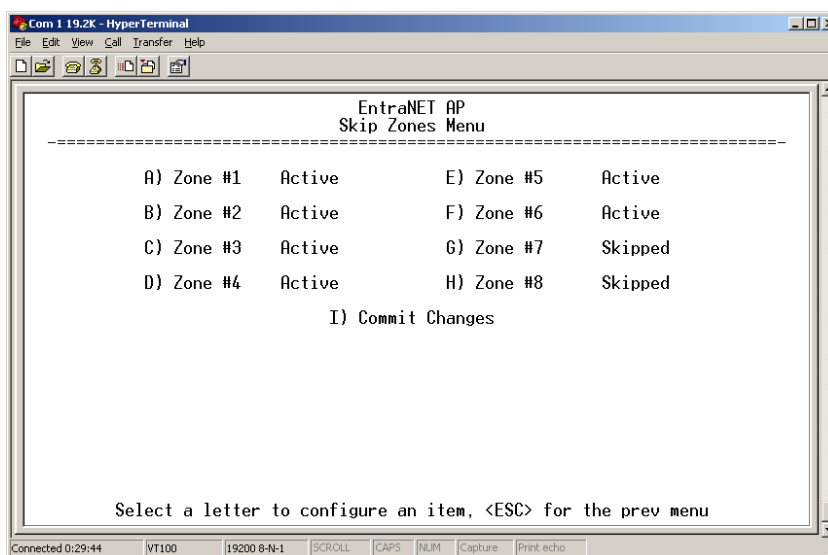


**Figure 3-19. Radio Configuration Menu**  
*From Access Point*

- RF Output Power**—(We recommend that you review this setting.) Use this selection to set the RF output level of the transceiver. Settings are displayed in dBm, and must comply with regulatory limitations for your area. See [Table 2-1](#) for default settings and range. [20-30; 30]
- Dwell Time**—Duration of one hop on a particular frequency in the hopping pattern. This field is only changeable on an AP; Remotes get their value from the AP upon association. Dwell time is the same as hop time. [7, 14, 28 msec; 14 msec]
- Contention Window Min**—Sets the number of random contention slots to use on first attempt. [0-15; 2]
- Contention Window Max**—Sets the **maximum** number of random contention slots to use. [0-15; 10]
- Broadcast Repeat Count**—Because broadcast messages are not acknowledged, noisy environments can prevent some Remotes from receiving a broadcast. This parameter sets the number of times that point-to-multipoint messages are transmitted by the AP. Higher values increase the reliability of communications, but also increase over-the-air congestion. [0-14; 3]

- **Unicast Retry Count**—Sets the **maximum** number of attempts made to deliver point-to-point messages. Higher values are more reliable, but increase over-the-air congestion. [0-14; 10]
- **Skip Zones** (*editable at AP only*)—Displays the current use of *frequency zones*. Each zone consists of 16 RF channels. See “*Skip Zones Menu*” on Page 53 for details.

## Skip Zones Menu



**Figure 3-20. Skip Zones Menu**

(“Commit changes” displayed only on AP, after a change is made)

This screen displays the current use of eight frequency operating zones in the network. You can toggle zones between **Active** and **Skipped** at APs by first typing the letter of the zone to be changed, and then pressing **[SPACE]** to toggle between the two options for each zone. The screen is read-only at Remote radios, and Remotes must be synchronized to the AP to display valid status.

Skipping zones is one way of dealing with constant interference on one or more frequencies. See “*A Word About Radio Interference*” on Page 150 for more interference-combatting techniques.

When you have made the desired changes to the *Skip Zones Menu*, select **Commit Changes** to implement the new settings. These changes are forwarded to all radios in the network through the AP beacon signal.

---

**NOTE:** In the USA, up to four zones may be skipped for 900 MHz systems, and a maximum of three skipped for 2.4 GHz systems, per FCC regulations. The skip function may be disabled in some radios, due to regulatory requirements in some countries.

---

Table 3-1 shows the frequency range covered by each zone for 900 MHz radios. Table 3-2 shows the same information for 2400 MHz radios.

**Table 3-1. Frequency Zones**  
(900 MHz systems)

ZONE 1	ZONE 2	ZONE 3	ZONE 4	ZONE 5	ZONE 6	ZONE 7	ZONE 8
902.200 to 905.200	905.400 to 908.400	908.600 to 911.600	911.800 to 914.800	915.000 to 918.000	918.200 to 921.200	921.400 to 924.400	924.600 to 927.600

**Table 3-2. Frequency Zones**  
(2400 MHz systems)

ZONE 1	ZONE 2	ZONE 3	ZONE 4	ZONE 5	ZONE 6	ZONE 7	ZONE 8
2401.6 to 2404.6	2404.8 to 2407.8	2408.0 to 2411.0	2411.2 to 2414.2	2414.4 to 2417.4	2417.6 to 2420.6	2420.8 to 2423.8	2424.0 to 2427.0

**NOTE:** Use caution when changing the operating band of 2.4 GHz radios. If a Remote and AP are set to different bands, and communication is lost with the AP, you might have to visit the Remote site to restore operation.

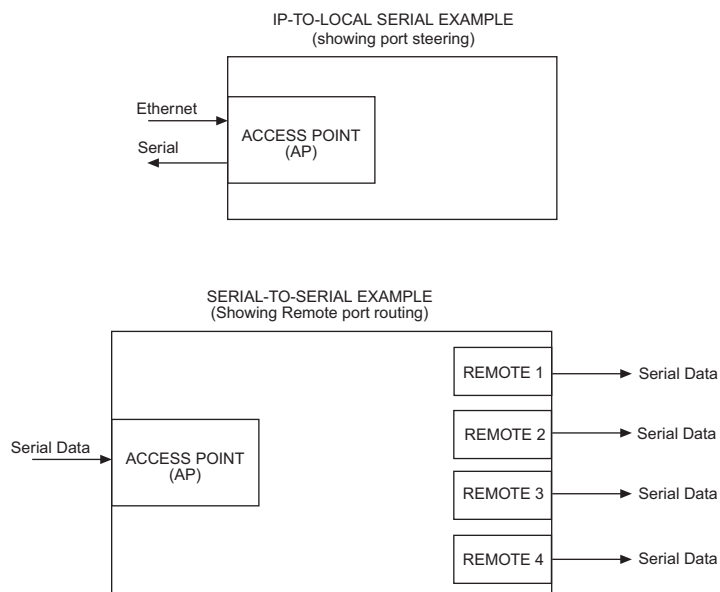
## 3.6 CONFIGURING THE SERIAL INTERFACES

### 3.6.1 Overview

To understand the operation of the radio system, it is helpful to visualize the AP and the Remotes as being in a single box, with the AP ports on one side and all of the Remotes on the other side (see Figure 3-21). In practice, the radios are typically separated by considerable distances, but thinking of them grouped in the same box is helpful for this discussion.

Most data routing is done at the AP, so you must also perform the majority of system configuration at the AP. The AP requires configuration of its local interfaces (Ethernet or Serial) and knowledge of its remote interfaces, which are physically located at the Remote radios. There are also a few parameters that you can configure at the individual Remote radios.





**Figure 3-21. Conceptual Views of Radio System Usage**

The AP includes an embedded *terminal server* that provides access to Remote serial ports using an IP or serial connection at the AP. In this capacity, it acts as a gateway between IP and remote serial devices (thus the name “serial gateway”), or a transparent over-the-air serial-to-serial connection.

### Serial-to-Serial Services

When the AP transceiver has remote serial units and is primarily passing RS-232 (serial-based) traffic, it might be necessary to implement serial-to-serial interface transfers, as shown in the lower part of [Figure 3-21](#). Additional information for serial-to-serial wireless networks is provided on Pages [123](#) and [132](#) of this manual.

### IP-to-Serial Services

When the AP transceiver is used as an IP-to-serial gateway, two types of IP terminal services are available—TCP and UDP. TCP provides a connection-oriented link, with end-to-end acknowledgment of data. This requires some added overhead, but provides confirmation that data has been successfully conveyed, which may be needed for mission-critical applications.

UDP, on the other hand, provides a best-effort delivery service with less overhead than TCP. It broadcasts data, transmitting information packets without an expected acknowledgment. This method minimizes overhead requirements and is acceptable for repetitive exchanges of information, where an occasional missed packet would not affect performance.

Most polled protocols are best served by UDP services, as the protocol itself has built-in recovery mechanisms (error correction). UDP

provides the needed multidrop operation by means of multicast addressing, where multiple remote devices receive and process the same poll message.

On the other hand, TCP services are best suited for applications that do not have a recovery mechanism and must have the guaranteed delivery that TCP provides despite its extra overhead. The IP-to-Serial example shows how to do this. See [“IP-to-Local Serial Application Example” on Page 121](#).

To configure either of these services, use the *Serial Configuration Menu* ([Figure 3-22 on Page 57](#)).

To configure IP-to-remote serial services, use the *Remote Serial Gateway Menu* ([Figure 3-28 on Page 64](#)).

## Configuration

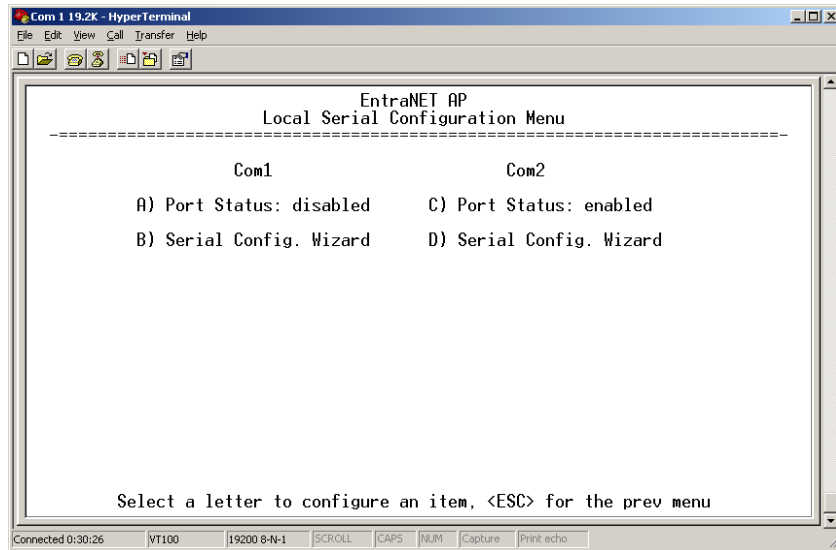
There are several configuration parameters for the remote serial gateway found under the *Serial Configuration Menu*. Note that some of the parameters are not applicable to IP-to-serial mode. After making changes to the configuration, you must use the **Commit Changes** option to force the transceiver to implement the requested changes.

If you are connecting EIA-232 serial devices to the transceiver, review these parameters carefully.

## Serial Configuration Wizard

The Serial Configuration Wizard, available through the *Local Serial Configuration Menu*, is recommended for configuration of serial ports. The Wizard uses a step-by-step process that eliminates conflicting settings and streamlines complex configurations.

## 3.6.2 Local Serial Configuration Menu



**Figure 3-22. COM1/2—Local Serial Configuration Menu**

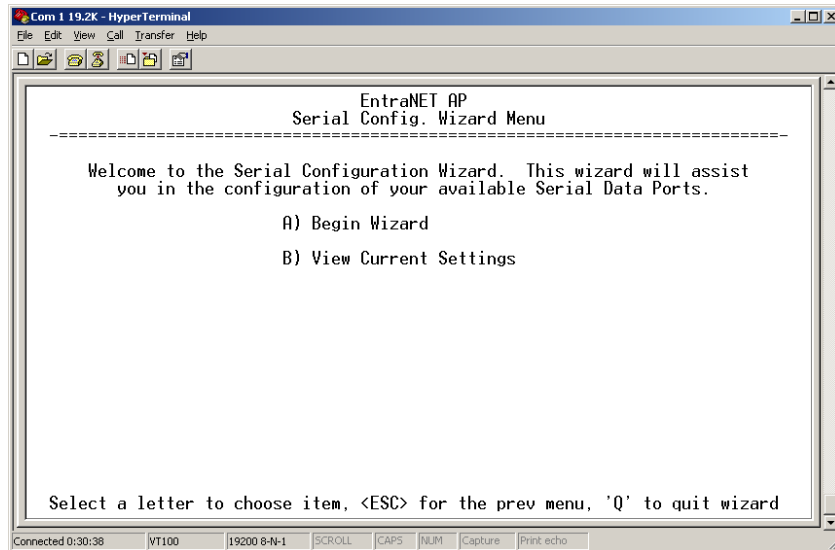
- **Port Status (COM1, COM2)**—Defines whether the specified port is enabled or disabled to pass payload data. COM1 is typically disabled to allow it to be used for console terminal control.

---

**NOTE:** If COM1 is inadvertently enabled, it will become impossible to log in using a console terminal connected to the COM1 connector. This problem can be remedied by typing the Hayes modem-compatible escape sequence of **[SHIFT] + + +** followed by **[ENTER]**. This restores COM1 to console terminal mode. You must log in again.

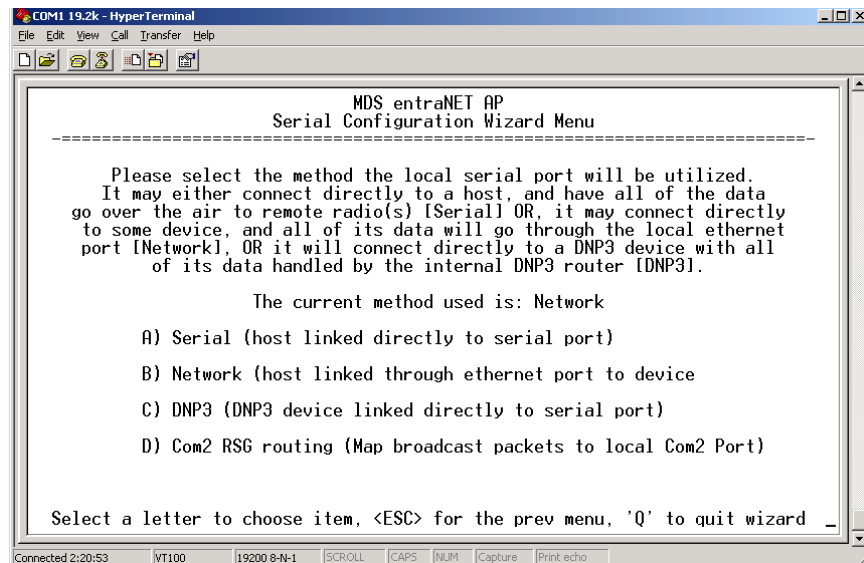
---

- **Serial Configuration Wizard**—This is a tool for configuration of the serial ports using a step-by-step process. When the Wizard is started, you can choose between beginning the step-by-step process, or simply viewing the current settings (see [Figure 3-23 on Page 58](#)).



**Figure 3-23. Serial Configuration Wizard (Initial Screen)**

To start the Serial Configuration Wizard, choose **Begin Wizard**. The Wizard presents an opening screen (Figure 3-24) where you select the method the host computer uses to connect to the radio.



**Figure 3-24. Serial Configuration Wizard Menu (Host Connection screen)**

Next, a series of screens are presented where you set all of the parameters needed for proper operation of the serial port(s). The screens provide text that assist you in making your selections.

At the end of the configuration process, the *View Current Settings Screen* is displayed, where you can review or change any of the settings. Once you are satisfied with the settings, you can commit the changes and exit the Serial Configuration Wizard by choosing the last selection on the *View Current Settings Screen*.

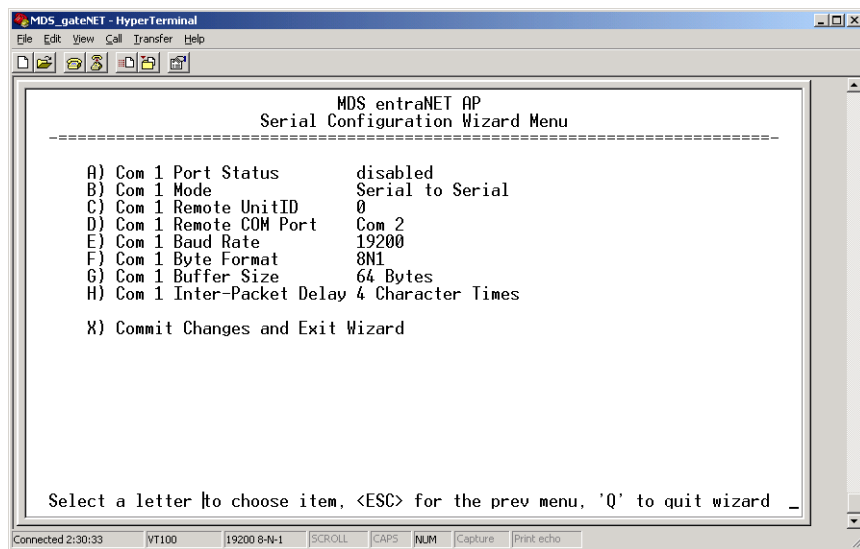
## View Current Settings Screen—Serial-to-Serial Example

If you choose **View Current Settings** from the *Serial Configuration Wizard Menu*, you see a summary screen (Figure 3-25) showing the serial configuration settings. This is the same screen that is also shown at the end of the configuration process. Here, you can choose the letter of an item to change, or exit the Serial Configuration Wizard completely.

---

**NOTE:** Selecting any item other than **Commit Changes and Exit Wizard** returns you to the configuration process. After making the necessary change(s), you can use the **Continue Wizard** selection repeatedly to reach the end of the configuration process, and then exit.

---



**Figure 3-25. Serial Configuration Current Settings Screen (Serial-to-Serial example)**

The following text explains the key settings for the *Serial Configuration Menu* (serial-to-serial example).

- **Port Status**—This selection is used to enable or disable the serial data port **for payload data** operation. Normally, COM1 is set to **Disabled** to permit console terminal operation.

---

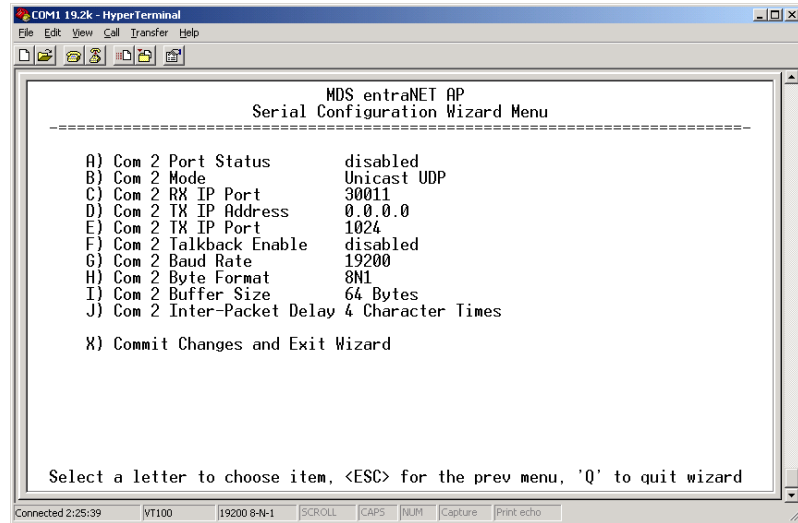
**NOTE:** When COM1 is enabled for data, management of the radio through COM1 is disabled. This problem can be remedied by typing the escape sequence **[SHIFT] + + +** followed by **[ENTER]**. This restores COM1 to console terminal mode. You must log in again.

---

- **Mode**—Set the method the host uses to connect to the radio.  
[Serial, Network; Network]
- **Remote UnitID**—Specify the Remote(s) to which transmissions are directed. Enter “broadcast” to send transmissions to all Remotes, or enter the Unit ID number of a particular Remote for unicast (directed) data. The Unit ID defaults to the last four digits of the radio serial number, but can be set to any 32-bit integer.  
[Remote ID, Broadcast; Broadcast]
- **Remote COM Port**—Choose which serial port on the Remote radios through which all data are sent (COM1 or COM2).  
[COM1, COM2; COM2]
- **Baud Rate**—Set the data rate (payload) for the COM port in *bits per second*. [1200–115200; 19200]
- **Byte Format**—Set the interface signaling parameters: baud rate (see **Baud Rate** above for allowable range), data bits, parity, and stop bits. [7N1, 7E1, 7O1, 8N1, 8E1, 8O1; 8N1]
- **Buffer Size**—Select the appropriate value for the buffer size for each serial message. The maximum AP buffer size for incoming serial data is 256 bytes. Incoming serial packets (from the RTU) larger than 256 bytes are split by the AP into 256-byte packets before being transmitted over the air. The associated remote(s), on receiving these packets, transmit them out the serial port as separate packets. This parameter does not affect serial data/packets received by the AP (from remotes) over the air and transmitted out of the local AP serial port. [32, 64, 128, 256 bytes; 64]
- **Inter-Packet Delay**—Set the number of characters that signify the end of a message (inter-character time-out). A transceiver receiving data through the serial port sends an end-of-message signal to the remote end. MODBUS® defines a “3.5-character” parameter. [0–65535; 4]
- **Commit Changes and Exit Wizard**—Implements the settings shown on the screen and closes the Serial Configuration Wizard.

## View Current Settings Screen—Unicast UDP Mode Example

Figure 3-26 shows a sample *View Current Settings Screen* for a system configured for Unicast UDP mode. The selections shown are similar to the serial-to-serial example above, but some items are UDP specific.



**Figure 3-26. Serial Configuration Current Settings Screen**

The following text explains the key settings for the *Serial Configuration Menu* (Unicast UDP example).

- **Port Status**—This selection is used to enable or disable the serial data port **for payload data** operation. Normally, COM1 is disabled to permit Console Terminal operation.

---

**NOTE:** When COM1 is enabled for data, management of the radio through COM1 is disabled. This problem can be remedied by typing the escape sequence `[SHIFT] + + +` followed by `[ENTER]`. This restores COM1 to console terminal mode. You must log in again.

---

- **Mode**—Used to set the method the host uses to connect to the radio. `[Serial, Network; Network]`
- **RX IP Port**—This selection is used to specify which local IP port address should be used to receive data from the host, as well as the IP address and port number of the host to send data **to** at the remote end.
- **TX IP Address**—This selection is used to specify the local IP address that will receive data from the host, as well as the IP

address and port number of the host to send data **to** (at the remote end).

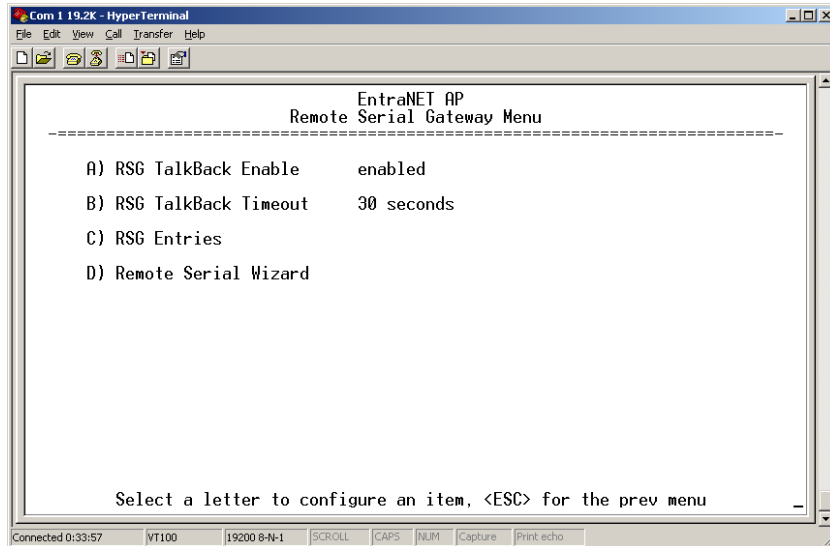
- **TX IP Port**—A dynamically assigned software port used by external applications such as HMI interfaces, host polling programs, and so on.
- **Talkback Enable**—Used to enable or disable Talkback mode. [Enabled, Disabled; Disabled]
- **Baud Rate**—This menu item is used to set the data rate (payload) for the COM port in bits per second. [1,200–115,200; 19200]
- **Byte Format**—This item allows you to set the interface signaling parameters: baud rate (see **Baud Rate** above for the allowable range), data bits, parity, and stop bits. [7N1, 7E1, 7O1, 8N1, 8E1, 8O1; 8N1]
- **Buffer Size**—This selection selects the size of the buffer available for passing serial traffic. The maximum AP buffer size for incoming serial data is 256 bytes. Incoming serial packets (from the RTU) larger than 256 bytes are split by the AP into 256 byte packets before being transmitted over the air. The associated remote(s), on receiving these packets, transmits them from the serial port as separate packets. This parameter does not affect serial data/packets received by the AP (from remotes) over the air and transmitted from the local AP serial port. [16, 32, 64, 128, 256; 64 Bytes]
- **Inter-Packet Delay**— Specifies the number of characters that signify the end of a message (inter-character time-out). A transceiver receiving data through the serial port sends an end-of-message signal to the remote end. MODBUS defines a “3.5-character” parameter. [0–65535; 4]
- **Commit Changes and Exit Wizard**—Implements the settings shown on the screen and closes the Serial Configuration Wizard.

### 3.6.3 Remote Serial Gateway Configuration (IP-to-Remote Serial)

The *Remote Serial Gateway (RSG) Menu* (Figure 3-27) controls the IP *encapsulation* behavior of all Remote menu radios. The gateway function is essentially a table with one entry for each Remote radio passing serial data. No further configuration is required at Remote radios.

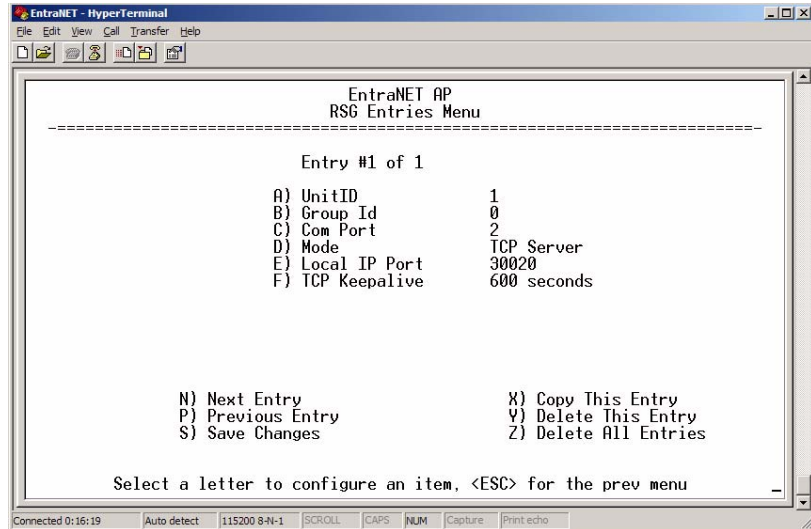
The AP can be configured to accept IP traffic to be exchanged with devices connected to the serial ports of one or more Remotes. Figure 3-27 shows the starting point for configuring the remote serial gateway settings.





**Figure 3-27. Remote Serial Gateway Menu—Initial Screen**

- **RSG Talkback Enable (UDP IP-to-Serial)**—When Talkback is enabled and the RSG is set up for UDP mode, a message from a Remote radio (usually a reply to a poll) is sent to the last IP address or port from which a message was received. **[Enabled, Disabled; Enabled]**
- **RSG Talkback Timeout**—Use this selection to set a time limit after which, if no data has been received from the IP host, the RSG talkback feature expires. When this happens, the RSG reverts to its configured IP address and port for upstream data destined for an IP host. **[Time in seconds; 30]**
- **RSG Entries**—This selection allows entry of key RSG parameters including Unit ID, COM port setting, Mode, and Local IP Port. This screen is shown in [Figure 3-28 on Page 64](#).
- **Remote Serial Wizard**—This tool assists you in adding or changing a configuration to your remote serial gateway entries. These are the same settings contained in *RSG Entries Screen*, but the Remote Serial Wizard presents a step-by-step series of screens with explanatory text to assist you in making your selections.



**Figure 3-28. Remote Serial Gateway (RSG) Entries Menu**  
*(TCP configuration; UDP is similar)*

- **Unit ID**—Enter **Broadcast**, or enter the Unit ID of the Remote for unicast (directed) data. The Unit ID defaults to the last four digits of the radio serial number, but can be set to any 32-bit integer. If set to **Broadcast**, then all remotes are targeted.
- **Group Id**—Identifies a group used for serial multicast traffic. When set to a non-zero value, the **Unit Id** and **COM Port** parameters are not available because the entry identifies a Group, and a Group does not use these parameters. **Unit Id** and **COM Port** parameters are available when this value is set to zero. [0-15; 0]
- **COM Port**—The remote serial port associated with this IP connection.
- **Mode**—The type of IP port, or socket, used by the AP for encapsulation of serial traffic. [TCP Server; UDP]
- **Local IP Port**—The IP port number at the AP to which the application must connect when exchanging data with the corresponding remote radio(s).
- **TCP Keepalive**—This value sets the number of seconds that a TCP connection can be inactive before it is disconnected. If the value is set to zero, the port is off. [0-600; 5]

---

**NOTE:** Although a Group is defined at the AP, the members of the group are defined at each remote radio. See *“Group Database Menu”* on Page 75 for more information.

---

## 3.7 SECURITY CONFIGURATION

The entraNET system contains built-in security features for your transceivers and the network. These options start with controlling

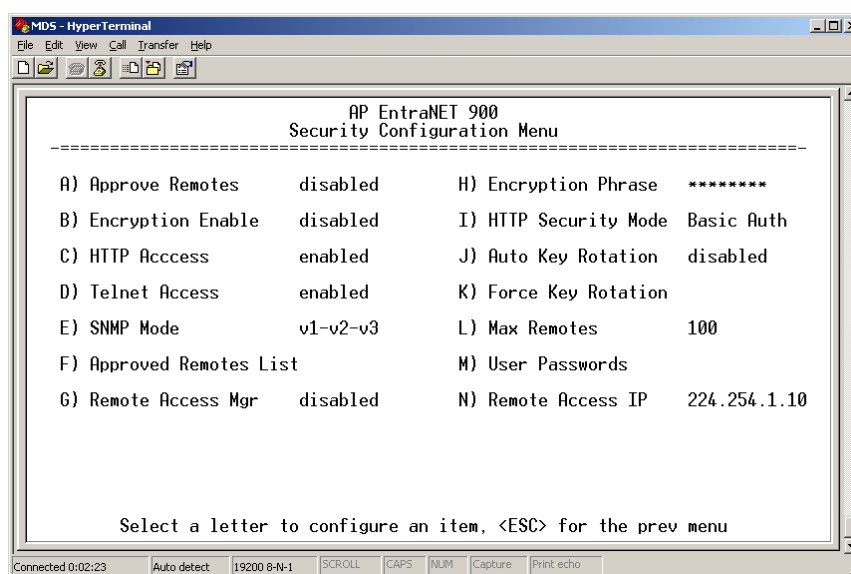
remote access to the network using Telnet, Web browser, and SNMP. Other areas include multiple levels of encryption and MD5-level security for HTTP connections. The *Security Configuration Menu* (Figure 3-29) contains all of the settings related to these functions.

**NOTE:** Security enhancements in entraNET 2.3.0 firmware necessitate that encryption **must** be turned **OFF** prior to upgrading entraNET Remote radios with the new firmware. Failure to turn encryption off results in loss of communication between an AP and entraNET Remote radios. Once the firmware upgrade is complete, you can re-enable encryption.

Additionally, any changes to encryption settings should be made first at all Remote radios, then at the AP. This prevents a loss of communication between the AP and Remote radios due to security mismatches. Communication loss requires a personal visit to each affected remote site, where restoration can be performed at the Remote itself (see *CHAPTER 4 REMOTE RADIO MANAGEMENT*, beginning on Page 99).

### 3.7.1 Security Configuration Menu

The *Security Configuration Menu* (Figure 3-29) allows settings of several parameters related to network access, user credentials, and encryption. A review of each item on the menu is important to safeguarding your network from unauthorized access. Review these settings occasionally to make sure they are applicable to the current state of your network.



**Figure 3-29. Security Configuration Menu**

- **Approve Remotes**—Enables authentication of Remote radios before granting access to the network. Enabling forces the entraNET radio to check the *Approved Remotes List* (described below) before continuing the authorization process. Before enabling this option, at least one entry must already exist in the *Approved Remotes List*. [**Enabled, Disabled; Disabled**]
- **Encryption Enable**— Enable encryption of over-the-air data packets. Enabling forces the transceiver to use 128-bit encryption on all over-the-air messages. This option requires that you have already configured the **Encryption Phrase** (see below). [**Enabled, Disabled; Enabled**]
- **HTTP Access**—Prevents remote access through HTTP (a Web browser) on Port 80. [**Enabled, Disabled; Enabled**]
- **Telnet Access**—Prevents remote access through Telnet sessions on Port 23. [**Enabled, Disabled; Enabled**]
- **SNMP Mode**— Prevents remote access through SNMP commands on Port 161. [**Disabled, v1 only; v2 only, v3 only, v1-v2, v1-v2-v3; v1-v2-v3**]
- **Approved Remotes List (Menu)**—Presents a menu where the creation and management of Remote radios allowed to communicate with the AP is performed. For more information, refer to *Approved Remotes List Menu* below.
- **Remote Access Manager**—Allows management of the Approved Remotes List using optional *GE MDS Remote Access Manager* software (Part Number 06-4490A01). Set the Remote multicast address to use with the **Remote Access IP** setting (listed below). [**Enabled, Disabled; Disabled**]
- **Encryption Phrase**—An alphanumeric phrase added to the encryption algorithm. You must enter a minimum of eight characters for this string. [**Any 8-41 character alphanumeric string; Blank**]

---

**NOTE:** When changing the **Encryption Phrase**, it is recommended that you change the most distant Remotes first, followed by the APs, so that proper association occurs.

---

- **HTTP Security Mode**—Select the security mode or level of log-in using an HTTP browser. Disabling **HTTP Access** prevents access through HTTP. **HTTP Security Mode** is functional if **HTTP Access** is enabled. [**Basic Auth, MD5 Digest; Basic Auth**]

**Basic** mode requires a password, but the actual password text is transmitted unencrypted.

**MD5 Digest** is more secure because it encrypts the password.

- **Auto Key Rotation**—Used to select whether or not the encryption key is automatically rotated (changed) periodically. [**Enabled, Disabled; Enabled**]

- **Force Key Rotation**—This selection invokes an immediate change in the encryption key. For this function to work, encryption must be enabled, a valid **Encryption Phrase** must be set, and key rotation must be enabled. Note that there is no feedback on the screen—the change takes place as soon as the menu selection is made.
- **Max Remotes**—Maximum number of Remotes permitted to be connected to (served by) this AP. [Default=50]
- **User Passwords**—Administrative and Guest password for this radio. Used at log-in using the COM1 Port, Telnet session, or a Web browser session.

To reset the admin password to the factory default (“admin”) (Figure 3-30):

1. At the login prompt, type **authcode**.
2. At the password prompt, type **authcode**.
3. At the authorization prompt, enter the authorization code.

[Up to eight case-sensitive, non-blank, alphanumeric characters; admin]

```
(none) login: authcode
Password:
MDS EntraNET Access Point

No directory, logging in with HOME=/
MDS entraNET
Device Name: AP EntraNET 900
Serial Number: 1437374

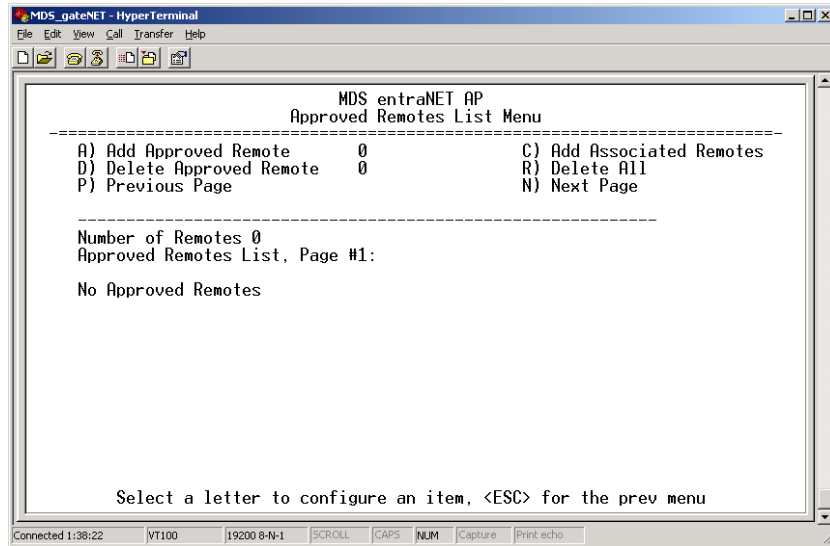
Enter Authorization Code>
```

**Figure 3-30. Reset Password to Factory Default**

**TIP:** For enhanced security, consider using a **misspelled** word. This helps protect against sophisticated hackers who use a database of common words (as in a dictionary attack) to determine a password. An even better approach is to use a password that includes some numbers. Making the password as long as possible (up to the full eight characters) also improves its security.

- **Remote Access IP**—Remote multicast address to use when running optional *GE MDS Remote Access Manager* software (see **Remote Access Manager** above). [Default=239.254.1.10]

## Approved Remotes List Menu



**Figure 3-31. Approved Remotes List Menu**

The AP restricts communication to only those Remotes included in the Approved Remotes List. Messages received from Remotes that are not in this list are discarded.

- **Add Approved Remote**—Enter the Remote serial number. This entry must consist of seven or more characters.  
 [Serial number of Remote—at least seven characters]
- **Delete Approved Remote**—Enter the Remote serial number.

---

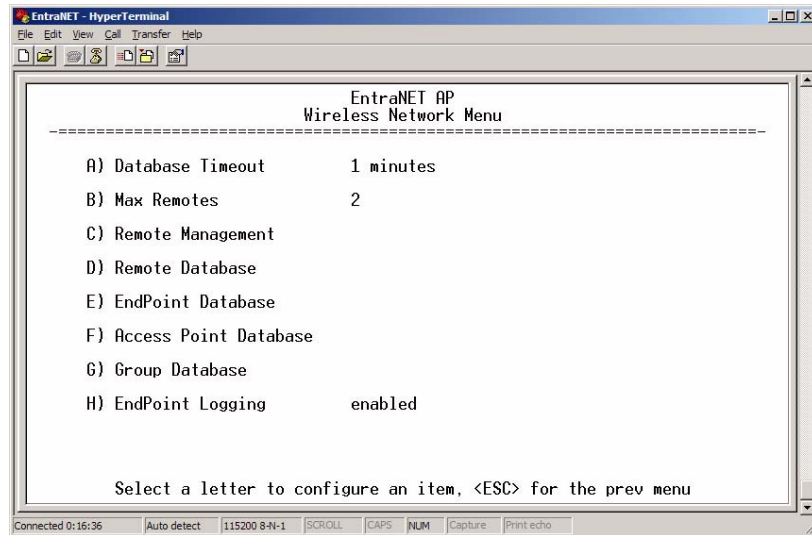
**NOTE:** For security, delete a decommissioned or stolen radio immediately.

---

- **Previous Page**—Returns you to the last page viewed within the *Approved Remotes Menu*.
- **Add Associated Remotes**—Adds all currently associated Remotes (1-1024) to the approved Remote list. Alternatively, you can enter each Remote serial number manually.
- **Delete All**—Completely purges all Remotes from the current list.
- **Next Page**—Moves you to the next page within the *Approved Remotes List Menu*.
- **Number of Remotes**—Shows the number of Remotes that are currently connected to the AP.
- **Approved Remotes List**—Simple listing of the serial numbers of Remotes that are authorized to communicate with this AP. If a Remote is not on this list, it cannot associate with this AP.

## 3.8 WIRELESS NETWORK MENU

The *Wireless Network Menu* (Figure 3-32) monitors the operation of Remote radios in the network, regardless of the type of data they are passing (Ethernet or serial) from the perspective of the AP. This information is stored in a local database at the AP, and is not sent to the Remotes.



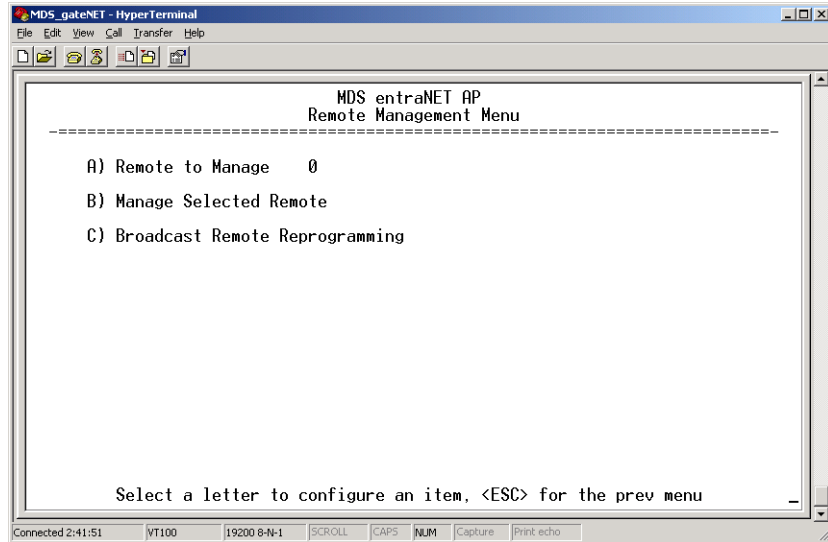
**Figure 3-32. Wireless Network Menu**

- **Database Timeout**—Number of minutes until a database entry expires. Remotes must be refreshed through a handshake process to stay in the database. This allows decommissioned or faulty radios to fall out of the database. [1-720; 10]
- **Max Remotes**—Maximum number of Remotes allowed to associate with the AP. [1-1024;100]
- **Remote Management**—Presents a menu for management of a particular Remote. See “[Remote Management Menu](#)” on [Page 70](#) for more information.
- **Remote Database**—Lists all Remotes connected to this AP. See “[Remote Database Menu](#)” on [Page 74](#) for more information.
- **Group Database**—Lists all Remotes connected to this AP that belong to a specific Group. See “[Group Database Menu](#)” on [Page 75](#) for more information.
- **Endpoint Database**—Lists the IP or MAC addresses of Ethernet endpoints connected to Remote radios. See “[Endpoint Database Menu](#)” on [Page 75](#) for more information.
- **Access Point Database**—Lists the APs in the wireless network. Inter-Access Point Protocol must be enabled (see “[Mobility Configuration Menu](#)” on [Page 49](#)) for this function to work). IAPP traffic can be passed using these transceivers. See “[Access Point Database Menu](#)” on [Page 76](#) for more information.

- **EndPoint Logging**—This selection is used to specify whether endpoint logging is enabled or disabled. [Enabled, Disabled; Enabled]

### 3.8.1 Remote Management Menu

The *Remote Management Menu* (Figure 3-33) allows selection of a particular Remote to manage, based on the radio Unit ID number (generally the last four digits of its serial number).



**Figure 3-33. Remote Management Menu**

- **Remote to Manage**—Radio address of the Remote to be managed (typically a four-digit code).
- **Manage Selected Remote**—Displays the screen shown in Figure 3-34 on Page 71, which contains several parameters used to set the characteristics of Remote radios in the network.
- **Broadcast Remote Programming**—Selecting this item brings up a submenu (Figure 3-36) where you can initiate the broadcast of new firmware images and Remote restart commands.

---

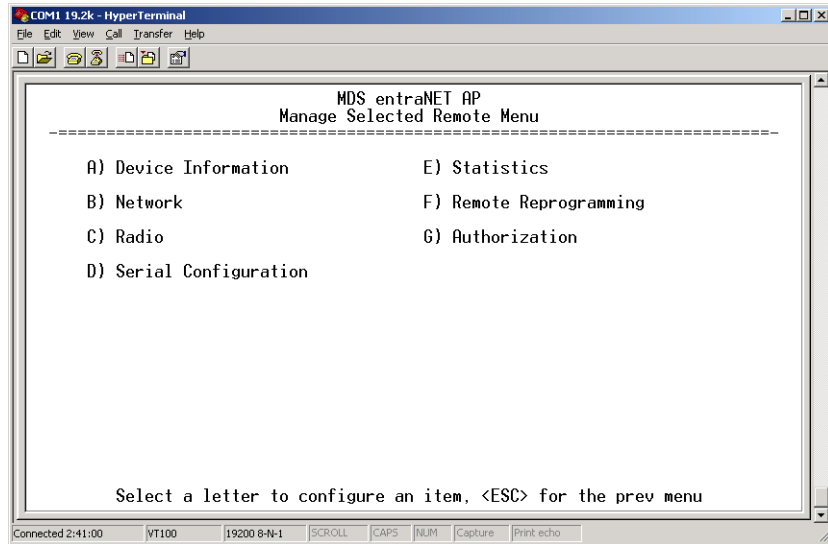
**NOTE:** Before programming a Remote radio over the air, be sure to set **ETHERNET BRIDGING** (see “*Bridge Configuration Menu*” on Page 51) from **ALL** (default) to either **DISABLED** or **NO BROADCAST/MULTICAST**.

Otherwise, you might experience sync errors, or programming might not complete. Excessive broadcast/multicast traffic from a connected LAN can also cause problems.

---

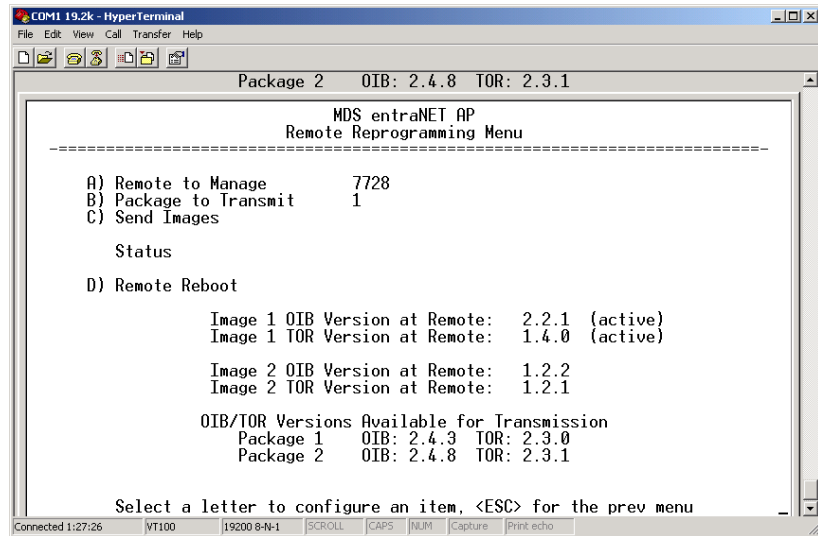


## Manage Selected Remote Menu



**Figure 3-34. Manage Selected Remote Menu**

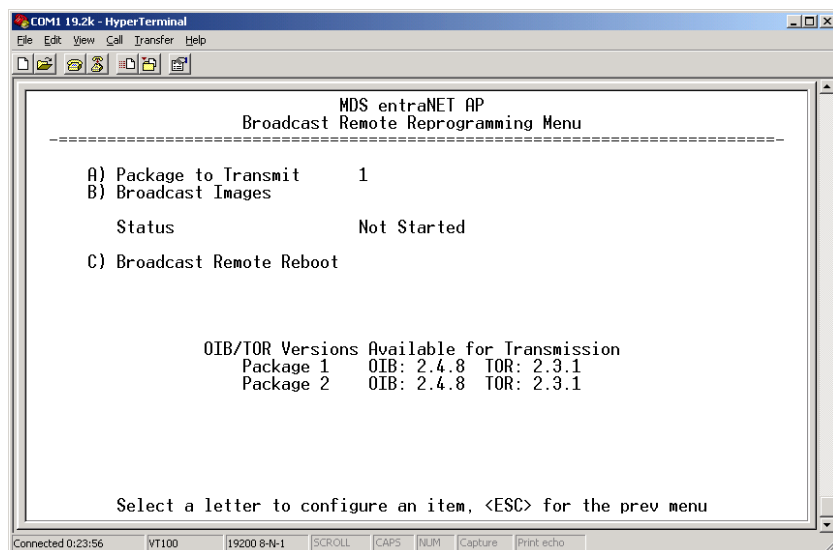
- **Device Information**—Selecting this item brings up a submenu (Figure 3-36) where you can change a Remote radio **Owner**, **Name**, and **Location**. Hardware and software version information, including the bootloader version, is also displayed.
- **Network**—Tool for control of the Ethernet port (enable or disable).
- **Radio**—Tool for setting the transmit power level (in dBm).
- **Serial Configuration**—Tool for configuring COM1 and COM2 parameters, including port mode, baud rate, *byte* format, inter-packet delay, and buffer size.
- **Statistics**—Presents packet throughput and retry data for the selected Remote.
- **Remote Reprogramming**—Opens a submenu (Figure 3-35 on Page 72) for sending new firmware images to specific Remotes, and for specifying the image that will be active when the radio is restarted.
- **Authorization**—Opens a submenu showing the authorized capabilities of the Remote entered in the Unit ID field (enabled or disabled): Ethernet capabilities, network management, serial capabilities, and multiple endpoints.



**Figure 3-35. Remote Reprogramming Menu (Single Remote)**

- **Remote to Manage**—This field shows the Unit ID of the Remote to be managed.
- **Package (Image) to Transmit**—There are two available firmware images in the AP. This allows selection of either image to be transmitted to the remote.
- **Send Images**—Begins transmitting the selected firmware image to the Remote.
- **Remote Reboot**—Restarts the Remote radio with one of the two firmware images.

### Broadcast Remote Reprogramming Menu



**Figure 3-36. Broadcast Remote Reprogramming Menu**

### **Broadcast reprogramming with different firmware versions on a network**

Broadcast reprogramming is used to upgrade the firmware of all radios in a network. If your network contains a mix of radios with 2.x and 3.x version firmware, it is normal to see the status message “Some Remotes Failed Programming”.

For example, if you select 2.x firmware to reprogram, only the older remotes will accept the image; if you select 3.x firmware, only new remotes will accept the firmware. Release 3.x firmware can only be installed on radios equipped with 2 MB expanded flash memory. Release 2.x is compatible only with older radios having 1 MB flash memory.

Use the [Manage Selected Remote Menu](#) on Page 71 to determine which radios were not upgraded.

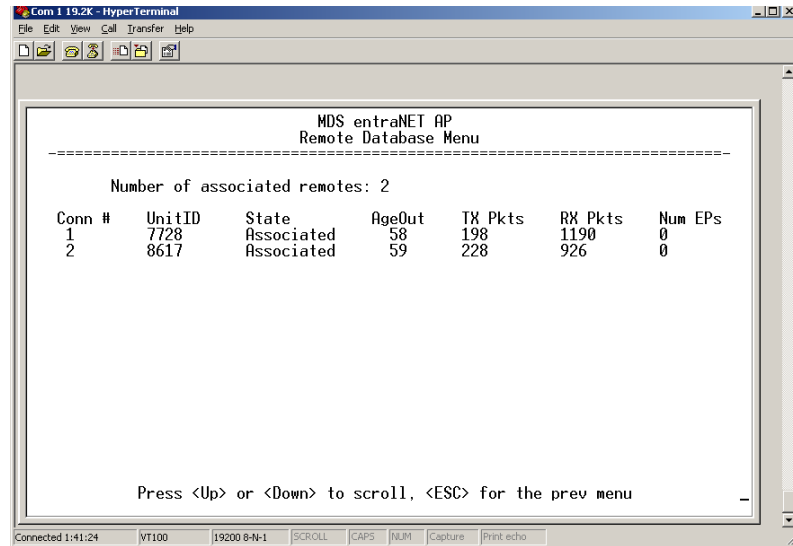
The Broadcasting Remote Reprogramming menu items are:

- **Package to Transmit**—Identifies which of the two available firmware images (1 or 2) will be sent to the associated Remotes.
- **Broadcast Images**—Starts transmission of the selected firmware package to all associated Remotes.
- **Status**—Shows either **Not Started**, or the progress (in percent) of a firmware image transmission. At the end of a transmission, the word **Complete** is shown.
- **Broadcast Remote Reboot**—Causes a reboot of all associated Remotes to the new (offline) firmware image. This image then becomes the active firmware file.

The bottom of this screen shows the software versions of the OIB and TOR boards inside the entraNET radio. The OIB is the interface board section of the transceiver; the TOR is the radio section of the transceiver. Both sections use different portions of the firmware package, which explains the difference in version numbers.

## Remote Database Menu

The *Remote Database Menu* (Figure 3-37) shows several parameters related to the associated Remotes. It is updated about once every 8 sec.



```

MDS entraNET AP
Remote Database Menu
-----
Number of associated remotes: 2
Conn #   UnitID   State    AgeOut   TX Pkts  RX Pkts  Num EPs
  1      7728    Associated  58      198     1190     0
  2      8617    Associated  59      228     926      0

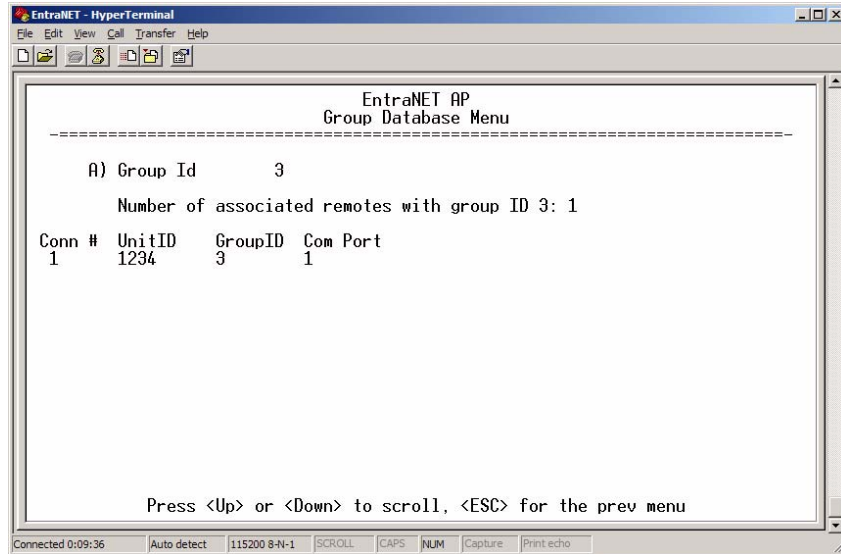
Press <Up> or <Down> to scroll, <ESC> for the prev menu
  
```

**Figure 3-37. Remote Database Menu**

- **UnitID**—The unit ID of the associated remote.
- **State**—Shows whether or not the Remote is connected to the AP.
- **AgeOut**—Number of minutes until the entry expires and is removed from the table. Each AP maintains a table with the addresses of the devices it communicates with. The **AgeOut** countdown restarts to the **Database Timeout** value every time a message to or from that device is detected. If no traffic with that device occurs, and it does not respond to a final handshake request, it then “ages out” of the table. An expired Remote must reconnect before it is again included in the table. See **Database Timeout** on the *Wireless Network Menu*, [Figure 3-32 on Page 69](#).
- **TX Pkts**—Number of packets sent to this Remote.
- **RX Pkts**—Number of packets received from this Remote.
- **Num EPs**—Number of endpoints connected to this Remote.

## Group Database Menu

The *Group Database Menu* (Figure 3-38) shows the remotes associated with this AP that belong to the specified Group ID.



**Figure 3-38. Group Database Menu**

- **Group ID**—Allows the selection of a particular group and displays the remote radios defined for the group. [0-15; 0]
- **UnitID**—The unit ID of the associated remote.
- **GroupID**—The ID number of the group.
- **Com Port**—The COM port that the remote uses to pass the serial multicast traffic associated with this Group ID.

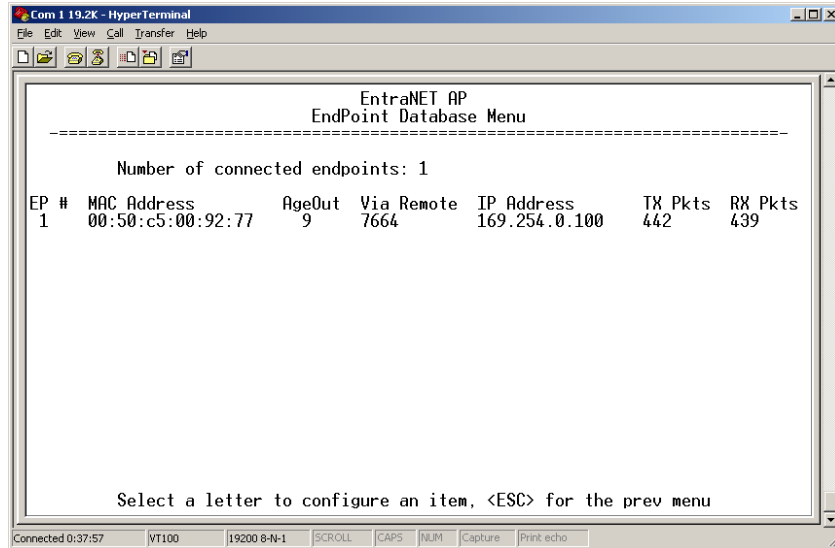
## Endpoint Database Menu

The *Endpoint Database Menu* (Figure 3-39 on Page 76) shows all non-entraNET Ethernet devices that are known to the transceiver; this is similar to the AP table of IP devices. The list shows endpoint MAC and IP addresses, as well as packet exchange data.

---

**NOTE:** A Remote does not have an IP address; rather, it acts as a transparent bridge for IP traffic to the connected Ethernet endpoint.

---



**Figure 3-39. Endpoint Database Menu**

*(Lists all equipment attached to Remote transceivers in the network)*

- **MAC Address**—Ethernet address of the endpoint device.
- **AgeOut**—Number of minutes until the device (address) is removed from the table.

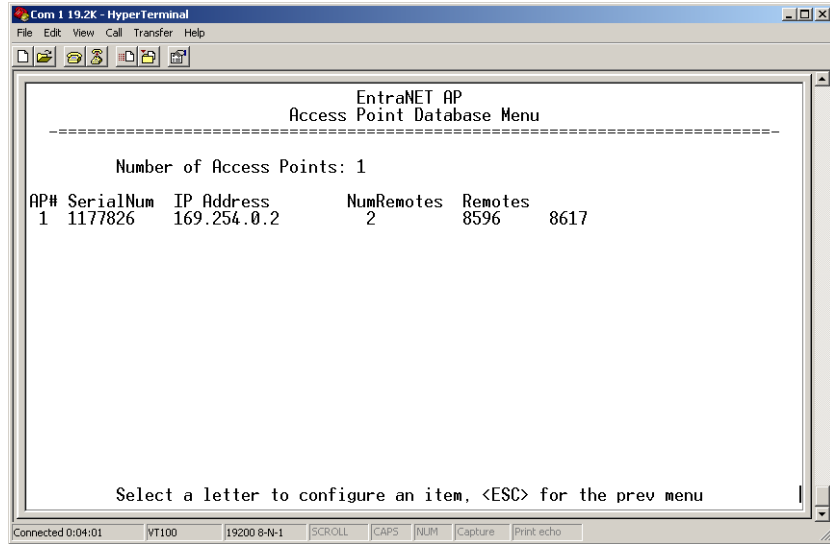
Each transceiver maintains a table with the addresses of the devices it communicates with. The age time countdown restarts to its default setting every time a message to or from that device is detected. If no traffic with that device happens, it then “ages out” of the table.

When traffic is detected, it is included again in the table.

- **Via Remote**—Unit ID of the transceiver connected to this device.
- **IP Address**—IP Address of endpoint device (not the Remote radio itself).
- **TxPkt**—Number of packets received from the endpoint device and passed over the air.
- **RxPkts**—Over-the-air data packets received by the transceiver and passed on to the endpoint device.

### Access Point Database Menu

The *Access Point Database Menu* (Figure 3-40) lists all APs contained in the wireless network, and includes details about each radio.

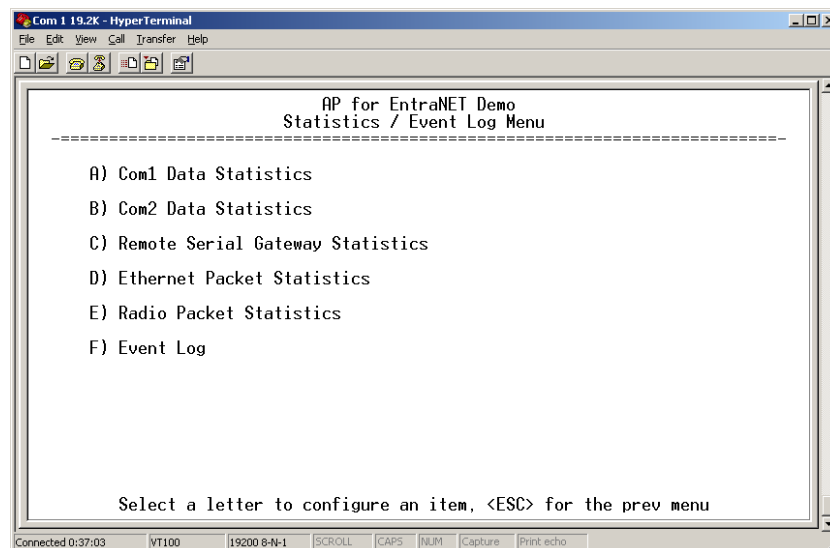


**Figure 3-40. Access Point Database**

- **Serial Number**—Factory-assigned serial number for the AP.
- **IP Address**—IP Address of the AP.
- **Number of Remotes**—Current number of Remotes connected to the AP.
- **List of Remotes**—Lists all Remotes (by Unit ID number) that are currently connected to the AP.

### 3.9 STATISTICS AND EVENT LOG

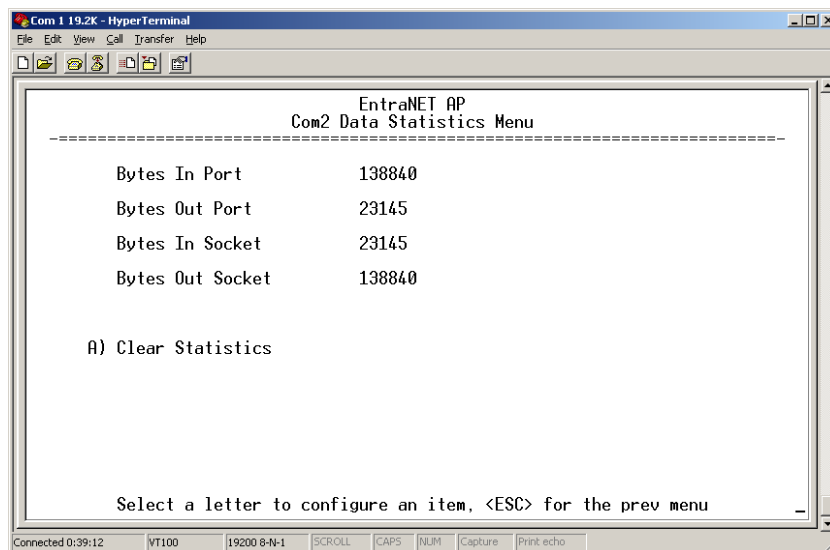
The *Statistics/Event Log Menu* (Figure 3-41) contains a variety of items related to the health and performance of the wireless network. Data throughput statistics, as well as past and present events and alarms, are all presented and stored in this menu area.



**Figure 3-41. Statistics/Event Log Menu (Main Screen)**

- **COM1/COM2 Data Statistics**—These screens show in and out bytes for the COM1 and COM2 ports.
- **Remote Serial Gateway Statistics**—Shows Unit ID, status, and throughput data for associated Remotes.
- **Ethernet Packet Statistics**—Shows vital data on packets, in and out bytes, errors detected, and lost Ethernet carriers.
- **Radio Packet Statistics**—Summarizes data packets sent and received by the radio, including overflows, good or failed data, retries, and timeouts.
- **Event Log**—Database of past and present events and alarms for the wireless network. A listing of event log codes appears in [Table 7-5 on Page 172](#).

### 3.9.1 COM1 and COM2 Data Statistics Menus



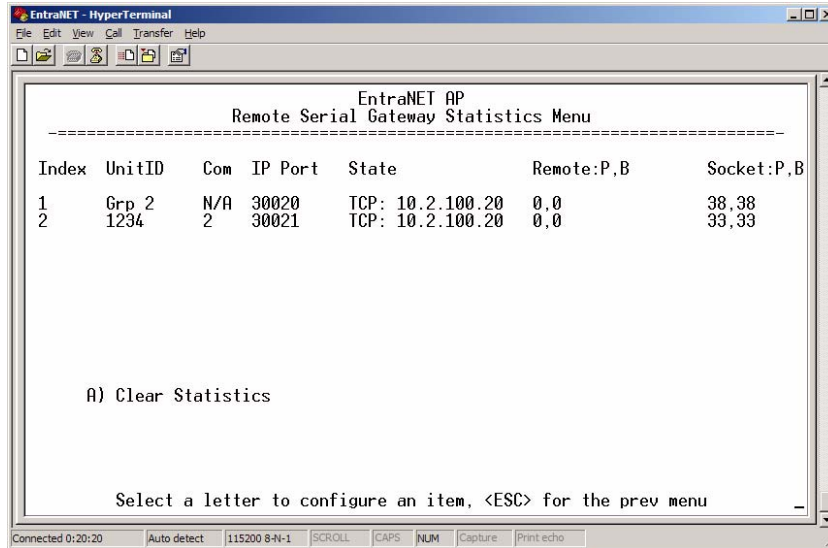
**Figure 3-42. Com1/2 Data Statistics Menu**

- **Bytes in on port**—Number of bytes received by the transceiver through the serial interface.
- **Bytes out on port**—Number of bytes transmitted by the transceiver through the serial interface.
- **Bytes in on socket**—Number of bytes received by the transceiver through the IP socket.
- **Bytes out on socket**—Number of bytes transmitted by the transceiver through the IP socket.



### 3.9.2 Remote Serial Gateway Statistics Menu

The *Remote Serial Gateway Statistics* menu (Figure 3-43) summarizes port activity for Remote Serial Gateway entries that have been set up for IP-to-Remote serial data. These values are reset to zero when a radio is restarted.



Index	UnitID	Com	IP Port	State	Remote:P,B	Socket:P,B
1	Grp 2	N/A	30020	TCP: 10.2.100.20	0,0	38,38
2	1234	2	30021	TCP: 10.2.100.20	0,0	33,33

A) Clear Statistics

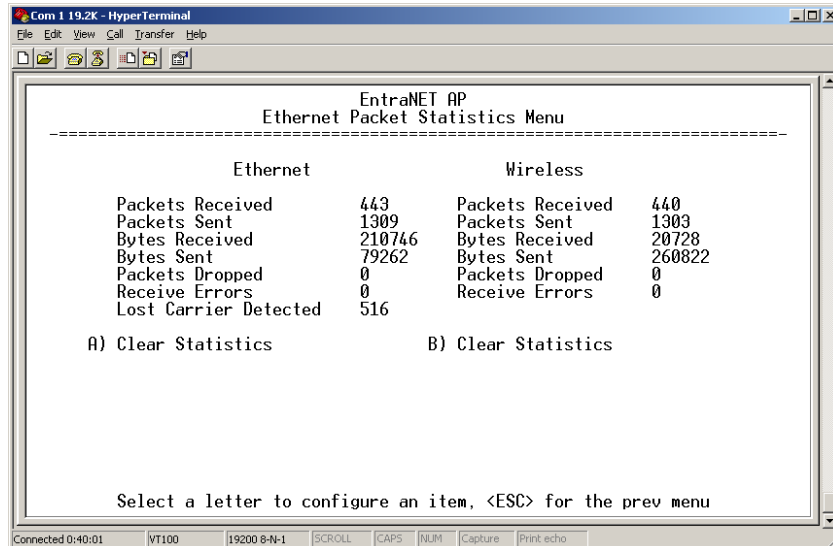
Select a letter to configure an item, <ESC> for the prev menu

**Figure 3-43. Serial Data Statistics Menu**  
(Both COM1 and COM2 are shown, if applicable)

- **Index**—Sequential number assigned to the associated Remote.
- **UnitID**—The unit ID of the associated Remote. Group IDs are displayed, when defined, to show statistics. A Group ID is identified as **Grp x**.
- **Com**—Communication port being monitored (**COM1** or **COM2**).
- **IP Port**—IP port associated with the listed device.
- **State**—State of the AP server for this Remote.  
[Listening; Connected]
- **Remote:P,B**—Displays the incoming port byte count.
- **Socket:P,B**—Displays the outgoing port byte count.

### 3.9.3 Ethernet and Wireless Packet Statistics Menu

The *Ethernet/Wireless Packet Statistics* menu (Figure 3-44) shows vital data on packets and bytes sent or received, and errors detected. The screen is updated approximately every 3 sec.



**Figure 3-44. Sample Packet Statistics Menu**

#### Ethernet Packet Statistics

- **Packets received**—Packets received through the Ethernet port of the transceiver.
- **Packets sent**—Packets sent through the Ethernet port of the transceiver.
- **Bytes received**—Data bytes received by this radio.
- **Bytes sent**—Data bytes sent by this radio.
- **Packets dropped**—Received packets dropped from a lack of buffers.
- **Receive errors**—Packets discarded after more than five retries.
- **Lost carrier detected**—Number of times the carrier signal on the Ethernet port has been missing. This count increases significantly when the Ethernet cable is inserted or removed.
- **Clear Statistics**—Resets the statistics counter.

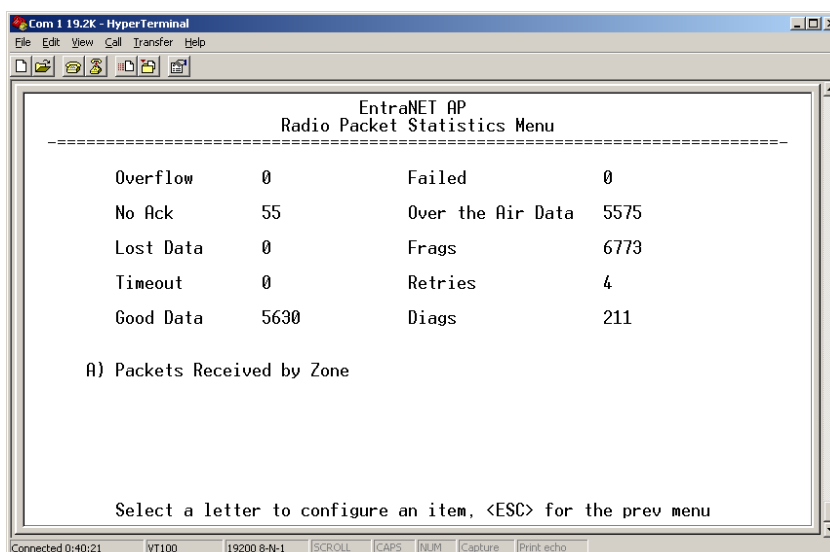
#### Wireless Packet Statistics

- **Packets received**—Over-the-air data packets received by this radio.
- **Packets sent**—Over-the-air data packets sent by this radio.
- **Bytes received**—Over-the-air data bytes received by this radio.
- **Bytes sent**—Over-the-air data bytes sent by this radio.
- **Packets dropped**—Received packets dropped from a lack of buffers.

- **Receive errors**—Packets that do not pass a Cyclic Redundancy Check (CRC). This may be due to transmissions corrupted by RF interference.
- **Clear Statistics**—Resets the statistics counter.

### 3.9.4 Radio Packet Statistics Menu

The previous screen dealt with Ethernet-related information. The *Radio Packet Statistics* screen (Figure 3-45) contains statistics that relate directly to over-the-air transmission of data. It provides valuable insight into the quality of the RF link between entraNET radios with respect to the handling of data packets.



**Figure 3-45. Radio Packet Statistics Menu**

- **Overflow**—TX packets with “LCP buffer overflow data” responses.
- **No Ack**—Number of packets that were sent but not acknowledged.
- **Lost Data**—TX packets lost; over-the-air retries exceeded.
- **Timeout**—TX data packets lost; contention timeout.
- **Good Data**—Data packets with CRC “good” responses.
- **Failed**—TX packets failed; data integrity failed.
- **Over the Air Data**—Data packets successfully delivered over the air.
- **Frag**—Total fragments of data received.
- **Retries**—Total number of times packets were re-transmitted.
- **Diags**—TX packets with “Remote not synchronized” data responses.

### 3.9.5 Event Log Menu

The microprocessor within the transceiver monitors many operational parameters and logs them. Events are classified into four levels of importance, which are described in [Table 3-3](#). Some of these events result from a condition that prevents the normal operation of the radio; these are “critical” events. These cause the radio to enter an “alarmed” state, and the POWER LED to blink, until the condition is corrected. All events are stored in the Events Log, which holds approximately 5,000 entries.

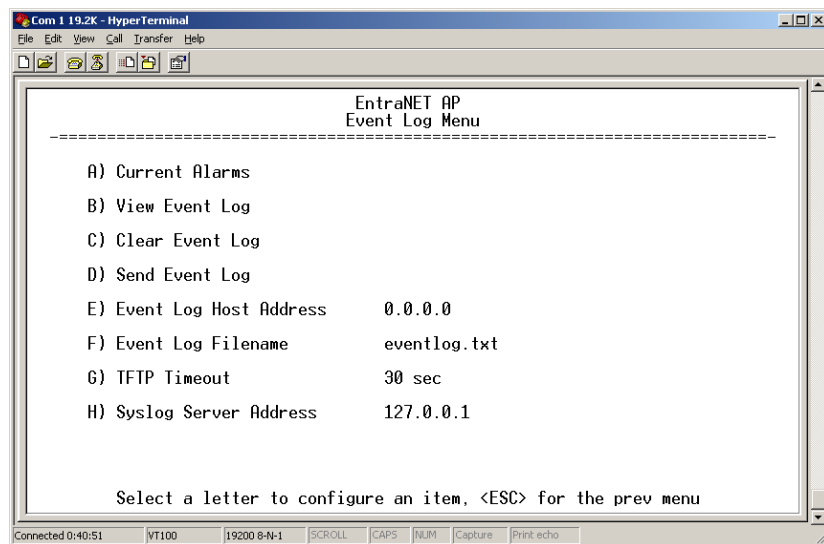
**Table 3-3. Event Classifications**

Level	Description or Impact
Informational	Normal operating activities
Minor	Does not affect radio operation
Major	Degraded radio performance, but still capable of operation
Critical	The radio cannot operate

#### Time and Date Stamping

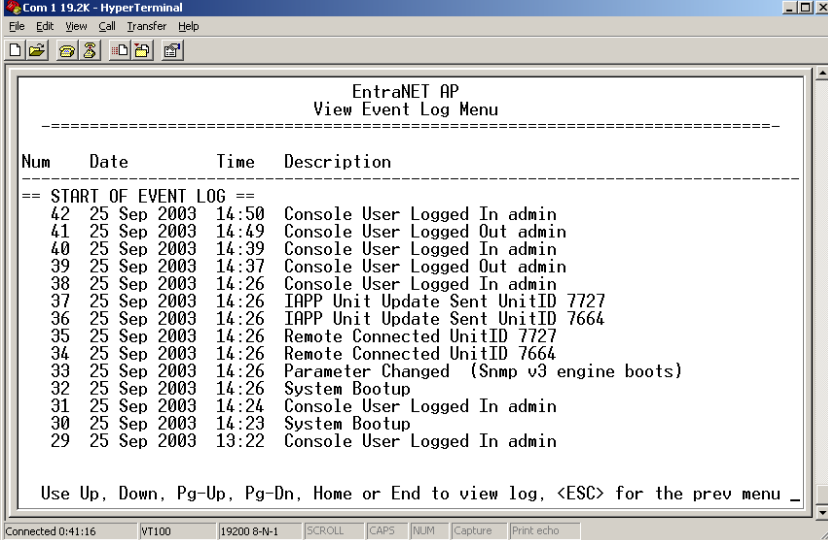
The events stored in the Event Log are time stamped using the time and date. You must manually enter the date and time at the AP.

See [“DEVICE INFORMATION MENU” on Page 84](#). The manually set time and date clock is backed up by an internal battery.



**Figure 3-46. Event Log Menu**

- **Current Alarms** (*Telnet or Terminal only*)—Lists events that have placed the radio in the alarmed state.
- **View Event Log** (see [Figure 3-47](#))—Lists events stored in the current log. Some of these events are stored in volatile memory, and are lost if power is removed.



```

Com 1 19.2K - HyperTerminal
File Edit View Call Transfer Help
-----
EntraNET AP
View Event Log Menu
-----
Num   Date       Time   Description
-----
== START OF EVENT LOG ==
42 25 Sep 2003 14:50 Console User Logged In admin
41 25 Sep 2003 14:49 Console User Logged Out admin
40 25 Sep 2003 14:39 Console User Logged In admin
39 25 Sep 2003 14:37 Console User Logged Out admin
38 25 Sep 2003 14:26 Console User Logged In admin
37 25 Sep 2003 14:26 IAPP Unit Update Sent UnitID 7727
36 25 Sep 2003 14:26 IAPP Unit Update Sent UnitID 7664
35 25 Sep 2003 14:26 Remote Connected UnitID 7727
34 25 Sep 2003 14:26 Remote Connected UnitID 7664
33 25 Sep 2003 14:26 Parameter Changed (Snmp v3 engine boots)
32 25 Sep 2003 14:26 System Bootup
31 25 Sep 2003 14:24 Console User Logged In admin
30 25 Sep 2003 14:23 System Bootup
29 25 Sep 2003 13:22 Console User Logged In admin
-----
Use Up, Down, Pg-Up, Pg-Dn, Home or End to view log, <ESC> for the prev menu _
-----
Connected 0:41:16 VT100 19200 8-N-1 SCROLL CAPS NUM Capture Print echo
  
```

**Figure 3-47. View Event Log Screen**

- **Clear Event Log**—Purges the log of all stored events.

**TIP:** Save your Event Log before clearing it to retain potentially valuable troubleshooting information. See [USING CONFIGURATION SCRIPTS](#) on Page 181 for an overview of how to transfer files from the transceiver to a computer on the network using TFTP (Trivial File Transfer Protocol).

- **Send Event Log** (*Telnet or Terminal only*)—Initiates TFTP transfer of the Event Log in a plain text (ASCII) file to a TFTP server on the connected LAN.
- **Event Log Host Address** (*Telnet or Terminal only*)—IP address of the computer on which the TFTP server resides.  
[Any valid IP address; 127.0.0.1]
- **Event Log Host Filename** (*Telnet or Terminal only*)—Name to be given to the Event Log file sent to the TFTP server for archiving.  
[Any 40-char alphanumeric string; eventlog.txt]

---

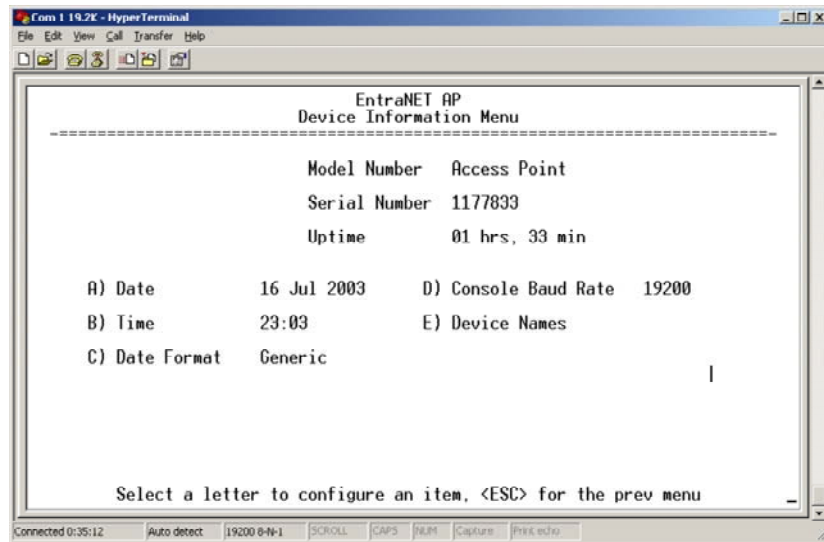
**NOTE:** You might want to change the Event Log file name to reflect the type of log you intend to archive, or its date.

---

- **TFTP Timeout** (*Telnet or Terminal only*)—Number of seconds the TFTP server waits for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer.  
[10 to 120 sec; 30]
- **Syslog Server Address**—The radio can also pass log messages to a syslog server as they occur. Use this field to enter the IP address of this server. [Valid server IP address]

## 3.10 DEVICE INFORMATION MENU

The *Device Information* menu (Figure 3-48) displays basic administrative data on the radio to which you are connected. It also provides a date and time display, Console Baud Rate setting, and customer-specific parameters under the Device Names selection.



**Figure 3-48. Device Information Menu**

- **Model** (*display only*)—Model type of the connected radio.
- **Serial Number** (*display only*)—Serial number of the connected radio.
- **Uptime** (*display only*)—Elapsed time since powering up the radio.
- **Date**—Current date being used for the transceiver logs (customer settable).
- **Time**—Current time of day (customer settable). Setting: HH:MM
- **Date Format**—Select a presentation format:
  - Generic = dd Mmm yyyy
  - European = dd-mm-yyyy
  - U.S.A. = mm-dd-yyyy

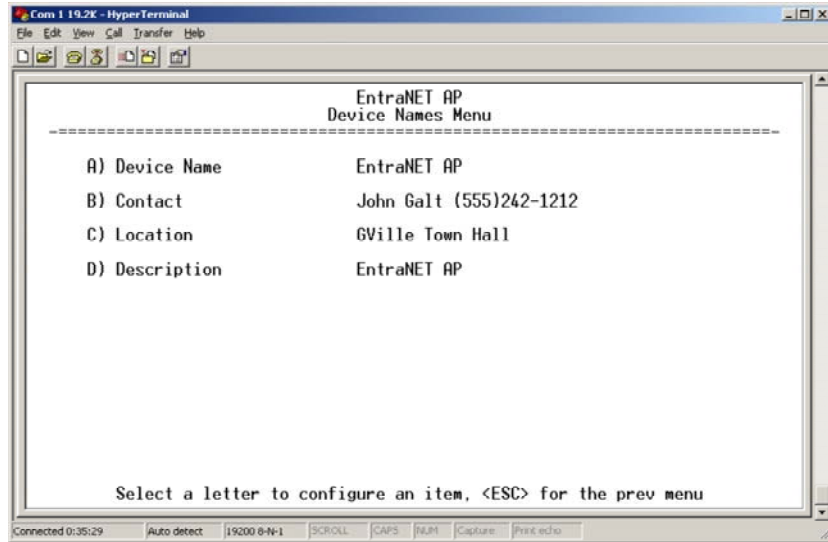
---

**NOTE:** The date and time are maintained by an internal battery module, which is not customer serviceable.

---

- **Console Baud Rate**—Allows setting the console baud rate to match the connected terminal.
- **Device Names Menu** (Figure 3-49)—The Device Name is used by the transceiver as the network realm name and as the entraNET MS screen heading. The contact, location, and description fields for each radio can be used to record whatever radio-specific information is useful to your organization. The information appears on this screen only.

## Device Names Menu



**Figure 3-49. Device Names Menu**

- **Device Name**—Device Name, used by the transceiver as the realm name for network security and menu headings.
- **Contact**—Customer defined; appears on this screen only.
- **Location**—Customer defined; appears on this screen only.
- **Description**—Customer defined; appears on this screen only.

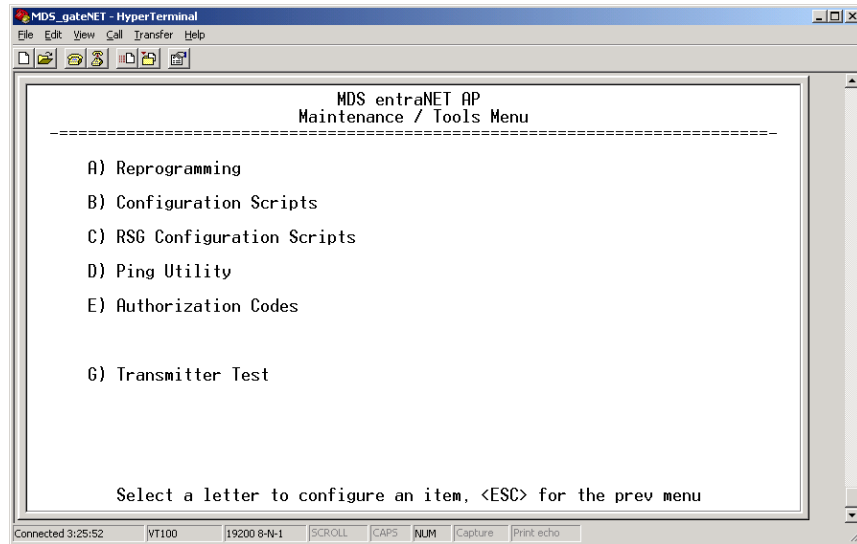
## 3.11 MAINTENANCE AND TOOLS

As part of operating your network, you might want to take advantage of product improvements, and to read and archive the configuration of your individual transceivers. The *Maintenance Menu* provides several tools to make this possible. This section provides detailed information on how to use these services.

Key maintenance tasks are:

- **Reprogramming**— Managing and selecting the radio operating system firmware resources. *See “[Reprogramming Menu](#)” on [Page 86](#).*
- **Configuration Scripts**—Saving and importing data files containing radio operating parameters or settings. *See “[Configuration Scripts Menu](#)” on [Page 87](#).*
- **RSG Configuration Scripts**—Scripts for configuring the Remote Serial Gateway. *See “[Remote Serial Gateway Configuration \(IP-to-Remote Serial\)](#)” on [Page 62](#).*
- **PING Utility**—Diagnostic tool to test network connectivity. *See “[PING Utility Menu](#)” on [Page 90](#).*

- Authorization Codes (Keys)—Alter the radio capabilities by enabling the built-in resources using purchased keys.  
*See “ Authorization Codes Menu” on Page 91.*
- Transmitter Test—Diagnostic commands for RF transmitter.  
*See “ Transmitter Test Menu” on Page 92.*



**Figure 3-50. Maintenance/Tools Menu**

### 3.11.1 Reprogramming Menu

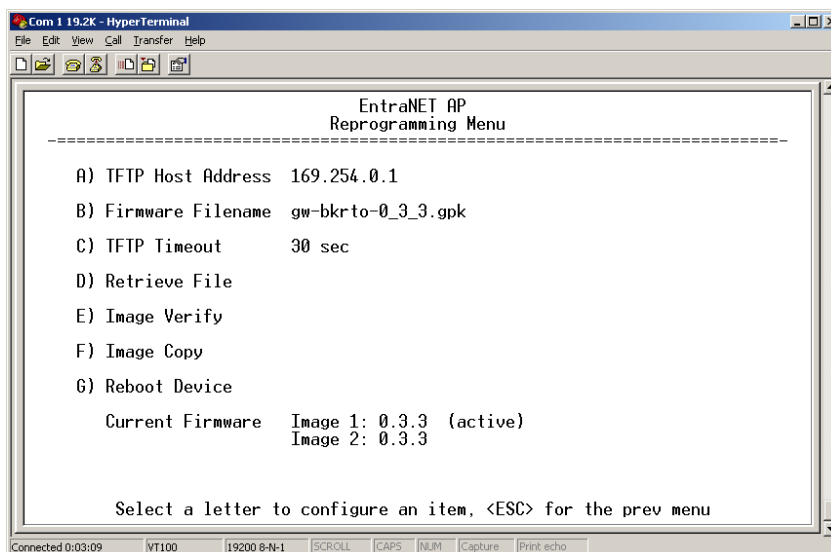
The AP transceiver has two copies of the firmware (microprocessor code) used for the operating system and applications. One copy is active and the second copy is standing by, ready to be used. Using the *Reprogramming Menu* (Figure 3-51), you can upload a new firmware release into the inactive position and place it in service whenever you desire.

---

**NOTE:** *See “UPGRADING AP FIRMWARE” on Page 179* for complete details on downloading new firmware code into the transceiver using TFTP.

---





**Figure 3-51. Reprogramming Menu**

- **TFTP Host Address**—IP address of the host computer from which to get the file. [Any valid IP address]
- **Firmware Filename**—Name of file to be received from the TFTP server. Verify that this string corresponds to the TFTP directory location. May require a sub-directory (for example: **entranet/bkrfto-1\_0\_0.gpk**). [Any 40-character alphanumeric string]
- **TFTP Timeout**—Time in seconds the TFTP server waits for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [10 to 120 sec; 30]
- **Retrieve File**—Initiate the file transfer from the TFTP server. Placed into inactive firmware position in the transceiver’s non-volatile memory. [Y, N]
- **Image Verify**—Verify the integrity of the firmware file held in the radio.
- **Image Copy**—Initiate the copying of the active firmware into the inactive image.
- **Reboot Device**—Initiate restarting the transceiver. This interrupts data traffic through this radio and the network, if performed on an AP. Use this command to toggle between firmware images.
- **Current Firmware**—Shows the current firmware revision level.

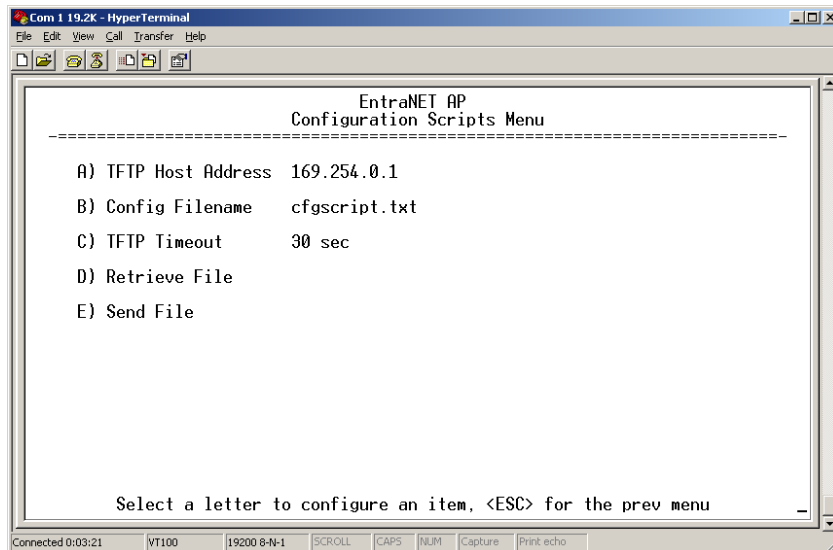
### 3.11.2 Configuration Scripts Menu

#### A Brief Description of Configuration Files

If you plan to have more than a few transceivers in your network, you might want to use the Configuration Scripts Menu ([Figure 3-52 on Page 88](#)) to configure similar radios from a common set of parameters. Over 50 customer settings that optimize the network are saved in a

configuration file (data file). However, only a few essential parameters need to be reviewed and altered to use the file with another transceiver.

A configuration file makes it easy to apply your unique settings to any transceiver(s) you wish. Configuration files also provide you with a tool to restore parameters to a known working set, in the event that a parameter is improperly set and performance is affected. See *“USING CONFIGURATION SCRIPTS”* on Page 181 for detailed instructions and a sample configuration file.



**Figure 3-52. Configuration Files Menu**

- **TFTP Host Address**—IP address of the computer on which the TFTP server resides. [Any valid IP address]
- **Config Filename**—Name of the file containing the configuration profile to be transferred to the TFTP server. The configuration information is in ASCII format. May require a sub-directory (for example: **config\entranet-config.txt**). [Any 40-character alphanumeric string]

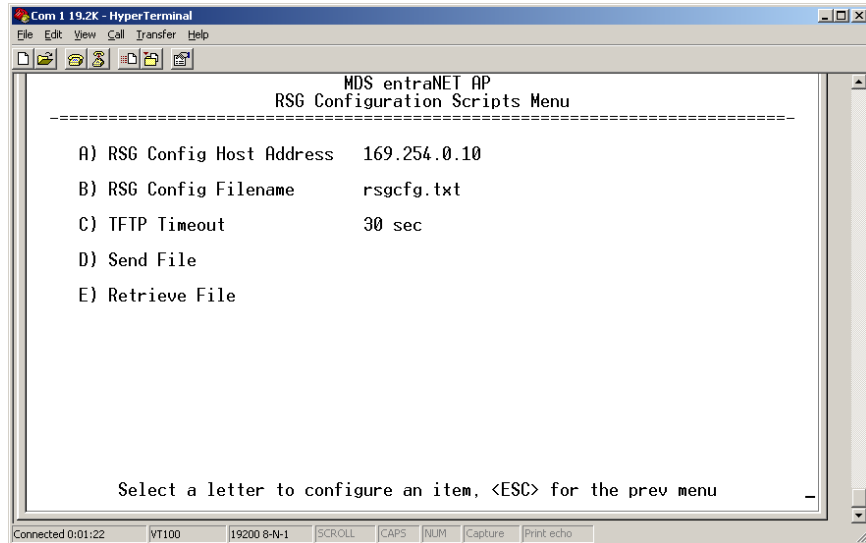
---

**NOTE:** The filename field is used in identifying the desired incoming file and as the name of file being exported to the TFTP server. Before exporting the configuration profile, you might want to name it something that reflects radio services or identification.

- **TFTP Timeout**—Time in seconds the TFTP server waits for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [10 to 120 sec; 30]
- **Retrieve File**—Initiate the file transfer of the configuration file from the TFTP server into the transceiver.
- **Send File**—Initiate the file transfer from the current configuration file to the TFTP server.

### 3.11.3 RSG Configuration Scripts Menu

The *RSG Configuration Scripts Menu* (Figure 3-53) is used to manage the download of configuration script files for the transceiver.

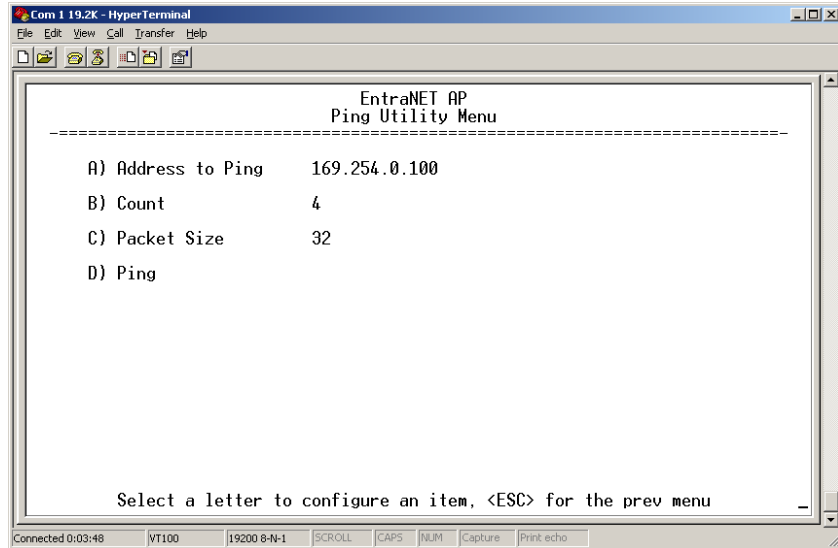


**Figure 3-53. RSG Configuration Script Menu**

- **RSG Config Host Address**—This is the IP address of the host computer. This computer also runs a TFTP server to transmit or receive configuration files.
- **RSG Config Filename**—The name of the file that has been created or uploaded from an existing AP. This file contains all of the programmable parameters of the transceiver.
- **TFTP Timeout**—This field shows the amount of time that the radio receiving information waits before reporting a fault condition.
- **Send File**—Sends the onboard configuration file to a remote host device.
- **Retrieve File**—This command initiates the download of the configuration file from the TFTP server PC.

## PING Utility Menu

Use the *PING Utility Menu* (Figure 3-54) to verify IP connectivity with LAN nodes or Ethernet endpoints.

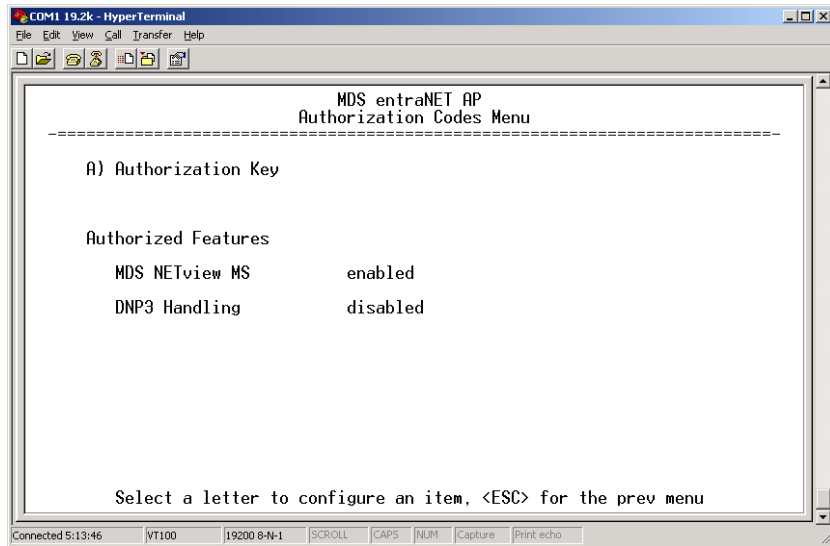


**Figure 3-54. PING Utility Menu**

- **Address to Ping**—Address to send a **PING**. [Any valid IP address]
- **Count**—Number of **PING** packets to be sent.
- **Packet Size**—Size in bytes of each **PING** data packet.
- **Ping**—Start sending **PING** packets to the address shown on the screen. The process can be stopped at any time by pressing **CTRL** C on the PC keyboard.

The screen then displays a detailed report of **PING** activity. Press any key after viewing the results to return to this menu.

### 3.11.4 Authorization Codes Menu



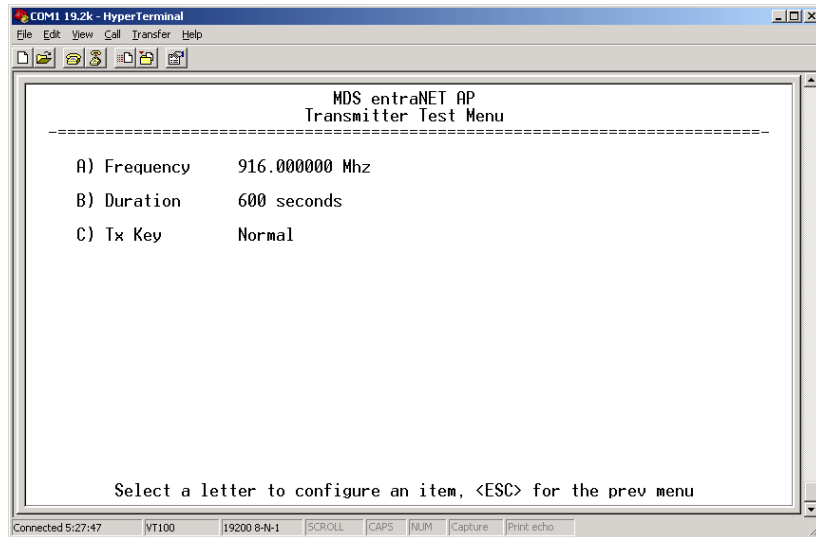
**Figure 3-55. Authorization Codes Menu**

- **Authorization Key**—Accept an Authorization Key into the transceiver’s non-volatile memory.
- **Authorized Features** (*display only*)—Presents a list of authorized features. At the time of publication, available features include GE MDS NETview MS and DNP3 Handling.

In the examples shown, GE MDS NETview MS is shown as an authorized and enabled feature, and DNP3 Handling is disabled. NETview MS software helps you monitor system performance, configure network elements, detect faults, and correct problems from the convenience of an office or from any other point in the network. For more information, refer to GE MDS publication 05-2973A01.

### 3.11.5 Transmitter Test Menu

This screen (Figure 3-56) allows testing of the radio transceiver RF transmitter section (power amplifier). Selections of specific frequencies and key duration, as well as transmit key behavior, can be modified from this screen. This function is useful for troubleshooting specific radio amplifier issues.



**Figure 3-56. Transmitter Test Menu**

- Frequency**—Used to set the carrier frequency used during transmitter testing.  
 [900 MHz radios: **902.200000-927.600000; 916.000000 MHz**]  
 [2.4 GHz radios: **2400.000000-2483.500000; 2400.000000 MHz**]
- Duration**—Sets the key duration time for transmitter testing.  
 [1-600 sec; **600**]
- TX Key**—Used to activate the transmitter on the test frequency. There are two modes: **Normal** and **Forced**. **Normal** is the default selection, and keeps the transmitter in standard *frequency hopping* configuration. **Forced** keys the transmitter on the specified test frequency. [**Normal, Forced; Normal**]

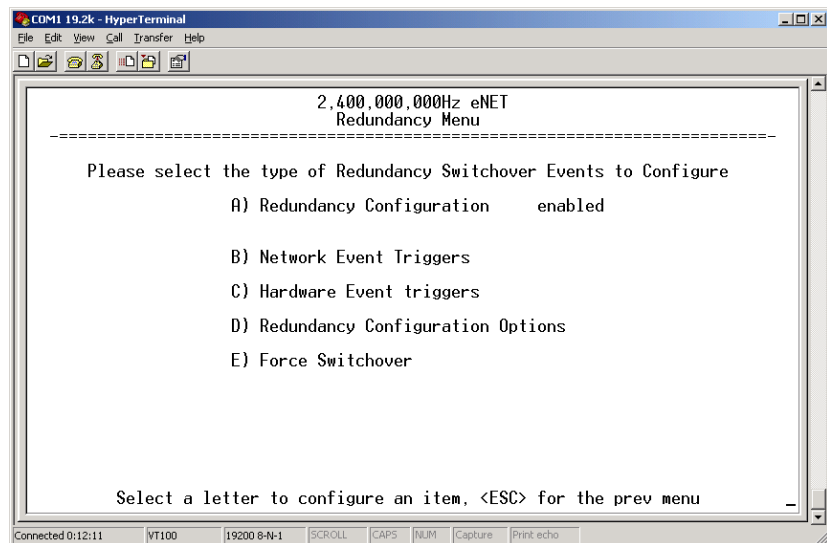
## 3.12 REDUNDANCY MENU

Redundancy is available only at the AP. The *Redundancy Menu* (Figure 3-57) is used in protected installations where a backup transceiver can be immediately placed online if a primary radio fails. This protects against “single point of failure” scenarios. The *Redundancy Menu* contains selections and settings that are used to manage redundancy functions.

---

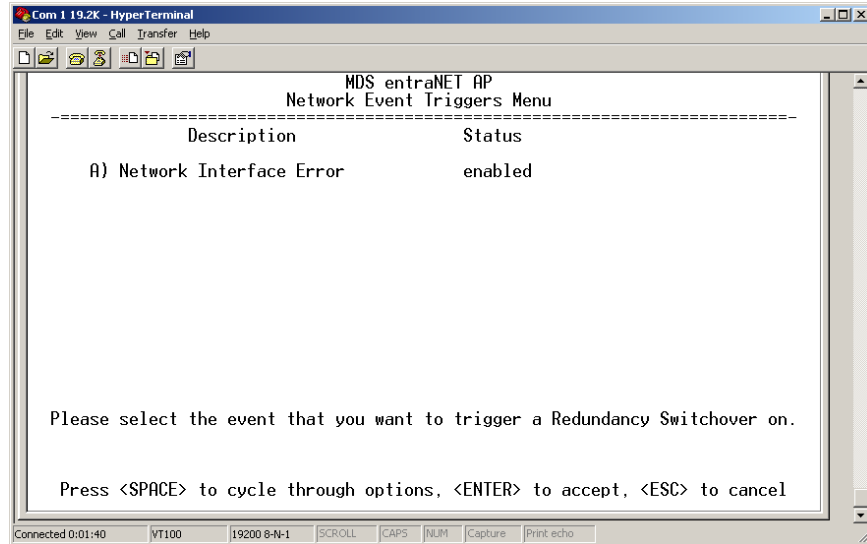
**NOTE:** Redundancy functions require the presence of a supervisory board (GE MDS Part No. 03-6061Axx). Ask your GE MDS representative for details.

---



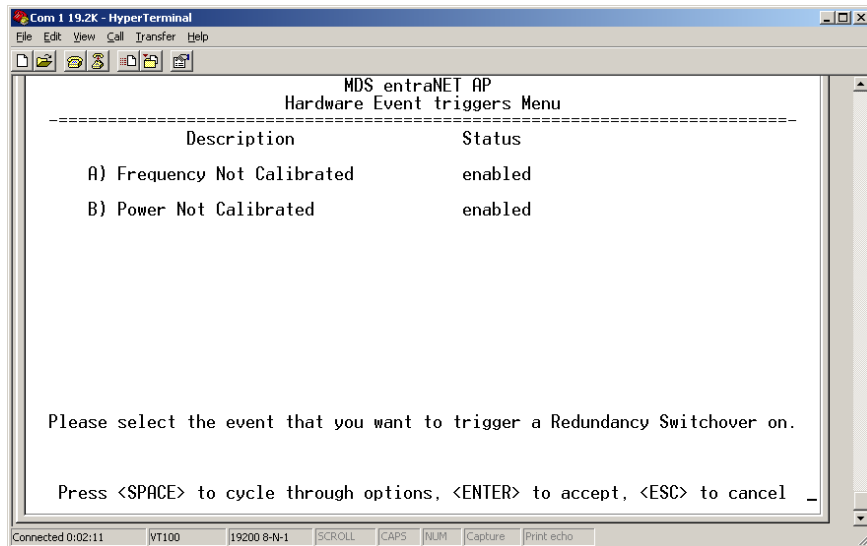
**Figure 3-57. Redundancy Menu**

- **Redundancy Configuration**—This selection is used to enable or disable redundancy operation. When the supervisory board detects an alarm condition, the currently selected transceiver is disabled, and the backup transceiver comes online. [**Enabled, Disabled; Enabled**]
- **Network Event Triggers**—This selection presents a submenu (see [Figure 3-58 on Page 94](#)) with Ethernet (network) alarm conditions.



**Figure 3-58. Network Event Triggers Menu**

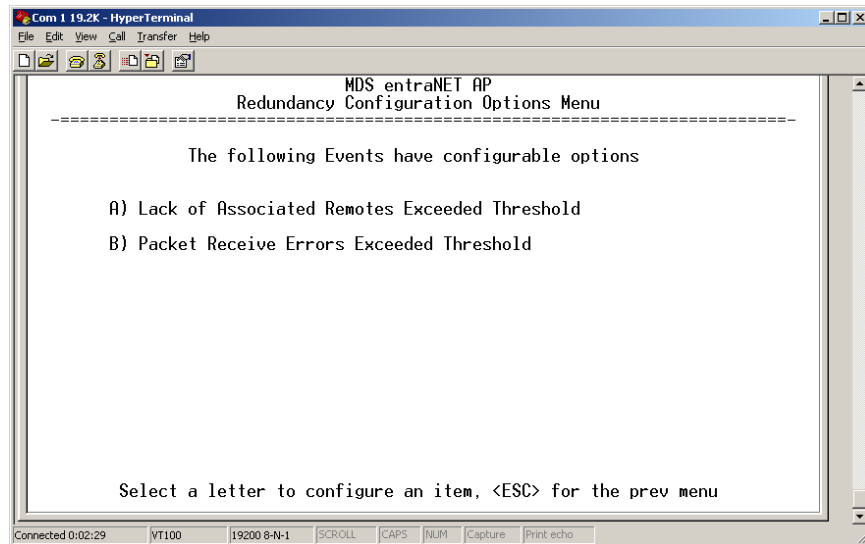
- Hardware Event Triggers**—This selection presents a submenu (see [Figure 3-59](#)) with parameters related to local alarm conditions.



**Figure 3-59. Hardware Event Triggers Menu**

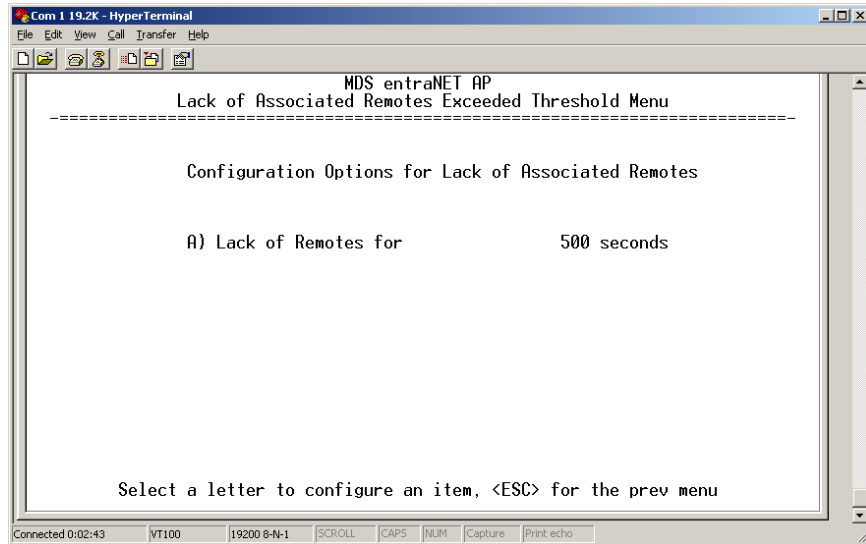
- Redundancy Configuration Options**—This selection presents a submenu (see [Figure 3-60 on Page 95](#)) for network event duration settings. For example, if a **PING** attempt fails after so many minutes, a contingency action is taken, such as the radio switches from the active to the standby radio.





**Figure 3-60. Redundancy Configuration Options Menu**

- **Force Switchover**—This selection invokes an immediate switchover from the active to the standby radio.
- **Network Interface Error**—This selection is used to enable or disable redundancy switchover on the occurrence of a Network Interface Error. [Enabled, Disabled; Enabled]
- **Frequency Not Calibrated**—This selection is used to enable or disable redundancy switchover if a frequency calibration error occurs. If this error occurs, the radio requires factory servicing. [Enabled, Disabled; Enabled]
- **Power Not Calibrated**—This selection is used to enable or disable redundancy switchover if an RF power calibration error occurs. If an error occurs, the radio requires factory servicing. [Enabled, Disabled; Enabled]
- **Lack of Associated Remotes Exceeded Threshold**—This selection shows another screen ([Figure 3-61 on Page 96](#)) where you can specify the duration of time that a redundant AP waits before considering itself to be malfunctioning. A system must have at least one associated Remote to be functional.

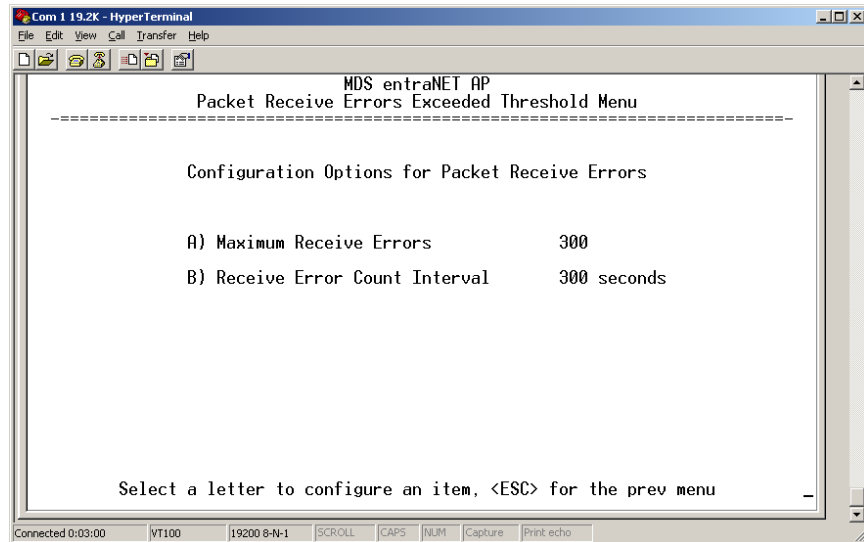


**Figure 3-61. Lack of Associated Remotes Exceeded Threshold Menu**

- **Packet Receive Errors Exceeded Threshold**—This selection shows another screen (see [Packet Rx Errors Exceeded Threshold Menu](#) below) where you can specify the number of packet errors that must be exceeded in a given time frame before a redundant AP considers itself to be malfunctioning.
- **Lack of Remotes for**—Number of seconds that a redundant AP waits before considering itself to be malfunctioning.

### **Packet Rx Errors Exceeded Threshold Menu**

This screen ([Figure 3-62](#)) contains two settings relating to Packet Receive errors. One setting sets the number of missed packets, and the other sets a time interval after which an error is declared. The settings work together, and both criteria must be met before a redundancy switchover occurs.



**Figure 3-62. Packet Rx Errors Exceeded Threshold Menu**

These configuration settings are intended for data-intensive applications and must be customized for your specific application.

**Maximum Receive Errors**—Specify the number of packet errors that must be exceeded before a redundant AP considers itself to be malfunctioning. This setting works in conjunction with the **Interval** setting below. [0-1000; 300]

- **Receive Error Count Interval**—This field is used for entering the number of seconds to count Packet Receive errors (works with **Maximum Receive Errors** above). [Time interval; 300 sec]

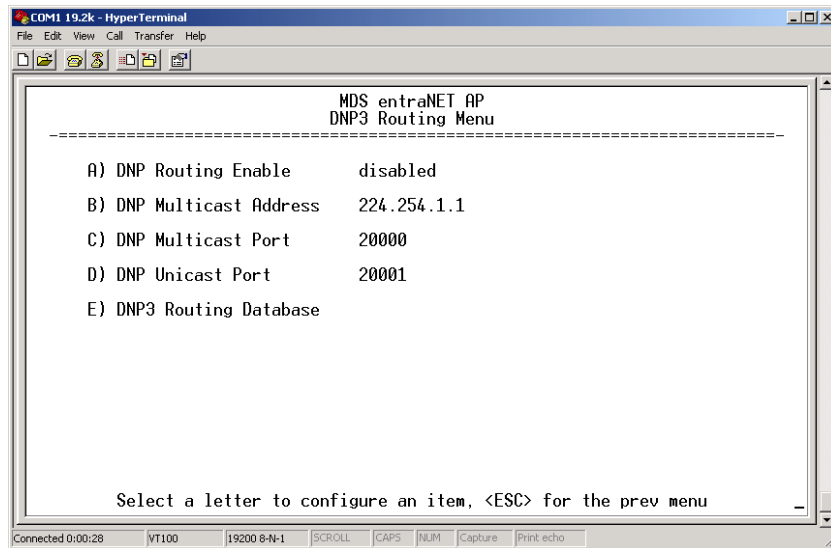
### 3.13 DNP3 ROUTING MENU

This menu (Figure 3-63) is used to configure the AP to support DNP3 protocol routing. See also *DNP3 Protocol-Aware Networks* on Page 8.

---

**NOTE:** Detailed information on the DNP3 protocol is available on the DNP Users' Group Web site at [www.dnp.org](http://www.dnp.org).

---



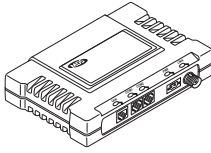
**Figure 3-63. DNP3 Routing Menu**

- **DNP Routing Enable**—Enables or disables the DNP3 routing function. [Enabled, Disabled; Disabled]
- **DNP Multicast Address**—Specifies the group address with which to exchange UDP-encapsulated messages with other IP devices that are DNP3 aware. This includes PCs, endpoint devices, and other APs. When a DNP3 packet is received and no routing information exists for the target device (see **DNP3 routing database** below), the AP sends the packet to all other IP devices in an attempt to find a radio that recognizes the address. [Valid IP address; 224.254.1.1]
- **DNP Multicast Port**—Specifies the IP port number used for all DNP3 Multicast messaging. [0-65535; 20000]
- **DNP Unicast Port**—This field specifies the IP port number used to establish a socket to other IP devices. This UDP port (along with the AP local IP address) is used to encapsulate DNP3 messages over IP. [0-65535; 20001]
- **DNP3 Routing Database**—This selection brings up a screen where the current DNP3 routing information known by the AP can be viewed.

---

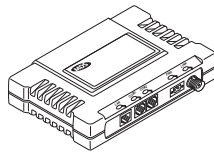
**NOTE:** For installations that include multiple APs, it is important to properly configure IAPP, which is located within the *Mobility Menu*. IAPP allows APs to share their DNP3 routing information.

---



# 4 REMOTE RADIO MANAGEMENT

4.1	INTRODUCTION	101
<hr/>		
4.2	Programming Methods	101
<hr/>		
4.2.1	Terminal Interface Mode .....	101
4.2.2	Remote Management via the AP .....	101
4.3	Log-in Procedure	101
<hr/>		
4.4	Commands	102
<hr/>		
4.4.1	Entering Remote Commands .....	102
4.5	Minimum Configuration for Remotes	102
<hr/>		
4.5.1	Detailed Command Descriptions .....	103
4.6	UPGRADING REMOTE FIRMWARE	117
<hr/>		



## 4.1 INTRODUCTION

Local configuration of Remote transceivers is performed through a PC terminal connected to the COM1 port of the radio. This section explains how to establish a console session with the Remote, and provides a complete list of commands.

## 4.2 Programming Methods

### 4.2.1 Terminal Interface Mode

You can use a PC program such as HyperTerminal to establish a terminal session with the Remote transceiver. The PC must be connected to the radio using its COM1 connector. Refer to *PC Connection and Log-In Procedures* on Page 37 for detailed cabling information.

**TIP:** You can access the HyperTerminal communications program on most PCs by selecting **Start > Programs > Accessories > Communications > HyperTerminal**.

You must use the following terminal settings to communicate with the Remote transceiver:

- 19,200 bps data rate
- 8 data bits
- no parity
- one stop bit (8N1)
- hardware flow control disabled
- ANSI or VT100 emulation

---

**NOTE:** The **exact** parameters given above must be used for terminal communication. Improper settings are a common cause of difficulty.

---

### 4.2.2 Remote Management via the AP

You can configure several Remote parameters over the air using the AP Management System. For more information on Remote Management using the AP, refer to *WIRELESS NETWORK MENU* on Page 69.

## 4.3 Log-in Procedure

You must log into the radio in order to issue commands. The log-in procedure for a Remote is somewhat different than for an AP. Follow the procedure below:

1. At the **entranet>** prompt, enter **login**.

2. At the **username** prompt, enter your username (**admin** is the default).
3. At the **Password** prompt, enter your password (**admin** is the default).

## 4.4 Commands

Table 4-1 on Page 103 provides a quick reference to the various commands for the Remote transceiver. Detailed descriptions for these commands follow in Section 4.5.1.

### 4.4.1 Entering Remote Commands

To enter a command:

- Type the command (including any spaces), and then press **ENTER**.

To request or set a value:

- Type the command, press **=**, and then press **ENTER**.

For example:

- Type **COMMAND\_ARGUMENT=** to query a setting or value.
- Type **COMMAND\_ARGUMENT=VALUE** to set values.

To get help with a command:

- Type the command, press **SPACE**, press **?**, and then press **ENTER**.

## 4.5 Minimum Configuration for Remotes

Remote radios require little configuration to operate, as most of the configuration is conducted at the AP. The minimum set of parameters that needs to be set for a Remote are:

**RADIO UNIT**—32-bit radio address. Defaults to the radio serial number, but is settable.

**RADIO NETADDR**—Radio network address. Must match the AP address.

**RADIO PWR** —RF output power setting in *decibels* (dB). The range is 20-30 for non-ETSI 900 MHz radios, 20-27 for non-ETSI 2400 MHz radios, and 10-20 for ETSI 2400 MHz radios.



**Table 4-1. Remote Commands—Quick Reference**

COMMAND	DESCRIPTION	COMMAND	DESCRIPTION
<b>_?</b> (after a command)	When entered after a command in this list, shows detailed information and allowable entries.	<b>HELP</b>	Lists commands supported for the logged-in user. See also the <b>?</b> command at the beginning of this table.
<b>ALARM</b>	Displays current alarm conditions by class.	<b>LOG</b>	Sets or displays the event log information.
<b>APLIST</b>	Sets or displays serial numbers of up to 50 APs with which the Remote can associate.	<b>LOGIN</b>	Secure log-in. Prompts for the case-sensitive username and password.
<b>AUTH</b>	Sets or displays the Authorization Key and a list of authorized features.	<b>LOGOUT</b>	Logs the user off and ends the terminal session.
<b>COM1</b>	Sets or displays the configuration of the COM1 port (baud rate, data format, buffer size, inter-packet gap).	<b>MESSAGE</b>	Sets the default priority level for message packets (low, normal, high).
<b>COM2</b>	Sets or displays the configuration of the COM2 port (baud rate, data format, buffer size, inter-packet gap).	<b>PASSWORD</b>	Sets the user log-in password for the user at the current access level or below.
<b>CONFIG</b>	Shows the dump configuration of all settable parameters.	<b>PROGRAM VERIFY</b>	Performs a checksum verification on one of six parameters.
<b>DEVICE</b>	Sets or displays the device configuration, including owner, company, and serial number.	<b>RADIO</b>	Sets or displays the radio configuration and status.
<b>DIRECT</b>	Sets or displays the configuration for direct mode operation.	<b>REBOOT</b>	Restarts the radio firmware.
<b>ENCRYPT</b>	Sets or displays the configuration for data encryption.	<b>SLEEP</b>	Sets the low-power operating mode: Sleep or Shutdown.
<b>ETH</b>	Sets or displays the Ethernet port configuration.	<b>STATS</b>	Shows radio statistics.
<b>HANDOFF</b>	Sets or displays the hand-off configuration.	<b>STATTRACKER</b>	When enabled (STATTRACKER ON), sends UDP packets from the Ethernet port on the Remote radio every time a wireless packet is received.
		<b>VER</b>	Displays the current version number.

## 4.5.1 Detailed Command Descriptions

### ALARM

Displays the current alarm conditions by severity level. For each level, the specific events that caused an alarm are listed, along with a brief description of each alarm. Alarm levels are:

- ALL**—All alarm classes
- INFORM**—Non-persistent information
- MINOR**—Minor alarm
- MAJOR**—Major alarm
- CRITICAL**—Critical alarm

Optional argument:

**HEX=** —Displays the hex bit codes for the current alarm condition by class. For each specific event that causes an alarm, the corresponding bit is set. Event numbers are matched to the appropriate hex code by a relationship of  $2^n$ .

## APLIST

Configures a list of approved APs.

Optional arguments:

**APx=<integer>** —Configures a list of approved APs. **x** is a number from 1–50, and **integer** is the serial number of an approved AP (1–99999999). To delete an entry, enter a serial number of 0; this indicates that the slot is not filled.

**AP1=<integer>**Serial Number of approved AP

**AP2=<integer>**Serial Number of approved AP

.

.

.

**AP50=<integer>**Serial Number of approved AP

**CLEAR**—Clears all entries in the AP list. Set **RESTRICT** to **OFF** before using this command to avoid restricting Remotes to associating with an empty list.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**RESTRICT=<ON|OFF>**—Turns on or off restricting registration to APs in the list.

**ON**—The Remote can only associate with an AP on the list.

**OFF**—The Remote can associate with any AP.

## AUTH

Displays the list of authorized features, or changes the Authorization Key that controls these features.

Optional arguments:

**KEY=<key>**—Enter a valid authorization key (1–16 characters), which is used to enable or disable software features.  
(Example: **AUTH KEY=123456abcdef**)

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

## COM1

Optional arguments:

**BAUD=<bps>**—Sets or displays the baud rate setting as 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 bps.

**BUFFER=<bytes>**—Sets or displays the maximum COM1 port buffer size (1–1500).

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**DEFAULT=<mode>**—Sets or displays the COM1 port default mode on startup. **DEFAULT** cannot be set to **DATA** unless the device has been authorized for serial payload.

**CONSOLE:** COM1 defaults to command-line mode.

**DATA:** COM1 defaults to transparent data mode.

**BSP:** COM1 defaults to in Basic Serial Protocol mode.

**INT\_LOOP:** COM1 defaults to internal loopback mode.

**EXT\_LOOP:** COM1 defaults to external loopback mode.

**FORMAT=<format>**—Sets or displays the COM1 port data characters, parity, and stop bits setting. Valid data parameters are:

**7N1**—seven char bits, no parity, one stop bit

**7N2**—seven char bits, no parity, two stop bits

**7O1**—seven char bits, odd parity, one stop bit

**7O2**—seven char bits, odd parity, two stop bits

**7E1**—seven char bits, even parity, one stop bit

**7E2**—seven char bits, even parity, two stop bits

**8N1**—eight char bits, no parity, one stop bit (default setting)

**8N2**—eight char bits, no parity, two stop bits

**8O1**—eight char bits, odd parity, one stop bit

**8O2**—eight char bits, odd parity, two stop bits

**8E1**—eight char bits, even parity, one stop bit

**8E2**—eight char bits, even parity, two stop bits

---

**NOTE:** Entering data formats other than those listed above might cause undesired operation.

---

**GROUP=<ID>**—Sets or displays the Group ID that this transceiver belongs to at the AP, for purposes of serial data multicasting (0-15).

**INTERGAP=**—Sets or displays the transceiver inter-packet gap status.

Optional arguments:

**IO**—For incoming and outgoing serial data.

**IN**—For incoming serial data only.

**IOL**—For incoming and outgoing (low latency) serial data.

**INL**—For incoming (low latency) serial data only.

**MODE=<mode>**—Sets the console port interface mode. **MODE** cannot be set to **DATA** unless the device has been authorized for serial payload. To escape from data mode, enter three consecutive + characters to COM1, with at least 100 ms between entries.

**CONSOLE**—Places COM1 in command-line mode.

**DATA**—Places COM1 in transparent data mode.

**BSP**—Places COM1 in Basic Serial Protocol mode.

**INT\_LOOP**—Places COM1 in internal loopback mode.

**EXT\_LOOP**—Places COM1 in external loopback mode.

**RXDELAYCHARS=**—Sets the inter-packet receive gap size in character times (1-65535).

**TXDELAY=**—Sets the inter-packet delay in milliseconds (1-65535). The minimum **TXDELAY** setting should be set to two times the **Dwelltime** setting. When **TXDELAY** is set to less than twice the **Dwelltime** setting, the measured inter-packet delay can increase up to one dwelltime (7, 14, or 28 ms) period.

## COM2

Sets or displays the COM2 port configuration.

Optional arguments:

**BAUD=<bps>**—Sets or displays baud rate setting as 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200 bps.

**BUFFER=<bytes>**—Sets or displays the COM2 port maximum buffer size (1–1500). The maximum Remote buffer size for incoming serial data is 1500 bytes. The Remote would then buffer up to 1500 bytes of serial data (from the RTU) before splitting the serial data into separate packets. Each packet, when transmitted over the air to an AP, is transmitted from the AP local serial port as a separate packet. This parameter does not affect serial data/packets received by the Remote over the air and transmitted out of the local Remote serial port.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**DEFAULT=<mode>**—Sets or displays the COM2 port default mode on startup. **DEFAULT** cannot be set to **DATA** unless the device has been authorized for serial payload.

**CONSOLE**—COM2 defaults to command-line mode.

**DATA**—COM2 defaults to transparent data mode.

**BSP**—COM2 defaults to Basic Serial Protocol mode.

**INT\_LOOP**—COM2 defaults to internal loopback mode.

**EXT\_LOOP**—COM2 defaults to external loopback mode.

**FLOWCTRL=<mode>**—Sets or displays the transceiver hardware flow control status.

Optional arguments:

**NONE**—Hardware flow control disabled

**CTS\_CTRL**—CTS (Clear-to-Send) flow control

**CTS\_RTS**—CTS follows RTS (Ready-to-Send) flow control

**RTS\_CTS**—DCE RTS/CTS hardware-based flow control

---

**NOTE:** You can use the CTS output from an entraNET radio for Data Carrier Detect (DCD) sense. It is always asserted (high) when flow control is set to **NONE**.

**CTS\_CTRL:** The radio asserts this line as long as it can accept data on the serial port. When the radio's internal serial buffers are full and it can't accept any more data on the port, it de-asserts (low) the CTS line.

**CTS\_RTS:** CTS follows RTS logic. When RTS is asserted by the DTE/PC and the internal serial buffers are not full, the radio asserts CTS as well. When RTS is de-asserted, CTS is de-asserted as well.

**RTS\_CTS:** In this case, RTS and CTS behave independently. RTS is asserted by the DTE/PC as long as it can accept radio data. When its buffers are full, the DTE/PC de-asserts its RTS line. The radio detects this change and stops transmitting data. The CTS line in this mode behaves the same as in CTS\_CTRL mode.

---

**FORMAT=<format>**—Sets or displays the COM2 port data characters, parity, and stop bits setting. Valid data parameters are:

**7N1**—seven char bits, no parity, one stop bit  
**7N2**—seven char bits, no parity, two stop bits  
**7O1**—seven char bits, odd parity, one stop bit  
**7O2**— seven char bits, odd parity, two stop bits  
**7E1**—seven char bits, even parity, one stop bit  
**7E2**—seven char bits, even parity, two stop bits  
**8N1**—eight char bits, no parity, one stop bit (default setting)  
**8N2**—eight char bits, no parity, two stop bits  
**8O1**—eight char bits, odd parity, one stop bit  
**8O2**—eight char bits, odd parity, two stop bits  
**8E1**—eight char bits, even parity, one stop bit  
**8E2**—eight char bits, even parity, two stop bits

---

**NOTE:** Entering data formats other than those listed above may cause undesired operation.

---

**GROUP=<ID>**—Sets or displays the Group ID that this transceiver belongs to at the AP, for purposes of serial data multicasting (0-15).

**INTERGAP**—Sets or displays the transceiver inter-packet gap status.

Optional arguments:

**IO**—For incoming or outgoing serial data.  
**IN**—For incoming serial data only.  
**IOL**—For incoming or outgoing (low latency) serial data.  
**INL**—For incoming (low latency) serial data only.

**MODE=<mode>**—Sets the console port interface mode. **MODE** cannot be set to **DATA** unless the device has been authorized for serial payload. To escape from data mode, enter three consecutive + characters to COM2 with at least 100 ms between entries.

**CONSOLE**—Places COM2 in command-line mode.

**DATA**—Places COM2 in transparent data mode.

**BSP**—Places COM2 in Basic Serial Protocol mode.

**INT\_LOOP**—Places COM2 in internal loopback mode.

**EXT\_LOOP**—Places COM2 in external loopback mode.

**RXDELAYCHARS=** —Sets the inter-packet receive gap size in character times (1-65535).

**TXDELAY=** —Sets the inter-packet delay in milliseconds (1-65535). The minimum **TXDELAY** setting should be set to two times the **Dwelltime** setting. When **TXDELAY** is set to less than twice the **Dwelltime** setting, the measured inter-packet delay can increase up to one dwelltime period (7, 14, or 28 ms).

## CONFIG

Saves or displays the current configuration. The output is in a format that can be copied back into the command line in order to set the configuration.

Optional arguments:

**SHOW**—Displays the current configuration. This is a read-only response.

**SAVE=FACT**—Programs the current configuration into the Factory Default configuration table. The factory default is used to restore the configuration when the system detects a data corruption.

## DEVICE

Displays the device configuration, and allows setting of the **OWNER**, **NAME**, and **LOCATION**.

Optional arguments:

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**COMPANY**—(*read only*) Displays the company name.

**MODEL**—(*read only*) Displays the radio model number.

**PRODUCT**—(*read only*) Displays the product name.

**REV**—(*read only*) Displays the software revision ID.

**OWNER**—Sets or displays the owner information (1-40 ASCII characters).

**NAME**—Sets or displays the radio name (1-40 ASCII characters).

**LOCATION**—Sets or displays the radio location (1-40 ASCII characters).

**UPTIME**—(*read only*) Displays the current system uptime in the format <YY-MM-DD hh:mm:ss>.

**SER**—Device serial number.

## DIRECT

Sets or displays the configuration for direct-mode operation (Remote-to-Remote). This is a special mode intended primarily for railroad applications where Remotes communicate with each other.

Optional arguments:

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**CWMIN**=<range integer>—In **ROOT** mode, this command sets the Minimum Contention Windows size (<**CWMAX**+1).

0: Min=0  
15: Max=15

**CWMAX**=<range integer>—In **ROOT** mode, this command sets the Maximum Contention Windows (>**CWMIN**-1).

0: Min=0  
15: Max=15

**DEFAULT**=<mode>—Sets or displays the default power-up state direct mode.

**ON**: Default direct state is Direct Mode.  
**OFF**: Default direct state is Infrastructure Mode.  
**EXT**: Default direct state is controlled by an external I/O pin.

**FEC**=<ON|OFF>—In **ROOT** mode, this command sets the Forward Error Correction setting.

**ON**: FEC on  
**OFF**: FEC off

**HOPTIME**=<ms>—In **ROOT** mode, this command sets the time between frequency hops:

7: 7 ms  
14: 14 ms  
28: 28 ms

**MODE**=<mode>—Sets operation to Direct or Infrastructure mode.

**ON**: Enter Direct mode  
**OFF**: Enter Infrastructure mode  
**EXT**: Enter Direct mode by external control

**NETADDR=<netaddr>**—Sets or displays the network (system) address (0-30000) when in direct mode.

**PWR=<range integer>**—In **ROOT** mode, this command sets the radio power setting in dBm (the range depends on the radio model).

**REPEAT=<range integer>**—In **ROOT** mode, this command sets the Broadbase Repeat Count.

**0:** Min=0  
**15:** Max=15

**RETRY=<range integer>**—In **ROOT** mode, this command sets the Maximum Unicast Retry Count.

**0:** Min=0  
**15:** Max=15

**SKIPZONES=<bitmap>**—In **ROOT** mode, this command sets the Skip Zones Binary Map (HEX: preceded by **0x**).

**bit0:ZONE1;** 1=Skipped 0=Active  
**bit1:ZONE2;** 1=Skipped 0=Active  
**bit2:ZONE3;** 1=Skipped 0=Active  
**bit3:ZONE4;** 1=Skipped 0=Active  
**bit4:ZONE5;** 1=Skipped 0=Active  
**bit5:ZONE6;** 1=Skipped 0=Active  
**bit6:ZONE7;** 1=Skipped 0=Active  
**bit7:ZONE8;** 1=Skipped 0=Active

**STATE=**—(*read only*) Displays the current Direct mode status.

Currently operating in Infrastructure mode  
Currently operating in Direct mode

**TYPE=**—Sets or displays the role of this radio in Direct mode.

**NODE:** Operates as one of the Node Remotes  
**ROOT:** Operates as the Single Root Remote

## ENCRYPT

Sets or displays the configuration for data encryption.

Optional arguments:

**MODE=<ON|OFF>**—Sets or displays the data encryption mode.

**ON:** Data encryption on  
**OFF:** Data encryption off

**PHRASE=<string>**—Sets or displays the Encryption Pass Phrase (8–41 characters).



**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

## ETH

Sets or displays the configuration of the Ethernet port. You can set the port to a specific Ethernet address (static mode), or the address can be determined automatically based on the first received packet (autoselect mode).

Optional arguments:

**ENDPT**=<string of bytes in hex that is the endpoint MAC address>—Sets or displays the Ethernet endpoint address, and sets the endpoint address behavior. The Ethernet address must be in the following format:  
**xx:xx:xx:xx:xx:xx**.

Set **ETH ENDPT** to the device's Ethernet address, or set the address to a string of zeros to use the address of the source of the first received packet.

**ENDPTMODE**=<auto, static>—Displays the endpoint IP address behavior:

**AUTO**—Endpoint address is automatically set to the source address of the first received packet.

**STATIC**—Endpoint address is manually configured.

**MODE**=<ON|OFF>—Determines whether the Ethernet port is enabled or disabled.

**ON**: Ethernet port is enabled.

**OFF**: Ethernet port is disabled.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

## HANDOFF

Sets or displays the hand-off configuration.

Optional arguments:

**ACKAVG**=<percent>—The percentage of hops for which data transmission was successful (an ACK for the hop was received). This average is sampled every hop over an interval as defined by **HANDOFF ACKAVGINT**.

**ACKAVGINT**=<integer>—**ACKAVG** averaging interval, defined as averaging ACKs received over 1, 2, 4, 8, 16, 32, 64, or 128 hops.

**ACKAVGTHRESH**=<percent>—The hand-off threshold for ACK averaging (1–99).

**BLOCKTIME**=<seconds>—Sets or displays the time in seconds (0–255) to block access to an AP after hand-off.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**COUNT=<integer>**—Number of hand-offs that occurred.

**MODE=<mode>**—Sets or displays the hand-off configuration, or disables hand-offs.

**OFF:** Hand-off is deactivated.

**ACK:** The Remote hands off when **ACKAVG=** is below the programmed threshold **ACKAVGTHRESH=**.

**RSSI:** The remote hands off when **RSSIAVG=** is below the programmed threshold **RSSIAVGTHRESH=**.

**ACKRSSI:** The remote hands off when either **ACKAVG=** or **RSSIAVG=** falls below its programmed threshold.

**RSSIAVG=<RSSI -dBm>**—Current RSSI average dBm. This average is determined by sampling, as defined by **RSSIAVGINT=**.

**RSSIAVGINT=<integer>**—RSSI sampling frequency, defined as:

- 1:One sample every 61 hops
- 2:Two samples every 122 hops
- 4:Four samples every 244 hops
- 8:Eight samples every 488 hops
- 16:16 samples every 976 hops
- 32:32 samples every 1952 hops
- 64:64 samples every 3904 hops
- 128:128 samples every 7808 hops
- 256:256 samples every 15616 hops

**RSSIAVGTHRESH=<RSSI -dBm>**—The hand-off threshold for RSSI averaging (–120 dBm to –50 dBm).

## HELP

Lists commands supported for the current user log-in level.

## LOG

Sets or displays the event log information, and displays the number of entries in the event log. Optional arguments are used to clear or display the log.

Optional arguments:

**CLEAR**—Clear the event log

**SHOW**—Show the event log

**TOTAL=** —Number of event log entries in log. Read only.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

---

**NOTE:** The entraNET remote does not have a real-time clock, but the AP does. When a remote synchronizes and associates with an AP, the actual date/time information is sent from the AP to the remote. This allows the remote to assign the actual date and time to event entries in the log. If the remote is not synchronized to an AP, event log entries on the remote are displayed with a date/time stamp that represents the remote's uptime (the amount of time since the last reboot of the remote) rather than an actual date/time stamp.

---

## LOGIN

This command is used for secure log-in to the radio. At the prompt, enter the case-sensitive username and password. Each of these entries can be up to eight characters long.

## LOGOUT

Logs the user out of the command interface.

## MESSAGE

Sets or displays the default packet priority.

Optional arguments:

**LOW**—Default priority setting is low.

**NORMAL**—Default priority setting is normal.

**HIGH**—Default priority setting is high.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

## PASSWORD

Sets the log-in password for the user at current access level or below.

Optional arguments:

**<username>**—The log-in username to be associated with the password.

## PROGRAM VERIFY=

Performs a checksum verification of one of the parameters listed below.

---

**NOTE:** Do not enter **PROGRAM** alone, without the **VERIFY=** qualifier, unless instructed by GE MDS technical personnel. Such an entry causes the radio to enter the Bootloader mode which, if improperly used, causes an undesired state in the radio.

*If you are instructed to enter the Bootloader mode by GE MDS, be aware that selecting **y** automatically changes the console baud rate to 115200 bps. Failure to change the terminal program to match this baud rate will cause communications errors.*

---

Optional arguments:

**ALL**—All images

**BOOT**—Bootloader Image

**APP1**—Firmware application image 1

**APP2**—Firmware application image 2

**TOR1**—Tor 1 Image

**TOR2**—Tor 2 Image

## RADIO

Sets or displays the radio configuration and status.

Optional arguments:

**AP=** —(*read only*) Displays the associated AP Serial Number.

**ASSOC=**—(*read only*) Displays whether or not the Remote radio has been associated with an AP.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**NETADDR=<string>**—The current network address (1-15 alphanumeric characters).

**PWR=<dBm>**—Sets or displays the current power setting. The value is in dBm, with an acceptable range of 0–30 for 900 MHz radios, 10–20 dBm for 2.4 GHz ETSI radios, or 17–27 dBm for 2.4 GHz non-ETSI radios.

**QUALITY=**—(*read only*) Displays the quality of the over-the-air link, expressed as a percent (0-100). Quality is calculated from the successful reception of ACK packets sent by the AP (0-100).

**REFRESH=<refresh>**—Connection refresh period in seconds (0–255). The Remote inherits the **database timeout** value from the AP and applies that value to the **refresh** parameter.

**RSSI=** —(*read only*) Shows the Received Signal Strength (RSSI). The value is shown in dBm, with a range of -120 to 0. This value is refreshed every 3 sec.

**SYNC=** —(*read only*) Shows the current state of radio synchronization.

**TX KEY=<on, off>**—Starts or stops the transmitter test.

**TX FREQ=<valid frequency range>**—Sets or displays the carrier frequency (in MHz) for transmitter tests. The valid range is 902.2–927.6 for 900 MHz radios, or 2400.6–2482 for 2.4 GHz radios.

**UNIT=<unit>**—The 32-bit user-programmable radio address, which defaults to the radio serial number, but can be changed.

## REBOOT

Restarts the radio firmware.

Optional arguments:

**SAME**—Restarts the radio with the active firmware image.

**OTHER**—Restarts the radio with the inactive image.

**APP1**—Restarts the radio with Application Image 1.

**APP2**—Restarts the radio with Application Image 2.

## SLEEP

Sets or displays the low-power operating mode. These modes are commonly used where power consumption must be kept to a minimum, such as in solar-powered installations.

Optional arguments:

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**DTRSENSE=<low, high>**—Select the level of RS-232 DTR signal used by the endpoint device to wake the radio:

**LOW:** DTR Active LOW

**HIGH:** DTR Active HIGH

When **WAKE** is set to **DTR**, the radio will wake on receiving this signal from the endpoint device.

**HANGTIME=<hangtime in ms>**—Minimum wake time in milliseconds (100–60000) before returning to Low Power mode.

**INDICATOR=<on|off>**—Indicates whether or not the Sleep indicator LED is active.

**ON:** Sleep Mode indicator is on.

**OFF:** Sleep Mode indicator is off.

**MODE=<mode>**—Set the mode as follows:

**NONE:** Normal operation; the radio does not sleep.

**SLEEP:** Sleep mode is enabled. In this mode, the radio draws less than 20 mA at 12 V. It can be brought back online (ready to send data) within 75 ms. Wake-up is accomplished by asserting the DTR line on the COM2 port, or by the appearance of payload data at the active COM port.

Sleep mode also works on the Ethernet interface, except that the endpoint device must not require Ethernet pulse signals in order to send data. This mode is similar to a PC Ethernet port “Wake on data” setting.

**SHUTDOWN:** Shutdown mode is enabled. In this mode, the radio draws less than 1 mA at a supply voltage of 12 Vdc. Note that this mode requires a longer wake-up time, almost as long as if the radio was de-powered.

**NOW=<setting>**—This command is used to place the radio into immediate Sleep or Shutdown mode.

**Sleep:** The radio immediately enters Sleep mode.

**Shutdown:** The radio immediately shuts down, drawing less than 1 mA at a supply voltage of 12 Vdc.

**WAKE=<dtr, data>**—Selects a control option to activate (enter) or deactivate (exit) Sleep or Shutdown modes.

**DTR:** Wake under DTR signal control.

**DATA:** Wake up on data.

## STATS

Displays radio statistics. If **<device>** (**RADIO**, **COM1**, **COM2**, **ETH**) is omitted, **all** statistics are displayed.

Optional arguments:

**ALL:** Displays all statistics.

**RADIO:** Displays radio packet statistics.

**COM1:** Displays COM1 packet statistics.

**COM2:** Displays COM2 packet statistics.

**ETH:** Displays Ethernet packet statistics.

**RESET:** Resets packet statistics for the indicated interface.

## STATTRACKER

When the **STATTRACKER** mode is turned on, the Remote transceiver sends UDP packets with a broadcast destination IP address. The command has a user-defined port number between 30000 and 60000, and sends packets consisting of:

- RSSI statistics
- Connectivity
- Packets received
- Packets transmitted
- Packets dropped
- Bytes received
- Bytes transmitted
- Receive byte errors
- Transmit byte errors
- Total fragments
- Total retries

The source MAC address in the UDP packet is the MAC address from the entraNET AP. These monitoring packets are sent every time there is over-the-air traffic.

This command is designed to work with the *GE MDS Mobility Application* available from GE MDS (Part No. 06-4157A01).

Optional arguments:

**ON:** Turns the Stattracker function on.

**OFF:** Turns the Stattracker function off.

**30000–60000:** Allowable range of port numbers that can be entered.

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

## VER

Displays the current software version information.

Optional arguments:

**CMD**—Displays all settable optional arguments and their current values. You can copy this list to a text file as a record of your configuration.

**CONFIG=** —Displays the Configuration Table version number.

**EVENT=** —Displays the Event List version number.

**H2H=** —Displays the Host-to-Host protocol version number.

**HREV=** —Displays the OIB board hardware version number.

**IMAGE=<image>**—Displays the number of the currently active image.

**LOG=** —Displays the current log version number.

**RADIO SW=** —Displays the current software version number (**xx.yy.zz**).

**SREV1=** —Displays the software version number (**xx.yy.zz**).

**SREV2=** —Displays the software version number (**xx.yy.zz**).

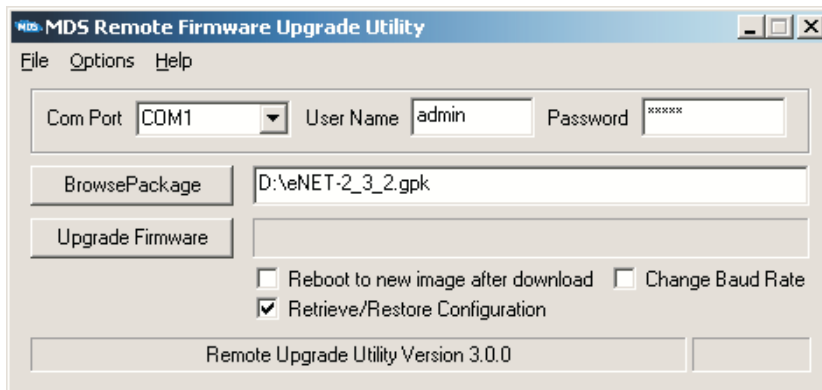
**XHREV=** —Displays the radio board hardware revision number.

**XSREV1=** —Displays the radio software version.

**XSREV2=** —Displays the radio software version.

## 4.6 UPGRADING REMOTE FIRMWARE

You can upgrade remote radio firmware using the *Remote Firmware Upgrade Utility* available from GE MDS. A local PC connection to the radio is required to use this utility.

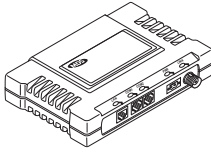


**Figure 4-1. Remote Firmware Upgrade Utility—Initial Screen**

A brief description of each screen item is given below.

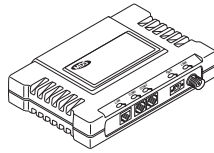
- **File**—Allows exiting the utility.
- **Options**—Select to extract S28 files, display the debugging log, or show file versions.
- **Help**—Shows the copyright and version information.
- **Com Port**—Identifies the COM port on the computer to be used for upgrading radio firmware.
- **User Name, Password**—Enter the username and password that have been configured at the radio.
- **Browse Package**—Allows selection of an upgrade file to be loaded into the radio. This functions in a similar manner to the Windows environment.
- **Upgrade Firmware**—This button initiates the file transfer to the radio.
- **Reboot to new image after download**—When checked, the radio reboots with the new firmware just loaded.
- **Change Baud Rate**—When checked, the utility automatically changes its baud rate to match that set in the radio.
- **Retrieve/Restore Configuration**—When checked, this saves a copy of your configuration. GE MDS recommends that you check this box before upgrading to ensure that you have a back-up copy of your configuration.





# 5 SAMPLE CONFIGURATIONS

5.1	INTRODUCTION	121
5.2	IP-to-Local Serial Application Example	121
	Establishing a Connection .....	121
5.3	IP-to-Remote Serial Application Example	122
5.3.1	Endpoint Device Connected to the AP .....	123
5.4	Point-to-Point, Serial-to-Serial Application Example	123
5.4.1	Step-by-step Instructions for Configuring a Point-to-Point Serial Connection .....	124
5.5	Point-to-Multipoint, Serial-to-Serial Application Example	132
5.5.1	Step-by-Step Instructions for Configuring a Point-to-Multipoint Serial Connection .....	133
5.6	Mixed-Mode Application Example	140
5.6.1	Operation and Data Flow .....	140
5.7	Group Broadcast Session Example	142



## 5.1 INTRODUCTION

This chapter provides details of how radios should be configured and connected for specific applications, such as IP-to-serial and serial-to-serial configurations. Only the most relevant parameters are shown for the sake of simplicity. All other parameters are assumed to be set at their default values.

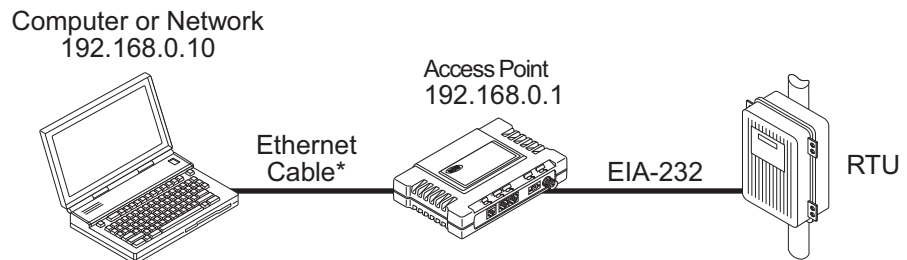
## 5.2 IP-to-Local Serial Application Example

You can use either UDP or TCP to establish communications with the entraNET radio. The choice depends on the type of device you are communicating with at the other end of the IP network. This example uses TCP to illustrate this function.

In TCP mode, the transceiver remains in a passive state, offering a socket for connection. When a request is received, data received by the AP serial port is sent out through the IP socket and vice versa, until the connection is closed or the link is interrupted. The TCP session has a 10-min time-out. If inactive for that time, it ends the session. The transceiver offers the port for connection again after this time. See [Figure 5-1](#) and [Table 5-1](#).

### Establishing a Connection

From the PC, establish a TCP connection to the IP address of the Remote transceiver and to the IP port as configured earlier (typically 30011). You can use a telnet client application to establish this connection. Data can now be sent between the PC and the endpoint device.



\*Use crossover cable for computer; straight-through cable for network

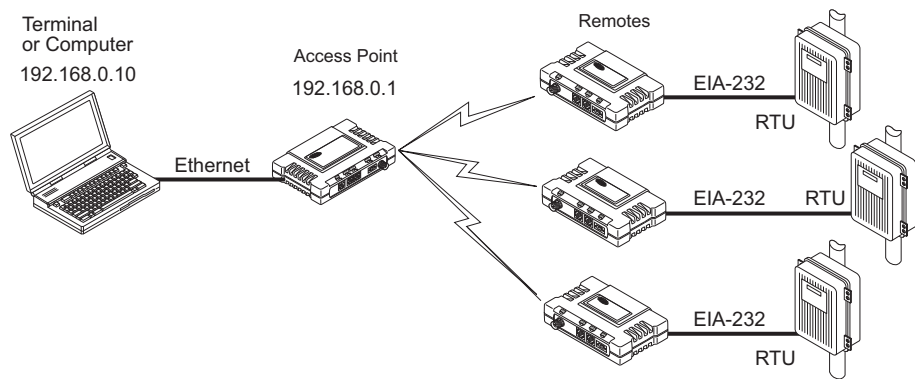
**Figure 5-1. IP-to-Local Serial Application Diagram**

**Table 5-1. IP-to-Local Serial Port Application Configuration**  
*IP-to-local serial connection (Local Serial Gateway)*

Radio Location	Menu Item	Setting
AP (COM2)	Port Status	Enabled
	Mode	TCP
	RX IP Port	30011
	Baud Rate	19200
	Byte Format	8N1
	Buffer Size	256 Bytes

### 5.3 IP-to-Remote Serial Application Example

This configuration makes any data sent or received with the AP with an IP port number appear using the serial port of a single Remote (or of all Remotes, if “Broadcast” is selected for Remote ID).



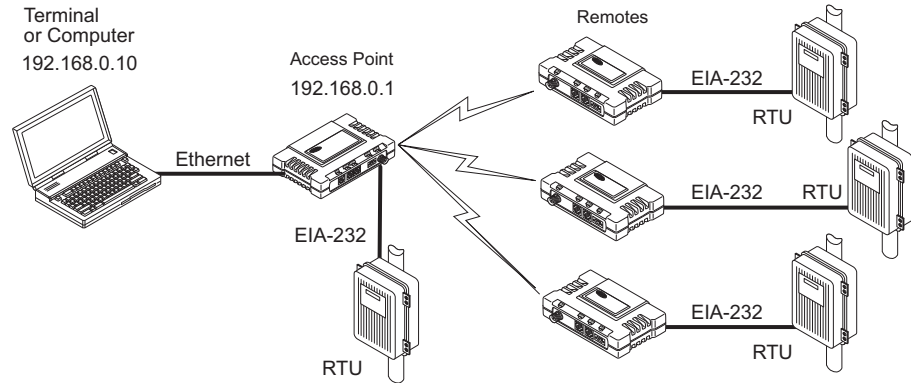
**Figure 5-2. IP-to-Remote Serial Application Diagram**

**Table 5-2. IP-to-Remote Serial Application Configuration**

MDS entraNET Radio Location	Menu Item	Setting
AP (COM2)	Remote ID	1155883
	COM Port	COM2
	Mode	TCP Server
	Radio IP Port	30066
Remote radio (COM2)	Mode	COM2 in transparent data mode
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4

### 5.3.1 Endpoint Device Connected to the AP

In this arrangement, information received using an AP Ethernet port is sent to the serial port of the Remotes **and** the AP local serial port. The reverse is also true, meaning that any data received from the serial port of any Remote **or** the AP local serial port is encapsulated into an IP packet and sent out the AP Ethernet port.



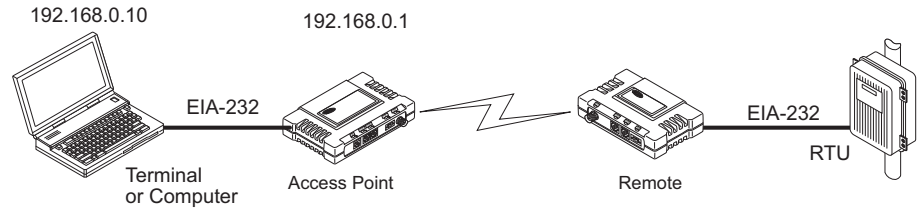
**Figure 5-3. Co-located Endpoint Device and AP**

**Table 5-3. IP-to-Remote Serial Application Configuration**

MDS entraNET Radio Location	Menu Item	Setting
AP (COM2)	Remote ID	1155883
	COM Port	COM2
	Mode	RSG COM2 Handler
	Radio IP Port	30066
Remote radio (COM2)	Mode	COM2 in transparent data mode
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4
	Intergap	TX data only

## 5.4 Point-to-Point, Serial-to-Serial Application Example

Once the transceivers are configured and the changes have been executed, they begin processing any data presented at the COM ports. Data presented at the AP COM port is packetized and sent over the air using a proprietary protocol to the Remote. Upon receiving the packet, the Remote sends the data from its COM port. Likewise, data presented at the Remote COM port is packetized, sent to the AP, stripped, and sent from the AP COM port. Note that this configuration does *not* use multicast addressing.



**Figure 5-4. Point-to-Point Serial-to-Serial Application Diagram**

Use the Serial Configuration Wizard (*Local Serial Configuration* menu) to make the settings listed in the table below. Following the table are step-by-step screen images of the Wizard.

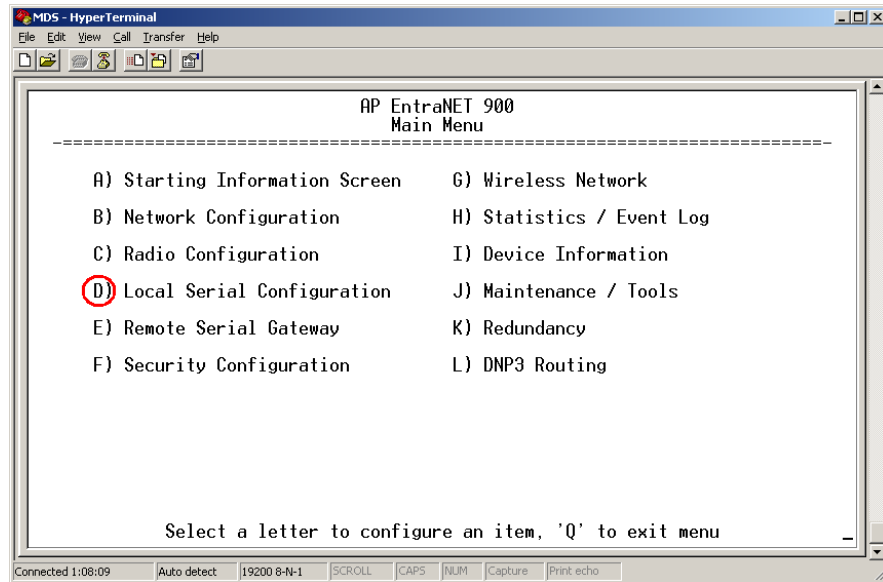
**Table 5-4. Point-to-Point Serial-to-Serial Configuration**

MDS entraNET radio Location	Menu Item	Setting
AP (COM2)	Port Status	Enabled
	Mode	Serial-to-Serial
	Remote UnitID	1155999 (example)
	Rem. COM Port	COM2
	Baud Rate	19200
	Byte Format	8N1
	Buffer Size	256 Bytes
	Inter-Packet Delay	4
Remote radio (COM2)	Mode	Data
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4

### 5.4.1 Step-by-step Instructions for Configuring a Point-to-Point Serial Connection

1. Connect a powered AP radio to a PC.
2. At the PC, open a connection with the Access Point radio using a terminal, Telnet, or Web browser session.
3. Press G to display the Main Menu.

4. From the Main Menu, press D to select *Local Serial Configuration*.

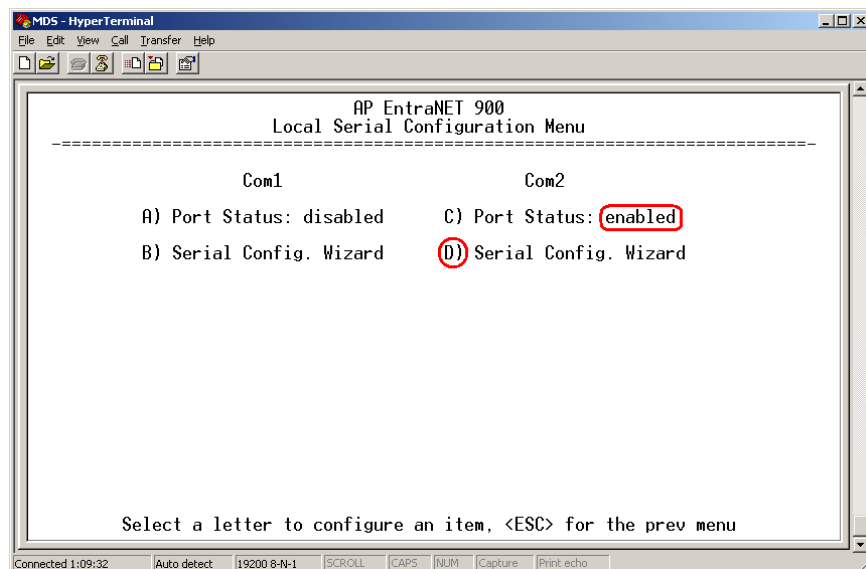


**Figure 5-5. Main Menu**

5. The *Local Serial Configuration* menu displays the status of the AP COM1 and COM2 ports (enabled or disabled). Set the COM2 port to “enabled”.

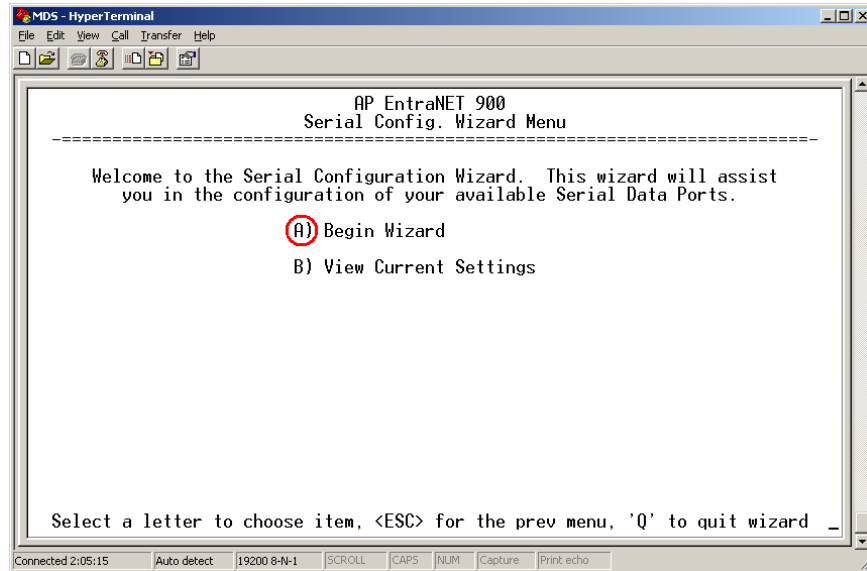
Press C to select COM2, then press **SPACE** to toggle between “enabled” and “disabled”. Press **ENTER** when “enabled” is displayed to select it.

Then press D to continue.



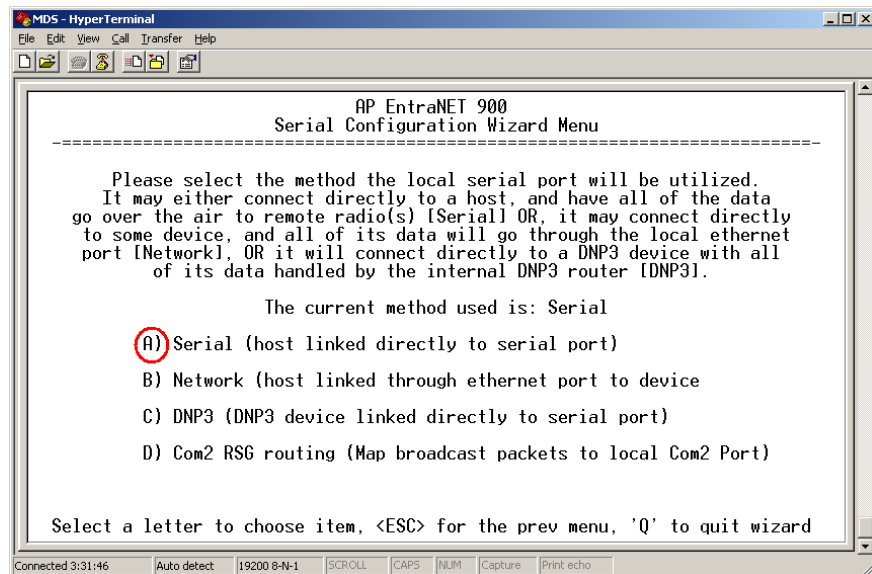
**Figure 5-6. Port Configuration Setting**

6. Press A to start the Serial Configuration Wizard.



**Figure 5-7. Begin the Serial Configuration Wizard**

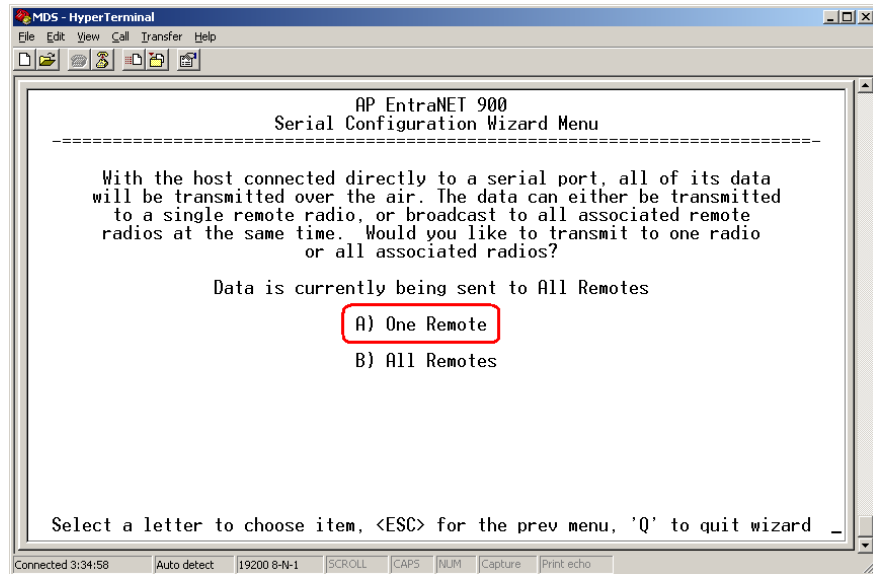
7. The first screen of the Serial Configuration Wizard prompts for the connection type. Press A to select “Serial”.



**Figure 5-8. Connection Type Selection Screen**

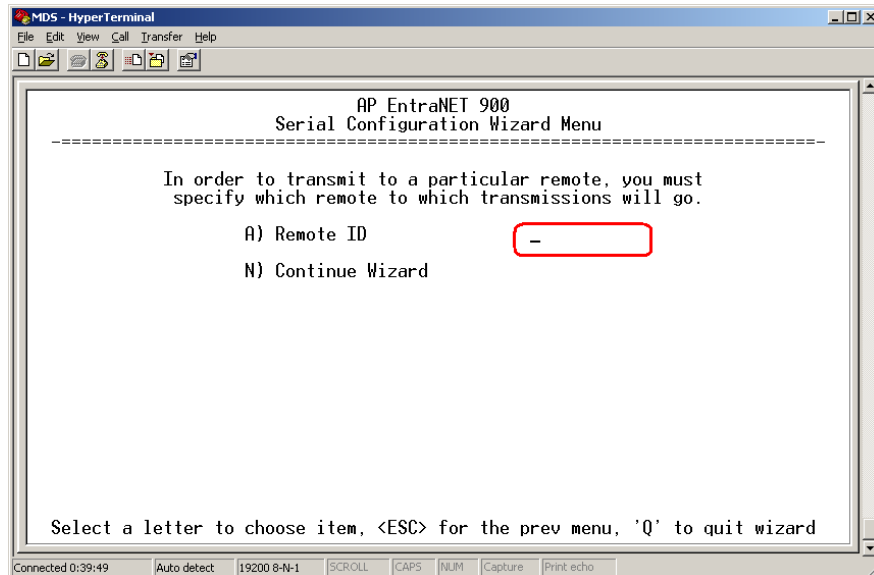


8. The Wizard displays a prompt to select a point-to-point or point-to-multipoint connection. Press A to select “One Remote” (point-to-point).



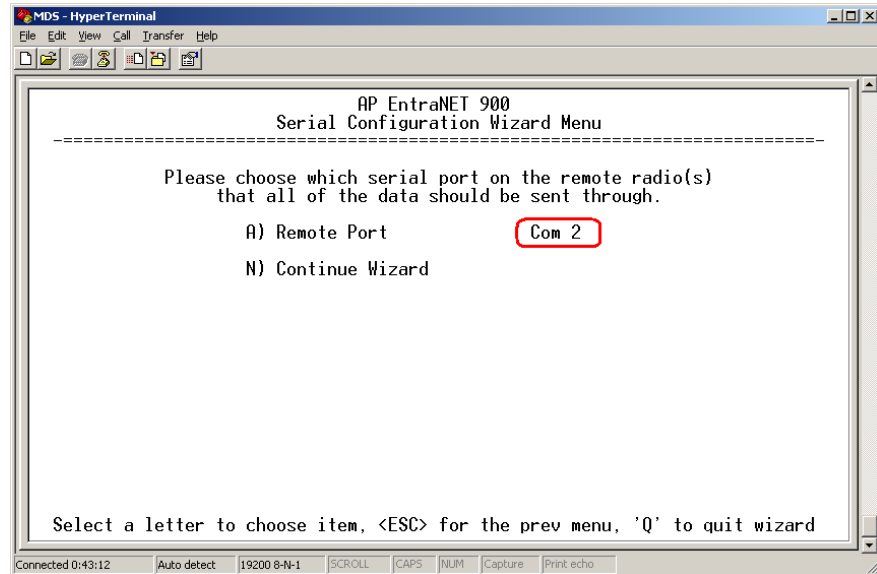
**Figure 5-9. Point-to-Point Selection**

9. The Wizard displays a prompt for the Unit ID of the single Remote radio. Press A to set the Remote ID (generally the last four digits of the Remote serial number). Type the Unit ID of the Remote radio. Press **ENTER** to accept the Unit ID. Then press N to continue.



**Figure 5-10. Set Remote Unit ID**

10. The next screen prompts for the input serial data port. Press A and then press **[SPACE]** to toggle to COM2. Press **[ENTER]** to accept the displayed selection. Then press N to continue.

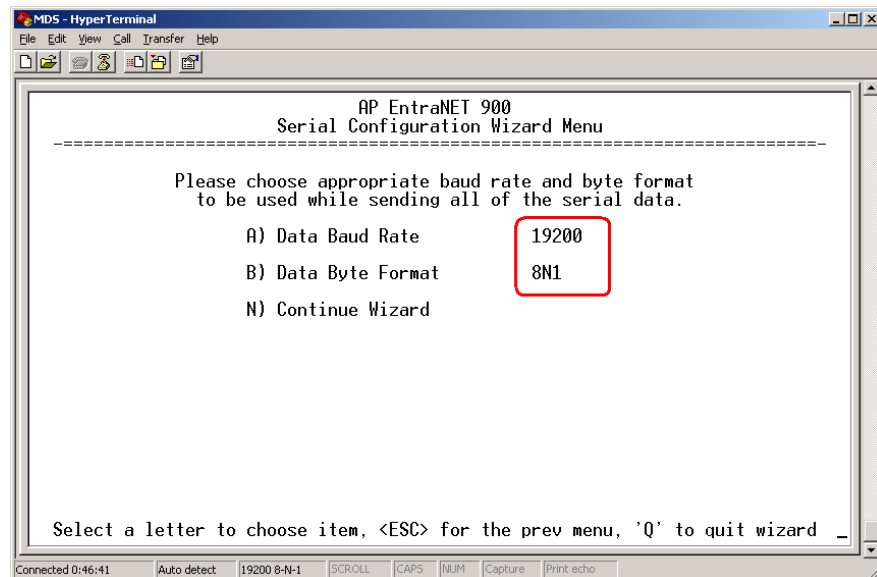


**Figure 5-11. Select Remote Port**

11. The next screen prompts for the baud rate and byte format.

Press A to set the Data Baud Rate. Press **[SPACE]** to cycle through the baud rate options until "19200" is displayed. Press **[ENTER]** to accept the Data Baud Rate.

Press B to set the Data Byte Format. Press **[SPACE]** to cycle through the byte format options until "8N1" is displayed. Press **[ENTER]** to accept the Data Byte Format. Then press N to continue.

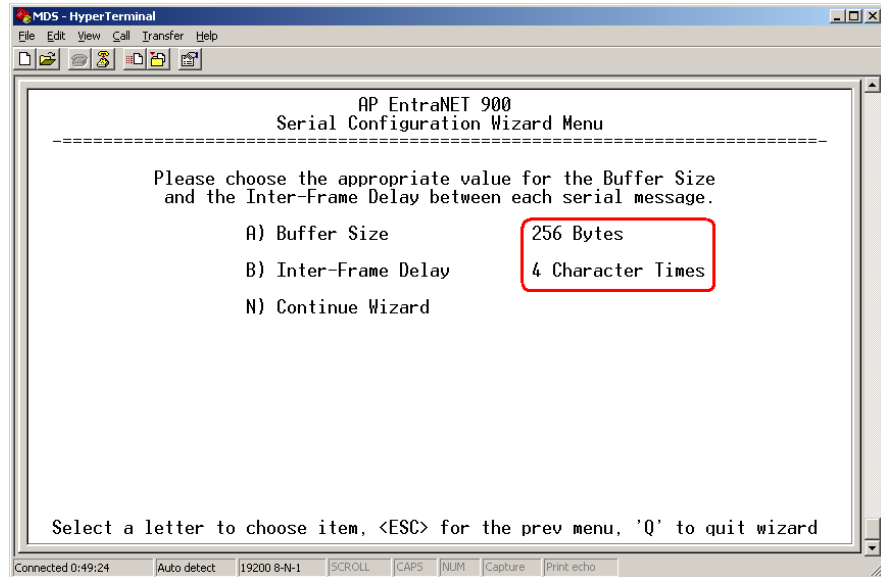


**Figure 5-12. Set Data Baud Rate and Data Byte Format**

12. The next screen prompts for the data buffer size and inter-packet frame delay.

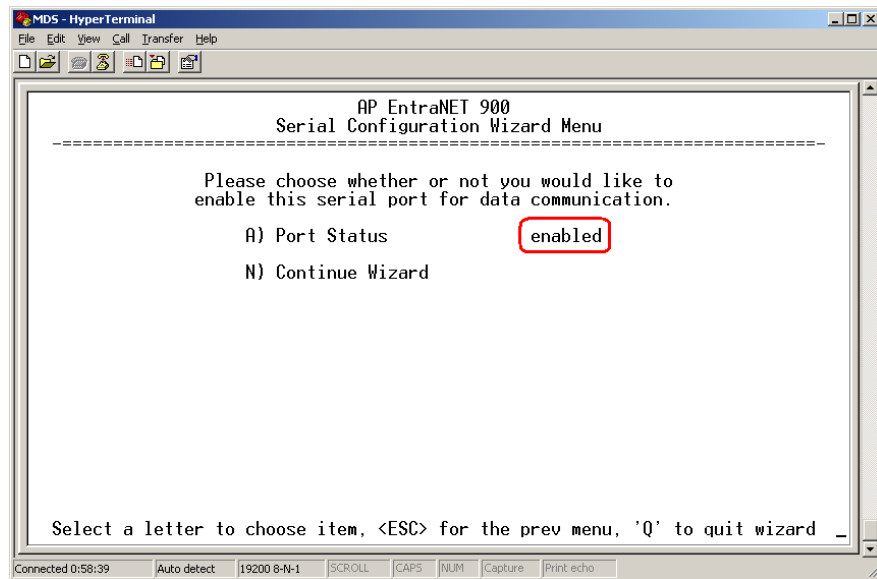
Press A to select Buffer Size. Press **[SPACE]** to cycle through the buffer size options until “256” is displayed. Press **[ENTER]** to accept the Buffer Size.

Press B to select Inter Frame Delay. Press **[SPACE]** to cycle through the options until “4 Character Times” is displayed. Press **[ENTER]** to accept the Inter Frame Delay. Then press N to continue.



**Figure 5-13. Set Buffer Size and Inter Frame Delay**

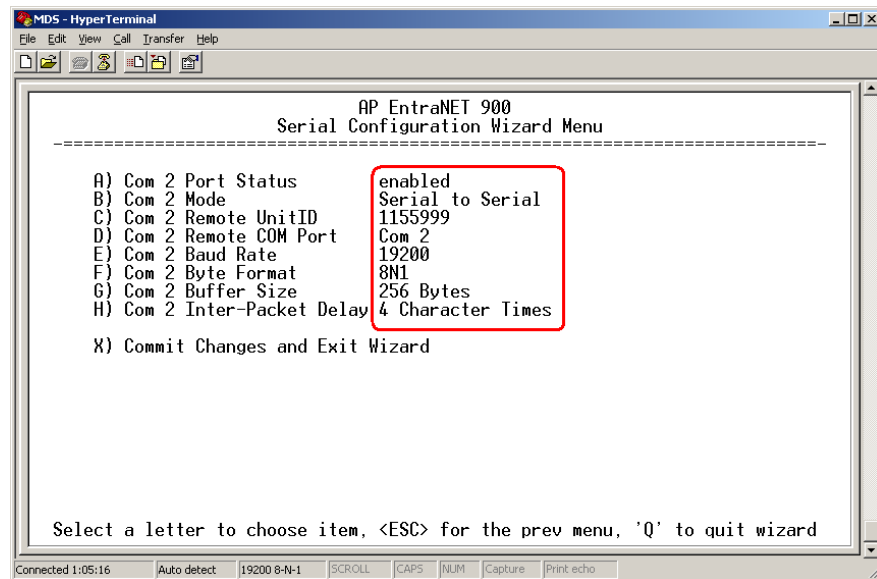
13. The next screen prompts for the Port Status. Press A to select Port Status. Press **[SPACE]** to toggle between “enabled” and “disabled”. Press **[ENTER]** when “enabled” is displayed. Then press N to continue.



**Figure 5-14. Enable Port**

14. The final screen displays all the previous settings for your review. The settings should be:

- COM2 Port Status: Enabled
- COM2 Mode: Serial to Serial
- COM2 Remote Unit ID: [Unit ID displayed]
- COM2 Remote COM Port: COM2
- COM2 Baud Rate: 19200
- COM2 Byte Format: 8N1
- COM2 Buffer Size: 256 Bytes
- COM2 Inter Packet Delay: 4 Character lines

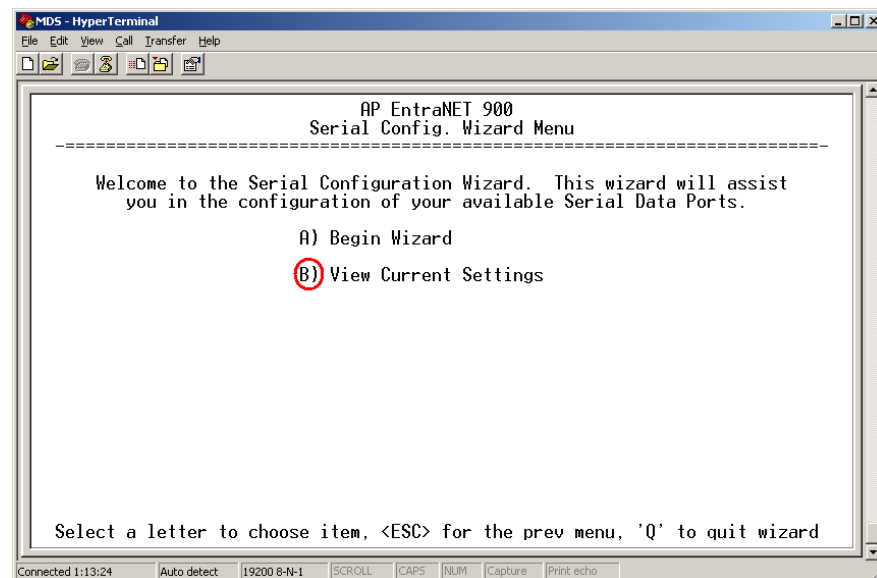


**Figure 5-15. Final Configuration Settings Display**

If the settings shown on screen match the ones listed above, press X to commit the changes and exit the Serial Configuration Wizard.

If not, press the letter of the item to change, press **[SPACE]** to cycle through the choices, and then press **[ENTER]** to accept the displayed choice. Then press N as many times as necessary to return to the settings display. When all the entries are correct, press X to commit the changes and exit the Serial Configuration Wizard.

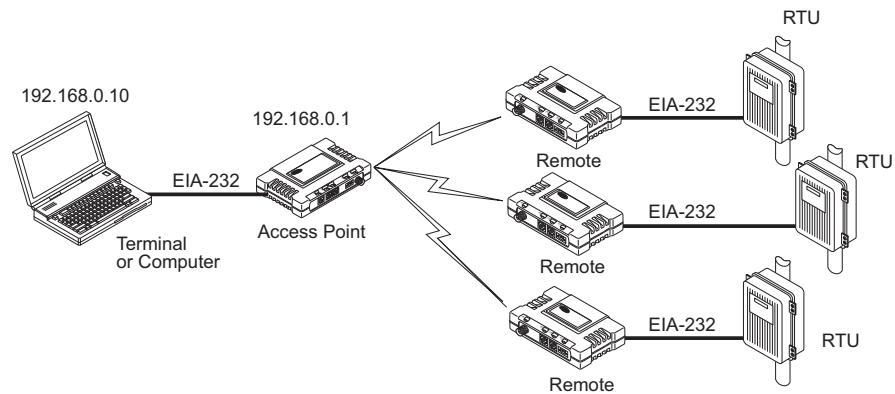
In the future, if you need to set up another radio or make changes, you can go directly to this screen by pressing B instead of A in step 5 above.



**Figure 5-16. View Current Settings**

## 5.5 Point-to-Multipoint, Serial-to-Serial Application Example

The operation and data flow for this mode is very similar to a point-to-point serial-to-serial application, except that it uses multicast addressing. The primary difference is that data presented at the AP COM port is packetized and sent to all of the Remotes. Upon receiving the packet from all of the Remotes, the data is stripped out of the packet and sent from the COM port. Likewise, data presented at any of the Remote COM ports is packetized, sent to the AP, stripped, and sent from the AP COM port.



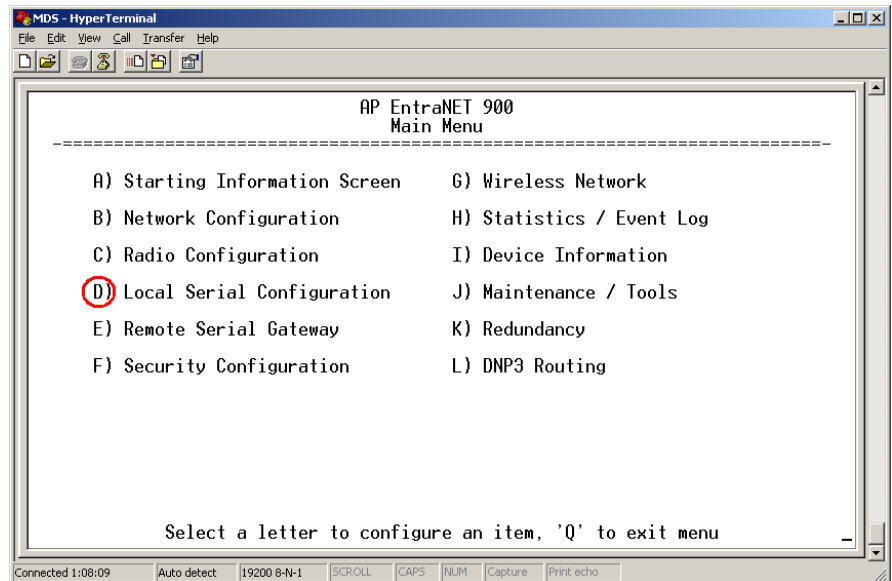
**Figure 5-17. Point-to-Multipoint Serial-to-Serial Diagram**

**Table 5-5. Point-to-Multipoint Serial-to-Serial Configuration**

MDS entraNET radio Location	Menu Item	Setting
AP (COM2)	Port Status	Enabled
	Mode	Serial-to-Serial
	Remote UnitID	Broadcast
	Remote COM port	COM2
	Baud Rate	19200
	Byte Format	8N1
	Buffer Size	256 Bytes
	Inter-Packet Delay	4
Remote radio (COM2)	Mode	Data
	Baud	19200
	Format	8N1
	Buffer	256
	DelayChars	4

## 5.5.1 Step-by-Step Instructions for Configuring a Point-to-Multipoint Serial Connection

1. Connect a powered AP radio to a PC.
2. At the PC, open a connection with the Access Point radio using a terminal, Telnet, or Web browser session.
3. Press G to display the Main Menu.
4. From the Main Menu, press D to select *Local Serial Configuration*.

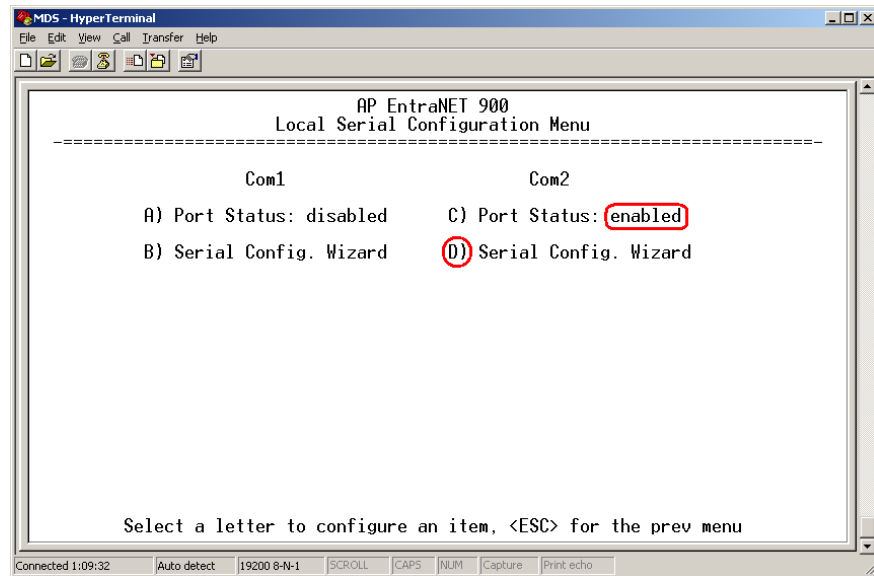


**Figure 5-18. Main Menu**

5. The *Local Serial Configuration* menu displays the status of the AP COM1 and COM2 ports (enabled or disabled). Set the COM2 port to “enabled”.

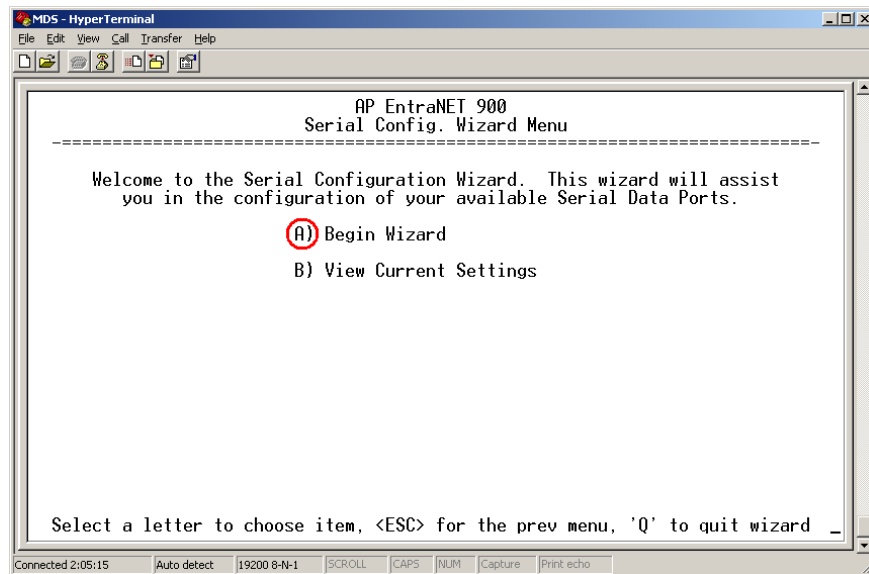
Press C to select COM2, then press **SPACE** to toggle between “enabled” and “disabled”. Press **ENTER** when “enabled” is displayed to select it.

Then press D to continue.



**Figure 5-19. Port Configuration Setting**

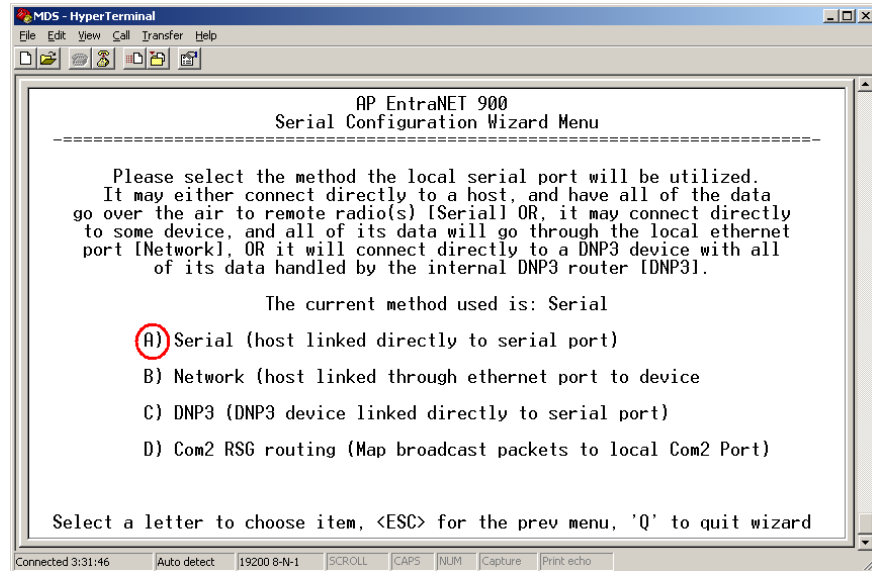
6. Press A to start the Serial Configuration Wizard.



**Figure 5-20. Begin the Serial Configuration Wizard**

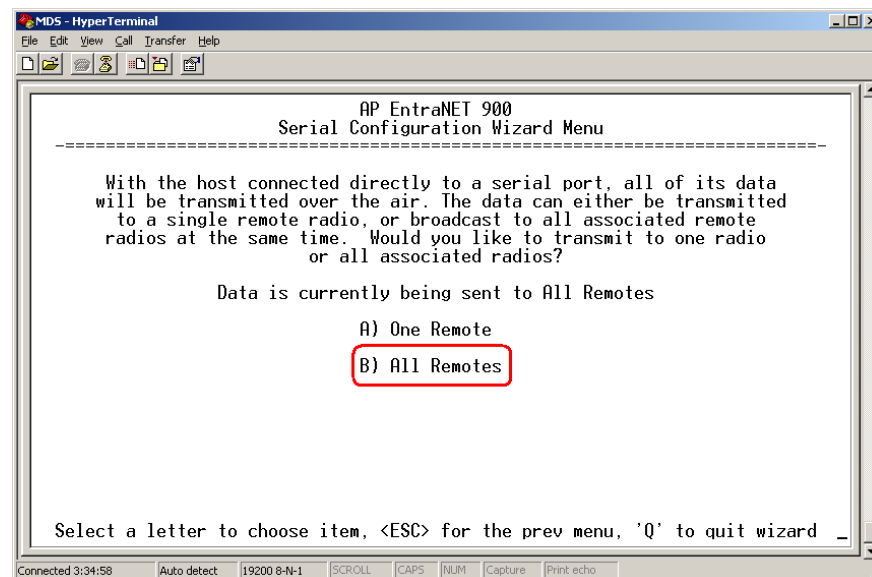


7. The first screen of the Serial Configuration Wizard prompts for the connection type. Press A to select “Serial”.



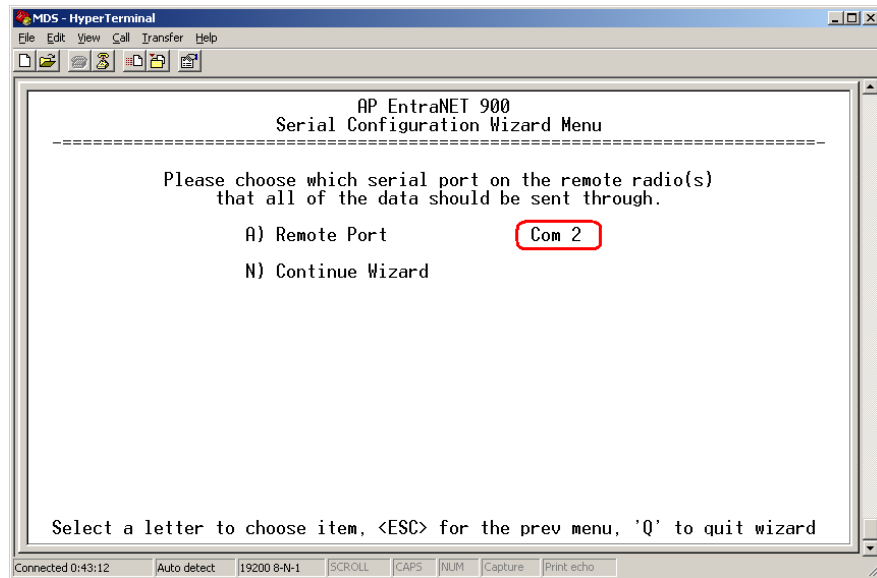
**Figure 5-21. Connection Type Selection Screen**

8. The Wizard displays a prompt to select a point-to-point or point-to-multipoint connection. Press B to select “All Remotes” (broadcast).



**Figure 5-22. Point-to-Multipoint Selection**

9. The next screen prompts for the input serial data port. Press A and then press **[SPACE]** to toggle to COM2. Press **[ENTER]** to accept the displayed selection. Then press N to continue.

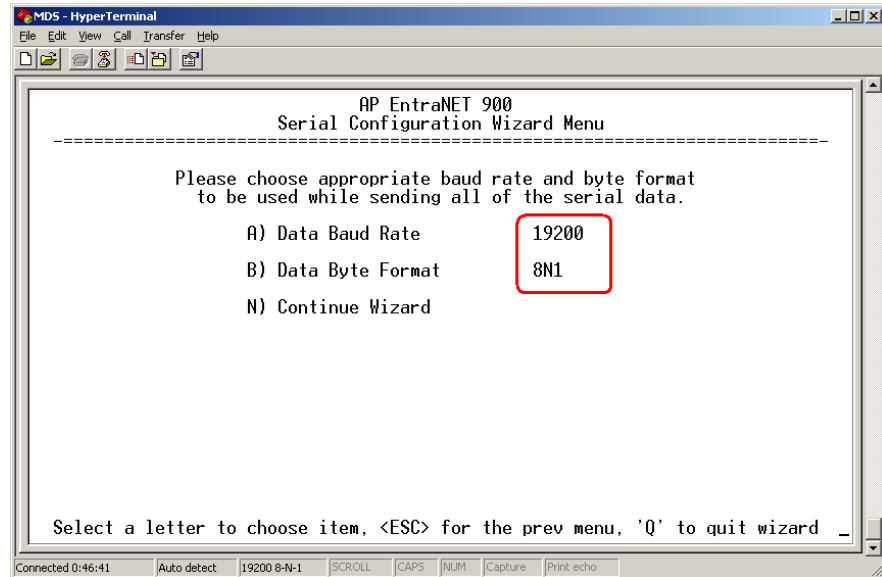


**Figure 5-23. Select Remote Port**

10. The next screen prompts for the baud rate and byte format.

Press A to set the Data Baud Rate. Press **[SPACE]** to cycle through the baud rate options until the baud rate for your equipment is displayed. In the example below, the baud rate is 19200. Press **[ENTER]** to accept the Data Baud Rate.

Press B to set the Data Byte Format. Press **[SPACE]** to cycle through the byte format options until “8N1” is displayed. Press **[ENTER]** to accept the Data Byte Format. Then press N to continue.

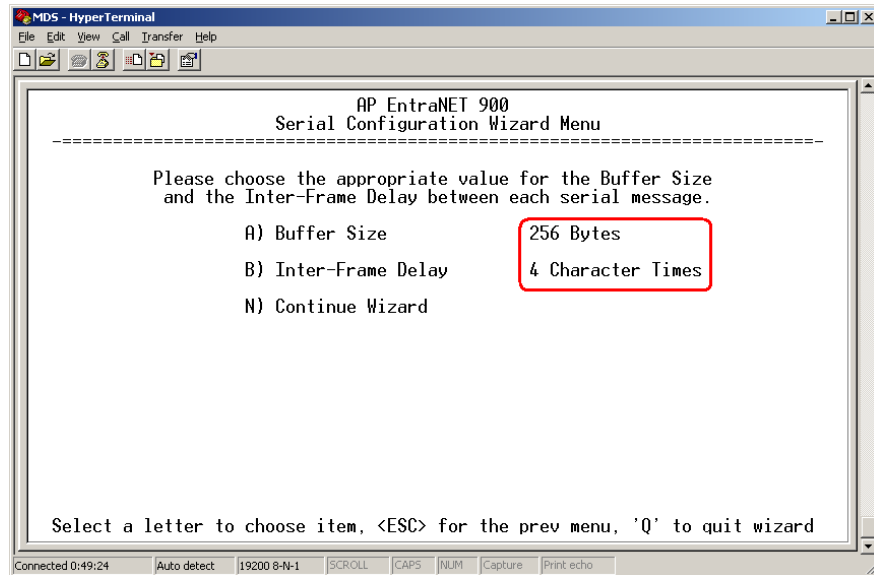


**Figure 5-24. Set Data Baud Rate and Data Byte Format**

11. The next screen prompts for the data buffer size and inter-packet frame delay.

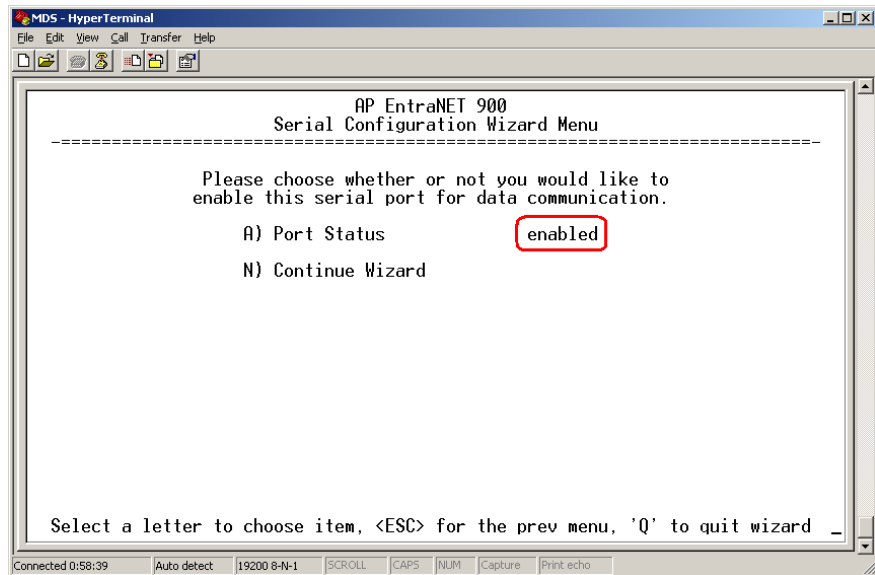
Press A to select Buffer Size. Press **[SPACE]** to cycle through the buffer size options until “256” is displayed. Press **[ENTER]** to accept the Buffer Size.

Press B to select Inter Frame Delay. Press **[SPACE]** to cycle through the options until “4 Character Times” is displayed. Press **[ENTER]** to accept the Inter Frame Delay. Then press N to continue.



**Figure 5-25. Set Buffer Size and Inter Frame Delay**

12. The next screen prompts for the Port Status. Press A to select Port Status. Press **[SPACE]** to toggle between “enabled” and “disabled”. Press **[ENTER]** when “enabled” is displayed. Then press N to continue.

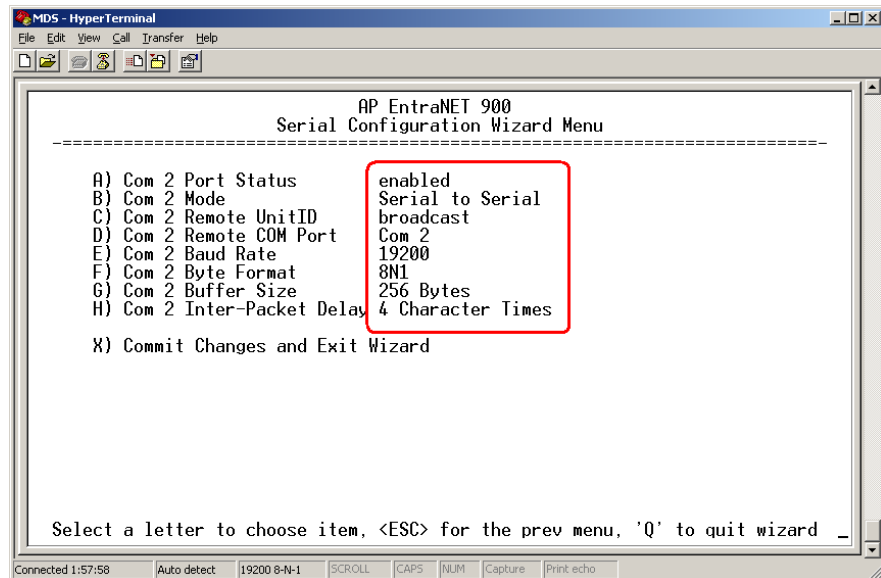


**Figure 5-26. Enable Port**

13. The final screen displays all the previous settings for your review. The settings should be:

- COM2 Port Status: Enabled
- COM2 Mode: Serial to Serial

- COM2 Remote Unit ID: broadcast
- COM2 Remote COM Port: COM2
- COM2 Baud Rate: 19200
- COM2 Byte Format: 8N1
- COM2 Buffer Size: 256 Bytes
- COM2 Inter Packet Delay: 4 Character lines

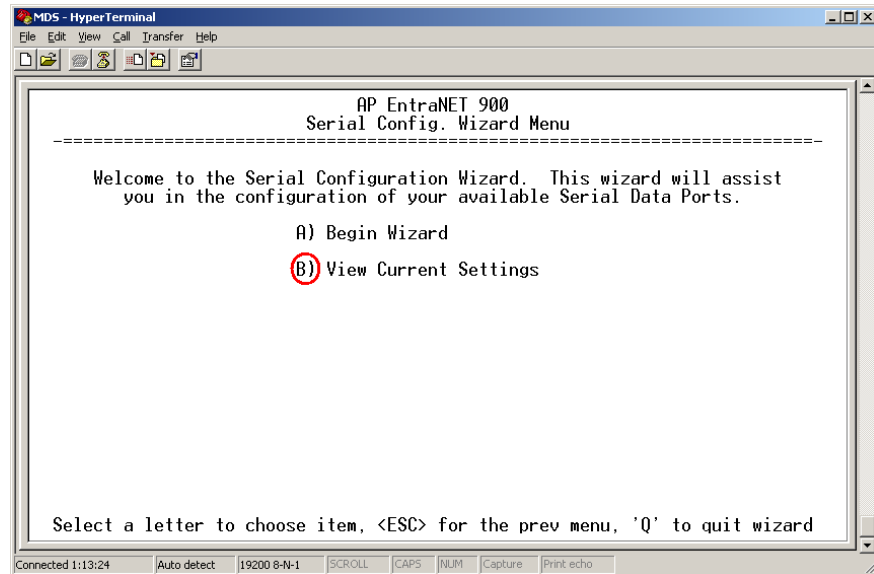


**Figure 5-27. Final Configuration Settings Display**

If the settings shown on screen match the ones listed above, press X to commit the changes and exit the Serial Configuration Wizard.

If not, press the letter of the item to change, press **SPACE** to cycle through the choices, or type the Unit ID if it is incorrect, then press **ENTER** to accept the displayed choice. Then press N as many times as necessary to return to the settings display. When all the entries are correct, press X to commit the changes and exit the Serial Configuration Wizard.

In the future, if you need to set up another radio or make changes, you can go directly to this screen by pressing B instead of A in step 5 above.



**Figure 5-28. View Current Settings**

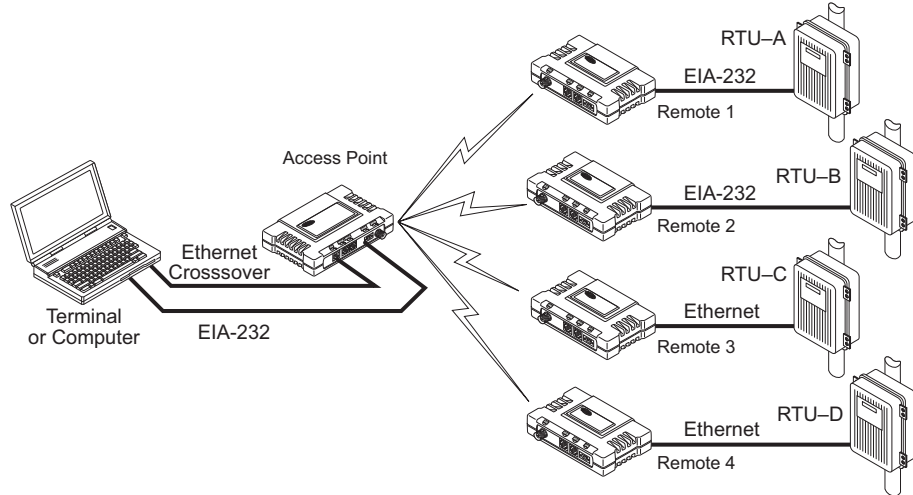
## 5.6 Mixed-Mode Application Example

In this configuration, the Host PC can use both TCP and serial-to-serial data paths to reach the endpoint devices. This can be helpful when a mixed collection of endpoint devices is present, where some endpoint devices operate over Ethernet while others are polled using a serial port. See [Figure 5-29 on Page 141](#) and [Table 5-6 on Page 141](#).

### 5.6.1 Operation and Data Flow

- Communicate with endpoint devices A and B by sending and receiving data from the AP COM2 port.
- Communicate with endpoint devices C and D by Telnetting to the IP address of each endpoint device.

- All communication paths can be used simultaneously.



**Figure 5-29. Mixed Modes Application Diagram**

**Table 5-6. Serial Port Application Configuration**

MDS entraNET radio Location	Menu Item	Setting
AP (COM2)	Port Status	Enabled
	Mode	Serial-to-Serial
	Remote UnitID	Broadcast
	Remote COM Port	COM2
	Baud Rate	19200
	Byte Format	8N1
	Buffer size	256 Bytes
	Inter-Packet Delay	4 Characters
Remote radios 1 and 2 (COM2)	Mode	Data
	Baud Rate	19200
	Data Format	8N1
	Buffer Size	256
	DelayChars	4
Remote radios 3 and 4 (ETH)	Mode	On

## 5.7 Configuring a Group Broadcast Session

The following procedure demonstrates how to configure a group broadcast session with Group ID 1:

1. Select **D** to enter the Remote Serial Wizard.

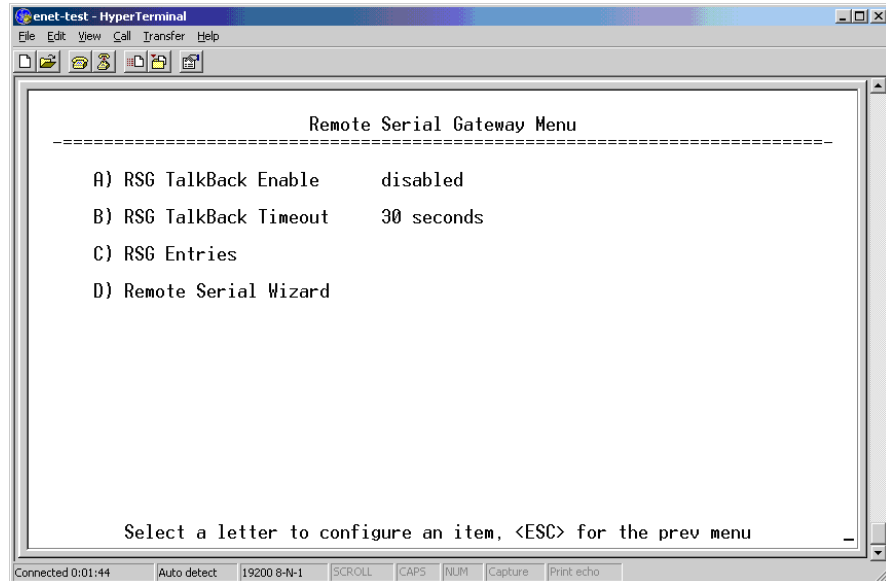


Figure 5-30. Remote Serial Wizard

2. Select **A** to choose TCP.

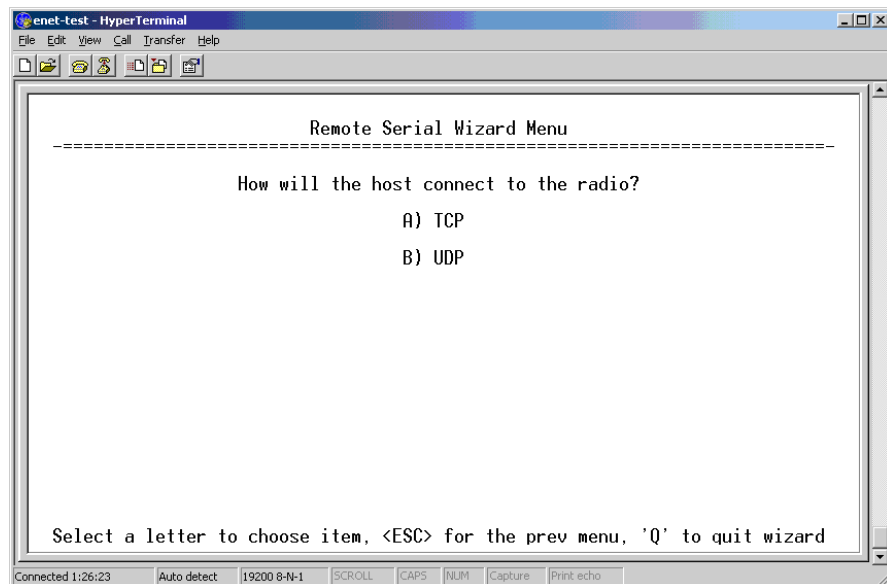
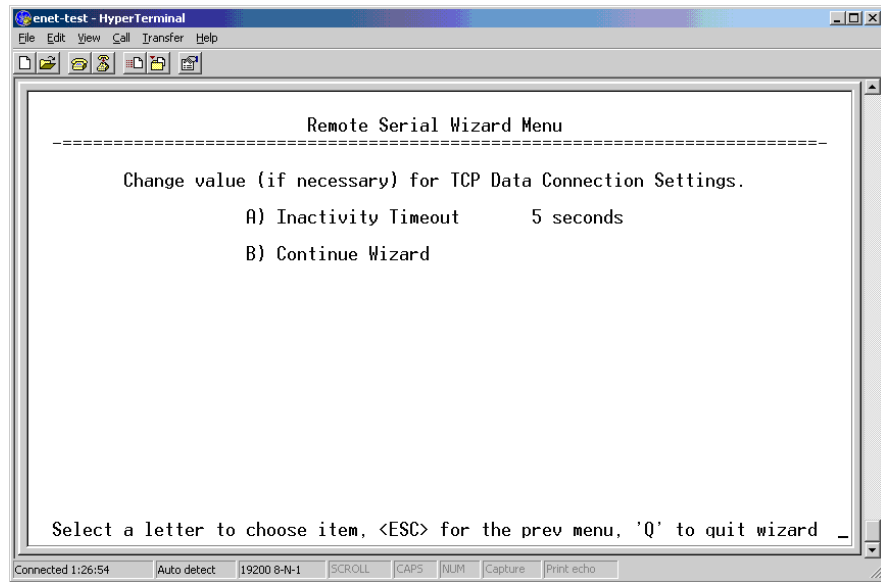


Figure 5-31. Select TCP Host Connection

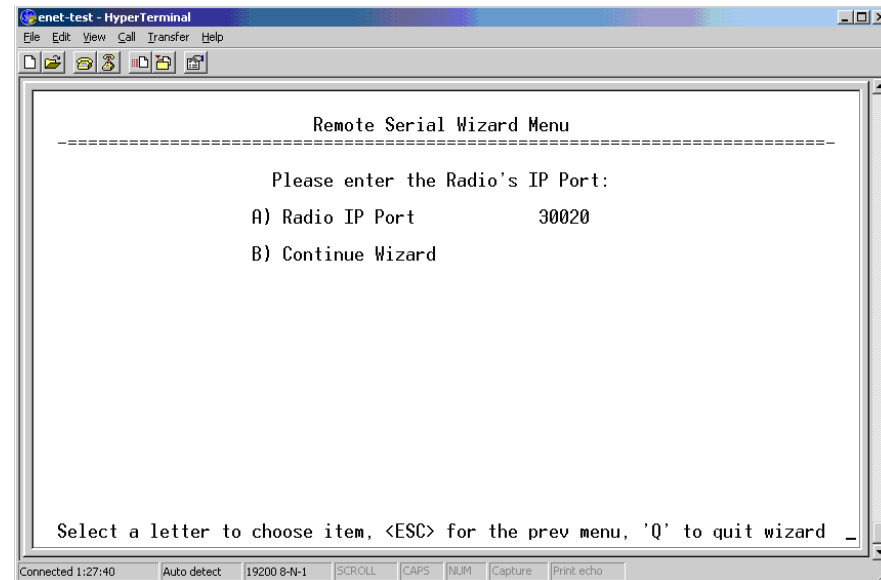


3. Select **B** to choose **Continue Wizard**.



**Figure 5-32. TCP Data Connection Settings**

4. Select **B** to choose **Continue Wizard**.



**Figure 5-33. IP Port Settings**

5. Select **C** to choose **Multicast to Some Remotes**.

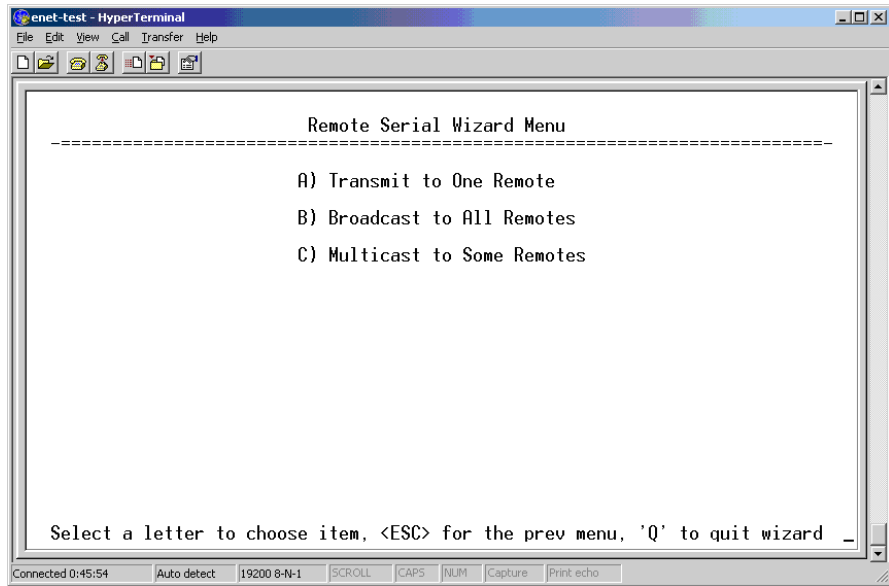


Figure 5-34. Multicast to Some Remotes

6. Select **B** to **Continue Wizard**.

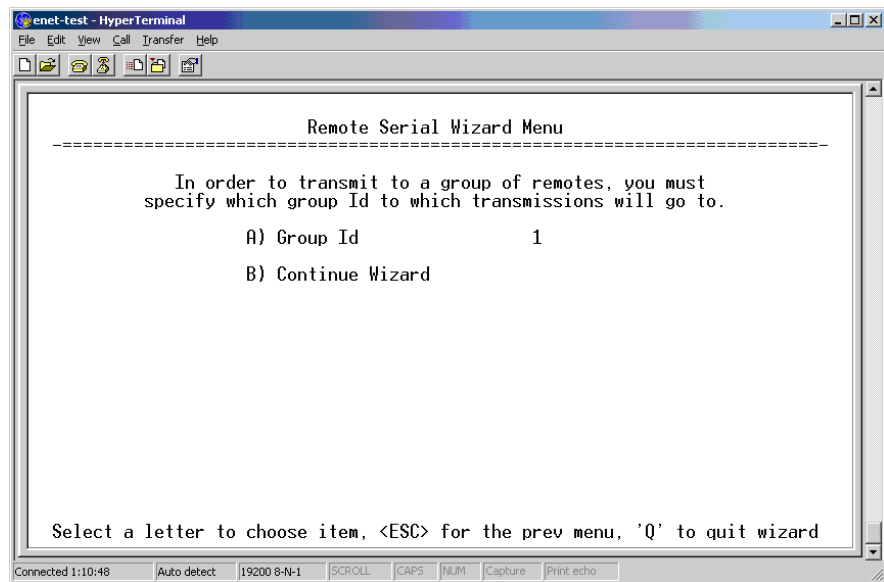
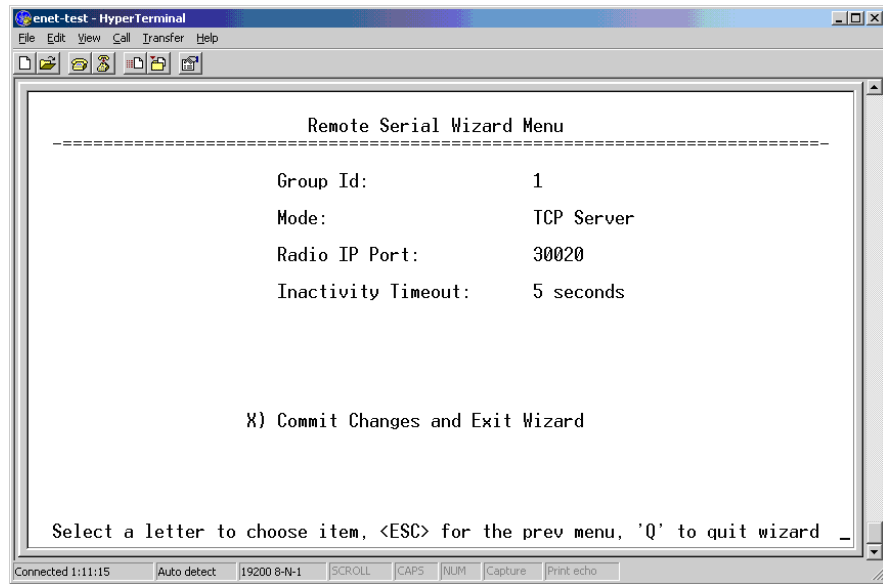


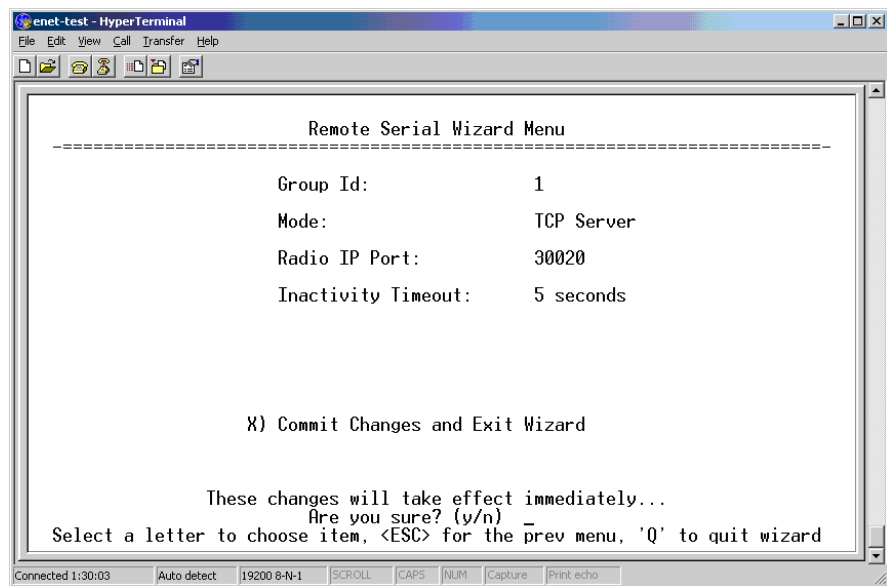
Figure 5-35. Group ID 1

7. Select **X** to **Commit Changes and Exit Wizard**.

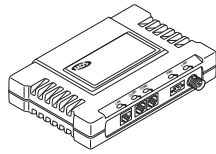


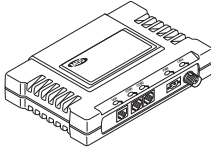
**Figure 5-36. Commit Changes and Exit Wizard**

8. Enter **Y** to confirm the changes.



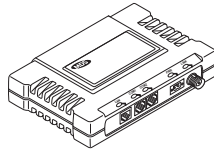
**Figure 5-37. Confirm Changes**





# 6 INSTALLATION

<b>6.1</b>	<b>INSTALLATION</b>	<b>149</b>
6.1.1	General Requirements .....	149
6.1.2	Site Selection .....	149
6.1.3	Conducting a Site Survey .....	150
	Terrain and Signal Strength .....	150
	A Word About Radio Interference.....	150
	Mounting Dimensions for Radios.....	152
6.1.4	Antenna and Feedline Selection .....	153
	Antennas .....	153
	Feedlines .....	154
<b>6.2</b>	<b>HOW MUCH OUTPUT POWER CAN BE USED? (U.S.A. and Canada, 900 MHz systems)</b>	<b>156</b>
6.2.1	Calculating System Gain .....	156
<b>6.3</b>	<b>HOW MUCH OUTPUT POWER CAN BE USED? (U.S.A. and Canada, 2400 MHz systems)</b>	<b>157</b>
6.3.1	Calculating System Gain .....	157
<b>6.4</b>	<b>HOW MUCH OUTPUT POWER CAN BE USED? (ETSI 2400 MHz systems)</b>	<b>158</b>
6.4.1	Calculating System Gain .....	159
<b>6.5</b>	<b>OPTIMIZING PERFORMANCE</b>	<b>160</b>
6.5.1	Principles of Wireless Network Operation .....	160
6.5.2	Aiming Directive Antennas for Maximum RSSI .....	162
	Procedure .....	162
6.5.3	Tips for Improving Data Throughput .....	163
	To Maximize Throughput of Data and Reduce Latency Time .....	163
	To Maximize Overall Data Performance .....	164

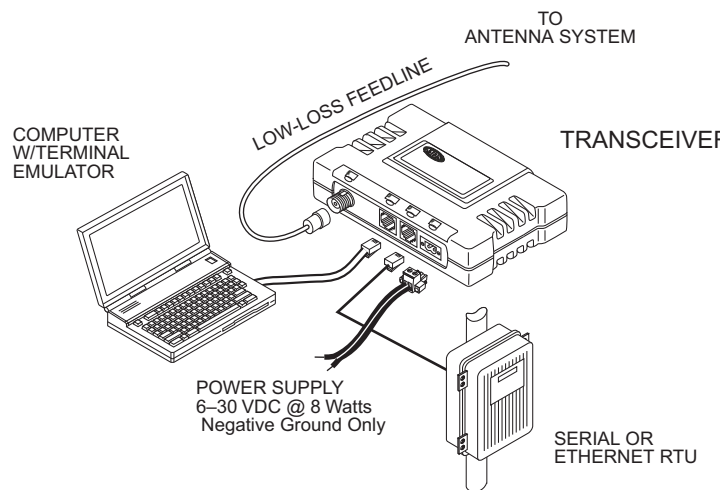


## 6.1 INSTALLATION PLANNING

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

### 6.1.1 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 6-1](#) shows a typical Remote installation.



**Figure 6-1. Typical Transceiver Installation**  
(Remote shown)

### 6.1.2 Site Selection

Suitable installation 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 affect system performance. If you are not familiar with the effects of terrain and other obstructions on radio transmission, the discussion below provides helpful information.

### 6.1.3 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 begins. This can be done with an on-the-air test (the 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 AP station site (one per system). Then visit the remote site(s) with a transceiver and a hand-held antenna. Connect a PC with a network adapter 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 AP station (shown by a lit LINK LED on the front panel) and measure the reported RSSI value using the **RADIO RSSI=** command. 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.

#### Terrain and Signal Strength

While the 900 MHz and 2400 MHz license-free bands offer 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 transceiver 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 differs from one system to another, a Received Signal Strength Indication (RSSI) of  $-100$  dBm or stronger provides acceptable performance in many systems. While the equipment works at lower-strength signals, signals stronger than  $-90$  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 transceiver COM1 port. See [“Aiming Directive Antennas for Maximum RSSI”](#) on Page 162 for details.

#### A Word About Radio Interference

The transceivers share the radio-frequency spectrum with other services and Part 15 (license-free) devices in the U.S.A. As such, near 100% error-free communications may not be achieved in a given location, and



some level of interference should be expected. However, 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 or 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, which 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 can 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.

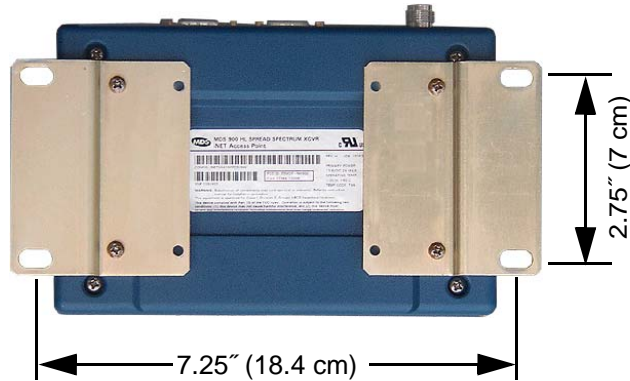
Another approach is to use a bandpass filter to attenuate all signals outside the desired band.

- Multiple AP radios can co-exist in proximity to each other with very minor interference. Each network address has a different hop pattern. You can achieve additional isolation by using separate directional antennas with as much vertical or horizontal separation as is practical.
- If constant interference is present in a particular frequency zone, it might be necessary to “skip” that zone from the hopping pattern. The radio includes built-in software to help you identify and remove blocked frequency zones from its hopping pattern. See [“Skip Zones Menu” on Page 53](#) for more information.
- If interference problems persist even after skipping some zones, try reducing the length of data streams. Groups of short data streams have a better chance of getting through interference than do long streams.
- Set the power output of all radios in a system for the lowest level necessary for reliable communications. This reduces the chance of causing unnecessary interference to nearby systems.

If you are not familiar with these interference-control techniques, contact your GE MDS Sales Representative or the GE MDS Technical Support Department for more information.

## Mounting Dimensions for Radios

Figure 6-2 shows the dimensions of the AP transceiver with mounting brackets attached. Figure 6-3 shows the same view for a Remote transceiver. When mounting entraNET transceivers, choose a location that provides easy access to the connectors on the end of the radio and an unobstructed view of the LED status indicators.



**Figure 6-2. AP Mounting Bracket Spacing**



**Figure 6-3. Remote Mounting Brackets Spacing**

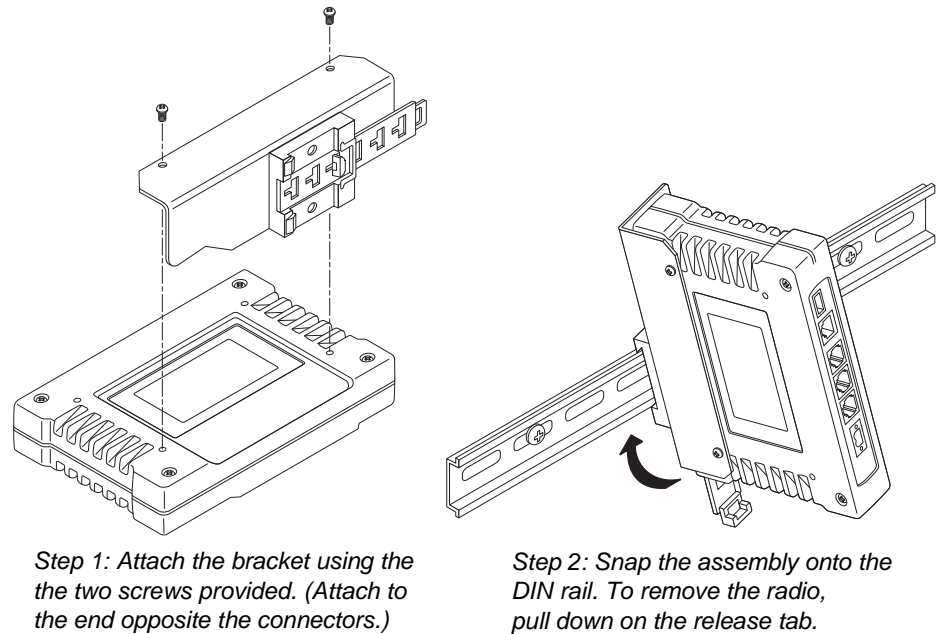
---

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

---

### ***DIN Rail Mounting Option***

The radio is available with an optional 35 mm DIN Rail Mounting Bracket (Part No. 03-4022A02). Equipment cabinets and racks of recent design often employ this type of mounting. A transceiver with a DIN bracket can be quickly installed or removed without tools. Figure 6-4 on Page 153 shows how the DIN rail bracket attaches to the back of the radio, and how the entire radio attaches to the mounting rail.



**Figure 6-4. DIN Rail Mounting Details for GE MDS Equipment**

## 6.1.4 Antenna and Feedline Selection

### Antennas

The equipment can be used with a number of antennas. The antenna type used depends on the physical size and layout of a system. Contact your GE MDS representative for specific recommendations on antenna types and hardware sources.

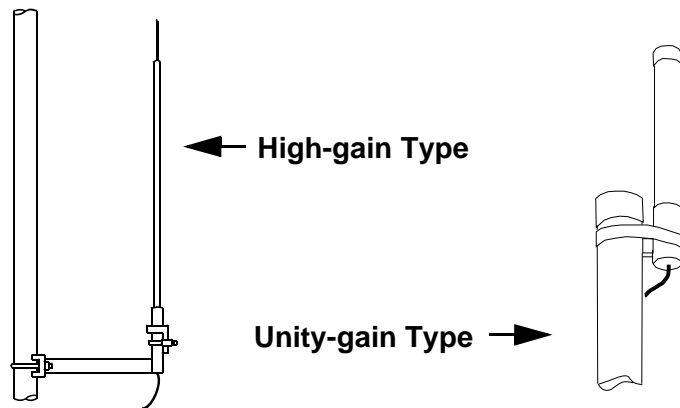
In general, an omnidirectional antenna ([Figure 6-5 on Page 154](#)) is used at the AP station site. This provides equal coverage to all of the remote sites.

---

**NOTE:** Antenna polarization is important. The wrong polarization causes a signal reduction of 20 dB or more. Most systems using a gain-type omnidirectional antenna at the AP station employ vertical polarization (elements oriented perpendicular to the horizon) of the signal; therefore, the Remote antenna(s) must also be vertically polarized.

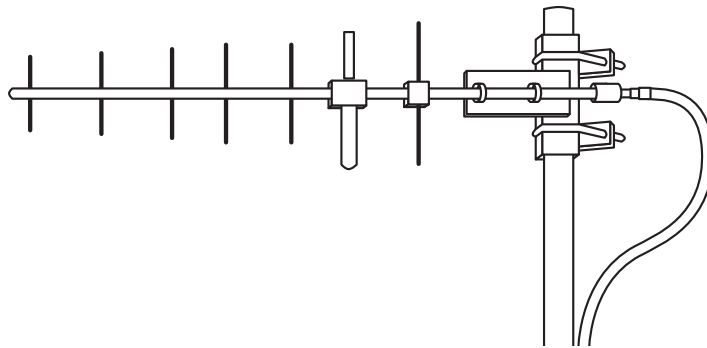
Horizontally polarized omnidirectional antennas are also available. Contact your GE MDS representative for details.

---



**Figure 6-5. Typical Omnidirectional Antennas**

At remote sites, and for radios in point-to-point LANs, a directional Yagi (Figure 6-6) antenna is generally recommended to minimize interference to and from other radio systems. Antennas are available from a number of manufacturers.



**Figure 6-6. Typical Yagi Antenna**  
*(mounted to mast)*

---

**NOTE:** It is essential that all antenna systems incorporate appropriate lightning protection. Information on lightning protection and grounding considerations can be obtained from the Polyphaser Corporation ([www.polyphaser.com](http://www.polyphaser.com)). The firm's Web site offers free engineering notes, as well as information on lightning protection devices.

---

### Feedlines

Carefully consider the choice of feedline used with the antenna. Poor-quality coaxial cables should be avoided, as they degrade both transmission and reception. Keep the cable as short as possible to minimize signal loss.

For 900 MHz systems with cable runs of less than 20 ft/6m, an inexpensive cable type such as Type RG-8A/U may be acceptable. For longer runs, or for 2400 MHz systems, GE MDS recommends using a low-loss cable type such as Andrew Corp. HELIAX® cable.

The choice of cable depends on the required length, cost considerations, and the amount of signal loss you can tolerate. [Table 6-1](#) lists several types of popular feedlines and indicates the signal losses (in dB) that result when using various lengths of cable at 900 MHz. [Table 6-2](#) shows the same data for 2400 MHz systems.

**Table 6-1. 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)
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

**Table 6-2. Length vs. Loss in Coaxial Cables at 2400 MHz**

Cable Type	10 Feet (3.05 m)	50 Feet (15.24 m)	100 Feet (30.48 m)	500 Feet (152.4 m)
LMR-400	0.70 dB	3.50 dB	6.61 dB	Unacceptable Loss
1/2 inch HELIAX	0.35 dB	1.73 dB	3.46 dB	17.3 dB
7/8 inch HELIAX	0.20 dB	0.99 dB	1.97 dB	9.85 dB
1-1/4 inch HELIAX	0.15 dB	0.73 dB	1.45 dB	7.50 dB
1-5/8 inch HELIAX	0.13 dB	0.63 dB	1.25 dB	6.25 dB

Maintaining Compliance at 900 MHz  
(U.S.A. and Canada Only)

[Table 6-3](#) outlines the minimum lengths of RG-214 coaxial cable that must be used with common GE MDS omnidirectional antennas **to maintain compliance with the FCC and IC maximum limit of +36 dBm** for license-free 900 MHz systems.

**Table 6-3. Minimum Feedline Length versus Antenna Gain**  
(RG-214 coaxial cable)

Antenna Gain (dBd)	Antenna Gain (dBi)	Minimum Feedline Length (Loss in dB)	Power Level at Minimum Length
Unity (0 dB)	2.15 dBi	3 meters (1.0 dB)	+31.15 dBi
3 dBd	5.15 dBi	3 meters (1.0 dB)	+34.15 dBi
5 dBd	7.15 dBi	3.1 meters (1.2 dB)	+35.95 dBi

## 6.2 HOW MUCH OUTPUT POWER CAN BE USED?

*(U.S.A. and Canada, 900 MHz systems)*

900 MHz transceivers are normally configured from the factory for +30 dBm (1 W) RF power output. This is the maximum transmitter output power allowed under FCC and Industry Canada 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 regions where ETSI standards apply, the maximum allowable RF output is generally limited to 100 mW (+20 dBm) on 2400 MHz. License-free operation on 900 MHz is not permitted. For more information, see [HOW MUCH OUTPUT POWER CAN BE USED? \(ETSI 2400 MHz systems\)](#) on Page 158.

---

### 6.2.1 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 10 dBi, and the feedline loss is 2 dB, the antenna system gain is 8 dB.
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, reduce the transmit power accordingly using the radio menu system (**Main Menu>Radio Configuration>RF Output Power Setpoint**), or introduce additional feedline loss. The EIRP of the antenna system should never exceed 36 dBi.

For convenience, [Table 6-4 on Page 157](#) 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 of 30 dBm (1 W).

**Table 6-4. Antenna System Gain versus Power Output Setting**  
(U.S.A. and Canada only)

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (in dBm)	EIRP (in dBm)
6 (or less)	30	36
8	28	36
10	26	36
12	24	36
14	22	36
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 6-1 on Page 155](#).

To convert dBm to Watts, refer to the chart shown on Page 193.

## 6.3 HOW MUCH OUTPUT POWER CAN BE USED?

(U.S.A. and Canada, 2400 MHz systems)

Non-ETSI 2400 MHz transceivers are normally supplied from the factory set for +27 dBm (0.5 Watt) RF power output; this is the maximum transmitter output power allowed under FCC and Industry Canada rules. The power must be **decreased** from this level if the antenna system gain exceeds 0 dBi. The allowable level depends on the antenna gain, feedline loss, and the transmitter output power setting.

---

**NOTE:** In regions where ETSI requirements apply, the maximum allowable RF output is generally limited to 100 mW (+20 dBm) on 2400 MHz. License-free operation on 900 MHz is not permitted. For more information, see [HOW MUCH OUTPUT POWER CAN BE USED? \(ETSI 2400 MHz systems\)](#) on Page 158.

---

### 6.3.1 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 10 dBi, and the feedline loss is 2 dB, the antenna system gain is 8 dB.

2. Subtract the antenna system gain from 27 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 19 dBm.
3. If the maximum transmitter power allowed is less than 27 dBm, reduce the transmit power accordingly using the radio menu system (**Main Menu>Radio Configuration>RF Output Power Setpoint**), or introduce additional feedline loss. The EIRP of the antenna system should never exceed 27 dBi.

For convenience, [Table 6-5](#) lists several antenna system gains, and shows the maximum allowable power setting. Note that a gain of 0 dB entitles you to operate the radio at the full power output of 27 dBm (0.5 W). To convert dBm to Watts, refer to [Table 8-4 on Page 193](#).

**Table 6-5. Antenna System Gain versus Power Output Setting**  
(U.S.A. and Canada only)

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (in dBm)	EIRP (in dBm)
0	27	27
5	22	27
7	20	27
9	18	27
12	15	27
15	12	27

\* 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 6-1 on Page 155](#).

## 6.4 HOW MUCH OUTPUT POWER CAN BE USED?

*(ETSI 2400 MHz systems)*

In regions where ETSI requirements apply, 2400 MHz transceivers are supplied from the factory with a +20 dBm (100 mW) RF power setting. This is the maximum EIRP transmitter output power allowed under ETSI standards. The power must be **decreased** from this level if the antenna system gain exceeds 0 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.





**NOTE:** Some EU countries mandate lower power outputs and frequency limitations from those referenced here. For example, in France, the transceiver may only be operated in band C (2.4528-2.4782 GHz) at a power level of 10 dBm. Be sure to check the requirements for your region before placing the transmitter on the air.

### 6.4.1 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 10 dBi, and the feedline loss is 2 dB, the antenna system gain is 8 dB.
2. Subtract the antenna system gain from 20 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 12 dBm.
3. If the maximum transmitter power allowed is less than 20 dBm, reduce the transmit power accordingly using the radio menu system (**Main Menu>Radio Configuration>RF Output Power Setpoint**), or introduce additional feedline loss. The EIRP of the antenna system should never exceed 20 dBi.

For convenience, [Table 6-6](#) lists several antenna system gains and shows the maximum allowable power setting of the radio. Note that a gain of 0 dB or less entitles you to operate the radio at the full power output of +20 dBm (100 mW). To convert dBm to Watts, refer to [Table 8-4 on Page 193](#).

**Table 6-6. Antenna System Gain versus Power Output Setting**  
(for ETSI compliance)

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (in dBm)	EIRP (in dBi)
0 (or less)	20	20
3	17	20
6	14	20
9	11	20
10	10	20

\* 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 6-2 on Page 155](#).

## 6.5 OPTIMIZING PERFORMANCE

After the basic operation of the radio has been established, you might wish to optimize network performance using some of the suggestions in this section. The effectiveness of these techniques varies with the design of your system and the format of the data being sent.

There are two major areas for possible improvement—the radio and the data network. The following sections provide you with a variety of items to check and, on many occasions, ways to correct or improve their performance.

### 6.5.1 Principles of Wireless Network Operation

The following points are of value in dealing with the networking aspects of the transceiver.

1. The AP serves as a network bridge:
  - The transceiver goes through a “listening and learning” period at start-up before it sends any packets over either of its ports. This lasts about 10 sec after the CPU operating system finishes its startup cycle.
  - The bridge code in the transceiver operates and makes decisions about packet forwarding just like any other bridge. The bridge code builds a list of source MAC addresses that it has seen on each of its ports. There are a few general rules that the transceiver follows when a packet is received on any port:
    - If the destination address is a multicast or broadcast address, forward the packet to all other ports.
    - If the destination address is not known, forward the packet to all other ports.
    - If the destination address is known, forward the packet to the port that the destination is known to be on (usually the RF port).
  - The bridge code uses Spanning Tree Protocol (STP) to prevent loops from being created when connecting bridges in parallel. For example, connecting two Remotes to the same wired LAN could create a loop if STP was not used. Every bridge running STP sends out Bridge Protocol Data Units (BPDUs) at regular intervals so that the spanning tree can be built and maintained. BPDUs are 60-byte multicast Ethernet *frames*.
2. Throughput calculations must take into account all overhead:
  - Throughput over the air is affected by several factors, including: how compressible the data is, how efficiently the over-the-air bandwidth is used (which varies by packet size and dwell time), and the quality of the link.

- The number of bytes they can fit into a hop, depending on hop time, is:

**Table 6-1. Number of bytes per hop**

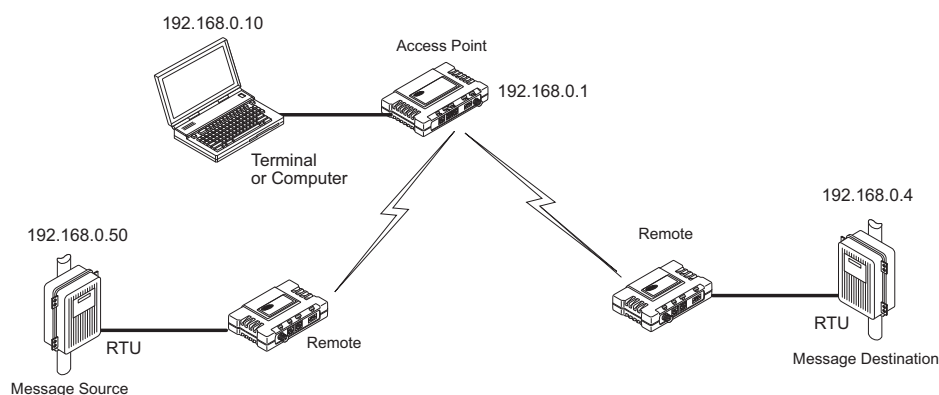
Hop time (MS)	FEC	Bytes/hop
7		45
7	FEC	11
14		139
14	FEC	59
28		324
28	FEC	151

Included in the byte count is 9 bytes of overhead per packet. So, at 7 ms without FEC, a 1000 byte packet requires 1009 bytes split into 45 bytes/hop, or 23 hops. 1026 bytes of data also requires 23 hops; however, a 1027-byte data packet requires 24 hops.

- If any transceiver in your network is connected to a large LAN, such as may be found in a large office complex, there might be undesired multicast or broadcast traffic over the air.

### 3. Station-to-Station Traffic

- When sending frames from one remote endpoint to another remote endpoint using an AP transceiver (see [Figure 6-7](#)), throughput is halved at best. This is because all frames must go through the AP. Therefore, in the previous 100 byte UDP example, the number of over-the-air bytes is 380 bytes (190 bytes times 2) if the frame must go station to station.



**Figure 6-7. Endpoint-to-Endpoint Communication Using an AP**

### 4. Interference has a direct correlation to throughput:

- Interference could be caused by any unnecessary traffic on the network from unrelated activities, or radio interference.

## 6.5.2 Aiming Directive Antennas for Maximum RSSI

The wireless 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  $-90$  dBm provide the basis for reliable communication that includes a 15 dB fade margin. As the distance between the AP 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 you can use to tell when the antenna is in a position that provides the optimum received signal.

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

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

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

### Procedure

1. Verify that the Remote is associated with an AP radio. Observe 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 **Radio Retries** and **No Ack** counts on the *Radio Packet Statistics Screen* ([Figure 3-45 on Page 81](#)). This information will be used later.
3. Clear the **Radio Statistics** history.
4. Read the RSSI level at the Remote (**RADIO RSSI=**).
5. Optimize the RSSI by slowly adjusting the direction of the antenna and watching for a peak in received signal strength. Get the RSSI indication several times after making each adjustment, so that the RSSI accurately reflects any change in the link signal strength. The higher the indication (less negative), the stronger the signal level (that is,  $-60$  is better than  $-70$ ).

6. View the **Radio Retries** and **No Ack** counts 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 **Radio Retries** and **No Ack** counts, the antenna might be aimed at an undesired signal source. Try a different antenna orientation.

### 6.5.3 Tips for Improving Data Throughput

Some suggestions are offered below for maximizing the throughput of the radio system. It is important to realize that an exact formula for every radio system cannot be given. Much depends on the number of radios contained in the radio system, the size of data strings being sent, the type of data being sent, zone quality (interference potential), and data speed. You should find several items here, however, that can be applied to your radio system.

#### To Maximize Throughput of Data and Reduce Latency Time

- *(AP only)* Increment the **Hop Time** to the maximum of 28 ms. This lowers the overhead, since it stays longer on a channel. The drawback is that if a particular channel becomes blocked, it will take longer to hop to another channel.  
(Main Menu>Radio Configuration>hop Time)
- Match the buffer sizes and hop times to accommodate the majority of message sizes. For example, a 7 ms hop time is best suited to short data bursts, such as in telemetry applications. A 28 ms hop time is better suited to large data strings, such as sending Web pages over the radio link.

The following table provides suggested settings for four different message sizes.

**Table 6-7. Hop Time Setting versus Message Size**

Hop Time (msec)	FEC Status*	Bytes per Packet
28	OFF	325
	ON	151
14	OFF	139
	ON	59
7	OFF	45
	ON	11

\* **FEC ON** is generally not recommended if optimal throughput is desired. The transceiver Repeat-Retry function is a more efficient means of ensuring message delivery.

---

**NOTE:** Reprogramming does not work over the air when the settings **Hop Time=7, FEC=On** and **Encryption=On** are used at the AP.

---

### To Maximize Overall Data Performance

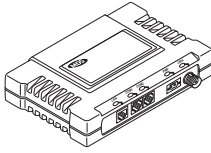
- Change the **Buffer Size** for serial ports to the maximum of 1500. Longer packets are sent over the air, reducing overhead. On the down side, if a packet is corrupted, it takes longer to retransmit.
- Use the *Packet Statistics Menu* to check **Packets Received by Zone**.

Counts should be evenly distributed across all zones. Block the zones at the AP that have poor performance.

(**Main Menu > Radio Configuration > Skip Zone Option**)

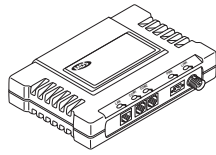
- Use the *Packet Statistics Menu* to check for errors, retries and dropped packets. Do the same with Ethernet traffic.

Note that with weak signals, interference, or hidden nodes, the optimal performance might be lower due to collisions and retries.



# 7 TROUBLESHOOTING AND RADIO TESTS

7.1 TROUBLESHOOTING	167
7.1.1 Interpreting the Front Panel LEDs .....	167
7.1.2 Troubleshooting Using the Embedded Management System ...	168
Serial Port and Remote Serial Statistics Menu .....	171
Diagnostic Tools .....	171
7.1.3 Using Logged Operation Events .....	172





## 7.1 TROUBLESHOOTING

Successful troubleshooting of a wireless system is not difficult, but requires a logical approach. It is best to begin troubleshooting at the AP radio, as the rest of the system depends on the AP for synchronization data. If the AP has problems, the operation of the entire wireless network is 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. The wireless aspect of the AP and the Remote radios to be connected must operate properly so data-layer traffic can function.

### **Radio Configuration**

There are over 50 parameters in the entraNET MS. With so many settings, a parameter might be incorrectly set, and then what was changed is forgotten.

To help you avoid these problems, we recommend creating an archive of the transceiver profile in a Configuration File when your installation is complete. This file can be reloaded into the transceiver to restore the radio to the factory defaults or to known working settings. For details on creating and archiving Configuration Files, see “[PING Utility Menu](#)” on Page 90.

### **GE MDS Assistance**

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

### **7.1.1 Interpreting the Front Panel LEDs**

An important set of troubleshooting tools are the LED status indicators on the front panel of the transceiver. They should be checked whenever a problem is suspected. [Table 2-2 on Page 26](#) describes the function of each status LED. [Table 7-1 on Page 168](#) provides suggestions for resolving common system difficulties using the LEDs, and [Table 7-3 on Page 169](#) provides other simple techniques.

**Table 7-1. Symptom-Based Troubleshooting Using LEDs**

Symptom	Possible Cause and Resolution
PWR LED does not turn on.	a. The voltage is too low, or is the wrong polarity. Check for the proper supply voltage at the power connector (6–30 Vdc). See <a href="#">Figure 2-4 on Page 20</a> for polarity details. b. This is a transient condition. Cycle the power and wait approximately 30 sec for the radio to restart. Recheck for normal operation.
LINK LED does not turn on.	a. The Remote network address does not match the desired AP. Verify that the system has a unique network address. b. The Remote is not yet associated with a transceiver having the same network address. Use the <b>RADIO</b> command to check the status of the process of associating the radio with the AP. 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). Also, check for the proper heading of the directional antennas as described in <a href="#">Aiming Directive Antennas for Maximum RSSI on Page 162</a> .
PWR LED is blinking.	The radio is reporting an alarm condition. View the current alarms and the Event Log. Correct the problem if possible ( <a href="#">see “Using Logged Operation Events” on Page 172</a> ). Blinking continues until the source of the alarm is corrected (for example, a valid IP address is entered, and so on).
LAN/ETH LED does not turn on.	a. Verify that the Ethernet cable is connected at both ends. b. Verify that the proper type of Ethernet cable (straight-through or crossover) is used. See <a href="#">Table 7-2</a> for the proper cable type.
COM1 or COM2 LED does not show traffic.	Check the configuration of the COM port and the remote serial gateway settings.

[Table 7-2](#) shows the proper type of Ethernet cable to use with the radio when connecting to external devices.

**Table 7-2. Proper Ethernet Cable Type**

Radio Type	Connected Device	Cable Type Required
AP	Hub or network switch	Straight-through
AP	PC	Crossover
Remote	PC	Straight-through
Remote	Hub or network switch	Select for the external device port

## 7.1.2 Troubleshooting Using the Embedded Management System

If following the suggestions in [Table 7-1](#) does not resolve the problem, there are additional tools and techniques that you can use. 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 7-3. Troubleshooting with the Embedded Management System**

Symptom	Possible Cause and Resolution
Remote does not associate	<ul style="list-style-type: none"> <li>a. Verify that the AP has a sufficiently large number in the “Max Remotes” parameter of the <i>Network Configuration Menu</i>.</li> <li>b. If “Approved Remotes” is enabled on the <i>Security Configuration Menu</i> (at the AP), verify that the correct serial number is listed in the Approved Remotes List.</li> <li>c. On the Remote, if “Restrict” is turned on in the APLIST command, verify that the AP is included in the list of Approved APs.</li> <li>d. Check for the proper heading of directional antennas as described in <a href="#">Aiming Directive Antennas for Maximum RSSI</a> on Page 162.</li> <li>e. The encryption mode is not set correctly in all radios on the network.</li> <li>f. If this occurs after upgrading firmware, disable encryption, then re-enter the encryption phrase using eight to 41 characters in all radio devices. Finally, re-enable encryption.</li> </ul>
Cannot access the <i>entraNET AP Menu</i> (through COM1)	<ul style="list-style-type: none"> <li>a. Check for secure cable connections. The serial data cable should be as short as possible, never exceeding 50 ft/15 m.</li> <li>b. If the radio is an AP, connect using a Telnet session or a Web browser.</li> <li>c. Disable the serial mode for COM1 <b>(Serial Gateway Configuration&gt;COM1 Serial Data Port&gt;Status&gt;Disabled)</b></li> </ul> <p>Or, if you know the radio data configuration, follow the numbered steps below:</p> <ol style="list-style-type: none"> <li>1. Connect to COM1 using a terminal set to VT100 and the port data baud rate.</li> <li>2. Enter + + + <input type="text" value="ENTER"/></li> <li>3. Change the terminal baud rate to match the transceiver console baud rate.</li> <li>4. Enter + + + <input type="text" value="ENTER"/></li> </ol>
Cannot access the Remote command interface	<ul style="list-style-type: none"> <li>a. Check for secure cable connections. Serial data cable should be as short as possible, never exceeding 50 ft (15 m).</li> <li>b. Connect to the AP menu and manage the Remote using the Serial Configuration menu. Check the configuration for COM1 or COM2, as applicable.</li> </ul>
Display on terminal or Telnet screen is garbled	Verify that the terminal or terminal emulator or Telnet application is set to VT100. Restart the terminal program.

**Table 7-3. Troubleshooting with the Embedded Management System (Continued)**

Symptom	Possible Cause and Resolution
Cannot pass IP data to the WAN.	<ol style="list-style-type: none"> <li>Verify the AP IP settings.</li> <li>Use the PING command to test communication with the AP and endpoints connected to Remote radios in the local radio system.</li> <li>If successful with the local PING, attempt to PING an IP radio attached to a radio.</li> <li>If successful with the LAN PINGS, try connecting to a known radio in the WAN.</li> </ol>
Wireless retry count is too high	<p>There may be Radio Frequency Interference (RFI).</p> <ol style="list-style-type: none"> <li>If omnidirectional antennas are used, consider changing to directional antennas. This often limits interference to and from other stations.</li> <li>Try skipping some zones where persistent interference is suspected, or packets per zone are disparate.</li> <li>The installation of a filter in the antenna feedline may be necessary. Consult GE MDS for further assistance.</li> </ol>
Password forgotten.	<ol style="list-style-type: none"> <li>Connect to the transceiver using a terminal through the COM1 port.</li> <li>Call GE MDS. Get a password-resetting Authorization Key.</li> <li>Enter the Authorization Key at the login prompt as a password.</li> </ol>

The following is a summary of how you can use several screens in the entraNET MS as diagnostic tools. For information on how to connect to the entraNET MS, see [“STEP 3—CONFIGURE THE AP” on Page 21](#).

### Ethernet Packet Statistics Menu

(See [Figure 3-44 on Page 80](#) for detailed information)

This screen provides detailed information on data exchanges between the radio you are viewing and the network through the network layer. These include:

#### Wireless Packet Statistics

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

#### Ethernet Packet Statistics

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

The most significant fields are **Retries**, **Retry Errors**, **Receive Errors**, and **Lost Carrier Detected**. If the data values are more than 10% of their sent and received counterparts, or the **Lost Carrier Detected** value is greater than a few dozen, there might be trouble with interference, or a loss of the Ethernet signal. Note that this does not refer to the over-the-air (RF) carrier, but only to the Ethernet carrier.

When troubleshooting throughput quality issues, a check should also be made of the *Radio Packet Statistics Screen* shown in [Figure 3-45 on Page 81](#). This menu provides a review of packet statistics from a radio link (RF) perspective.

It is also helpful to check the RSSI of incoming signals. If the RSSI levels in each zone are within a few decibels (dB) of each other, but less than  $-90$  dBm, then check the aiming of the antenna system. See *“Aiming Directive Antennas for Maximum RSSI”* on [Page 162](#) for details.

---

**NOTE:** The average signal level should be  $-95$  dBm or stronger for reliable performance with an allowance for fade margin.

---

Another place to look for trouble is in **Packets Received by Zone**. The packets should be evenly distributed across all zones (1-5% variation). If they are not, interference in the disparate zones should be suspected. Blocking these zones can eliminate or reduce harmful interference. See *“Skip Zones Menu”* on [Page 53](#) for more information.

When dealing with radio interference troubles, be sure to review *A Word About Radio Interference* on [Page 150](#).

### Serial Port and Remote Serial Statistics Menu

(See [Figure 3-43 on Page 79](#) for detailed information)

This screen provides top-level information on data exchanges between the radio serial ports and the network through the wireless and the Ethernet (data) layers. These include:

- Bytes In On Port xxx
- Bytes In On Socket xxx
- Bytes Out On Port xxx
- Bytes Out On Socket xxx

You can use this information as an indicator of port activity at the data and IP levels.

### Diagnostic Tools

(See [MAINTENANCE AND TOOLS](#) on [Page 85](#))

The AP *Maintenance Menu* contains a tool that is especially useful to network technicians—the **PING** utility. Use the **PING** utility to verify the reachability of Ethernet devices connected to the network.

### 7.1.3 Using Logged Operation Events

(See [Event Log Menu](#) on Page 82)

The transceiver 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” event. There are also normal or routine events such as those marking the restarting of the system, implementation of parameter changes, and external access to the entraNET MS. Informational events are stored in temporary (RAM) memory that is lost in the absence of primary power, while alarms are stored in permanent memory (flash memory) until cleared by your request. [Table 3-3](#) summarizes these classifications.

**Table 7-4. Event Classifications**

Level	Description or Impact	Storage
Informational	Normal operating activities	Flash Memory
Minor	Does not affect radio operation	RAM
Major	Degraded radio performance but still capable of operation	RAM
Critical	Prevents the radio from operating	RAM

These events are stored in the transceiver Event Log, and can be a valuable aid in troubleshooting radio problems or detecting attempts to breach network security.

[Table 7-5](#) lists all of the transceiver event codes and provides a brief description of their meaning.

**Table 7-5. MDS entraNET Event Codes**

Index	Event Type	Event Name String	Clear String	Set String
0	EVENT_IPADDR	IP Address	Valid	Invalid
1	EVENT_IPMASK	IP Mask	Valid	Invalid
2	EVENT_MACADDR	MAC Address	Valid	Invalid
3	EVENT_SYSTEM_ERROR	System Error	Cleared	Please Reboot
4	EVENT_BRIDGE	Network Interface	OK	Error
5	EVENT_FREQ_CAL	Frequency	Calibrated	Not Calibrated
6	EVENT_POWER_CAL	Power	Calibrated	Not Calibrated
7	EVENT_FLASH_TEST	Flash Test	Passed	Failed
8	EVENT_RSSI_CAL	RSSI	Calibrated	Not Calibrated
9	EVENT_RAD_NO_NETWORK_ADDRESS	Net Address	Programmed	Not Programmed

**Table 7-5. MDS entraNET Event Codes**

Index	Event Type	Event Name String	Clear String	Set String
10	EVENT_RAD_RX_TIMEOUT	RX Timeout	Cleared	Set
11	EVENT_RAD_NVMEM_FAULT	NV Memory Fault	Cleared	Set
12	EVENT_RAD_NOT_CALIBRATED	TOR Not Calibrated	Cleared	Set
13	EVENT_RAD_OUT_OF_LOCK	TOR Synthesizer	Locked	Out of Lock
14	EVENT_RAD_AUTHORIZATION_FAULT	Authorization Fault	Cleared	Set
15	EVENT_RAD_HARDWARE_MISMATCH	TOR Hardware	OK	Mismatched
16	EVENT_RAD_TOR_FIRMWARE_STATE	TOR Firmware	OK	Not Programmed
17	EVENT_RADIO_PARM_NOT_SET	TOR Parm not set	Cleared	Set
18	EVENT_SPARE18	Spare 18	Cleared	Set
19	EVENT_SPARE19	Spare 19	Cleared	Set
20	EVENT_SPARE20	Spare 20	Cleared	Set
21	EVENT_SPARE21	Spare 21	Cleared	Set
22	EVENT_SPARE22	Spare 22	Cleared	Set
23	EVENT_SPARE23	Spare 23	Cleared	Set
24	EVENT_SPARE24	Spare 24	Cleared	Set
25	EVENT_SPARE25	Spare 25	Cleared	Set
26	EVENT_SPARE26	Spare 26	Cleared	Set
27	EVENT_SPARE27	Spare 27	Cleared	Set
28	EVENT_SPARE28	Spare 28	Cleared	Set
29	EVENT_SPARE29	Spare 29	Cleared	Set
30	EVENT_SPARE30	Spare 30	Cleared	Set
31	EVENT_SPARE31	Spare 31	Cleared	Set
33	EVENT_BOOTUP	System Bootup	--	--
34	EVENT_REBOOT	User Selected Reboot	--	--
35	EVENT_REPROG_STARTED	Reprogramming	--	Started
36	EVENT_REPROG_COMPLETE	Reprogramming	--	Complete
37	EVENT_REPROG_FAILED	Reprogramming	--	Failed
38	EVENT_TELNET_LOGIN	Telnet User	Logged Out	Logged In
39	EVENT_HTTP_LOGIN	HTTP User	Logged Out	Logged In
40	EVENT_LOG_CLEAR	Event Log Cleared	--	--
41	EVENT_REMOTE_CONN	Remote	Disassociated	Associated
42	EVENT_DHCP_SERVER	DHCP Server	Enabled	Disabled
43	EVENT_DHCP_CLIENT	DHCP Client	Enabled	Disabled

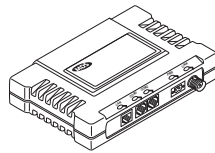
**Table 7-5. MDS entraNET Event Codes**

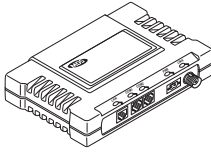
Index	Event Type	Event Name String	Clear String	Set String
44	EVENT_DHCP_ADDRESS	Obtained DHCP Address	--	--
45	EVENT_TIME_NOT_SET	Date or time Not Set	--	--
46	EVENT_TIME_BY_USER	Date or time Changed by User	--	--
47	EVENT_TIME_FROM_SERVER	Date or time from Server	--	--
48	EVENT_CONSOLE_LOGIN	Console User	Logged Out	Logged In
49	EVENT_CONSOLE_LOCKDOWN	Console Access	--	Locked for 5 minutes
50	EVENT_TELNET_LOCKDOWN	Telnet Access	--	Locked for 5 minutes
51	EVENT_HTTP_LOCKDOWN	HTTP Access	--	Locked for 5 minutes
52	EVENT_PARM_CHANGED	Parameter Changed	--	--
53	EVENT_CFGSCRIPT	Configuration Script	Generated	Received
54	EVENT_AUTH_KEY	Auth Key Entered	Valid	- Invalid
55	EVENT_AUTH_DEMO	Demo Authorization	Enabled	Expired
56	EVENT_MAX_DEMOS	Max Demos	Reset	Reached
57	EVENT_RAD_TEMPERATURE	TOR Temperature	OK	Out of Range
58	EVENT_RAD_RX_SIGNAL	RX Signal Strength	OK	LOW
59	EVENT_RAD_RF_PWR_OUTPUT	RF Output Power	OK	Out of Range
60	EVENT_RAD_PWR_DC_IN	TOR DC Input	OK	Out of Range
61	EVENT_RAD_DATA_FRAMING	LCP Data Framing	Cleared	Error
62	EVENT_RAD_DATA_PARITY	LCP Data Parity	Cleared	Error
63	EVENT_RAD_NO_UNIT_ADDR	TOR Unit Address	OK	Not Programmed
64	EVENT_IAPP_PEER	IAPP Peer	Removed	Added
65	EVENT_INTERNAL_ERROR	Internal Error	--	--
66	EVENT_IAPP_UNIT_UPDATE	IAPP Unit Update	Received	Sent
67	EVENT_SHRD_KEY_CHAL	Shared Key Challenge	Passed	Failed
68	EVENT_REDUND_LACK_REMOTES	Redundant Lack of Remotes	Switchover	Switchover



**Table 7-5. MDS entraNET Event Codes**

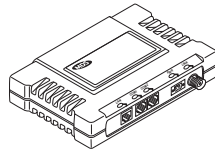
<b>Index</b>	<b>Event Type</b>	<b>Event Name String</b>	<b>Clear String</b>	<b>Set String</b>
69	EVENT_REDUND_RECV_ERR	Redundant Packet Receive	Switchover	Switchover
70	EVENT_REDUND_FORCED	Forced Redundant	Switchover	Switchover
71	EVENT_ICOPY_STARTED	Image Copy	--	Started
72	EVENT_ICOPY_COMPLETE	Image Copy	--	Complete
73	EVENT_ICOPY_FAILED	Image Copy	--	Failed
74	EVENT_ENDPOINT_ADDED	Endpoint	Removed	Added
75	EVENT_BROADCAST_REPROG	Broadcast Reprogram	Complete	Started





# 8 TECHNICAL REFERENCE

8.1	UPGRADING AP FIRMWARE	179
8.2	USING CONFIGURATION SCRIPTS	181
	Sample of an Exported Configuration File.....	182
	Editing Configuration Files.....	186
8.3	DATA INTERFACE CONNECTORS	187
8.3.1	LAN/ETH Port .....	187
8.3.2	COM1 Port .....	188
8.3.3	COM2 Port .....	189
8.4	TECHNICAL SPECIFICATIONS	189
8.5	dBm-WATTS-VOLTS CONVERSION CHART	193



## 8.1 UPGRADING AP FIRMWARE

GE MDS occasionally offers upgrades to the transceiver firmware. One version of the firmware provides core software resources for all radio models. Uploading new firmware into the radio does not alter any privileges provided by Authorization Keys, and does not require the transceiver to be taken offline until you want to operate the radio from the new firmware image in the radio.

You must use the entraNET MS for all firmware activities, including uploading from a TFTP server.

---

**NOTE:** To upgrade the Remote firmware, refer to *UPGRADING REMOTE FIRMWARE* on Page 117.

---

You can initiate the uploads through any of the three entraNET MS gateways:

- **Terminal emulator**—Connect a PC directly to the transceiver COM1 port using a serial cable, and use a terminal emulator program on the PC such as HyperTerminal.
- **Telnet**—Use a network connection for text-based access to the Management System.
- **Web browser**—Connect a PC directly to the transceiver LAN port or associated network and open a Web browser on the PC.

For information on downloading firmware code, visit the GE MDS Web site at [www.gemds.com/service/technical/support](http://www.gemds.com/service/technical/support).

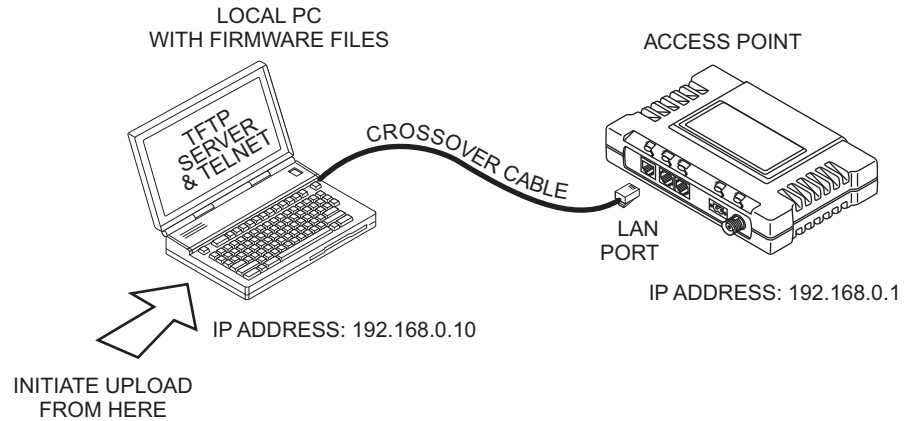
### ***Upgrading the Transceiver Firmware***

To install firmware using TFTP, you need:

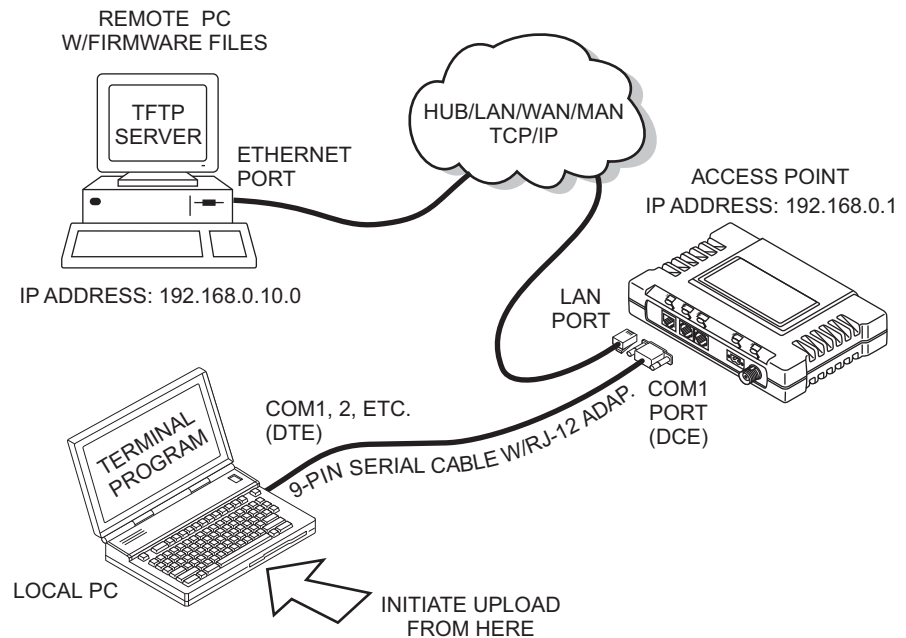
- A PC with a TFTP server running. You can download a TFTP server from the GE MDS Web site at [www.gemds.com/service/technical/support/downloads.asp](http://www.gemds.com/service/technical/support/downloads.asp).
- The IP address of the PC running the TFTP server.

If you do not know your computer IP address (Windows PC), select **Start>Run** and enter **winipcfg** or **ipconfig** to determine this information. The radio IP address can be found under the *Network Configuration Menu*. (See “*Network Configuration Menu*” on Page 45.)

There are several options for connecting the transceiver and computer control point to the firmware server. [Figure 8-1](#) and [Figure 8-2](#) show two variations. With either method, it is essential that all of the equipment be on the same subnet.



**Figure 8-1. Upgrade Configuration—Option 1**  
*(TFTP Server and Firmware File on Same CPU)*



**Figure 8-2. Upgrade Configuration—Option 2**  
*(TFTP server and firmware file on remote server)*

**NOTE:** Transferring the radio firmware image file, which is approximately 3 MB, might take several minutes, depending on traffic between the TFTP server and the transceiver.

Regardless of your connection to the transceiver, loading firmware or configuration files into the flash RAM within the radio is much slower than loading software onto a PC hard drive or RAM.

## Upgrade Procedure

To upgrade the transceiver firmware file (**filename.gpk**), use the procedure below.

1. Launch a TFTP server on a PC connected either directly or over a LAN to the transceiver Ethernet port (LAN). Configure the server to allow downloads from the directory containing the firmware image file.
2. Connect to the entraNET MS using a Web browser or Telnet session over the LAN, or Terminal emulator using the COM1 port, whichever is easier.
3. Go to the *entraNET MS Reprogramming Menu*.  
(**Main Menu>Maintenance Menu>Reprogramming Menu**)
4. Fill in the information for the following:
  - **TFTP Host Address**—IP Address of server (host computer) running TFTP server.
  - **Retrieve File**—Name of file (**filename.gpk**) to be pulled from the TFTP server holding the firmware file.
5. Pull the firmware file through the TFTP server into the entraNET radio.  
(**Main Menu>Maintenance Menu>Reprogramming Menu>Retrieve File**)
  - Transfer status messages are displayed at the PC. You can cancel the transfer at any time by pressing **CTRL** C.
  - If the transfer does not start, verify that the AP and the PC can **PING** each other.
6. Restart the transceiver with the new firmware image to make it active.  
**Main Menu>Maintenance Menu>Reprogramming Menu>Reboot Device**
7. Test the transceiver for normal operation.

*End of procedure.*

## 8.2 USING CONFIGURATION SCRIPTS

You can create and download configuration scripts from the transceiver that contain a wealth of information about the radio. This file can serve many purposes, including to keep a copy of the radio configuration at a point in time. These files can also be used to view the setup of a radio without connecting to it. Examining archival files can be a useful source of information during troubleshooting.

The next few sections describe the contents of this file, and explain how to use it as a template for configuring multiple transceivers with the

same profile. Ultimately, you can upload standardized files into the transceiver to speed up the installation process.

You can also upload configuration files into a transceiver to restore the settings of a radio using a previously saved configuration of the radio. This is particularly convenient after finishing a test using some experimental settings.

### Sample of an Exported Configuration File

The following is a sample of a typical configuration file produced by a transceiver that contains over 150 parameters, many of which are user definable. The presentation is slightly altered to allow notes to appear below associated parameter lines. Some of the values used in the calibration of the built-in test equipment were deleted to reduce space. Use this presentation as a guide to the type of information contained in the file. See [“Editing Configuration Files” on Page 186](#) for further information.

---

**NOTE:** The parameter names and the data values from the Exported Configuration File are shown in bold text. Any description is found below in an indented paragraph. Descriptions for parameters that are functionally identical to both COM1 and COM2 are not repeated.

---

#### *Beginning of Configuration File*

**; MDS entraNET**  
**; Created 01-03-2003 6:59:41**  
**IP Address: 192.168.1.1**

The IPv4 address of this radio. This field is unnecessary if DHCP is enabled.

Changing the IP value over the network causes a loss of communication with other devices unaware of the new address.

---

**IP Netmask: 255.255.255.0**

The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled.

**IP Gateway: 0.0.0.0**

The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled.

**Ethernet Address: 00:06:3D:00:00:5D**

The physical Ethernet MAC address of the radio. This value is set at the factory and cannot be changed.



**Model Number: 900**

The radio model number. This value is set at the factory and cannot be changed.

**Serial Number: 1026295**

The radio serial number. This value is set at the factory and cannot be changed.

**Unit Name: Library Admin Office**

A name for this radio. It appears at the top of every menu screen.

**Owner: Hilltop College MIS**

The name of the owner of this radio.

**Contact: John Galt X232**

The contact person for this radio.

**Description: Link to Campus Server**

A brief description of this radio.

**Location: Hollister Bldg. RM450**

The physical location of this radio.

**Com2 Port Config: 8N1**

The character size, parity type, and number of stop bits to be used.

**Max Remotes Allowed: 50**

The maximum number of Remotes allowed to connect to this AP.

**Device Mode: Access Point**

Configures the radio to act as a Remote or an AP. The Access Point option is not allowed unless the radio was purchased with it, or an Authorization Key was purchased to allow it.

**Hop Time: 28**

The amount of time that a radio spends at any given frequency. This field is controlled by the AP. Remotes obtain the appropriate value upon association with the AP.

**Network Address: 100**

The ID of the network that this radio belongs to. The radio only communicates with devices having identical network addresses.

**Date Format: Generic**

Specifies the date format:

- Generic: dd Mmm yyyy
- European: dd-mm-yyyy
- U.S.A.: mm-dd-yyyy

**Console Baud: 19200**

The baud rate of the serial menu console. The default value is 19200 bps.

**Company Name: MDS**  
**Version Name: 06-1234567**  
**Product Name: entraNET**  
**RF Output Power Setpoint: 30**

The desired amount of RF output power, measured in dBm.

**Active Boot Image: 0**  
**Skipped Hop Zone1: Active**  
**Skipped Hop Zone2: Skip**  
**Skipped Hop Zone3: Active**  
**Skipped Hop Zone4: Active**  
**Skipped Hop Zone5: Active**  
**Skipped Hop Zone6: Active**  
**Skipped Hop Zone7: Active**  
**Skipped Hop Zone8: Active**  
**Skipped Hop Zone9: Active**  
**Skipped Hop Zone10: Active**  
**Firmware TFTP Host IP: 63.249.227.105**

Address of the TFTP host from which firmware images are downloaded.

**Firmware TFTP Filename: entraNET-bkrto-3\_0\_0.gpk**  
**Eventlog TFTP Host IP: 192.168.1.3**

Address of the TFTP host to which to send the event log.

**Eventlog TFTP Filename: eventlog.txt**  
**Config Script TFTP Host IP: 192.168.1.33**

Address of the TFTP host to which to send or receive the configuration script.

**Config Script TFTP Filename: entraNET\_config.txt**  
**SNMP Read Community: public**

Community string for read access using SNMPv1.

**SNMP Write Community: private**

Community string for write access using SNMPv1.

**SNMP Trap Community: public**

Community string sent with traps using SNMPv1.

**SNMP Trap Manager #1: 0.0.0.0**

The IP address of an SNMP manager to receive traps.

**SNMP Trap Manager #2: 0.0.0.0**  
**SNMP Trap Manager #3: 0.0.0.0**  
**SNMP Trap Manager #4: 0.0.0.0**

**Auth trap enable: disabled**

Setting to enable SNMP authentication traps.

**Trap Version: v1 Traps**

The SNMP trap format.

**Package 1 Version: 1.1.0**

Indicates the version of firmware in Image 1.

**Package 2 Version: 1.1.0****TFTP Timeout: 20****COM1 Serial Data Enable: disabled**

Setting to enable the COM1 data mode.

**COM1 Serial Data Mode: UDP**

IP protocol for the COM1 data mode.

**COM1 Serial Data Baud Rate: 9600**

Baud rate for the COM1 data mode.

**COM1 Serial Data Tx IP Address: 0.0.0.0**

COM1 data is sent to this IP address.

**COM1 Serial Data Tx IP Port: 0**

COM1 data is sent to this IP port.

**COM1 Serial Data Rx IP Port: 0**

COM1 data is received on this IP port.

**COM2 Serial Data Enable: enabled****COM2 Serial Data Mode: UDP****COM2 Serial Data Baud Rate: 9600****COM2 Serial Data Tx IP Address: 169.254.10.2****COM2 Serial Data Tx IP Port: 0****COM2 Serial Data Rx IP Port: 0****COM1 Serial Data Rx IP Address: 0.0.0.0**

COM1 data is received on this IP address.

**COM2 Serial Data Rx IP Address: 169.254.0.2****COM2 Serial Data Flow Control: disabled**

Setting to enable hardware flow control (RTS/CTS) in COM2 data mode.

**SNTP Server IP: 0.0.0.0**

The IPv4 address of NTP/SNTP time server.

**COM1 Serial Data Delimiter Chars: 4**

Minimum number of characters that constitute a gap in inter-packet delay for COM1.

**COM2 Serial Data Delimiter Chars: 4**

**COM1 Serial Data Buffer Size: 20**

Number of output characters buffered in inter-packet delay for COM1.

**Com2 Serial Data Buffer Size: 20**

**RF Frequency Hopping Format: USA or CANADA**

*(read only)* The frequency-hopping rules the radio operates under.

**SNMP Enable: disabled**

Enable or disable the SNMP agent.

**Approved Remotes List Enable: disabled**

Enable or disable the Approved Remotes List.

**Encryption Enable: disabled**

Enable or disable over-the-air data encryption.

**HTTP Enable: enabled**

Enable or disable the HTTP interface.

**Telnet Enable: enabled**

Enable or disable the Telnet interface.

**HTTP MD5 Authentication: disabled**

Enable or disable MD5 digest authentication.

*End of Configuration File*

## Editing Configuration Files

Once the AP radio operation is fine-tuned, use the [Configuration Scripts Menu](#) on Page 87 to save a copy of the configuration onto a PC. The file can then be used as a template to generate modified copies adjusted to match other devices. You can modify the configuration files using a text editor or an automated process (not provided by GE MDS).

We recommend that you review and update the following parameters for each individual radio. Other parameters may also be changed.

**Table 8-1. Common User-Definable 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 appears in entraNET MS headings.	Any 20-character alphanumeric string

**Table 8-1. Common User-Definable Parameters (Continued)**

Field	Comment	Range
Location	Used only as reference for network administration	Any 40-character alphanumeric string
Radio Net(work) Address	Used to identify different groups or locations	1-20000

Save each resulting file with a unique name. We recommend using directories and file names that reflect the location of the radio to facilitate its identification.

### Editing Rules

- You may include only parameters you want to change.
- Change only the parameter values.
- Capitalization counts in some field parameters (for example, **System Mode**)
- Comment fields
  - a. Edit or delete anything on each line to the right of the comment delimiter (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.
  - c. Comments after parameters included in files exported from a transceiver do not need to be present in your customized files.

## 8.3 DATA INTERFACE CONNECTORS

The entraNET transceivers use three types of data interface connectors. The first, the LAN/ETH port (LAN on the AP, ETH on the remote), is a metallized RJ-45 connector. The other two are standard modular types—RJ-12 for the COM1 port, and RJ-45 for the COM2 port. This section provides illustrations and pinout information for all of these data connectors.



The transceiver meets U.S.A. FCC Part 15, Class A limits when used with shielded data cables not exceeding 3 ft/0.9m.

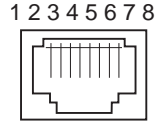
### 8.3.1 LAN/ETH Port

Use this port to connect to an Ethernet network at an AP or to the endpoint of a Remote.

- To connect a PC directly to the AP LAN port, an RJ-45 to RJ-45 crossover cable is required. At the Remote, a straight-through cable is required.

- To connect the AP to an Ethernet hub or bridge, use a straight-through cable.

The connector uses standard Ethernet RJ-45 cables and wiring. Use the pinout graphic and table below to construct a custom cable, if required.

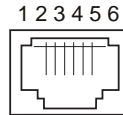


**Figure 8-3. LAN/ETH Port (RJ-45) Pinout**  
(viewed from the outside of the radio)

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

### 8.3.2 COM1 Port

Connect a PC to the Remote transceiver COM1 port (RJ-12) for diagnostics and configuration. Pinout information for the COM1 port is provided in [Figure 8-4](#) and [Table 8-2](#).



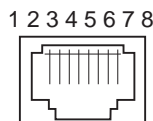
**Figure 8-4. COM1 Port (DCE)**  
(viewed from the outside of the radio)

**Table 8-2. COM1 Port Pinout, RS-232 Interface**

Pin	Functions	COM1 Port (DCE)
1	Unused	
2	Unused	
3	Unused	
4	Receive Data (RXD)	Out
5	Transmit Data (TXD)	In
6	Ground	—

### 8.3.3 COM2 Port

Connect a terminal device to the transceiver COM2 port (RJ-45) for payload data connection. Pinout information for the COM2 port is provided in [Figure 8-5](#) and [Table 8-3](#).



**Figure 8-5. COM2 Port (DCE)**  
(viewed from the outside of the radio)

**Table 8-3. COM2 Port, EIA-232 Interface**

Pin	Functions	COM2 Port (DCE)
1	Unused	
2	Data Carrier Detect (DCD)	Out
3	Data Terminal Ready (DTR)	In
4	Signal Ground (GND)	—
5	Receive Data (RXD)	Out
6	Transmit Data (TXD)	In
7	Clear-to-Send (CTS)	Out
8	Request-to-Send (RTS)	In

## 8.4 TECHNICAL SPECIFICATIONS

Below are the technical specifications for entraNET 900 and 2400 models. Specifications that are unique to a particular model are identified by frequency range (900 MHz or 2400 MHz).

### GENERAL

Data Rate:	106 kbps over the air
Frequency Band:	900 MHz models: 902–928 MHz ISM band 2400 MHz models: 2401.6–2477.8 MHz in the following bands: 2401.6–2427.0 MHz (Band A) 2427.2–2452.6 MHz (Band B) 2452.8–2478.2 MHz (Band C)
Configurations:	Access Point, Remote
Spreading Mode:	Frequency Hopping Spread Spectrum (FHSS)
Frequency Channels:	Selectable; 64 to 128 in increments of 16
MTBF (Reliability):	Consult factory for on-file data
Startup Time:	AP: approximately 30 sec Remote: approximately 1 sec
Time Required for Remote to Connect with AP:	Typically less than 1 sec

## RADIO CHARACTERISTICS

---

System Gain:	2400 MHz: 131 dB 900 MHz: 136 dB
Carrier Power:	900 MHz: 20-30 dBm 2400 MHz: 20-27 dBm 2400 MHz ETSI: 10-20 dBm
Output Impedance:	50 ohms
Occupied Bandwidth:	200 kHz
Modulation:	Two-level CPFSK (Continuous-Phase FSK)
Receiver Sensitivity:	2400 MHz: typically -104 dBm (1 x 10 <sup>-6</sup> BER) 900 MHz: typically -105 dBm (1 x 10 <sup>-6</sup> BER)
Frequency Hopping Range:	Eight user-definable 3.2 MHz-wide zones, each containing 16 frequencies
Hop Pattern:	Based on network address
Frequency Stability:	30 ppm

### TRANSMITTER:

Duty Cycle:	Continuous
Spurious:	-67 dBc

### RECEIVER:

Type:	Double-conversion superheterodyne
Intermodulation:	59 dB minimum (EIA)
Desensitization:	70 dB
Spurious:	60 dB

## PHYSICAL INTERFACE

---

Ethernet Port:	10BaseT, RJ-45, 10 Mbps
Serial Port:	RS-232/V.24, RJ-45, DCE 1,200-115,200 bps asynchronous
Antenna Connector:	TNC female
LED Indicators:	LAN (AP), ETH (Remote), COM1, COM2, PWR, LINK

## DATA CHARACTERISTICS

---

Protocols Supported:	<ul style="list-style-type: none"> <li>• IEEE (Institute of Electrical and Electronic Engineers) 802.3 (single device at Remote) (Ethernet)</li> <li>• IP or Ethernet (DHCP, ICMP (Internet Control Message Protocol), UDP, TCP, ARP)</li> <li>• Encapsulation over IP (tunneling) for serial async multidrop protocols, including MODBUS, DNP.3, Bisync, BSAP, DF1, TotalFlow, Poll Select</li> </ul>
----------------------	--



## TRANSCEIVER MANAGEMENT

---

Methods Supported (AP):	<ul style="list-style-type: none"> <li>• HTTP (embedded Web server)—pending</li> <li>• Telnet</li> <li>• Local console using COM1 port</li> <li>• SNMPv1/2/3. MIB II, Enterprise MIB—pending</li> <li>• SYSLOG</li> <li>• GE MDS NETview MST<sup>TM</sup>—pending</li> </ul>
Methods Supported (Remote):	Local console using COM1 port

## ENVIRONMENTAL

---

Temperature Range:	-40C to +70C (-33.8F to +158F)
Humidity:	95% at +40°C (104°F); non-condensing
Input Power:	6.0*–30 Vdc (13.8 Vdc nominal) *Measured at the radio connector, not the source
Power Consumption:	7.05 W maximum at 1 W RF output (see below for details by model and voltage)
Transmit:	<u>900 MHz AP:</u> 1175 mA at 6 Vdc 525 mA at 13.8 Vdc 270 mA at 30 Vdc  <u>900 MHz Remote:</u> 1025 mA at 6 Vdc 600 mA at 13.8 Vdc 240 mA at 30 Vdc  <u>2400 MHz AP:</u> 1091.7 mA at 6 Vdc 488.5 mA at 13.8 Vdc 253.3 mA at 30 Vdc  <u>2400 MHz Remote:</u> 941.7 mA at 6 Vdc 433.8 mA at 13.8 Vdc 223.3 mA at 30 Vdc
Receive:	<u>900 MHz AP:</u> 510 mA at 6 Vdc 220 mA at 13.8 Vdc 115 mA at 30 Vdc  <u>900 MHz Remote:</u> 260 mA at 6 Vdc 120 mA at 13.8 Vdc 65 mA at 30 Vdc  <u>2400 MHz AP:</u> 533.3 mA at 6 Vdc 230.1 mA at 13.8 Vdc 119.7 mA at 30 Vdc  <u>2400 MHz Remote:</u> 283.3 mA at 30 Vdc 130.1 mA at 13.8 Vdc 69.7 mA at 30 Vdc
Sleep (all remotes):	130 mA at 6 Vdc 15 mA at 12 Vdc 8 mA at 30 Vdc

Shutdown (all remotes): 0.37 mA at 6 Vdc  
0.55 mA at 12 Vdc  
0.78 mA at 30 Vdc

## MECHANICAL

---

Case:	Cast aluminum
Mounting Options:	Flat surface mount brackets, 35 mm DIN rail
Dimensions (Excluding mtg. hardware):	AP: 3.15 H x 17.2 W x 11.2 D cm (1.25 H x 6.75 W x 4.5 D in.)  Remote: 2.5 x 12.7 x 8.9 cm (1 H x 5 W x 3.5 D in.)
Weight:	AP: 1.4 lb/635 g Remote: 1.04 lb/472 g

## AGENCY APPROVALS

---

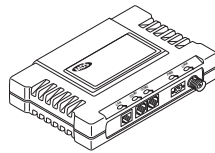
- FCC Part 15.247
- Industry Canada RSS-210 and RSS-139
- ETSI
- CSA/US Class 1, Div. 2; Groups A, B, C and D hazardous locations
- Contact GE MDS for information on availability and governmental approvals in other countries

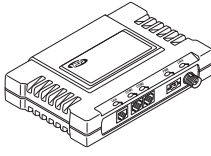
## 8.5 dBm-WATTS-VOLTS CONVERSION CHART

Use [Table 8-4](#) to determine the equivalent voltage or wattage of an RF power expressed in dBm.

**Table 8-4. dBm-Watts-Volts Conversion—for 50 Ohm systems**

dBm	V	Po	dBm	V	Po	dBm	mV	Po	dBm	$\mu$ V	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	.01 $\mu$ W	-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				
+40	22.5	10W	-11	.064		-60	0.225	.001 $\mu$ W			
+39	20.0	8W	-12	.058		-61	0.200		-107	1000	
+38	18.0	6.4W	-13	.050		-62	0.180		-108	900	
+37	16.0	5W	-14	.045		-63	0.160		-109	800	
+36	14.1	4W	-15	.040		-64	0.141		-110	710	.01pW
+35	12.5	3.2W	-16	.0355					-111	640	
+34	11.5	2.5W							-112	580	
+33	10.0	2W							-113	500	
+32	9.0	1.6W							-114	450	
+31	8.0	1.25W							-115	400	
+30	7.10	1.0W							-116	355	
+29	6.40	800mW							-117	325	
+28	5.80	640mW							-118	285	
+27	5.00	500mW							-119	251	
+26	4.45	400mW							-120	225	.001pW
+25	4.00	320mW							-121	200	
+24	3.55	250mW							-122	180	
+23	3.20	200mW							-123	160	
+22	2.80	160mW							-124	141	
+21	2.52	125mW							-125	128	
+20	2.25	100mW							-126	117	
+19	2.00	80mW							-127	100	
+18	1.80	64mW							-128	90	
+17	1.60	50mW							-129	80	.1fW
+16	1.41	40mW							-130	71	
+15	1.25	32mW							-131	61	
+14	1.15	25mW							-132	58	
+13	1.00	20mW							-133	50	
+12	.90	16mW							-134	45	
+11	.80	12.5mW							-135	40	
+10	.71	10mW							-136	35	
+9	.64	8mW							-137	33	
+8	.58	6.4mW							-138	29	
+7	.500	5mW							-139	25	
+6	.445	4mW							-140	23	.01fW
+5	.400	3.2mW									
+4	.355	2.5mW									
+3	.320	2.0mW									
+2	.280	1.6mW									
+1	.252	1.25mW									





## 9 TERMS AND ABBREVIATIONS

If you are new to wireless IP or Ethernet systems, some of the terms used in this guide may be unfamiliar. The following glossary explains many of these terms and is helpful in understanding the operation of the transceiver system.

**Access Point (AP)**—The transceiver in the network that provides synchronization information to one or more associated Remote radios.

**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*.

**Associated**—Condition in which the frequency hopping pattern of the Remote is synchronized with the AP station in a network, is recognized by the AP, and is ready to pass traffic.

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

**bps**—Bits per second. 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.

**Data Communications Equipment**—See *DCE*.

**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. A chart for dBm-Watts-Volts conversion can be found on Page 193.

**DCE**—Data Communications Equipment. In data communications terminology, this is the “modem” side of a computer-to-modem connection. The transceiver COM1 and COM2 ports are 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.

**DES**—Data Encryption Standard. More information on DES is available at [www.itl.nist.gov/fipspubs/fip46-2.htm](http://www.itl.nist.gov/fipspubs/fip46-2.htm).

**DHCP**—Dynamic Host Configuration Protocol. An Internet standard that allows a client (that is, 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 contacts a DHCP server on the network and requests an IP address. The DHCP server provides 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.

**DNP3**—Distributed Network Protocol 3. DNP3 is an industry-standard protocol that was initially created for communication between electrical substation devices. Today, this non-proprietary protocol is being widely adopted for a variety of other applications. Although DNP3 is typically employed in a client-server environment, this serial protocol is one of only a few that allow peer-to-peer communication between devices without the need for a *host computer*. It does this in the same way that IP supports peer-to-peer communication in an Ethernet environment.

**Encapsulation**—Process 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 (for example, 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**—Ethernet or IP data equipment connected to the ports of the transceiver.

**Fade Margin**—The greatest tolerable reduction in average received signal strength 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.

**FHSS**—Frequency Hopping Spread Spectrum. A common transmission technique used by license-free transceivers.

**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 transceivers, 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.

**Frequency Zone**—A segment of radio spectrum containing the transmitters lower and upper frequency limits. For a chart of 900 MHz and 2400 MHz frequency zones, see [Table 3-1](#) and [Table 3-2 on Page 54](#).

**Group ID**—The identification number of the group.

**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, instructing the connected device to delay further transmission until CTS again returns to the high state.

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

**HTTP**—Hypertext Transfer Protocol

**IAPP**—Inter-Access Point Protocol. A protocol by which APs share information between the Remotes that are connected to them. This allows relevant data to travel across commonly-connected radio subnetworks from outlying Remotes to other outlying Remotes.

**ICMP**—Internet Control Message Protocol

**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 transceiver CPU.

**Intergap**—See *Inter-Packet Delay*

**Inter-Packet Delay**—A technique used in GE MDS devices that accommodates protocols that do not tolerate gaps in the middle of a frame (for example, MODBUS ASCII). In these protocols, gaps are interpreted by the connected device as an end-of-frame indication,

which may cause errors. Inter-packet delay resolves this through the use of buffers.

**kbps**—kilobits per second. See *bps*.

**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.

**MAS**—Multiple Address System. A radio system where a central master station communicates with several remote stations for the purpose of gathering telemetry data. [Figure 1-2 on Page 7](#) shows an example of a MAS system.

**MCU**—Microcontroller Unit. This is the processor responsible for controlling system start-up, synthesizer loading, hop timing, and key-up control.

**MD5**—Message-Digest algorithm 5. 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 check out “RFC 1321” on the Internet.

**Microcontroller Unit**—See *MCU*.

**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 APs as it moves through the APs' territory. In order to do this, the station employs roaming and Mobile IP.

**MTBF**—Mean Time Between Failures

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

**Network Address**—User-definable integer that is used to identify a group of transceivers that form a communications network. The AP 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.

**PHY**—Physical layer of the Ethernet LAN.



**PING**—**P**acket **I**nternet **G**roper. 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**—Refers to the ability of a transceiver to connect to an AP from multiple locations without the need to reconfigure the network settings. For example, a transceiver located in one place and connected to an AP can be turned off, moved to another place, turned back on; and, when the right information is entered, can immediately reconnect to the AP without 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 endpoint device.

**Remote**—A transceiver in a network that communicates with an associated AP radio.

**RFI**—Radio Frequency Interference

**Roaming**—The ability of a station to automatically switch its wireless connection between various APs as the need arises. A station may roam from one AP to another because the signal strength or quality of the AP signal has degraded below what another AP can provide. When two APs are co-located for redundancy, roaming allows the stations to switch between the radios 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 associated. As the station comes in range of a new station, it switches its connection to the stronger signal. Roaming refers to a station's logical, not necessarily physical, move between APs within a specific network and IP subnet.

**RSSI**—Received Signal Strength Indicator

**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 relative received signal quality. High ratios likely result in better signal detection and performance.

**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. A “guaranteed delivery” protocol used to set up a connection between two devices with acknowledgements (ACK/NACK), and retries if the data is not received properly. Requires more overhead than UDP (see below) but is sometimes required in mission-critical systems.

**Terminal Server**—A device that provides a common connection point for serial terminals (PCs, printers, endpoint devices, and so on) to a Local or Wide Area Network (LAN/WAN). The terminal converts serial data from these terminals into Internet Protocol (IP). The entraNET AP contains a built-in terminal server.

**Throughput**—A measure of the quantity of data sent and the speed with which it is transferred in a network.

**TFTP**—Trivial File Transfer Protocol

**UDP**—User Datagram Protocol. A basic transmission protocol with low overhead requirements but with no acknowledgement or retry capability. It is often used for broadcast transmission where acknowledgements are not required, and incomplete messages are discarded by the receiving station.

---

# INDEX

---

## A

- AC Power Adapter Kit 12
- Access Point 3
  - Database 69
  - Database Menu 76
  - local console 36
  - menu structure 32
  - operating parameters 22
  - Telnet 36
  - Web browser 36
- accessories 12
- ACKAVG 111
- ACKAVGINT 111
- ACKAVGTHRESH 111
- Add
  - Approved Remote 68
  - Associated Remotes 68
- Address to Ping 90
- Administrator Password 23
- AgeOut 74, 76
- ALARM 103
- ALL 113, 116
- antenna
  - aiming 162
  - directional 4, 151
  - feedline 154
  - location 149
  - omni-directional 4, 12
  - placement 6
  - port 19
  - selection 153
  - system gain vs. power output setting, table 157, 158, 159
  - Yagi 12, 154
    - illustrated 154
- AP 6, 114
- APLIST 103
- APP1 114, 115
- APP2 114, 115
- applications
  - long range wireless LAN 6
- Approve Remotes 66
- Approved
  - Remotes List 66, 68
  - Remotes List Menu 68
- APx 104
- ASSOC 114
- Associated Remotes 44
- attenuator 19
- AUTH 104
  - Trap Enable 51
- Authorization 71
  - Codes Menu 91
  - Key 91

Authorized Features 91

Auto Key Rotation 66

## B

- band
  - 2400 MHz 5
  - 900 MHz 5
- BAUD 104, 106
  - Rate 60, 62
- BLOCKTIME 111
- BOOT 114
- BPS (bits-per-second), defined 195
- Bridge
  - Configuration 46
  - Configuration Menu 51
  - Forward Delay 51
  - Hello Time 51
  - Priority 51
- Broadcast
  - Images 73
  - Remote
    - Programming 70
    - Reboot 73
    - Reprogramming Menu 72
    - Repeat Count 52
    - reprogramming 73
- Browse Package 118
- BSP Routing Enable 49
- BUFFER 104, 106
  - Size 60, 62
- Byte
  - defined 195
  - Format 60, 62
- Bytes
  - in on port 78
  - in on socket 78
  - out on port 78
  - out on socket 78
  - received 80
  - sent 80

## C

- cable
  - coaxial 155
  - data equipment to DATA INTERFACE connector 101
  - DB-25 to RJ-45 9
  - EIA-232 Shielded Data 12
  - Ethernet crossover 12, 22, 36, 38, 40
  - Ethernet straight-thru 12
  - serial communications 36
  - straight-through 36, 38, 40
  - TNC Male-to-N Female Adapter 12
- Change Baud Rate 118
- CLEAR 104, 112
  - Event Log 83

- Statistics 80, 81
- CMD 104, 106, 108, 109, 111, 112, 113, 114, 115, 117
- COM 79
  - Data Statistics 78
  - Data Statistics Menu 78
  - Port 64, 75
- COM1 37, 39, 104, 116, 188
  - port 9, 21
- COM2 106, 116, 189
  - port 9
- Commands 102
  - most often used commands 103
  - network configuration 103
  - remote 102
  - SKIP (set/display frequency zone to skip) 54
- communication rules 6
- COMPANY 108
- CONFIG 108, 117
  - Filename 88
- configuration
  - AP 21
  - Remote 23
  - remote serial gateway 62
  - script 22, 181
  - Scripts Menu 87
- connection
  - IP-to-serial 27
  - serial-to-serial 27
- connectors 18
  - data interface 187
- Console Baud Rate 84
- Contact 85
- Contention Window
  - Max 52
  - Min 52
- Count 90, 112
- CRC 81
- crossover cable 38, 40
- Current
  - Alarms 82
  - Firmware 44, 87
  - IP Address 47
  - IP Gateway 48
  - IP Netmask 47
  - User 44
- CWMAX 109
- CWMIN 109
- Cyclic Redundancy Check 81
- D**
  - data communications equipment 9
  - data throughput
    - improving 163
  - Database Timeout 69
  - Date 84
    - Format 84
  - date
    - stamp 82
  - DB-25 to RJ-45 cable 9
  - dB<sub>i</sub>, defined 195
  - dB<sub>m</sub>, defined 195
  - DCE 9
    - defined 196
  - Decibel (dB), defined 195
  - DEFAULT 104, 106, 109
  - Delete
    - All 68
    - Approved Remote 68
  - Description 85
  - DEVICE 108
  - Device
    - Information 45, 71
    - Information Menu 84
    - Name 43, 85
    - Names Menu 85
    - Status 43
      - Alarmed 43
      - Operational 43
  - Diags 81
  - dimensions 152
  - DIN
    - rail 152
    - rail brackets 4
    - Rail Mounting Bracket 13
  - DIRECT 109
  - directional antenna 4
  - Display
    - skipped frequency zones (SKIP command) 54
  - DNP
    - Multicast
      - Address 98
      - Port 98
    - Routing Enable 98
    - Unicast Port 98
  - DNP3 8
    - Routing 45
    - Routing Database 98
    - Routing Menu 97
  - DTE, defined 196
  - DTRSENSE 115
  - Duration 92
  - Dwell Time 52
- E**
  - EIA-232 5, 56
    - signaling 9
  - Enable
    - skipped zone (SKIP command) 54
  - encapsulation 62
  - ENCRYPT 110
  - Encryption 5, 11, 64
    - Enable 66
    - Phrase 66
  - Endpoint
    - Database 69
    - Database Menu 75
    - device 123
    - Logging 69
  - ENDPT 111
  - ENDPTMODE 111
  - entraNET Transceiver models 4
  - Equalization, defined 196

- error correction 56
- ETH 111, 116
- Ethernet 5
  - Bridging 51
  - crossover cable 22
  - device connection to remote 25
  - LAN 4
  - Packet Statistics 78
  - Packet Statistics Menu 80
- Event 117
  - codes 172
  - Log 78
    - Host Address 83
    - Host Filename 83
    - Menu 82
- Event Log Menu 82
- F**
- Fade margin, defined 196
- Failed 81
- FEC 48, 109
- feedline 154
  - selection 153
- firmware
  - Filename 87
  - upgrading 179
- FLOWCTRL 106
- Force
  - Key Rotation 67
  - Switchover 95
- FORMAT 105, 107
- Forward Error Correction 48
- Fragments 81
- Frame, defined 197
- Frequency 92
  - hopping 5
    - defined 197
  - Not Calibrated 95
  - zone, defined 197
  - Zones 54
- fuse 12, 20
- G**
- gain
  - system 156
- MDS entraNET models 6
- GE MDS Security Suite 4, 10
- Good Data 81
- Group 105, 107
  - Database 69
  - Database Menu 75
  - ID 64, 75
- Guest Password 23
- H**
- H2H 117
- HANDOFF 111
- HANGTIME 115
- Hardware
  - Event Triggers 94
  - Event Triggers Menu 94
  - flow control, defined 197
- HELP 112
- HEX 103
- HIGH 113
- hop time 52
- Hopping, defined 197
- HOPTIME 109
- Host computer, defined 197
- HREV 117
- HTTP 11, 64
  - Access 66
  - Security Mode 66
- HyperTerminal 21, 23, 36, 37, 101
- I**
- IAPP 98
  - Enable 49
  - Multicast
    - Address 49
    - Port 49
    - TTL 49
  - Unicast Port 49
- Illustrations
  - antenna, Yagi 154
  - bench test setup 19
  - point-to-point link 7
  - remote station arrangement 149
  - typical MAS network 7
- IMAGE 117
- Image
  - Copy 87
  - Verify 87
- Index 79
- INDICATOR 115
- Installation
  - connecting transceiver to data equipment 101
  - requirements 149
  - site
    - selection 149
    - survey 150
- interference 151, 161
  - about 150
- INTERGAP 105, 107
- Inter-Packet Delay 60, 62
- IP 6, 26
  - Address 22, 23, 26, 43, 76, 77
  - Address Mode 47
  - Configuration 46
  - netmask 23
  - Port 79
  - to-remote serial configuration 62
  - to-Serial Services 55
- K**
- KEY 104
- L**
- Lack of Associated Remotes Exceeded Threshold 95
- Lack of Remotes for 96
- LAN port 17, 22, 38, 40
- LAN/ETH 187
- latency time
  - reducing 163
- Latency, defined 197
- LED

- COM1 25, 26
- COM1/ETH 24
- COM2 25, 26
- ETH 25
- functions 26
- LAN 38, 40
- LAN/ETH 26
- LINK 24, 26, 150, 162
- PWR 25, 26, 43, 82
- troubleshooting with 168
- Legacy Wireless Products 9
- line-of-sight 5
- LINK 25
- List of Remotes 77
- Local
  - console 36
  - Console session 37, 42
  - IP Port 64
  - Serial Configuration 44
  - Serial Configuration Menu 57
- Location 44, 85, 109
- LOG 112, 117
- LOGIN 113
- log-in
  - AP 21
  - procedure 101
  - Remote 23
- LOGOUT 113
- long range wireless LAN 6
- Lost carrier detected 80
- Lost Data 81
- LOW 113
- M**
- MAC 4, 6
  - Address 76
- Maintenance/Tools 45
  - Menu 86
- Manage Selected Remote 70
- Max Remotes 67, 69
- Maximum Receive Errors 97
- MCU (Microcontroller Unit), defined 198
- MD5 Digest 66
- Media Access Controller 4
- menu
  - access point database 76
  - approved remotes list 68
  - authorization codes 91
  - broadcast remote reprogramming 72
  - COM data statistics 78
  - configuration scripts 87
  - device information 84
  - device names 85
  - DNP3 routing 97
  - endpoint database 75
  - ethernet packet statistics 80
  - event log 82
  - group database 75
  - hardware event triggers 94
  - lack of associated remotes exceeded threshold 96
  - local serial configuration 57
  - maintenance/tools 86
  - manage selected remote 71
  - mobility 98
  - network event triggers 94
  - packet RX errors exceeded threshold 97
  - PING utility 90
  - radio packet statistics 81
  - redundancy 93
    - configuration options 95
  - remote
    - database 74
    - management 70
    - serial gateway 62, 63
    - serial gateway entries 64
    - serial gateway statistics 79
  - reprogramming 86
  - RSG configuration scripts 89
  - security configuration 65
  - serial configuration wizard 58
  - statistics/event log 77
  - transmitter test 92
  - wireless network 69
  - wireless packet statistics 80
- MESSAGE 113
- Mobility
  - Configuration 46
  - Configuration Menu 49
- Mobility Menu 98
- MODE 60, 61, 64, 105, 108, 109, 110, 111, 112, 115
  - terminal interface 101
- MODEL 84, 108
- mounting
  - bracket 152
  - dimensions 152
- Multiple Address System (MAS)
  - defined 198
  - network, illustrated 7
- N**
- NAME 108
- net address 23, 48
- NETADDR 110, 114
- NETview MS software 8, 31
- Network 71
  - address 24
    - defined 198
  - bridge 160
  - configuration commands 103
  - Ethernet 4
  - Event Triggers 93
    - Menu 94
  - Interface Error 95
  - wide diagnostics, defined 198
  - wireless LAN 6
- Network Configuration 44
- Next Page 68
- No Ack 81
- NORMAL 113
- NOW 116
- Num EPs 74
- Number of Remotes 68, 77

- O**
- omni-directional antenna 4, 12
- Operating
  - Commands 101–117
  - parameters (Access Point) 22
- OTHER 115
- Over the Air Data 81
- Overflow 81
- OWNER 108
- P**
- Package to Transmit 72, 73
- Packet
  - Receive Errors Exceeded Threshold 96
  - Size 90
- Packets
  - dropped 80
  - received 80
  - sent 80
- password 23, 113, 118
  - Administrator 23
  - Guest 23
  - protection 5
- performance
  - optimizing 160
- PHRASE 110
- Ping 26, 90
  - test setup 26
- PING Utility Menu 90
- PLC (Programmable Logic Controller), defined 199
- Point-to-multipoint system
  - defined 198
- Point-to-point system
  - link, illustrated 7
- Poll, defined 199
- port
  - Access Point interface connectors 18
  - antenna 19
  - COM1 9, 21, 23, 31, 36, 37, 39, 188
  - COM2 9, 25, 189
  - ETH 25
  - Ethernet Remote interface connectors 18
  - LAN 17, 22, 31, 36, 37, 38, 40, 47
  - LAN/ETH 187
  - Status 59, 61
- Power
  - How much can be used (ETSI, 2400 MHz)? 158
  - How much can be used (USA/Canada, 2400 MHz)? 157
  - How much can be used (USA/Canada, 900 MHz)? 156
  - Not Calibrated 95
- Previous Page 68
- Procedures
  - antenna and feedline selection 153
  - connecting data equipment to DATA INTERFACE connector 101
  - site selection 149
  - troubleshooting 167–175
- PRODUCT 108
- PROGRAM VERIFY 113
- Protected Network Station 9
- protocol
  - DNP3 8
  - HTTP 11, 64
  - IP 25
  - SNMP 11, 31, 64
  - TCP 9, 121
  - UDP 9, 121
- PWR 110, 114
- Q**
- QUALITY 114
- R**
- RADIO 114, 116
  - NETADDR 102
  - PWR 102
  - UNIT 102
- Radio 71
  - bench test setup, illustrated 19
  - Configuration 44
  - Configuration Menu 52
  - Packet Statistics 78
    - Menu 81
- RADIOSW 117
- RBE 4
- Reboot 114
  - Device 87
  - to new image after download 118
- Receive
  - Error Count Interval 97
  - errors 80, 81
- Received Signal Strength Indication 150
- Redundancy 45
  - Configuration 93
  - Configuration Options 94
    - Menu 95
- Redundancy Menu 93
- REFRESH 114
- release notes 3
- Remote 6
  - access channels 5
  - Access IP 67
  - Access Manager 66
  - COM Port 60
  - commands 102
  - Database 69
  - Database Menu 74
  - Firmware Upgrade Utility 117
  - IP 5
  - Management 69
    - Menu 70
    - via the AP 101
  - minimum configuration 102
  - P,B 79
  - radio firmware 117
  - radio, defined 199
  - Reboot 72
  - Reprogramming 71
  - Serial Gateway 45
    - Configuration 62
    - Entries Menu 64
    - Menu 62, 63
    - Statistics 78

- Statistics Menu 79
- Serial Wizard 63
- station
  - typical arrangement, illustrated 149
  - to Manage 70, 72
  - transceiver 3
  - UnitID 60
- REPEAT 110
- Report-by-Exception 4
- Reprogramming Menu 86
- RESET 116
- RESTRICT 104
- Retries 81
- Retrieve File 87, 88, 89
- Retrieve/Restore Configuration 118
- RETRY 110
- REV 108
- RF
  - Output Power 23, 52
  - power divider 19
- RS-232 55
- RSG
  - Config Filename 89
  - Config Host Address 89
  - Configuration Scripts Menu 89
  - Entries 63
  - Talkback Enable 63
  - Talkback Timeout 63
- RSSI 19, 114, 150, 162
- RSSIAVG 112
- RSSIAVGINT 112
- RSSIAVGTHRESH 112
- RX
  - IP Port 61
  - Pkts 74, 76
- RXDELAYCHARS 105, 108
- S**
- SAME 115
- SAVE 108
- SCADA 7
  - defined 199
- screen
  - serial configuration current settings 61
  - view current settings 59, 61
- script
  - configuration 181
  - editing 186
- Security
  - Configuration 45
  - Configuration Menu 65
  - risks and solutions 10
  - suite 4
- Send
  - Event Log 83
  - File 88, 89
  - Images 72
- SER 109
- Serial 5
  - Configuration 71
  - Current Settings Screen 61
  - Wizard 56
  - Wizard Menu 58
- gateway 9, 55
- interfaces 54
- Number 44, 77, 84
- to-Serial Example 59
- to-Serial Services 55
- serial
  - device connection to remote 25
- services
  - IP-to-serial 55
  - serial-to-serial 55
- Set
  - frequency zone to skip (SKIP command) 54
- SHOW 108
- signal strength 19
- Simple Network Management Protocol 5
- site
  - selection 149
  - survey 150
- Skip
  - command (set/display frequency zone to skip) 54
  - Zones 53
    - Menu 53
- SKIP command (set/display frequency zone to skip) 54
- SKIPZONES 110
- SLEEP 115
- SNMP 5, 11, 31, 64
  - Agent Configuration Menu 50
  - Configuration 46
  - Mode 50, 66
  - Read community 50
  - Trap community 50
  - Traps 11
  - V3 Agent ID 50
  - v3 Auth Password 50
  - v3 Password Mode 51
  - v3 Priv Password 50
  - Write community 50
- Socket
  - P,B 79
- software
  - GE MDS Security Suite 10
  - NETview MS 8, 31
- spread-spectrum 4, 5
- SREV1 117
- SREV2 117
- Starting Information Screen 44
- STATE 110
- State 74, 79
- Static IP
  - Address 47
  - Gateway 47
  - Netmask 47
- Statistics 71
  - Event Log 45
  - Event Log Menu 77
- STATS 116
- STATTRACKER 116
- Status 73



- straight-through cable 38, 40
- SWR (Standing Wave Ratio)
  - defined 200
- SYNC 114
- Syslog Server Address 83
- system gain 156
  - calculating 157, 159
- T**
- Tables
  - antenna system gain vs. power output setting 157, 158, 159
  - troubleshooting 169
- tabletop testing 19, 21
- Talkback Enable 62
- TCP 9, 55, 121
  - Keepalive 64
- Technical reference 179–193
- Technical specifications 189–195
- Telnet 5, 36, 64
  - Access 66
  - Connection 22
  - session 35, 38, 42
- terminal
  - equipment 25
  - Interface Mode 101
  - server 55
  - session 35
  - settings 101
- test setup 18
- Testing
  - bench setup, illustrated 19
- TFTP
  - Host Address 87, 88
  - Timeout 83, 87, 88, 89
- Time 84
- time stamp 82
- Timeout 81
- TOR1 114
- TOR2 114
- Transceiver
  - connecting to data equipment 101
- transmission
  - Control Protocol 9
  - path 150
- Transmitter Test Menu 92
- transparent over-the-air serial-to-serial connection 55
- Trap
  - Manager 51
  - Version 50
- Troubleshooting 167–175
  - table 169
- TX
  - FREQ 114
  - IP Address 61
  - IP Port 62
  - Key 92, 114
  - Pkts 74
- TXDELAY 106, 108
- TxPkt 76
- TYPE 110
- U**
- UDP 9, 55, 61, 121
  - IP-to-Serial 63
- Unicast
  - Retry Count 53
  - UDP 61
    - Mode Example 61
- Unit 114
  - Update Enable 49
- UnitID 64, 74, 75, 79
- Upgrade Firmware 118
- Uptime 44, 84, 109
- User
  - Datagram Protocol 9
  - interface 35
    - Telnet session 35
    - terminal session 35
    - Web browser session 35
  - Name 118
  - Password 67, 118
- V**
- VER 117
- Via Remote 76
- View
  - Current Settings Screen 59, 61
  - Event Log 82
- W**
- WAKE 116
- Web
  - browser 5, 40, 42, 64
- Wireless
  - MAC Configuration 46
    - Menu 48
  - Network 45
  - Network Menu 69
  - Packet Statistics Menu 80
- X**
- X Address 48
- XHREV 117
- Y**
- Yagi antenna 12



## ***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: [gemds.techsupport@ge.com](mailto:gemds.techsupport@ge.com)

FAX: 585 242-8369      Web: [www.gemds.com](http://www.gemds.com)

### **FACTORY SERVICE**

---

Component-level repair of radio 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 will be issued a Service Request Order (SRO) number. The SRO number will help 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.

A statement should accompany the radio describing, in detail, the trouble symptom(s), and a description of any associated equipment normally connected to the radio. It is also important to include the name and telephone number of a person in your organization who can be contacted if additional information is required.

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 at 585-241-5540 (FAX: 585-242-8400), or by e-mail at [gemds.productservices@ge.com](mailto:gemds.productservices@ge.com).



Digital Energy  
MDS

GE MDS, LLC  
175 Science Parkway  
Rochester, NY 14620  
General Business: +1 585 242-9600  
FAX: +1 585 242-9620  
Web: [www.gemds.com](http://www.gemds.com)

