

Microwave Data Systems Inc.  
**MDS Mercury Series™**



**Wireless IP/Ethernet Transceiver**  
Covering AP and Remote Units

**DRAFT**

MDS 05-4446A01, Rev. 03  
SEPT. 2008



**GE MDS**  
industrial wireless networks



---

# TABLE OF CONTENTS

---

## **1 PRODUCT OVERVIEW AND APPLICATIONS..... 1**

### **1.1 ABOUT THIS MANUAL..... 3**

- 1.1.1 Start-Up Guide .....3
- 1.1.2 Online Access to Manuals .....3
- 1.1.3 Conventions Used in This Manual .....3

### **1.2 PRODUCT DESCRIPTION..... 4**

- 1.2.1 Model Offerings .....6
- 1.2.2 GE MDS P23 Protected Network (Redundant) Configuration .....7
- 1.2.3 External GPS PPS Option .....7

### **1.3 APPLICATIONS ..... 7**

- 1.3.1 Fixed Data System .....8
- 1.3.2 Wireless LAN .....8
- 1.3.3 Point-to-Point LAN Extension .....9
- 1.3.4 Serial Radio Network Connectivity .....9
- 1.3.5 Multiple Protocols and/or Services .....10
- 1.3.6 Wireless LAN with Mixed Services .....11
- 1.3.7 Upgrading Older Wireless Network with Serial Interfaces .....12

### **1.4 NETWORK DESIGN CONSIDERATIONS..... 12**

- 1.4.1 Extending Network Coverage with Repeaters .....12
- 1.4.2 Protected Network Operation using Multiple Access Points .....14
- 1.4.3 Collocating Multiple Radio Networks .....15

### **1.5 GE MDS CYBER SECURITY SUITE..... 16**

### **1.6 ACCESSORIES ..... 17**

## **2 TABLETOP EVALUATION AND TEST SETUP..... 19**

### **2.1 OVERVIEW..... 21**

### **2.2 STEP 1—CONNECT THE ANTENNA PORTS ..... 21**

### **2.3 STEP 2—CONNECT THE PRIMARY POWER ..... 22**

2.4	STEP 3—CONNECT PC TO THE TRANSCEIVER.....	23
2.5	STEP 4—REVIEW TRANSCEIVER CONFIGURATION .....	23
2.5.1	Getting Started .....	23
2.5.2	Procedure .....	23
2.5.3	Basic Configuration Defaults .....	23
2.6	STEP 5—CONNECT LAN OR SERIAL DATA EQUIPMENT .....	24
2.7	STEP 6—CHECK FOR NORMAL OPERATION.....	26
<b>3</b>	<b><i>EMBEDDED MANAGEMENT SYSTEM.....</i></b>	<b>29</b>
3.1	MS INTRODUCTION .....	31
3.1.1	Differences in the User Interfaces .....	31
3.2	ACCESSING THE MENU SYSTEM .....	33
3.2.1	Methods of Control .....	34
3.2.2	PC Connection and Log In Procedures .....	34
3.2.3	Navigating the Menus .....	38
3.3	BASIC OVERVIEW OF OPERATION .....	40
3.3.1	Starting Information Screen .....	40
3.3.2	Main Menu .....	42
3.4	CONFIGURING NETWORK PARAMETERS .....	43
3.4.1	Network Configuration Menu .....	43
3.4.2	Ethernet Port Configuration Menu .....	51
3.4.3	Bridge Configuration .....	52
3.4.4	SNMP Agent Configuration .....	53
3.4.5	AP Location Push Config Menu .....	55
3.4.6	SNTP Server Configuration .....	57
3.5	RADIO CONFIGURATION.....	58
3.5.1	Radio Configuration Menu .....	58
3.5.2	Serial Port Configuration .....	67
3.6	MODBUS / TCP SERVER CONFIGURATION .....	80
3.6.1	Modbus/TCP in Mercury Transceivers—An Overview .....	80
3.6.2	Menu Selections .....	80
3.7	SECURITY CONFIGURATION MENU .....	85
3.7.1	Device Security Menu .....	86
3.7.2	Wireless Security Menu .....	87

3.7.3	IEEE 802.1x Device Authentication .....	89
3.7.4	Manage Certificates .....	91
<b>3.8</b>	<b>REDUNDANCY CONFIGURATION (AP ONLY) .....</b>	<b>93</b>
<b>3.9</b>	<b>GPS CONFIGURATION (REMOTE ONLY) .....</b>	<b>98</b>
<b>3.10</b>	<b>DEVICE INFORMATION MENU .....</b>	<b>100</b>
<b>3.11</b>	<b>PERFORMANCE INFORMATION MENU .....</b>	<b>101</b>
<b>3.12</b>	<b>MAINTENANCE/TOOLS MENU .....</b>	<b>113</b>
3.12.1	Auto Firmware Upgrade Menu (AP Only) .....	124
<b>3.13</b>	<b>PERFORMANCE OPTIMIZATION .....</b>	<b>127</b>
3.13.1	Proper Operation—What to Look For .....	129

## **4 TROUBLESHOOTING & RADIO MEASUREMENTS ..... 133**

<b>4.1</b>	<b>TROUBLESHOOTING .....</b>	<b>135</b>
4.1.1	Interpreting the Front Panel LEDs .....	135
4.1.2	Troubleshooting Using the Embedded Management System .....	136
4.1.3	Using Logged Operation Events .....	139
4.1.4	Alarm Conditions .....	140
4.1.5	Correcting Alarm Conditions .....	141
4.1.6	Logged Events .....	142
<b>4.2</b>	<b>RADIO (RF) MEASUREMENTS .....</b>	<b>143</b>
4.2.1	Antenna System SWR and Transmitter Power Output .....	143
4.2.2	Antenna Aiming—For Directional Antennas .....	144

## **5 PLANNING A RADIO NETWORK ..... 147**

<b>5.1</b>	<b>INSTALLATION PLANNING .....</b>	<b>149</b>
5.1.1	General Requirements .....	149
5.1.2	Site Selection .....	151
5.1.3	Terrain and Signal Strength .....	151
5.1.4	Antenna & Feedline Selection .....	151
5.1.5	How Much Output Power Can be Used? .....	155
5.1.6	Conducting a Site Survey .....	155

5.1.7 A Word About Radio Interference .....	156
5.2 dBm-WATTS-VOLTS CONVERSION CHART .....	158

## **6 TECHNICAL REFERENCE..... 159**

6.1 DATA INTERFACE CONNECTORS .....	161
6.1.1 LAN Port .....	161
6.1.2 COM1 Port .....	162
6.2 SPECIFICATIONS .....	162
6.3 NOTES ON SNMP .....	165
6.3.1 Overview .....	165

## **7 GLOSSARY OF TERMS & ABBREVIATIONS..... 169**

### **Copyright Notice**

This publication is protected by U.S.A. copyright law. Copyright 2008, GE MDS. All rights reserved.

### **ISO 9001 Registration**

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

### **To our Customers**

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

**Related Materials on the Internet**—Data sheets, frequently asked questions, case studies, application notes, firmware upgrades and other updated information is available on the GE MDS Web site at [www.GEmds.com](http://www.GEmds.com).

### **About GE MDS**

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

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

Our durable products and comprehensive solutions has made GE MDS 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



Professional installation required. The transceiver described here emits radio frequency energy. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard. **Do not allow people to come closer than 20.7 cm (8.15 inches) to the antenna when the transmitter is operating. This calculation is based on an 18 dBi panel antenna. Refer also to the table below, which lists required separation distances.** Additional 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).

Device complies with Power Density requirements at 20cm separation:	Yes
Required separation distance for 18dBi ant. (in cm):	20.7
Required separation distance for 13dBi ant. (in cm):	12.2

### ERP Compliance

To maintain regulatory compliance for Effective Radiated Power (ERP) of 1-Watt per MHz, the following table of transmit power settings must be observed for the listed bandwidths and antenna types approved. Consult the factory for other antenna options of lower gain.

Antenna Gain	Radio Configuration	Radio Power Setpoint (dBm)	Power Density (dBm/MHz)
13 dBi	Omni antenna, 1.75 MHz BW	20	29.3
13 dBi	Omni antenna, 3.5 MHz BW	23	27.7
13 dBi	Omni antenna, 5 MHz BW	23	29.1
13 dBi	Omni antenna, 7 MHz BW	23	27.7
13 dBi	Omni antenna, 10 MHz BW	23	24.7
13 dBi	Omni antenna, 14 MHz BW	23	24.8
18 dBi	Panel antenna, 1.75 MHz BW	14	29.0
18 dBi	Panel antenna, 3.5 MHz BW	17	29.7
18 dBi	Panel antenna, 5 MHz BW	19	29.9
18 dBi	Panel antenna, 7 MHz BW	20	29.8
18 dBi	Panel antenna, 10 MHz BW	23	29.7
18 dBi	Panel antenna, 14 MHz BW	23	29.8

## CSA/us Notice



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

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

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

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

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

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

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

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



### **EXPLOSION HAZARD!**

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

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

## FCC Part 15 Notices

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

Part 15 rules also require that the Effective Isotropic Radiated Power (EIRP) from a Mercury Series installation not exceed 36 dBm. Refer to *Antenna & Feedline Selection* on Page 151 for more information.

## Manual Revision and Accuracy

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





# 1 **PRODUCT OVERVIEW AND APPLICATIONS**

## **Contents**

<b>1.1 ABOUT THIS MANUAL .....</b>	<b>3</b>
1.1.1 Start-Up Guide .....	3
1.1.2 Online Access to Manuals .....	3
1.1.3 Conventions Used in This Manual .....	3
<b>1.2 PRODUCT DESCRIPTION .....</b>	<b>4</b>
1.2.1 Model Offerings .....	6
1.2.2 GE MDS P23 Protected Network (Redundant) Configuration .....	7
1.2.3 External GPS PPS Option .....	7
<b>1.3 APPLICATIONS .....</b>	<b>7</b>
1.3.1 Fixed Data System .....	8
1.3.2 Wireless LAN .....	8
1.3.3 Point-to-Point LAN Extension .....	9
1.3.4 Serial Radio Network Connectivity .....	9
1.3.5 Multiple Protocols and/or Services .....	10
1.3.6 Wireless LAN with Mixed Services .....	11
1.3.7 Upgrading Older Wireless Network with Serial Interfaces .....	12
<b>1.4 NETWORK DESIGN CONSIDERATIONS .....</b>	<b>12</b>
1.4.1 Extending Network Coverage with Repeaters .....	12
1.4.2 Protected Network Operation using Multiple Access Points .....	14
1.4.3 Collocating Multiple Radio Networks .....	15
<b>1.5 GE MDS CYBER SECURITY SUITE .....</b>	<b>16</b>
<b>1.6 ACCESSORIES .....</b>	<b>17</b>



## 1.1 ABOUT THIS MANUAL

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

### 1.1.1 Start-Up Guide

The Mercury Series *Start-Up Guide* (Part No. 05-4558A01) is a companion publication to the Reference Manual. It is a smaller book, with a specific purpose—to guide an installer in the basic steps for getting a transceiver on the air and communicating with other units in a network. It provides only the essential information installers require for getting their equipment up and running in the shortest time possible.

### 1.1.2 Online Access to Manuals

In addition to printed manuals, many users need access to documents electronically. This is especially useful when you need to access documentation while traveling, or want to share a document with another user in the field. Electronic documents also allow searching for a specific term or subject, especially in larger manuals.

Access manuals for our equipment anytime from our Web site at [www.GEmds.com](http://www.GEmds.com). Simply click the **Downloads** tab at the top of the home page and select **Product Manuals** from the drop-down list. A search window appears to help you locate the manual you need.

Online manuals are provided as PDF files in the Adobe® Acrobat® standard. If necessary, download the free reader for PDF files from [www.adobe.com](http://www.adobe.com).

### 1.1.3 Conventions Used in This Manual

#### On-Screen Menu Items

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

[available settings or range; default setting]

## Menu Strings

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

**Main Menu>>Network Configuration>>Network Name**

By following this order of menus, you can quickly reach the desired menu.

## 1.2 PRODUCT DESCRIPTION

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

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

Based on multi-carrier Orthogonal Frequency Division Multiplexing (OFDM), the transceiver features high speed/low latency, basic Quality of Service (QoS) for prioritizing traffic, Ethernet and serial encapsulation, and network roaming. It also provides enhanced security features including AES encryption and IEEE 802.1x Device Authentication, making the Mercury system the best combination of security, range, and speed of any industrial wireless solution on the market today.



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

### **Rugged Packaging**

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

**Simple Installation**

Mercury Transceivers are designed for rapid and trouble-free installation. For basic services, you simply connect the antennas (3650 MHz and GPS, as required), connect your data equipment, apply primary power, and set some operating parameters. No license is required for operation in the USA, Canada, and many other countries. Check requirements for your region before placing the equipment into service.

Most installations employ an omni-directional antenna at the Access Point (AP) location and remote stations. Fixed Remote stations often employ a directional antenna aimed at the AP. Regardless of the type used, antennas are a vital part of the system and must be chosen and installed correctly. Refer to *INSTALLATION PLANNING* on Page 149 for guidance on choosing suitable antennas and installation sites.

**Secure Operation**

Data network security is a vital issue in today's wireless world. Mercury transceivers provide multiple tools to help you build a network that minimizes the risk of eavesdropping and unauthorized access. Some are inherent in the radio's operation, such as the use of 3650 MHz spread-spectrum transmissions; others include data encryption, enabling/disabling channels, and password protection.

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

**Robust Radio Operation**

The transceivers are designed for operation in the license-free 3650 MHz Industrial, Scientific, and Medical (ISM) band. They provide reliable communications over long distances, even in the presence of weak signals or interference.

Range depends on many factors, including terrain, building density, antenna gain, and speed of travel. The unit is designed for successful application in a variety of environments, and offers the best combination of range, speed and robustness available in an industrial wireless package today. By using multiple Access Points, a network can be created that provides consistent, reliable coverage over a large metropolitan area. See *SPECIFICATIONS* on Page 162 for more information on transmission range.

**Flexible Services**

Users with a mix of equipment having Ethernet and serial data interfaces can use this equipment via a Remote transceiver. The transceiver provides services in data networks that are migrating from legacy serial/EIA-232-based hardware to the faster and more easily interfaced Ethernet protocol.

**Flexible Management**

You can locally or remotely configure, commission, troubleshoot, and maintain the transceiver. Four different modes of access are available: local RS-232 console terminal, local or remote IP access (via Telnet or SSH), web browser (HTTP, HTTPS), and SNMP (v1/v2/v3).

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

### **Transceiver Features**

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

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

## **1.2.1 Model Offerings**

The transceiver comes in two primary models—Access Point and Remote. Unique hardware is used for each model. Of the Remote radios, there are two sub-types available: **Standard Remote** and **Max Remote**, both of which support Ethernet and serial services. [Table 1-1](#) summarizes each radio's interface services.

**Table 1-1. Transceiver Models and Data Interface Services**

<b>Model</b>	<b>Sub-Type</b>	<b>Ethernet/LAN<sup>1</sup></b>	<b>COM1<sup>1</sup></b>	<b>USB</b>	<b>Integrated WiFi</b>
Access Point	N/A	Yes	Yes	No	No
Remote	Standard Remote	Yes	Yes	No	No
	Max Remote	Yes	Yes	Yes	Yes

**NOTES**

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

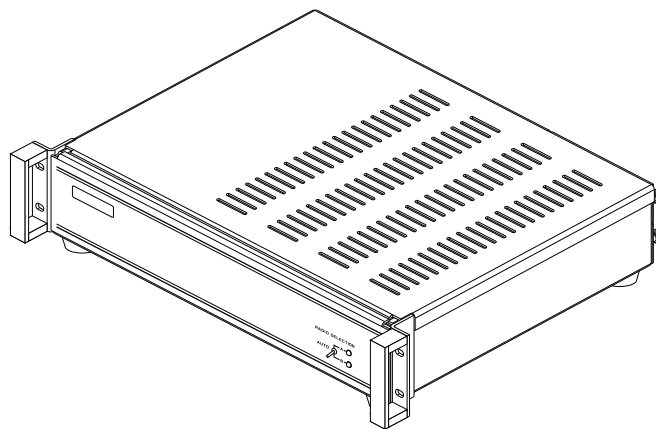
### **Access Point or Remote?—Identification Tip**

The outward appearance of AP and Remote radios is nearly identical, however, the hardware for each type is different and they are *not* interchangeable. An quick way to identify them is to observe the color of the gasket seal in the center of the radio case. **APs have a black gasket, while Remote units have a yellow gasket.**

In addition to gasket color, a label on the top of each radio identifies it as an AP or Remote unit. If the label shows an —A suffix, it is an AP. If it shows a —B suffix, it is a Remote.

### 1.2.2 GE MDS P23 Protected Network (Redundant) Configuration

For mission-critical applications, a Protected Network Station is also offered. This unit incorporates two Access Points, two power supplies, and a switchover logic board that automatically selects between Transceiver A and Transceiver B as the active radio. [Figure 1-2](#) shows the protected chassis. For system-level information on this product, refer to MDS publication 05-4161A01.



**Figure 1-2. MDS P23 Protected Network Station**  
*(incorporates two transceivers, with automatic switchover)*

### 1.2.3 External GPS PPS Option

The External GPS Precise Positioning Service (PPS) option allows for an external GPS device to provide the PPS input to the Mercury. This is useful in installations where multiple radios require GPS timing. This option prevents each Mercury from requiring its own GPS antenna. Refer to the electrical specifications in the [External GPS PPS Option section on Page 164](#). This option is only available in hardware revision 1.0.2 or later.

## 1.3 APPLICATIONS

The following sections provide illustrations of typical transceiver installations. This is an overview only. A Network Administrator should be involved in all installation planning activities.

### 1.3.1 Fixed Data System

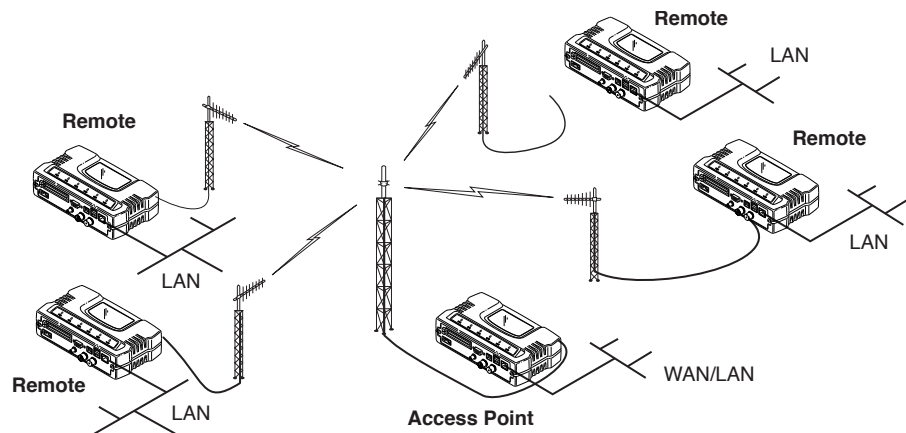
Mercury transceivers support high-speed data communications in an industrial environment. In this application, Remote radios roam between different Access Points, providing seamless transitions and continuous coverage throughout a municipal area.

### 1.3.2 Wireless LAN

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

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

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

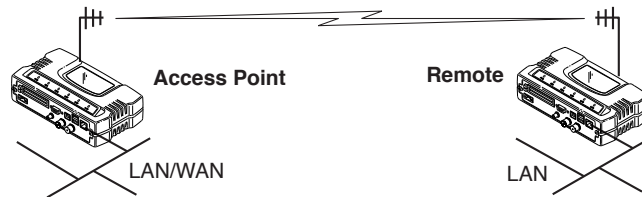


**Figure 1-3. Typical Wireless LAN**

### 1.3.3 Point-to-Point LAN Extension

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



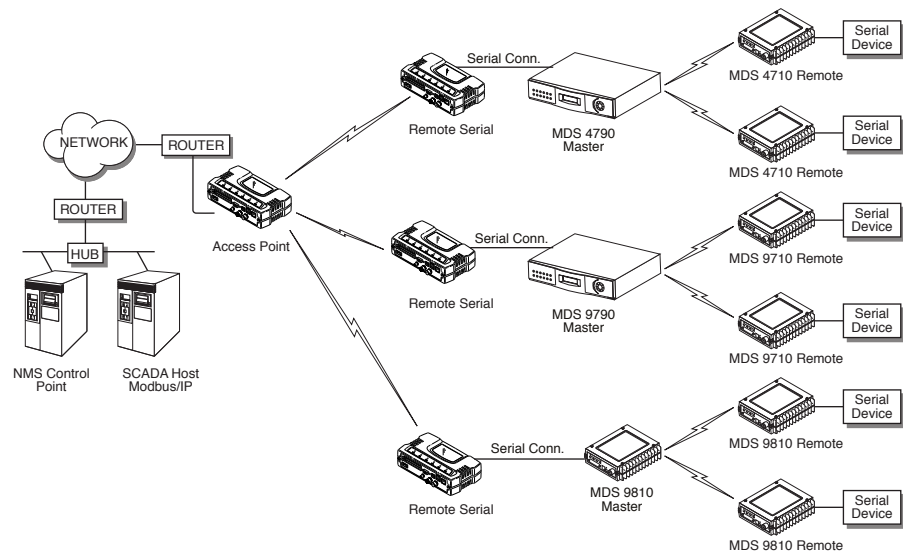


**Figure 1-4. Typical Point-to-Point Link**

### 1.3.4 Serial Radio Network Connectivity

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

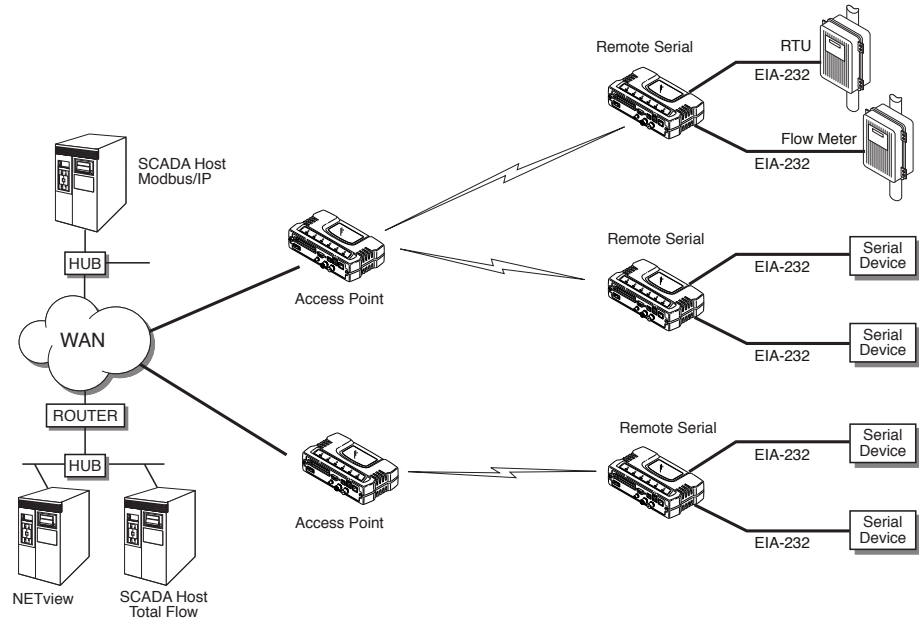
A Remote transceiver with its serial port connected to a GE MDS serial-based radio, such as the MDS x790/x710, MDS TransNET and others, provides a path for bringing the data from the older radio into the IP/Ethernet environment of a Mercury-based system.



**Figure 1-5. Backhaul Network**

### 1.3.5 Multiple Protocols and/or Services

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



**Figure 1-6. Multiple Protocol Network**

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

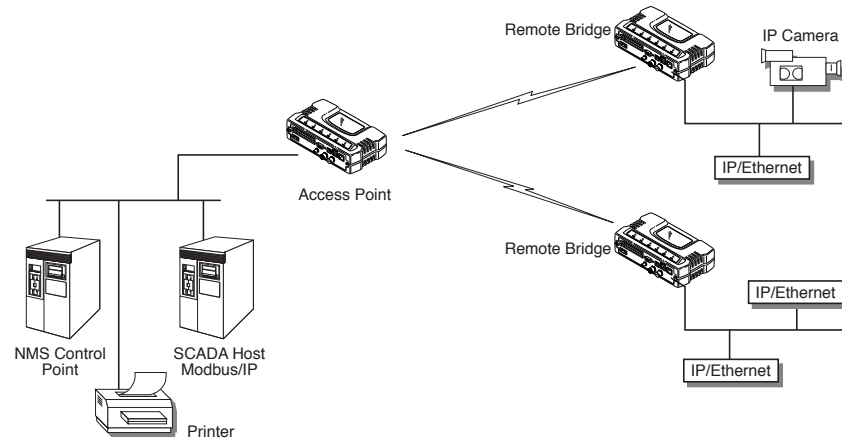
### 1.3.6 Wireless LAN with Mixed Services

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

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

IP-based devices that may be used with the transceiver include new, powerful Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). These, as well as other devices, may be used in applications ranging from SCADA/telemetry monitoring, web-based

video, security monitoring, and Voice over IP. Figure 1-8 shows a typical wireless IP network.



**Figure 1-7. Extended-Range LAN with Mixed Applications**

### 1.3.7 Upgrading Older Wireless Network with Serial Interfaces

Millions of wireless data products have been installed in the last two decades for licensed and license-free operation, many of them manufactured by GE MDS. There are several ways that these systems can benefit from incorporating Mercury equipment. The chief advantages are interface flexibility (serial and Ethernet in one unit), and higher data throughput. By taking advantage of its built-in serial and Ethernet interfaces, the transceiver is well suited to replace leased lines, dial-up lines, or existing 3650 MHz multiple address data transceivers.

#### Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with Mercury transceivers. Legacy equipment can be connected to the transceiver through the COM1 port with a DB-25 to DB-9 cable wired for EIA-232 signaling. The COM1 port acts as a Data Communications Equipment (DCE) port.

---

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

---

## 1.4 NETWORK DESIGN CONSIDERATIONS

### 1.4.1 Extending Network Coverage with Repeaters

#### What is a Repeater System?

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

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

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

Although the range between fixed transceivers can be up to 40 km (25 miles) over favorable terrain, it is possible to extend the range considerably by connecting two units together at one site in a □back-to-back□ fashion, creating a repeater as shown in Figure 1-9. Use this arrangement whenever the objective is to utilize the maximum range between stations. In this case, using high-gain Yagi antennas at each location provides more reliable communications than their counterparts □ omnidirectional antennas.

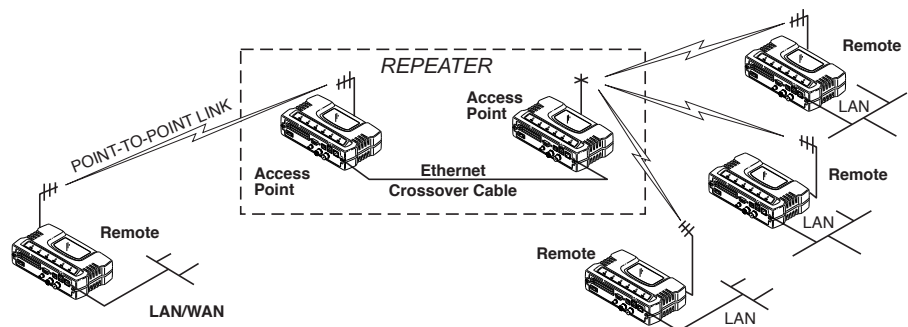


Figure 1-8. Typical LAN with a Repeater Link

#### Overview

Two transceivers may be connected □back-to-back□ through the LAN ports to form a repeater station. If the transceivers are connected directly to each other, you must use an Ethernet cross-over cable. This configuration is sometimes required in a network that includes a distant Remote that would otherwise be unable to communicate directly with the Access Point station due to distance or terrain.

The geographic location of a repeater station is especially important. Choose a site that allows good communication with *both* the Access Point and the outlying Remote site. This is often on top of a hill, building, or other elevated terrain from which both sites can be □seen□

by the repeater station antennas. A detailed discussion on the effects of terrain is given in [Section 5.1.2, Site Selection](#) (beginning on [Page 151](#)).

The following paragraphs contain specific requirements for repeater systems.

### **Antennas**

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

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

### **Network Name**

The two radios that are wired together at the repeater site *must* have different network names. For information on how to set or view the network names, see [STEP 3 CONNECT PC TO THE TRANSCEIVER](#) on [Page 23](#).

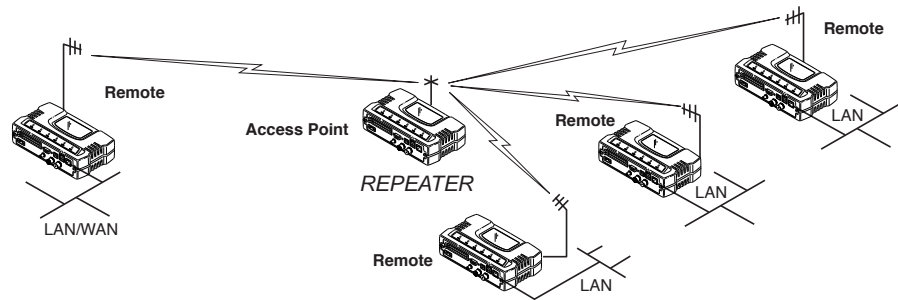
### **TDD Sync Mode**

To avoid interference between the two APs that form a repeater station, they should be synchronized so that they will transmit at the same time and receive at the same time. This eliminates the possibility of one AP transmitting while another is trying to receive.

This can be accomplished by setting the **TDD Sync Mode** parameter in the **Frequency Configuration** menu to **GPS Required**. See [Frequency Control Menu](#) on [Page 60](#) for details.

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

You can extend a wireless network by using the Access Point as a repeater to re-transmit the signals of all stations in the network. (See [Figure 1-10](#) on [Page 14](#).)



**Figure 1-9. Typical Store-and-Forward Repeater Arrangement**

As with the conventional repeater described in Option 1 above, the location of a store and forward repeater is also important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This can be on the top of a hill, building, or other elevated terrain from which all sites can be seen by the repeater station antenna. A detailed discussion on the effects of terrain is given in Section 5.1.2, *Site Selection* (beginning on Page 151).

### 1.4.2 Protected Network Operation using Multiple Access Points

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

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

Two or more Access Points can be configured identically, each with its own independent antenna. In this scenario, Remotes will associate with one of the available Access Points. In case of a failure of that AP, the Remotes will quickly associate with another Access Point, re-establishing connectivity to the end devices. Because only one Access Point operates at any given time, collisions between APs is not possible.

### 1.4.3 Collocating Multiple Radio Networks

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

## The Network Name and the Association Process

The Network Name is the foundation for building individual radio networks. Remotes in a network with the same network name as an Access Point (AP) unit are associated with that AP.

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

### Co-Location for Multiple Networks

It may be desirable to co-locate Access Points at one location to take advantage of an excellent location that can serve two independent networks. Configure each network with a unique Network Name, and install each AP's antenna with at least 10 feet of vertical separation to minimize RFI.

To co-locate APs, configure them with Time Division Duplex (TDD) Sync set to **GPS Required**. Configure all APs that are within range of each other with the same pattern, but with a unique Hop Pattern Offset. For more information, see [Frequency Control Menu](#) on Page 60.

---

**NOTE:** Transceivers are shipped with the Network Name set to **MDS-Mercury** as a factory default.

---

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

When multiple radio networks operate in close physical proximity to other wireless networks, individual units may not operate reliably under weak signal conditions and may be influenced by strong radio signals on adjacent bands. This radio frequency interference cannot be predicted with certainty, and can only be determined by experimentation. If you need to co-locate two units, start by using the largest possible vertical antenna separation between the two AP antennas on the same support structure. If that does not work, consult with your factory representative about other techniques for controlling radio frequency interference between the radios. (See [A Word About Radio Interference](#) on Page 156 for more details.)

## 1.5 GE MDS CYBER SECURITY SUITE

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

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

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

<b>Security Vulnerability</b>	<b>GE MDS Cyber Security Solution</b>
Unauthorized access to the backbone network through a foreign remote radio	<ul style="list-style-type: none"> <li>• IEEE 802.1x device authentication</li> <li>• Approved Remotes List (local) Only those remotes included in the AP list will associate</li> </ul>
□Rogue□ AP, where a foreign AP takes control of some or all remote radios and thus remote devices	<ul style="list-style-type: none"> <li>• IEEE 802.1x device authentication</li> <li>• Approved AP List A remote will only associate to those APs included in its local authorized list of APs</li> </ul>
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	<ul style="list-style-type: none"> <li>• Failed-login lockdown After five tries, the transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.</li> </ul>
Denial of service, where Remote radios could be reconfigured with bad parameters, bringing the network down.	<ul style="list-style-type: none"> <li>• Remote login with SSH or HTTPS</li> <li>• Local console login</li> <li>• Disabled HTTP and Telnet to allow only local management services</li> </ul>
Airsnort and other war-driving hackers in parking lots, etc.	<ul style="list-style-type: none"> <li>• 3650 MHz operation is not interoperable with standard 802.11 wireless 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>• AES-128 encryption</li> </ul>
Unprotected access to configuration via SNMPv1	<ul style="list-style-type: none"> <li>• Implement SNMPv3 secure operation</li> </ul>
Intrusion detection	<ul style="list-style-type: none"> <li>• Provides early warning via SNMP through critical event reports (unauthorized, logging attempts, etc.)</li> <li>• Unauthorized AP MAC address detected at Remote</li> <li>• Unauthorized Remote MAC address detected at AP</li> <li>• Login attempt limit exceeded (Accessed via: Telnet, HTTP, or local)</li> <li>• Successful login/logout (Accessed via: Telnet, HTTP, or local)</li> </ul>



## 1.6 ACCESSORIES

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

**Table 1-3. Accessories**

Accessory	Description	GE MDS Part No.
AC Power Adapter Kit	A small power supply module designed for continuous service. UL approved. Input: 120/220; Output: 13.8 Vdc @ 2.5 A	01-3682A02
Omni-Directional Antennas	Rugged antennas well suited for use at Access Point installations. Consult with your factory Sales Representative for details	--
Yagi Antenna (Directional)	Rugged antennas well suited for use at fixed Remote sites. Consult with your factory Sales Representative for details.	--
GPS Receiving Antennas	A variety of GPS antennas (active and passive) are available. Consult with your factory Sales Representative for details.	--
TNC Male-to-N Female Adapter	One-piece RF adaptor plug.	97-1677A161
TNC Male-to-N Female Adapter Cable	Short length of coaxial cable used to connect the radio's TNC antenna connector to a Type N commonly used on large diameter coaxial cables.	97-1677A159 (3 ft./1m) 97-1677A160 (6 ft./1.8m)
Ethernet RJ-45 Crossover Cable (CAT5)	Cable assembly used to cross-connect the Ethernet ports of two transceivers used in a repeater configuration. (Cable length ≈ 3 ft./1M)	97-1870A21
2-Pin Power Plug	Mates with power connector on transceiver. Screw terminals provided for wires, threaded locking screws to prevent accidental disconnect.	73-1194A39
Ethernet RJ-45 Straight-thru Cable (CAT5)	Cable assembly used to connect an Ethernet device to the transceiver. Both ends of the cable are wired identically. (Cable length ≈ 3 ft./1M)	97-1870A20
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-25 male connector on one end, and a DB-9 female on the other end. Two lengths available (see part numbers at right).	97-3035L06 (6 ft./1.8m) 97-3035L15 (15 ft./4.6m)
EIA-232 Shielded Data Cable	Shielded cable terminated with a DB-9 male connector on one end, and a DB-9 female on the other end, 6 ft./1.8m long.	97-1971A03
Flat-Surface Mounting Brackets & Screws	Brackets: 2" x 3" plates designed to be screwed onto the bottom of the unit for surface-mounting the radio.	82-1753-A01
	Bracket screws: 6-32/1/4" with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
Fuse	Internal fuse, 5.0 Ampere	29-1784A04

**Table 1-3. Accessories (Continued)**

<b>Accessory</b>	<b>Description</b>	<b>GE MDS Part No.</b>
DIN Rail Mounting Bracket	Bracket used to mount the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4022A03
COM1 Interface Adapter	DB-25(F) to DB-9(M) shielded cable assembly (6 ft./1.8 m) for connection of equipment or other EIA-232 serial devices previously connected to □legacy□ units. (Consult factory for other lengths and variations.)	97-3035A06
Bandpass Filter	Antenna system filter that helps eliminate interference from nearby paging transmitters.	20-2822A02
Ethernet Surge Suppressor	Surge suppressor for protection of Ethernet port against lightning.	29-4018A01



# 2 TABLETOP EVALUATION AND TEST SETUP

## Contents

2.1 OVERVIEW .....	21
2.2 STEP 1 □CONNECT THE ANTENNA PORTS.....	21
2.3 STEP 2 □CONNECT THE PRIMARY POWER .....	22
2.4 STEP 3 □CONNECT PC TO THE TRANSCEIVER.....	23
2.5 STEP 4 □REVIEW TRANSCEIVER CONFIGURATION .....	23
2.5.1 Getting Started .....	23
2.5.2 Procedure .....	23
2.5.3 Basic Configuration Defaults .....	23
2.6 STEP 5 □CONNECT LAN OR SERIAL DATA EQUIPMENT .....	24
2.7 STEP 6 □CHECK FOR NORMAL OPERATION .....	26



## 2.1 OVERVIEW

GE MDS recommends that you set up a □tabletop network□ to verify the basic operation of the transceivers. This allows experimenting with network designs, configurations, or network equipment in a convenient location. This test can be performed with any number of radios.

When you are satisfied that the network is functioning properly in a benchtop setting, perform the field installation. Complete information for field installation, including mounting dimensions and antenna selection, is provided in *INSTALLATION PLANNING* on Page 149.

---

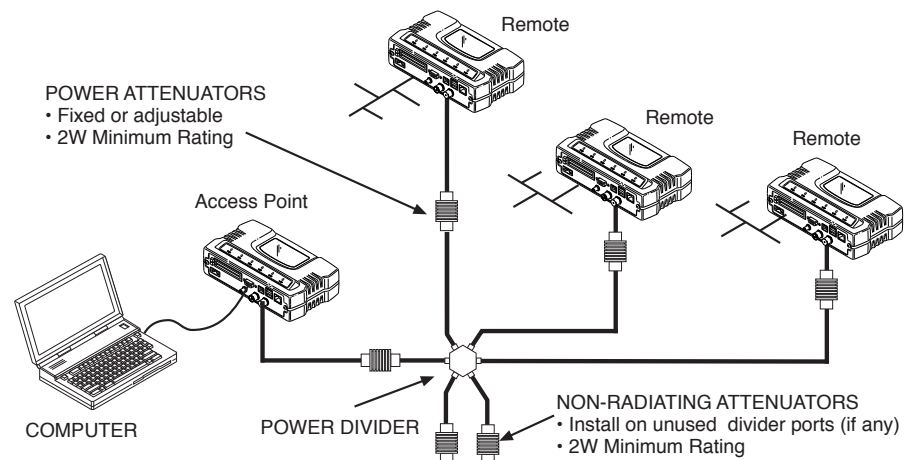
**NOTE:** It is important to use a □Network Name□ that is different from any currently in use in your area during the testing period.

---

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

## 2.2 STEP 1 □CONNECT THE ANTENNA PORTS

Figure 2-1 shows the tabletop arrangement. Connect the antenna ports of each transceiver as shown. This provides stable radio communications between each unit and prevents interference to nearby electronic equipment.



**Figure 2-1. Typical Setup for Tabletop-Testing of Radios**

---

**NOTE:** Use attenuation between all units in the test setup. The amount of attenuation required depends on the number of units tested and the desired signal strength (RSSI) at each transceiver during the test. In no case should a signal greater than  $-50$  dBm be applied to any transceiver in the test setup. GE MDS recommends an RF power output level of  $+20$  dBm from the AP. Remote power is not setable. (See [Radio Configuration Menu](#) on Page 58.)

---

## 2.3 STEP 2 CONNECT THE PRIMARY POWER

The primary power at the transceiver's power connector must be within  $10.5$ — $30$  Vdc and be capable of continuously providing 30 Watts. Typical power consumption for  $13.8$  Vdc and  $24$  Vdc operation are listed in [SPECIFICATIONS](#) on Page 162.

A Phoenix two-pole power connector with screw-terminals is provided with each unit. Strip the wire leads to  $6$  mm ( $0.25$ " ). Be sure to observe proper polarity with the positive lead (+) on the left and negative (−) on the right, as shown in [Figure 2-2](#).

---

**NOTE:** The transceiver typically requires about 30 seconds to power up, and might require several minutes to associate with another unit, if GPS is required for time synchronization.

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

---

**CAUTION**  
POSSIBLE  
EQUIPMENT  
DAMAGE

Only use the transceiver with negative-ground power systems. Make sure the polarity of the power source is correct.



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

## 2.4 STEP 3 □ CONNECT PC TO THE TRANSCEIVER

Connect a PC's Ethernet port to the LAN port using an Ethernet cross-over cable. The LAN LED should light. Alternatively, you can use a serial cable to connect to the COM1 port (Figure 2-3 on Page 25).

## 2.5 STEP 4 □ REVIEW TRANSCEIVER CONFIGURATION

### 2.5.1 Getting Started

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

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

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

### 2.5.2 Procedure

The following is a summary of the configuration procedure that must be done on each unit in the system. Key parameters are shown on the Embedded Management System overview (Figure 3-1 on Page 32). A lists of parameters is located in two tables □ Table 4-5 on Page 140 and Table 4-7 on Page 142. Detailed information on using the Management System can be found in *MS INTRODUCTION* on Page 31.

---

**NOTE:** The Management System supports the use of □ configuration files □ to help consistently configure multiple units. These are explained in *Configuration Scripts Menu* on Page 119.

---

### 2.5.3 Basic Configuration Defaults

Table 2-1 provides a selection of key operating parameters, their range, and default values. All of these are accessible through a terminal emulator connected to the COM1 serial port or through a Web browser connected to the LAN port (see Figure 5-1 on Page 149 for hookup).

---

**NOTE:** Access to the transceiver's Management System and changes to all parameters requires entering a security password.

---

**Table 2-1. Basic Configuration Defaults**

Item	Menu Location	Default	Values/Range
Network Name	Main Menu>> Radio Configuration>> Network Name	MDS-Mercury	¥ 1—15 alphanumeric characters ¥ Case-sensitive; can be mixed case
IP Address	Main Menu>> Network Configuration>> IP Address	192.168.1.1	Contact your network administrator
RF Output Power	Main Menu>> Radio Configuration>> Transmit Power	+30 dBm (1.0 Watt)	AP: -30 to +30 dBm RM: 0 to +30 dBm (Max. 1.0 Watt)
Unit Password	Main Menu>> Device Information>> User Password	admin (lower case)	¥ 1—13 alphanumeric characters ¥ Case-sensitive; can be mixed case

For benchtop evaluation, configure:

- ¥ **Frequency Mode** = Single Channel
- ¥ **Single Frequency Channel** = 0
- ¥ **RF Bandwidth** = 1.75
- ¥ **TDD Sync** = Free Run

For more information on configuring these parameters, see [□Frequency Control Menu□](#) on Page 60.

A unique IP address and subnet are required to access all IP-based management interfaces (telnet, SSH, SNMP, and Web), either through the LAN port or remotely over-the-air.

## 2.6 STEP 5 □ CONNECT LAN OR SERIAL DATA EQUIPMENT

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

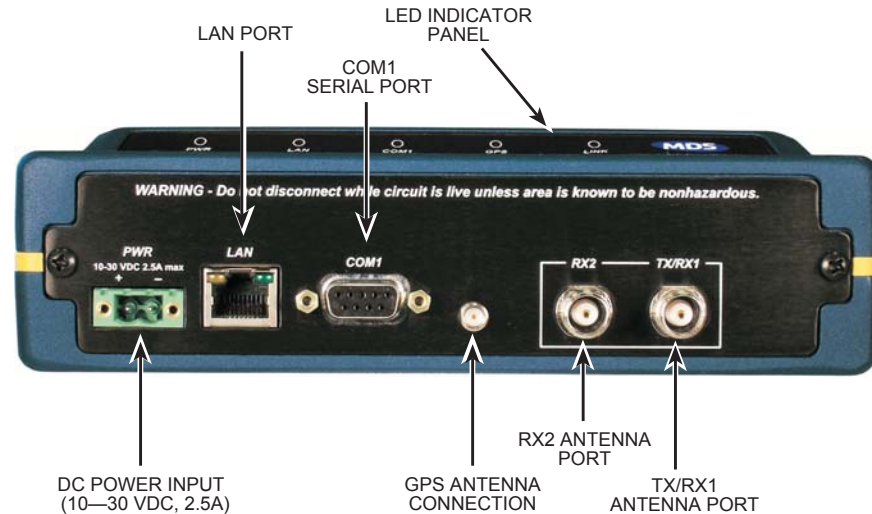
[Figure 2-3 on Page 25](#) shows the interface connectors on the front panel of the transceiver.

---

**NOTE:** The use of shielded Ethernet cable is recommended for connection to the radio □ETH port. The radio meets regulatory emission standards without shielded cable, but shielding reduces the possibility of interference in sensitive environments, and is in keeping with good engineering practice.

---





**Figure 2-3. Transceiver Interface Connectors**

- ⌘ **LED INDICATOR PANEL** □ Displays the basic operating status of the transceiver. Section 2.7 on page 26 contains detailed information.
- ⌘ **COM1 SERIAL PORT** □ DB-9 connector used for management of the transceiver using a connected PC. *MS INTRODUCTION on Page 31* provides complete connection details.
- ⌘ **LAN PORT** □ Connection point for Ethernet Local Area Network. The connector has integrated LEDs to indicate signal activity as follows: A steady green LED indicates that a link has been achieved; a flashing green LED indicates data activity; and a yellow LED indicates 100 Mbps operation.
- ⌘ **PWR** □ DC power connection for the transceiver. Power source must be 10 Vdc to 30 Vdc, negative ground, and capable of providing at least 25 watts.
- ⌘ **GPS ANTENNA PORT** □ Coaxial connector (SMA-type) for connection of a GPS receiving antenna. Provides 3.5 Vdc output for compatibility with powered (active) GPS antennas. Do not short this connector, as you might cause damage to the internal power supply. The GPS receiving antenna's gain must be 16 dBi or less.

---

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

- ⌘ **RX2 ANTENNA PORT** □ *Reserved for future functionality.* Coaxial connector (TNC-type) for attachment of a second 3650 MHz receiving antenna used in space diversity arrangements.
- ⌘ **TX/RX1 ANTENNA PORT** □ Coaxial connector (TNC-type) for attachment of the main station antenna (transmit and receive).

## 2.7 STEP 6 □ CHECK FOR NORMAL OPERATION

Once the data equipment is connected, you can check the transceiver for normal operation.

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

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

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



Figure 2-4. LED Indicator Panel

If the radio network seems to be operating properly based on observation of the unit's LEDs, use the **PING** command to verify the link integrity with the Access Point.

Table 2-2. Transceiver LED Functions

LED Label	Activity	Indication
PWR	ON	Primary power (DC) present
	Blinking	Unit in □Alarmed□ state
	OFF	Primary power (DC) absent
LAN*	ON	LAN detected
	Blinking	Data TX/RX
	OFF	LAN not detected, or excessive traffic present
COM1 (MGT System)	Blinking	Data TX/RX
	OFF	No data activity

**Table 2-2. Transceiver LED Functions (Continued)**

LED Label	Activity	Indication
GPS	ON	Internal GPS receiver is synchronized with the satellite network.
	Blinking	AP modem is synchronizing with the GPS timing.
	OFF	Internal GPS receiver is not synchronized with the satellite network.
LINK (Access Point)	ON	Default state
	OFF	Not transmitting. Usually occurs while waiting for GPS sync.
LINK (Remote)	ON	Associated to AP
	OFF	Not associated with AP

\* The LAN connector has two integrated LEDs to indicate signal activity as follows: A steady green LED indicates that a link has been achieved; a flashing green LED indicates data activity, and a yellow LED indicates 100 Mbps operation.





# 3 EMBEDDED MANAGEMENT SYSTEM

## Contents

3.1	MS INTRODUCTION.....	31
3.1.1	Differences in the User Interfaces .....	31
3.2	ACCESSING THE MENU SYSTEM .....	33
3.2.1	Methods of Control .....	34
3.2.2	PC Connection and Log In Procedures .....	34
3.2.3	Navigating the Menus .....	38
3.3	BASIC OVERVIEW OF OPERATION.....	40
3.3.1	Starting Information Screen .....	40
3.3.2	Main Menu .....	42
3.4	CONFIGURING NETWORK PARAMETERS .....	43
3.4.1	Network Configuration Menu .....	43
3.4.2	Ethernet Port Configuration Menu .....	51
3.4.3	Bridge Configuration .....	52
3.4.4	SNMP Agent Configuration .....	53
3.4.5	AP Location Push Config Menu .....	55
3.4.6	SNTP Server Configuration .....	57
3.5	RADIO CONFIGURATION .....	58
3.5.1	Radio Configuration Menu .....	58
3.5.2	Serial Port Configuration .....	67
3.6	MODBUS / TCP SERVER CONFIGURATION .....	80
3.6.1	Modbus/TCP in Mercury Transceivers□An Overview .....	80
3.6.2	Menu Selections .....	80
3.7	SECURITY CONFIGURATION MENU .....	85
3.7.1	Device Security Menu .....	86
3.7.2	Wireless Security Menu .....	87
3.7.3	IEEE 802.1x Device Authentication .....	89
3.7.4	Manage Certificates .....	91
3.8	REDUNDANCY CONFIGURATION (AP ONLY).....	93

3.9 GPS CONFIGURATION (REMOTE ONLY)..... 98

3.10 DEVICE INFORMATION MENU..... 100

3.11 PERFORMANCE INFORMATION MENU ..... 101

3.12 MAINTENANCE/TOOLS MENU..... 113

    3.12.1 Auto Firmware Upgrade Menu (AP Only) ..... 124

3.13 PERFORMANCE OPTIMIZATION ..... 127

3.13.1 Proper Operation□What to Look For ..... 129

## 3.1 MS INTRODUCTION

The transceiver's embedded management system is accessible through the COM1 (serial) port, the LAN (Ethernet) port, and using over-the-air Ethernet. Telnet, SSH, HTTP/HTTPS, and SNMP are the Ethernet-based interfaces. Essentially, the same capabilities are available through any of these paths.

For support of SNMP software, a set of MIB files is available for download from the GE MDS Web site at [www.GEmds.com](http://www.GEmds.com). An overview of SNMP commands can be found at *SNMP Agent Configuration* section on Page 53 of this manual.

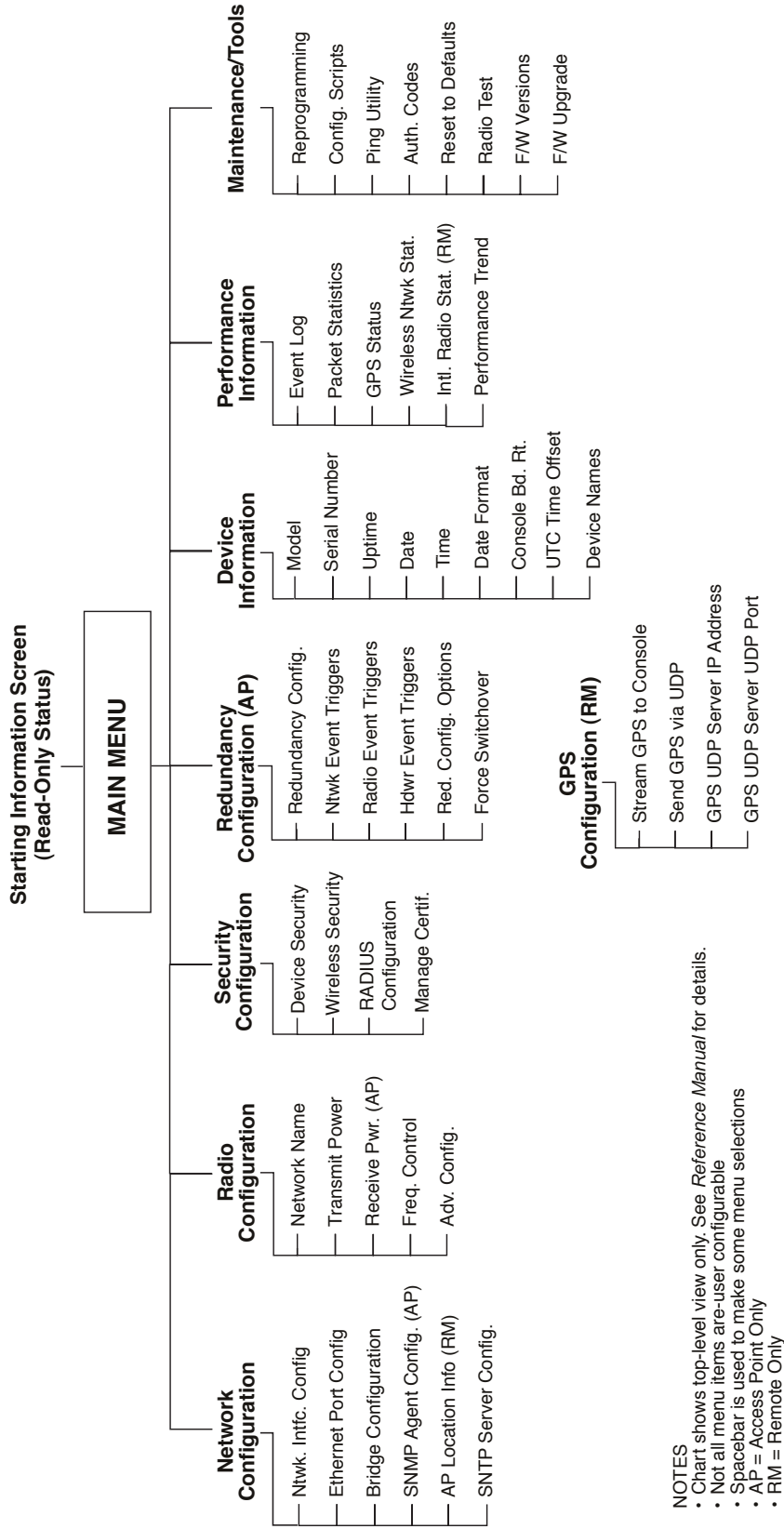
The transceiver's Management System and its functions are divided into seven functional groups as listed below.

- ¥ Section 3.3, *BASIC OVERVIEW OF OPERATION* (beginning on Page 40)
- ¥ Section 3.4, *CONFIGURING NETWORK PARAMETERS* (beginning on Page 43)
- ¥ Section 3.5, *RADIO CONFIGURATION* (beginning on Page 58)
- ¥ Section 3.7, *SECURITY CONFIGURATION MENU* (beginning on Page 85)
- ¥ Section 3.13, *PERFORMANCE OPTIMIZATION* (beginning on Page 127)
- ¥ Section 3.12, *MAINTENANCE/TOOLS MENU* (beginning on Page 113)

Each of these sections has a focus that is reflected in its heading. The section you are now reading provides information on connecting to the Management System, how to navigate through it, how it is structured, and how to perform top-level configuration tasks. [Figure 3-1 on Page 32](#) shows a top-level view of the Management System (MS).

### 3.1.1 Differences in the User Interfaces

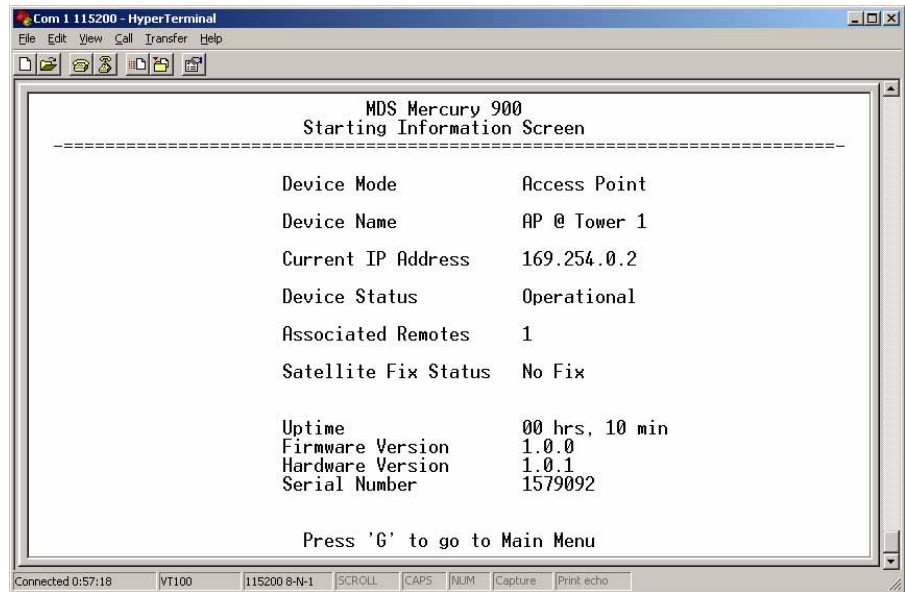
Although there are slight differences in navigation among the user interfaces, the content is very similar. You will notice a few differences in capabilities as the communications tool is driven by limitations of the access channel. [Figure 3-2](#) and [Figure 3-3 on Page 33](#) show examples of the Starting Information Screen as seen through a console terminal and a web-browser, respectively.



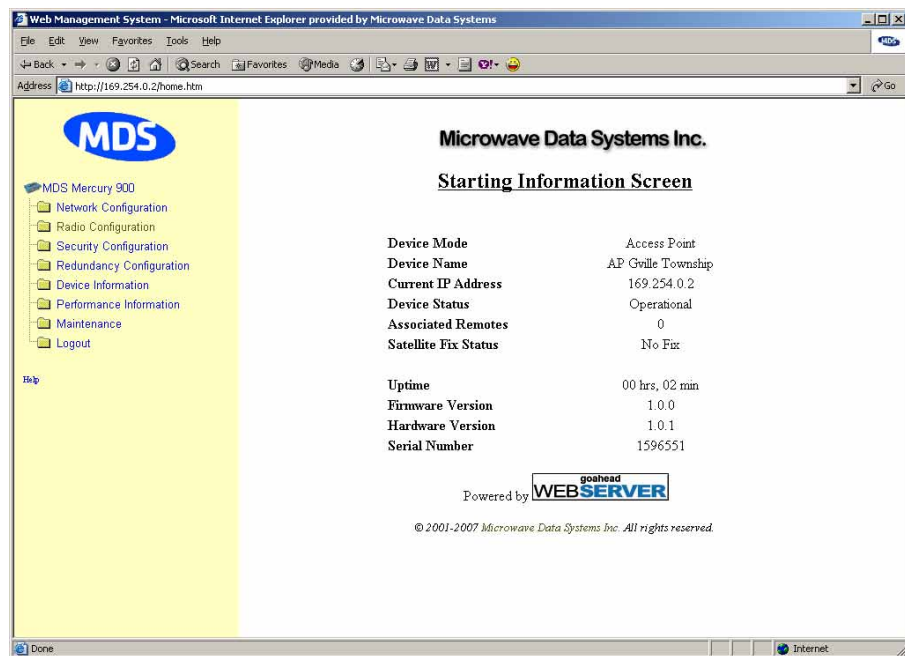
- NOTES
- Chart shows top-level view only. See *Reference Manual* for details.
  - Not all menu items are user-configurable
  - Spacebar is used to make some menu selections
  - AP = Access Point Only
  - RM = Remote Only

Figure 3-1. Embedded Management System Top-Level Flowchart





**Figure 3-2. View of MS with a text-based program**  
*(Console Terminal shown Telnet has similar appearance)*



**Figure 3-3. View of the MS with a Browser**  
*(Selections at left provide links to the various menus)*

## 3.2 ACCESSING THE MENU SYSTEM

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

### 3.2.1 Methods of Control

Access the unit's configuration menus in one of several ways:

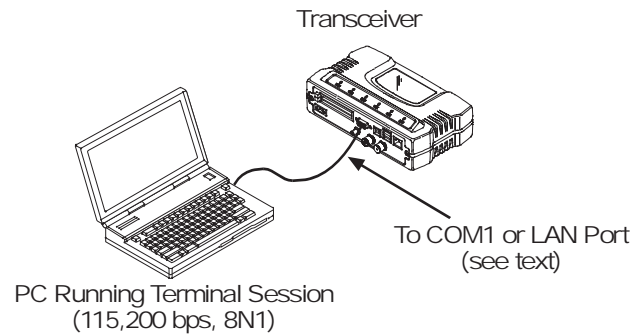
- ¥ **Local Console** □ *This is the primary method used for the examples in this manual.* Connect a PC directly to the COM1 port using a serial communications cable and launch a terminal communications program such as HyperTerminal (found on most PCs by selecting **Start>>Programs>>Accessories>>Communications>>HyperTerminal**). This method provides text-based access to the unit's menu screens. Console control is a hardware-based technique, and is intended for local use only (maximum recommended cable length of 50 ft./15 m).
- ¥ **Telnet or SSH\*** □ Connect a PC to the unit's LAN port, either directly or via a network, and launch a Telnet session. This method provides text-based access to the unit's menu screens in a manner similar to a Local Console session. You can run Telnet sessions locally or remotely through an IP connection.
- ¥ **Web Browser\*** □ Connect a PC to the unit's LAN port, either directly or via a network, and launch a web browser session (*for example*, Internet Explorer, Firefox, etc.). Enter the IP address of the device to be managed into the browser's address field.

This method provides a graphical representation of each screen, just as you would see when viewing an Internet web site. The appearance of menu screens differs slightly from other methods of control, but the content and organization of screen items is similar. Web browser sessions may be run locally or remotely using an IP connection.

\* When connecting directly to a radio, a *crossover* cable is required. When connecting using a network, switch, or router, a *straight-through* cable is required.

### 3.2.2 PC Connection and Log In Procedures

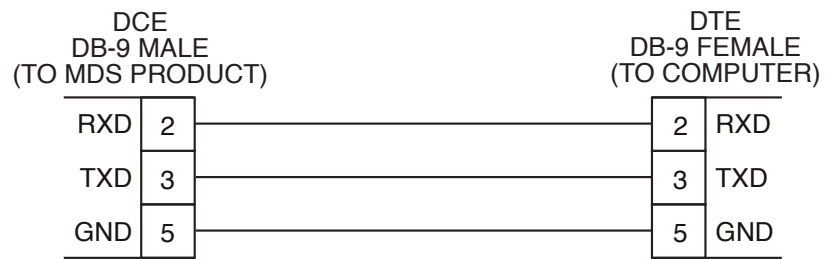
The following steps describe how to access the radio's menu system. These steps require a PC to be connected to the unit's COM1 or LAN port as shown in [Figure 3-4 on Page 35](#).



**Figure 3-4. PC Configuration Setup**

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

1. Connect a serial communications cable between the PC and the unit's COM1 port. If necessary, a cable may be constructed for this purpose as shown in [Figure 3-5](#).



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

2. Launch a terminal emulation program such as HyperTerminal and configure the program with the following settings:
  - ¥ 115,200 bps data rate
  - ¥ 8 data bits, no parity
  - ¥ One stop bit, and no flow-control
  - ¥ Use ANSI or VT100 emulation.

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

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

3. Press the **[ENTER]** key to receive the **login:** prompt.
4. Enter the username (default username is **admin**). Press **[ENTER]**.

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

---

**NOTE:** Passwords are case sensitive. Do not use punctuation mark characters. You may use up to 13 alpha-numeric characters.

---

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



**Figure 3-6. Starting Information Screen** □ **Local Console Session**

### **Starting a Telnet Session**

---

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

---

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

---

**NOTE:** When using Ethernet to access the unit, you might need to change your computer □s IP address to be on the same subnet as the radio. You can identify or verify the unit □s IP address by using a Local Console session to communicate with the radio through its COM1 Port and viewing the Starting Information Screen.

---

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

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

---

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

---

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

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

The unit responds with a Starting Information Screen (see [Figure 3-6 on Page 36](#)). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

---

**NOTE:** Passwords are case sensitive. Do not use punctuation mark characters. You may use up to 13 alpha-numeric characters.

---

### **Starting a Web Browser Session**

---

**NOTE:** Web access requires that you know the IP address of the unit you are connecting to. If you do not know the address, start a Local Console session (see [Starting a Local Console Session \(Recommended for first-time log-in\)](#) on Page 35) and access the Starting Information Screen. The IP address is displayed on this screen.

---

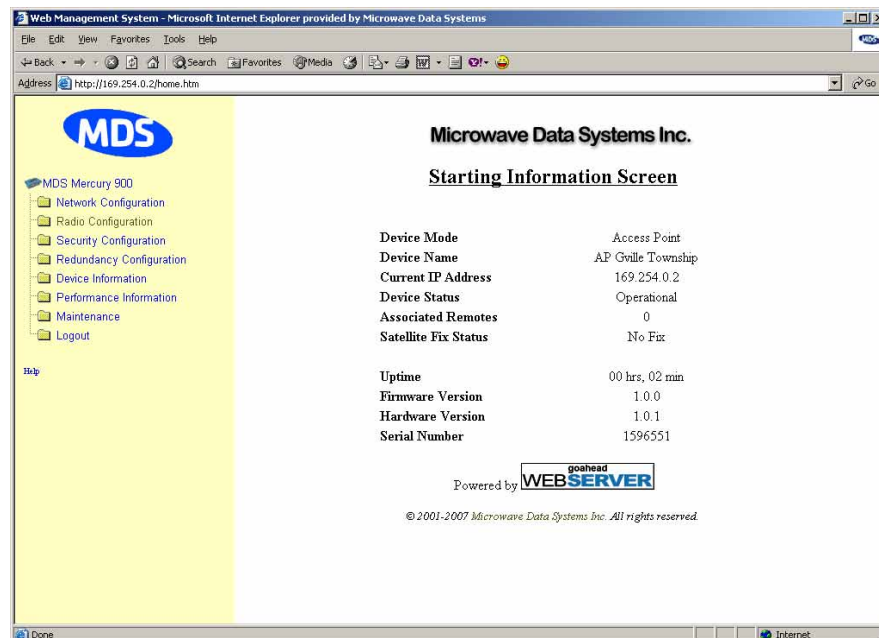
1. Connect a PC to the unit's LAN port, either directly or using a network. If connecting directly, use an Ethernet *crossover* cable; if connecting using a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.
2. Launch a Web-browser session on your computer (i.e., Internet Explorer, Firefox, etc.).
3. Type the unit's IP address and press **[ENTER]** .
4. A log-in screen is displayed ([Figure 3-7 on Page 38](#)) where you enter a user name and password to access the unit's menu system. Note that the default entries are made in *lower case*. (Default User Name: **admin**; Default Password: **admin**)



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

**NOTE:** Passwords are case sensitive. Do not use punctuation mark characters. You may use up to 13 alpha-numeric characters.

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



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

## 3.2.3 Navigating the Menus

### Via Terminal Telnet or SSH Sessions

*Recommended for first-time log-in*

Local Console, Telnet, and SSH sessions use multi-layered text menu systems that are nearly identical. To move further down a menu tree, you type the letter assigned to an item of interest. This takes you to an

associated screen where settings may be viewed or changed. In most cases, pressing the **[ESCAPE]** key moves the screen back one level in the menu tree.

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

---

**NOTE:** Early versions of PuTTY might not operate when using SSH to connect to the transceiver. The latest version (0.60 at the time of publication) does work with the transceiver's internal server. Both the latest released and the latest development snapshot can be downloaded from:  
[www.chiark.greenend.org.uk/~sgtatham/putty/](http://www.chiark.greenend.org.uk/~sgtatham/putty/)

---

When you arrive at a screen with user-controllable parameter fields, you select the menu item by pressing an associated letter on the keyboard. If there is a user definable value, the field will clear to the right of the menu item and you can type the value you wish to use. Follow this action by pressing the **[ENTER]** key to save the changes. If you make a mistake or change your mind before pressing the **[ENTER]** key, simply press **[ESCAPE]** to restore the previous value.

In some cases, when you type a letter to select a parameter, you will see a prompt at the bottom of the screen that says **Choose an Option**. In these screens, press the keyboard **[SPACEBAR]** to step through the available selections. When the desired option appears, press the **[ENTER]** key to choose that selection. In some cases, you can change several parameters and then save them with a single keystroke. Use the **[ESCAPE]** key to cancel the action and restore the previous values.

### **Logging Out Via Terminal Emulator or Telnet**

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

---

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

---

### **Navigating via Web Browser**

Navigating with a Web browser is straightforward with a framed **home** page. The primary navigation menu is permanently located on the left-hand side of this page. Simply click the desired menu item to make it active.

### **Logging Out Via Web Browser**

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

---

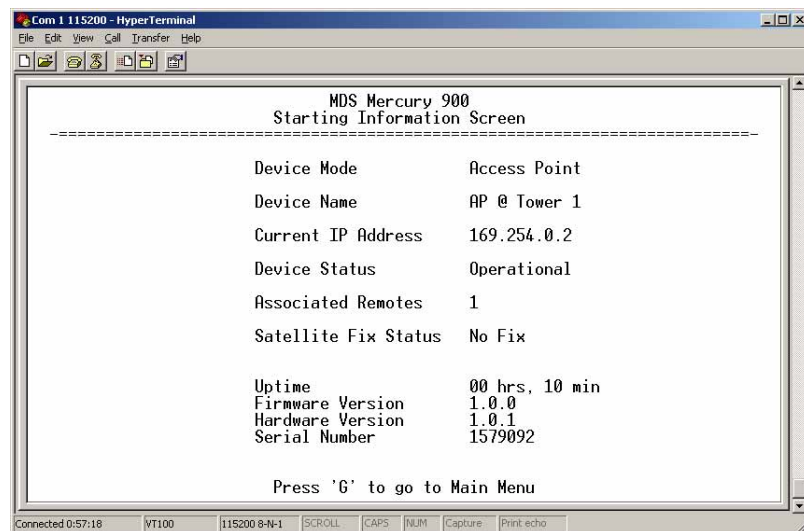
**NOTE:** In the menu descriptions that follow, parameter options/range, and any default values are displayed at the end of the text between square brackets. Note that the default setting is always shown after a semicolon: [available settings or range; default setting]

---

## 3.3 BASIC OVERVIEW OF OPERATION

### 3.3.1 Starting Information Screen

Once you have logged into the Management System, the Starting Information Screen (Figure 3-9) appears with an overview of the transceiver and its current operating conditions.



**Figure 3-9. Starting Information Screen**  
(AP screen shown; Remote similar, differences noted below)

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

*At Access Point:*

- ¥ **Operational** □ Unit operating normally.
- ¥ **Initializing** □ This is the first phase after boot-up.
- ¥ **Synchronizing** □ Unit is waiting for the GPS receiver to obtain a satellite fix and for its internal clock to synchronize to the GPS timing signals.



¥ **Alarmed** □ The unit is has detected one or more alarms that have not been cleared.

*At Remote:*

¥ **Scanning** □ The unit is looking for an Access Point beacon signal.

¥ **Ranging** □ Unit is adjusting power, timing, and frequency with an AP.

¥ **Connecting** □ The unit has found a valid beacon signal for its network.

¥ **Authenticating** □ Device is attempting device authentication.

¥ **Associated** □ The unit has successfully synchronized and associated with an Access Point.

¥ **Alarmed** □ The unit is has detected one or more alarms that have not been cleared.

---

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

---

¥ **Associated Remotes (AP Only)** □ Indicates the number of Remotes that have achieved association with the AP.

¥ **Connection Status (Remote Only)** □ Indicates whether the Remote has an RF connection with an AP.

¥ **Satellite Fix Status** □ Indicates whether internal GPS receiver has achieved synchronization with GPS satellite signals.

¥ **Uptime** □ Elapsed time since the transceiver was last booted up.

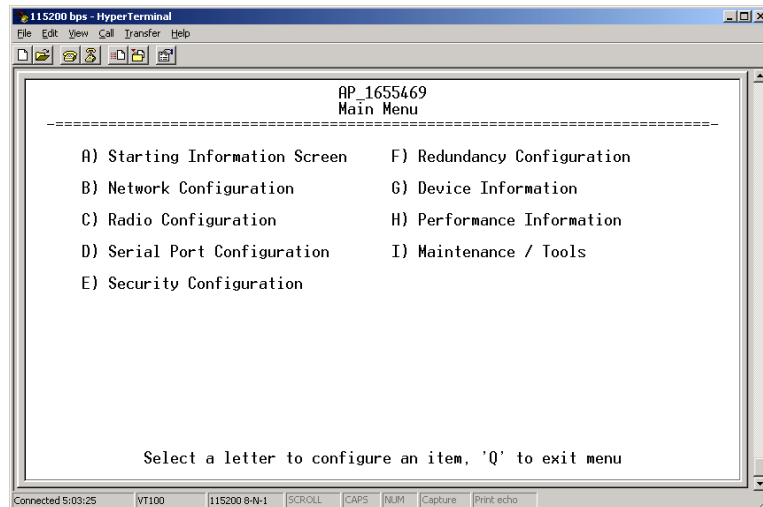
¥ **Firmware Version** □ Version of firmware that is currently active in the unit.

¥ **Hardware Version** □ Hardware version of the transceiver □s printed circuit board.

¥ **Serial Number** □ Make a record of this number. Provide this number when purchasing Authorization Codes to upgrade unit capabilities in the future. (See □*Authorization Codes*□ on Page 123.)

### 3.3.2 Main Menu

The Main Menu is the entry point for all user-controllable features. The transceiver **Device Name** appears at the top of this and all other screens as a reminder of the unit you are currently controlling.



**Figure 3-10. Main Menu (AP)**

(AP screen shown; Remote similar, differences noted below)

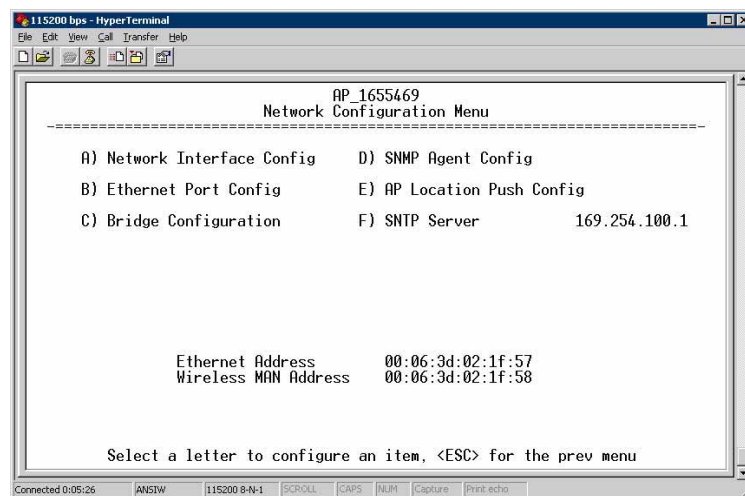
- ✂ **Starting Information Screen** □ Select this item to return to the Starting Information screen described above.
- ✂ **Network Configuration** □ Tools for configuring the data network layer of the transceiver. (See □ *CONFIGURING NETWORK PARAMETERS* □ on Page 43)
- ✂ **Radio Configuration** □ Tools to configure the wireless (radio) layer of the transceiver. (See □ *RADIO CONFIGURATION* □ on Page 58)
- ✂ **Serial Port Configuration** □ Menus for tailoring the COM1 port for data mode operation (data only). (See □ *Serial Port Configuration* □ on Page 67)
- ✂ **Security Configuration** □ Tools to configure the security services available with the transceiver's environment. (See □ *SECURITY CONFIGURATION MENU* □ on Page 85)
- ✂ **Redundancy Configuration** □ (AP Only) Allows setting of the criteria for switchover in the event of loss of associated Remotes or excessive packet receive errors.
- ✂ **GPS Configuration** □ (Remote Only) View/set parameters related to GPS streaming location output. (See □ *GPS CONFIGURATION (REMOTE ONLY)* □ on Page 98)
- ✂ **Device Information** □ Top level device fields such as model, serial number, date/time, etc. (See □ *DEVICE INFORMATION MENU* □ on Page 100)

- ¥ **Performance Information** □ Status information relating to the radio and data layer □ s performance in the radio network. (See □ *PERFORMANCE INFORMATION MENU* □ on Page 101)
- ¥ **Maintenance/Tools** □ Tools for upgrading firmware code and testing major unit capabilities. (See □ *MAINTENANCE/TOOLS MENU* □ on Page 113)

## 3.4 CONFIGURING NETWORK PARAMETERS

### 3.4.1 Network Configuration Menu

The *Network Configuration Menu* is the home of several parameters that you should review and set as necessary before placing a transceiver into service.



**Figure 3-11. Network Configuration Menu**

- ¥ **Network Interface Config** □ Presents a menu where you can view or set various parameters (VLAN Status, IP Configuration, and DHCP Server Configuration).
- ¥ **Ethernet Port Config** □ Presents a menu for defining the status of the Ethernet port (enabled or disabled), port follows association, and Ethernet filtering configuration. Detailed explanations of this menu are contained in *Ethernet Port Configuration Menu* on Page 51.
- ¥ **Bridge Configuration** □ View/set options for Ethernet Bridge operation.
- ¥ **SNMP Agent Config** □ View/set SNMP configuration parameters. See □ *SNMP Agent Configuration* □ on Page 53 for more information.

- ¥ **AP Location Push Config** □ Presents a submenu for configuring an AP to automatically force connected remotes to receive the AP Locations file from the AP. See □ *AP Location Push Config Menu* □ on Page 55 for details.
- ¥ **SNTP Server** □ Address of SNTP server (RFC 2030) from which the transceiver will automatically get the time-of-day. You can also manually set the date and time. A Mercury unit tries to get the time and date from the SNTP server only if an IP address is configured. It will continue to retry every minute until it succeeds.

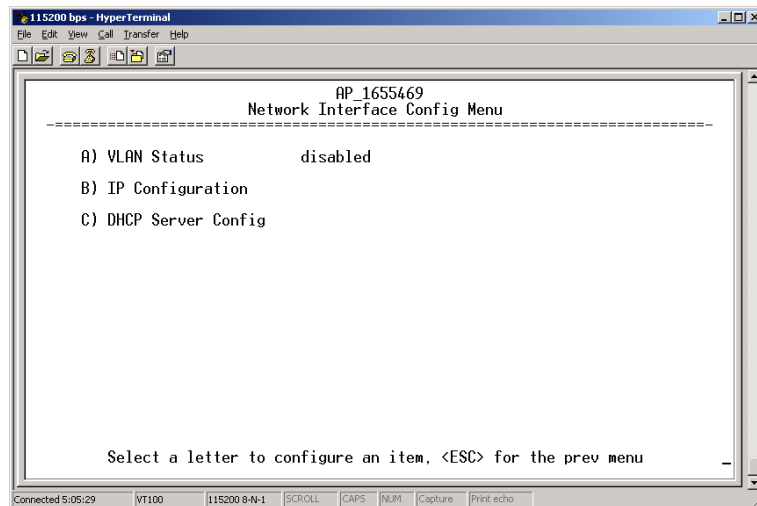
The transceivers use UTC (Universal Time Coordinated) with a configurable time offset. [0]

---

**NOTE:** The Mercury gets time of day data from the GPS receiver if the receiver gets a satellite fix.

---

### Network Interface Configuration Submenu



**Figure 3-12. Network Interface Configuration Submenu**

- ¥ **VLAN Status** □ This selection is used to enable or disable virtual LAN operation. For details, refer to *VLAN Configuration Menu* on Page 45. [enable, disabled; disabled]
- ¥ **IP Configuration** □ This selection presents a submenu for configuring the local IP address of the transceiver. Detailed explanations are provided in the section titled *IP Configuration Menu* on Page 50.
- ¥ **DHCP Server Config** □ Menu for configuration of DHCP services by the Access Point. DHCP provides □ on-the-fly □ IP address assignments to other LAN devices, including Mercury Series units. For details, refer to *DHCP Server Configuration (Data and Mgmt)* on Page 48.

## VLAN Configuration Menu

The VLAN Configuration menu (Figure 3-13) becomes active and visible when you enable **VLAN Status** on the Network Interface Configuration Menu, and you press the Enter key.

---

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

---

### **About Virtual LAN in Mercury**

A VLAN is essentially a limited broadcast domain, meaning that all members of a VLAN receive broadcast frames sent by members of the same VLAN but *not* frames sent by members of a different VLAN. For more information, refer to the IEEE 802.1Q standard.

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

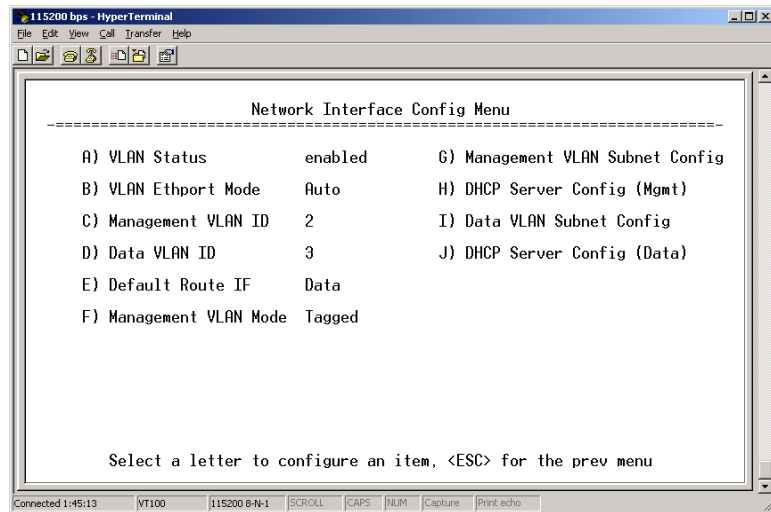
The Ethernet port of an Access Point radio is normally configured as a trunk port. This type of port expects incoming frames to have a **VLAN ID** tag and sends outgoing frames with a VLAN tag as well.

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

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

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

## Network Interface Configuration Menu □ VLAN Items

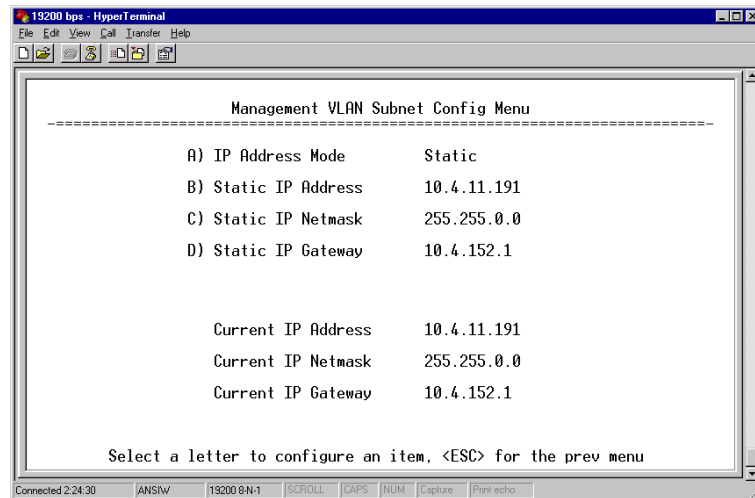


**Figure 3-13. VLAN Configuration Menu**

- ¥ **VLAN Status** □ Defines whether the radio handles Ethernet frames in □ extended □ 802.1Q mode or in □ normal □ mode in the Ethernet port. If configured with a trunk port, the Mercury passes all tagged traffic regardless of the VLAN ID. The Mercury only uses the **Data VLAN ID** parameter when the ETH port is configured as an Access Port.  
**[enabled, disabled; disabled]**
- ¥ **VLAN Ethport Mode** □ Defines if the Ethernet port acts as a trunk port or as an access port. Auto mode defines the port as a trunk port in an AP, or an access port in a Remote radio.  
**[Auto, Trunk, Access; Auto]**
- ¥ **Management VLAN ID** □ Defines the VLAN ID for traffic directed to the radio itself, other than the terminal server process. This VLAN ID is used for filtering and for tagging purposes.  
**[1-4094; 2]**
- ¥ **Data VLAN ID** □ Defines the VLAN ID assigned to traffic directed to and from the Ethernet port and the terminal server process in the radio. This VLAN ID is used for filtering and tagging purposes. **[1-4094; 3]**
- ¥ **Default Route IF** □ Defines the VLAN that contains the default gateway in the radio. **[MGMT, DATA; MGMT]**
- ¥ **Management VLAN Mode** □ Applies the VLAN tag to management frames. **[Tagged, Native; Tagged]**.
- ¥ **Management VLAN Subnet Config** □ Presents a screen where you can set the IP Address Mode, Static IP Address, and Static IP Netmask (see [Figure 3-14 on Page 47](#)).
- ¥ **DHCP Server Config (Mgmt)** □ Presents a screen where you can view or set the DHCP server status and address information for management functions (see [Figure 3-15 on Page 48](#)).

- ¥ **Data VLAN Subnet Config** □ Presents a screen where you can view or set the IP mode and address information (see [Figure 3-17 on Page 49](#)).
- ¥ **DHCP Server Config (Data)** □ Presents a screen where you can view or set DHCP server status and address information for data functions (see [Figure 3-16 on Page 49](#)).

### **Management VLAN Subnet Configuration Menu**



**Figure 3-14. Management VLAN Subnet Configuration Menu**

**NOTE:** Changes to any of the following parameters while communicating over the network (LAN or over-the-air) might cause a loss of communication with the unit you are configuring. You must re-establish communication using the new IP address.

- ¥ **IP Address Mode** □ Defines the source of the IP address of this device. Only static IP addressing mode is available when VLAN Status is enabled. [**Static, Dynamic; Static**]
- ¥ **Static IP Address** □ The IPv4 local IP address. [**192.168.1.1**]
- ¥ **Static IP Netmask** □ The IPv4 local subnet mask. This value is used when the radio attempts to send a locally initiated message, either from the terminal server, or from a management process. [**255.255.0.0**]

The lower three lines of the screen (**Current IP Address**, **Current IP Netmask**, **Current IP Gateway**) show the current addressing configured at the transceiver. **Current IP Gateway** only displays on this screen if **Default Route IF** on the **Network Interface Config** menu ([Figure 3-13 on Page 46](#)) is set to **Management**.

Selecting option I from the menu in [Figure 3-13 on Page 46](#) displays the screen shown in [Figure 3-17 on Page 49](#). Note that the IP address is different even though it is the same physical unit. This is because this IP address is defined for a different VLAN.

## DHCP Server Configuration (Data and Mgmt)

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

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

---

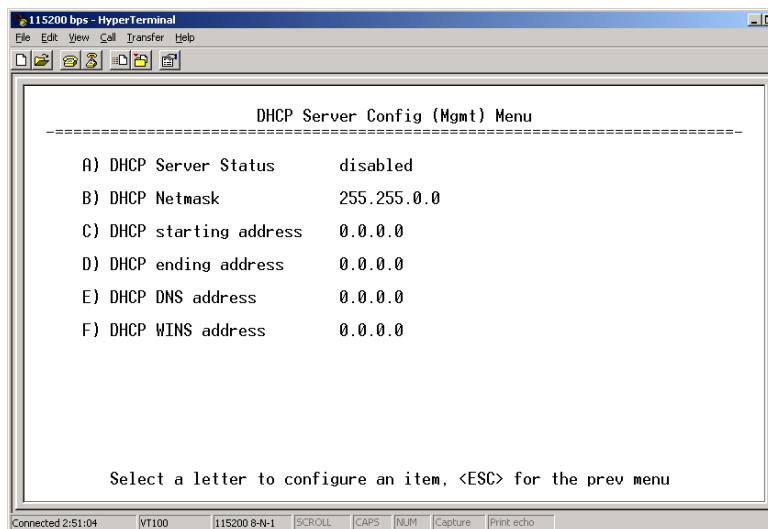
**NOTE:** There should be only one active DHCP server in a network. If more than one DHCP server exists, network devices might randomly get their IP address from different servers every time they request one.

---

**NOTE:** Combining DHCP and IEEE 802.1x device authentication might result in a non-working radio if the DHCP server is located at a Remote radio. If possible, place the DHCP server at the AP location.

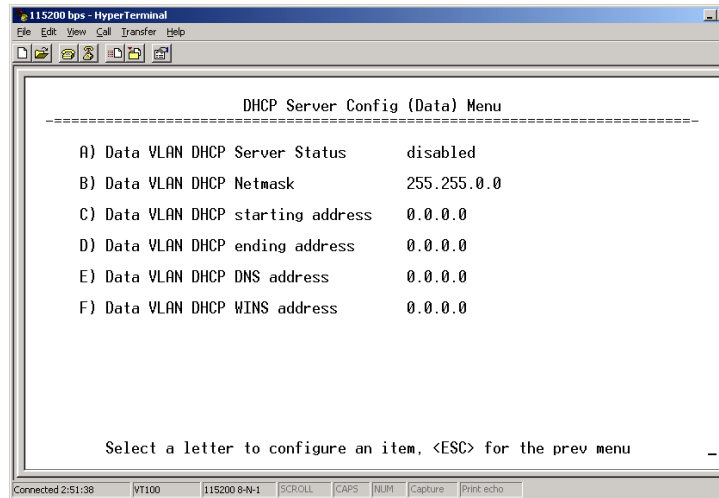
A DHCP server can be run at a Remote, but it is not recommended if 802.1x Device Authentication is in use and if the AP gets its IP address from the DHCP server on the Remote. In this case, the Remote cannot authenticate to allow the AP to get its address, because the AP needs an address to perform 802.1x device authentication. This results in an unsolvable condition where the AP needs to get an IP address from DHCP at the Remote, but it can't get the address until it is authenticated.

---



**Figure 3-15. DHCP Server Configuration (Mgmt) Menu**

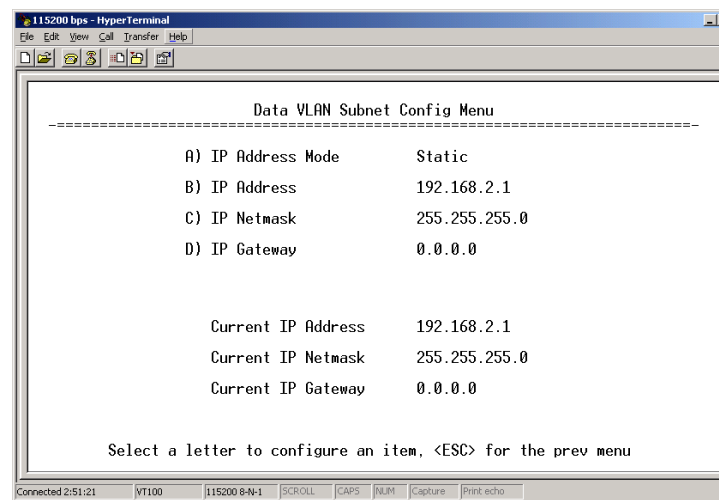




**Figure 3-16. DHCP Server Configuration (Data) Menu**

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

### **Data VLAN Subnet Configuration Menu**

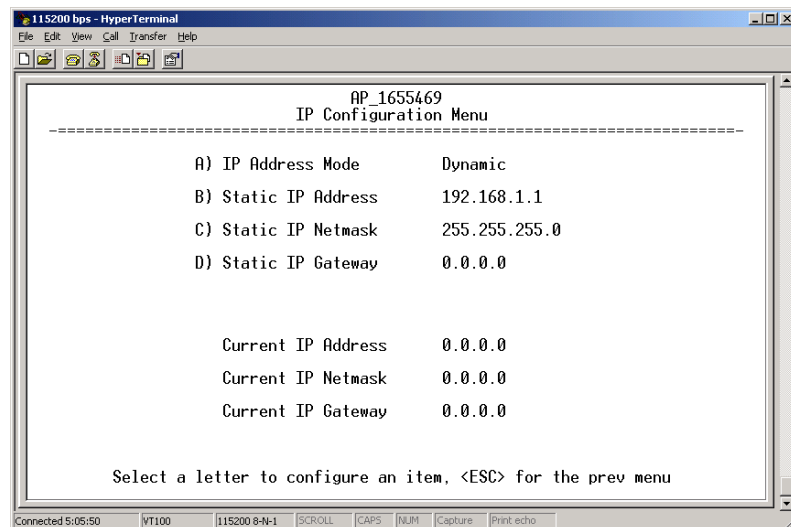


**Figure 3-17. Data VLAN Subnet Configuration Menu**

- ¥ **IP Address Mode** □ Defines the source of this device's IP address. Only static IP addressing mode is available when VLAN Status is enabled [**Static; Static**]
- ¥ **IP Address** □ The IPv4 local IP address. [**192.168.1.1**]
- ¥ **IP Netmask** □ The IPv4 local subnet mask. This value is used when the radio attempts to send a locally initiated message, from either the terminal server or the management process. [**255.255.0.0**]
- ¥ **IP Gateway** □ The IPv4 address of the default gateway device, typically a router. [**0.0.0.0**]

The lower three lines of the screen (**Current IP Address**, **Current IP Netmask**, and **Current IP Gateway**) show the current addressing configured at the transceiver. **Current IP Gateway** only displays on this screen if **Default Route IF** on the **Network Interface Config** menu (Figure 3-13 on Page 46) is set to **Data**.

## IP Configuration Menu



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

---

**CAUTION:** Changes to 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 must re-establish communication using the new IP address.

---

- ¥ **IP Address Mode** □ Defines the source of this device's IP address. [**Static, Dynamic; Static**]
- ¥ **Static IP Address** (*User Review Recommended*) □ Essential for connectivity to the transceiver's MS using the LAN port. Enter any valid IP address that is unique within the network. This field is unnecessary if DHCP is enabled. [**192.168.1.1**]

- ⌘ **Static IP Netmask** □ The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled. [255.255.0.0]
- ⌘ **Static IP Gateway** □ The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled. [0.0.0.0]

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

### 3.4.2 Ethernet Port Configuration Menu

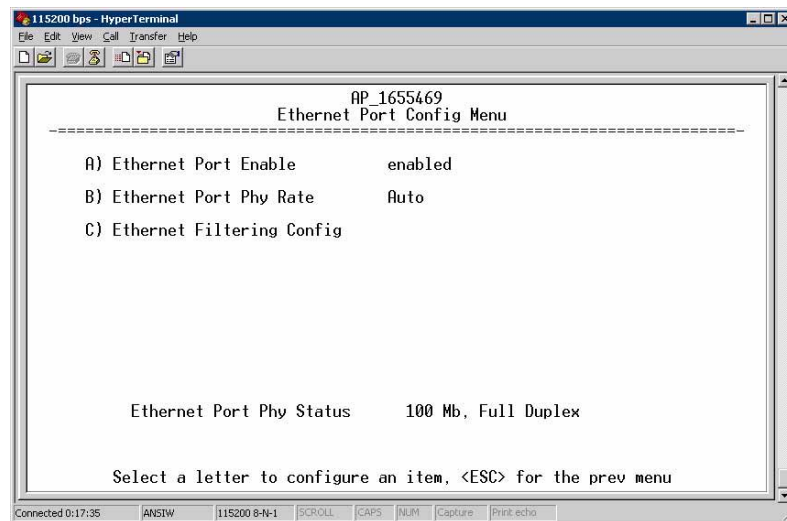
The transceiver allows for special control of the Ethernet interface, to allow traffic awareness and availability of the backhaul network for redundancy purposes.

---

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

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

---

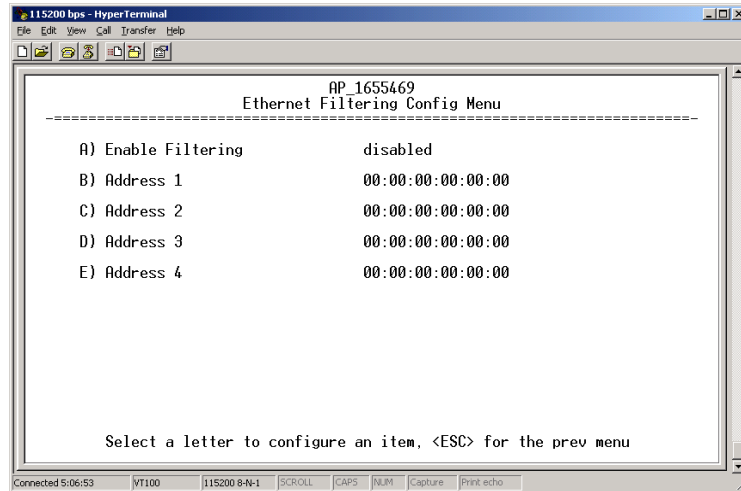


**Figure 3-19. Ethernet Port Configuration Menu**

- ⌘ **Ethernet Port Enable** □ Allows enabling/disabling Ethernet traffic for security purposes. Setting it to **enabled** enables the port. [enabled, disabled; enabled]
- ⌘ **Ethernet Port Phy Rate** □ The Ethernet port's configured speed.
- ⌘ **Eth Port Follows Association (Remote Only)** □ When enabled, the Ethernet port is disabled when not associated. [enabled, disabled; disabled]

¥ **Ethernet Filtering Config** □ Allows enabling/disabling filtering and specifying of Ethernet addresses.

### Ethernet Filtering Configuration Menu

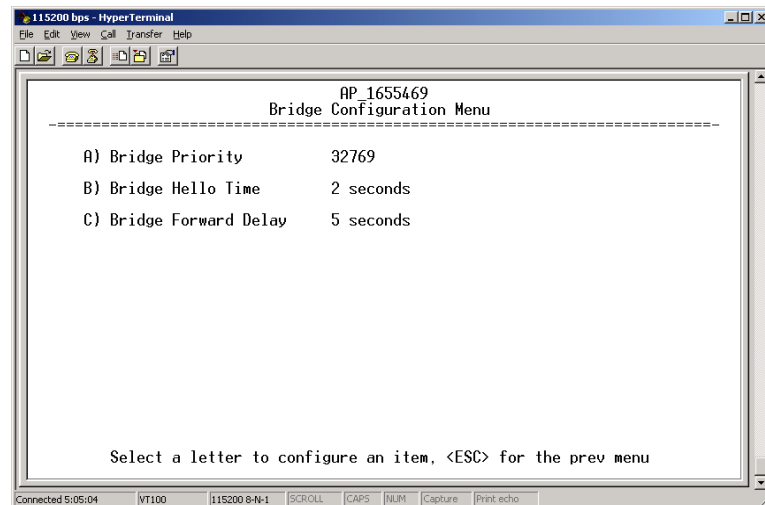


**Figure 3-20. Ethernet Filtering Configuration Menu**

¥ **Enable Filtering** □ Activates Ethernet filtering.  
[enabled, disabled; disabled]

¥ **Address 1, 2, 3, 4** □ Ethernet address fields. When filtering is enabled, the Mercury only accepts traffic on its Ethernet port from the configured addresses.  
[Valid IP address string]

### 3.4.3 Bridge Configuration



**Figure 3-21. Bridge Configuration Menu**

¥ **Bridge Priority** □ View/set the priority of the bridge in the spanning tree. [0-65535; 32769]

- ¥ **Bridge Hello Time** □ View/set spanning tree hello time. This parameter affects how often the bridge sends a spanning tree Bridge Protocol Data Unit (BPDU). [1-10 seconds; 2 seconds]
- ¥ **Bridge Forward Delay** □ View/set spanning tree forwarding delay. Affects how long the bridge spends listening and learning after initialization. [4-30 seconds; 5 seconds].

### 3.4.4 SNMP Agent Configuration

The transceiver contains over 100 custom SNMP-manageable objects as well as the IETF standard RFC1213 for protocol statistics, also known as MIB II. You can use off-the-shelf SNMP managers to access the transceiver's SNMP Agent's MIB, such as Castle Rock Computing *SNMPc* and Hewlett Packard *OpenView*. The transceiver's SNMP agent supports SNMPv1, v2, and v3.

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

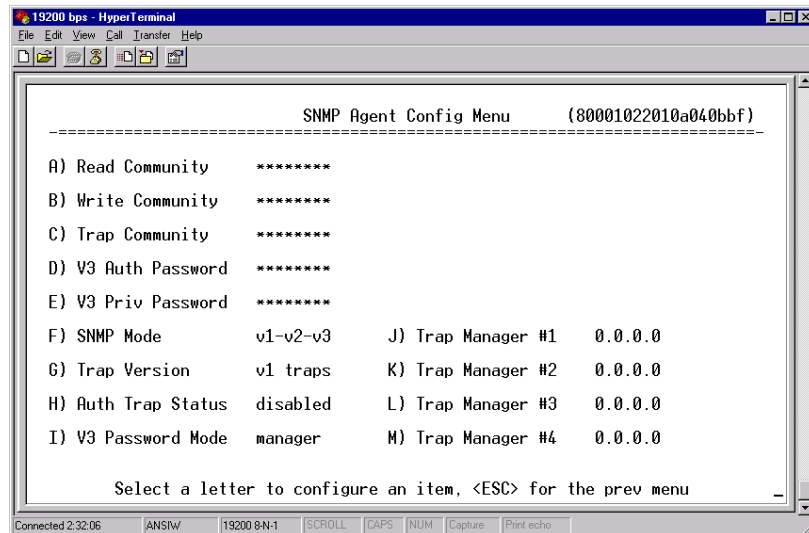
- ¥ **msdreg.mib** □ MDS sub-tree registrations
- ¥ **mds\_comm.mib** □ MDS Common MIB definitions for objects and events common to the entire product family
- ¥ **mercury\_reg.mib** □ MDS sub-tree registrations
- ¥ **mercurytrv1.mib** □ SNMPv1 enterprise-specific traps
- ¥ **mercurytrv2.mib** □ SNMPv2 enterprise-specific traps
- ¥ **mercury\_comm.mib** □ MIB definitions for objects and events common to the entire Mercury Series
- ¥ **mercury\_ap.mib** □ MIB definitions for objects and events for an Access Point transceiver
- ¥ **mercury\_rem.mib** □ Definitions for objects and events for a Remote radio
- ¥ **mercury\_sec.mib** □ For security management of the radio system

---

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

In addition, some management systems might require that you compile the MIB files in the order shown above.

---



**Figure 3-22. SNMP Server Configuration Menu**

This menu provides configuration and control of vital SNMP functions.

- ⌘ **Read Community String** □ SNMP community name with SNMPv1/SNMPv2c read access. This string can contain up to 30 alpha-numeric characters.
- ⌘ **Write Community String** □ SNMP community name with SNMPv1/SNMPv2c write access. This string can contain up to 30 alpha-numeric characters.
- ⌘ **Trap Community String** □ SNMP community name with SNMPv1/SNMPv2c trap access. This string can contain up to 30 alpha-numeric characters.
- ⌘ **V3 Authentication Password** □ Authentication password stored in flash memory. This is used when the Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for Authentication (currently, only MD5 is supported). This string can contain up to 30 alpha-numeric characters.
- ⌘ **V3 Privacy Password** □ Privacy password stored in flash memory. Used when the SNMP Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for privacy (DES encryption). This string can contain between 8 and 30 alpha-numeric characters.
- ⌘ **SNMP Mode** □ This specifies the mode of operation of the radio □ s SNMP Agent. The choices are: **disabled**, **v1\_only**, **v2\_only**, **v3\_only**, **v1-v2**, and **v1-v2-v3**. If the mode is **disabled**, the Agent does not respond to any SNMP traffic. If the mode is **v1\_only**, **v2\_only**, or **v3\_only**, the Agent responds only to that version of SNMP traffic. If the mode is **v1-v2** or **v1-v2-v3**, the Agent responds to the specified version of SNMP traffic. [**v1-v2-v3**]