System Guide

Microwave Data Systems Inc.

MDS *entra*NET

Access Point

Serial Remote

Ethernet Remote

Wireless IP/Ethernet Transceivers

Firmware Release 1.x

MDS 05-4055A01, Rev. A (PRELIMINARY)
April 2003

industrial/wireless/performance

Contents

5 PLANNING AN MDS iNET 900 NETWORK

Copyright Notice

ISO 9001 Registration

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

Related Documentation

Installer Guide—The associated MDS *entra*NET 900 Installer Guide, P/N 05-xxxxA01 (pending), is provided with the transceiver and is limited to essential information for installers. It assumes a basic level of understanding of the material in this manual, including antenna selection, the use of radio communication site survey tools and techniques, and network design.

Related Materials on the Internet—Data sheets, frequently asked questions, case studies, application notes, firmware upgrades and other valuable information are available on the MDS Web site at www.microwavedata.com.

About Microwave Data Systems Inc.

Almost two decades ago, MDS began building radios for business-critical applications. Since then, we've installed more than 500,000 radios in over 110 countries. To succeed, we overcame impassable terrain, brutal operating conditions and disparate, complex network configurations. We also became experts in wireless communication standards and system applications worldwide. The result of our efforts is that today, thousands of utilities around the world rely on MDS-based wireless networks to manage their most critical assets.

The majority of 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, under an ISO 9001 registered quality system which allows us to control and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, MDS is the wireless leader in industrial automation—including oil and gas production and transportation, water/wastewater treatment, supply and transportation, electric transmission and distribution and many other utility applications. MDS is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for 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 MDS. We'll always put the performance of your network above all. Visit us at www.microwavedata.com for more information.

Manual Revision and Accuracy

While every reasonable effort has been made to ensure the accuracy of this manual, product improvements may result in minor differences between the manual and the product shipped to you. If you have additional questions or need an exact specification for a product, please contact our Customer Service Team using the information at the back of this guide. In addition, manual updates can often be found on the MDS Web site at www.microwavedata.com.

OPERATIONAL & SAFETY NOTICES

RF Exposure

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

CSAus Notice (Approval Pending)

This product is suitable for use in Class I, Division 2, Groups A, B, C and D or non-hazardous locations only.

The transceiver has been recognized for use in these hazardous locations by the Canadian Standards Association (CSA). The CSA certification for the transceiver is as a Recognized Component for use in these hazardous locations, in accordance with CSA STD C22.2 No. 213-M1987.

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 must be in accordance with the transceiver's instruction 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 MDS must be used.

WARNING

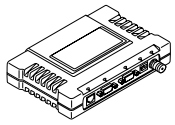
EXPLOSION HAZARD!

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

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

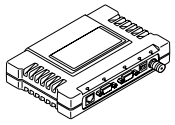
FCC Part 15 Notice

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



1 PRODUCT OVERVIEW AND APPLICATIONS

Contents



1.1 PRODUCT DESCRIPTION

This manual presents installation and operating instructions for the MDS entraNET 900 system. It is for use by *professional installers* who are expected to install, operate, and perform basic maintenance on the system.

The MDS entraNET 900 system is an easy-to-install wireless solution that supports long range Serial and Ethernet data transmission at speeds up to 115.2 kbps. The system includes an Access Point transceiver (AP) and two types of Remote transceivers—Serial or Ethernet. These units serve a variety of network configurations. Figure 1-1 shows each model of the entraNET family.

Figure 1-1. MDS entraNET 900 Transceivers

Rugged Packaging

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

Simple Installation

Basic installation typically employs an omni-directional antenna at the Access Point location and a directional antenna at each associated Remote. The antenna is a vital link in the system and must be chosen and installed correctly. Refer to *INSTALLATION* on Page 103 for guidance on choosing proper sites and antennas.

For basic services, you simply hook up an antenna, connect your Ethernet LAN to the transceiver's LAN port, apply primary power, check and set a few operating parameters as necessary and you are done. No license is required for operation in the U.S.A., Canada, and many other countries.

Secure Operation

Data network security is a vital issue in today's wireless world. The MDS entraNET's design provides 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 spread-spectrum transmission; other techniques include data encryption, enabling/disabling remote access channels, and password protection.

Remember, security is not a one-step process that can be simply turned on and forgotten. It must be practiced and enforced at multiple levels, 24 hours-a-day and 7 days-a-week. Section 1.4 on Page 10 contains additional information about entraNET's security tools.

Robust Radio Operation

The transceivers are designed for frequency-hopping spread-spectrum operation in the license-free 900 MHz band. They can provide reliable communications up to distances of 30 miles (50 km) or more under favorable conditions. The units employ digital signal processing (DSP) techniques for high performance operation, even in the presence of weak signals or interference.

Flexible Services

Users with a mixture of equipment having Ethernet and serial data interfaces can choose a combination of both types of remotes on the same cell or Access Point. This flexibility allows the transceiver to provide services in data networks that are on a path from legacy serial/EIA-232-based hardware to the faster and more easily interfaced Ethernet world.

Flexible Management

Configuration, commissioning, troubleshooting and other maintenance activities can be done locally or remotely. Four different modes of access are available: local RS-232 console, local or remote IP access through Telnet, web browser access, and via SNMP. The text-based interfaces (RS-232 console and Telnet) are implemented in the form of easy-to-follow menus, and the terminal server configuration includes a "wizard" to help you set up the units correctly.

Transceiver Features

The MDS entraNET 900's design makes the installation and configuration easy, while allowing for changes in the future.

- Long Range—30 miles (50 km) over favorable terrain, with sufficient antenna height in a point-to-multipoint configuration
- Industrial-Grade Product—Extended temperature range for trouble-free operation in extreme environments
- Robust Radio Communications—Designed to operate in high-interference environments
- Robust Network Security—Prevents common attack schemes and hardware from gaining access or control of network. Common attack events are logged and reported by alarms.
- Fast, 115.2 kbps data speed—Much faster than 9.6 kbps radios
- Plug-and-Play Connectivity—Ethernet bridge configuration option requires very little setup
- Serial Ports—Gateway for serial interface based equipment to IP/Ethernet networks with embedded terminal server

1.1.1 Model Offerings

The MDS entraNET 900 comes in two primary models—an Access Point and a Remote. In addition, two types of Remotes are available—an Ethernet Remote, and a Serial Remote. Table 1-1 summaries the different interface abilities for each type.

An Ethernet remote will serve only one MAC address, even if a bridge or hub is used.

Table 1-1. MDS entraNET 900 Models and Data Interface Services

Model	ETH[1]	COM1[1]	COM2
Access Point	Yes	Yes	Yes
Ethernet Remote	Yes	Yes	No
Serial Remote	No	--	Yes

NOTES

1. Provides access to the embedded Management System only. No data transfer capability.

1.2 APPLICATIONS

The following sections give descriptions of typical entraNET installations. Most installations will require planning by a network manager.

1.2.1 Long Range Wireless LAN

The wireless LAN is the most common application of the entraNET 900 system. It consists of a central control station (Access Point) and one or more associated Remote units, as shown in Figure 1-2 on Page 6. 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 it is connected to.

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

A Remote transceiver can only talk over-the-air to an Access Point (AP) unit. Peer-to-peer communications between Remotes can only take place indirectly through the AP. An AP can only talk over-the-air to Remote units, however two APs can communicate with each other through their Ethernet connectors utilizing a common LAN/WAN.

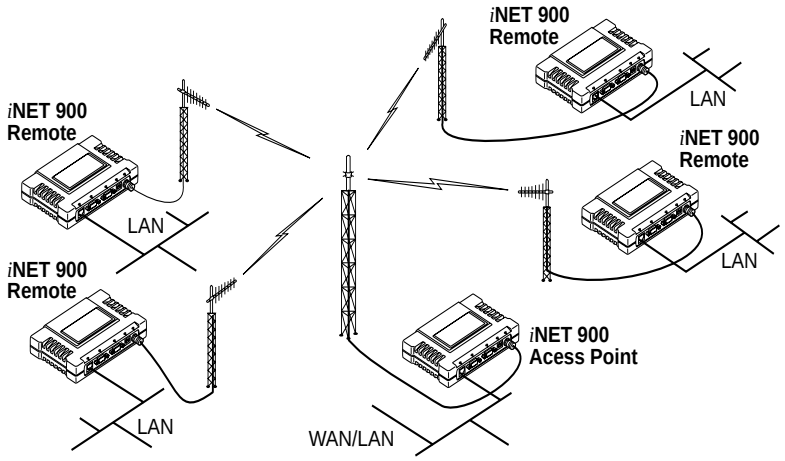


Figure 1-2. Typical wireless LAN

1.2.2 Multiple Protocols and/or Services

Prior to the introduction of the entraNET 900, two radios were often required to service two different types of devices (typically connected to different SCADA hosts). An entraNET 900 provides this functionality through a single AP radio. Each of the two groups of remote radios 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 1-3 on Page 6.

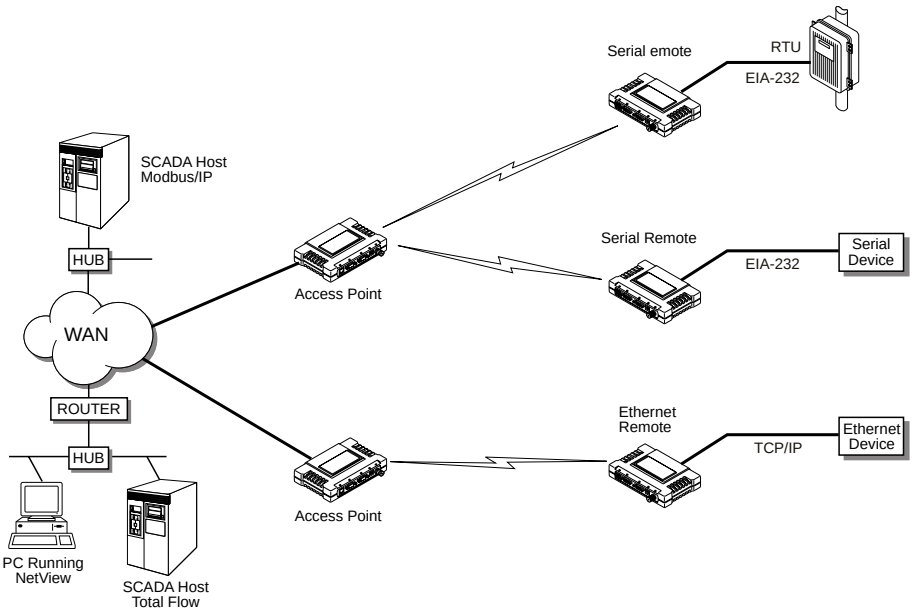


Figure 1-3. Multiple Protocol Network

By using a single AP the cost of infrastructure deployment is cut in half, with only one antenna, one feedline, and one lightning protector required. Other cost reductions come from the system as a whole,

including reduced management requirements via the MDS NETview MS application. Finally, entraNET offers a nearly unlimited potential for future applications that run over IP and Ethernet.

1.2.3 Upgrading Older Wireless Network with Serial Interfaces

Millions of wireless data products have been sold in the last two decades for licensed and license-free operation, many of them manufactured by Microwave Data Systems. There are several ways that these systems can benefit from the more flexible MDS entraNET 900 equipment—more flexible serial and Ethernet interfaces, and higher data throughput.

MDS entraNET 900 units are well suited to replace leased or dial-up lines, or existing 900 MHz data transceivers by taking advantage of the transceiver's serial and Ethernet interfaces.

Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with MDS entraNET 900 units with little or no special configuration. This equipment can be connected to MDS entraNET 900 units through the COM1 or COM2 port with a DB-25 to DB-9 cable wired for EIA-232 signaling. The COM2 port supports all standard EIA-232 signaling and acts as a data-terminal equipment device (DTE).

Several previous MDS-brand products had non-standard signal lines on their interface connectors; for example, to control the unit sleep function. These special functions are not provided nor supported by the MDS entraNET 900 unit at this time. Always consult the legacy equipment manual(s) for interface pinout information prior to making connections.

Supplement legacy wireless network with IP services

The MDS entraNET 900 Dual Gateway model can support up to two serial devices and one Ethernet connection at the same time. The serial interfaces (COM1 and COM2) operate in two different modes: Connectionless serial-to-serial (UDP) and connection-oriented IP-to-serial (TCP).

In the UDP (connectionless serial-to-serial) mode, the transceiver supports point-to-multipoint serial-port to serial-port connectivity. In the TCP (connection-oriented IP-to-serial) mode, the transceiver supports point-to-point Ethernet/IP to serial port connectivity.

For further details on Serial Gateway interface modes, see *"CONFIGURING THE SERIAL INTERFACES"* on Page 32.

1.3 NETWORK DESIGN CONSIDERATIONS

1.3.1 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. As with any other store-and-forward device, it introduces additional end-to-end transmission delay but provides longer-range connectivity.

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

The geographic location of a repeater station is especially important. A site must be chosen that allows good communication from the repeater to *both* the Access Point and outlying remote sites. This location is often on top of a hill, 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 105).

Using a Remote as a Store-and-Forward Repeater

A wireless network can be extended through the use of an alternate arrangement using the Access Point as a repeater to re-transmit the signals of all stations in the network. The repeater is a standard transceiver configured as an Access Point. (See Figure 1-4.)

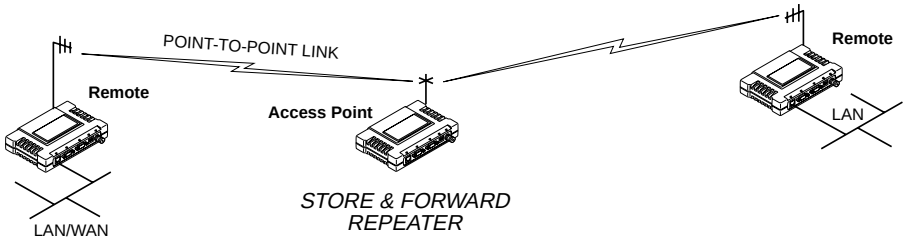


Figure 1-4. Typical network with store-and-forward repeater

1.3.2 Protected Network Operation through Multiple Access Points

Although MDS entraNET 900 units have a very robust design and have undergone intensive testing before shipment it is possible for isolated failures to occur. Down time can be further reduced 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 happening.

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

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

1.3.3 Co-locating Multiple Networks

Many wireless networks can operate in relatively close physical proximity to one another providing 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 MDS entraNET 900 networks. It is part of a beacon signal broadcast by the Access Point (AP) to any Remote units with the same Network Name. Remotes that join the network are referred to as being "associated" with the Access Point unit.

Multiple APs with the same Network Name should be avoided unless a redundant system is being deployed. Using the same Network Name in multiple APs may result in Remotes associating with undesired APs and preventing data exchange from occurring.

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 Redundancy

You can co-locate Access Points at one location for load-sharing or redundancy, provided they have the same Network Name. Provide some vertical separation between the antennas to minimize RFI between them.

Co-Location for Multiple Networks

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

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

Can radio-frequency interference (RFI) disrupt my Network?

When multiple MDS entraNET 900 networks operate in close physical proximity to other wireless networks, individual units may not operate reliably under weak signal conditions and may be influenced by strong radio signals in adjacent bands. This radio frequency interference cannot be predicted and can only be determined by experimentation. If you need to co-locate two transceivers, 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 MDS technical support personnel about other techniques for controlling radio frequency interference between the radios. (See *"A Word About Radio Interference"* on Page 108 for more details.)

1.4 SECURITY TECHNIQUES & TOOLS

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

The MDS entraNET 900 is capable of dealing with many common security issues. Table 1-2 profiles security risks and how the MDS entraNET 900 provides a solution for minimizing vulnerability.

Table 1-2. Security Risk Management

Security Risk	The MDS entraNET 900 Solution
Unauthorized access to the backbone network through a foreign remote radio	√ Approved Remotes List Only those remotes included in the AP list will associate
"Rogue" AP, where a foreign AP takes control of some or all remote radios and thus remote devices	√ Approved AP List A remote will only associate to those AP included in its local authorized list of AP
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	√ Failed-login lockdown After 3 tries, a transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.

Table 1-2. Security Risk Management

Security Risk	The MDS entraNET 900 Solution
Denial of service, where Remote radios could be reconfigured with bad parameters bringing the network down.	√ Remote login √ Local console login √ Disabled HTTP & Telnet to allow only local management services
Airsnort and other war-driving hackers in parking lots, etc.	√ 900 MHz FHSS does not talk over the air with standard 802.11b cards √ The transceiver cannot be put in a promiscuous mode √ Proprietary data framing
Eavesdropping, intercepting messages	√ 128-bit encryption
Key cracking	√ Automatic Rotating Key algorithm
Replaying messages	√ 128-bit encryption with rotating keys
Unprotected access to configuration via SNMPv1	√ Enable/disable SNMPv1 operation
Potential, ongoing attacks	√ Provides early warning via SNMP through critical event reports (unauthorized, logging attempts, etc.)

1.4.1 Intrusion Detection via SNMP Traps

In addition to the operative tools and techniques, the MDS entraNET 900 can provide SNMP-based network management systems with traps (alarms) that represent potentially suspicious activities or events. These include:

- Unauthorized AP MAC address detected at Remote
- Unauthorized Remote MAC address detected at AP
- Login attempt limit exceeded
  (Accessed via: Telnet, HTTP, or local)
- Successful login/logout
  (Accessed via: Telnet, HTTP, or local)

1.5 ACCESSORIES

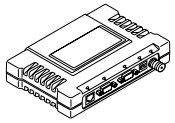
The transceiver can be used with one or more of the accessories listed in Table 1-3. Contact the factory for ordering details.

Table 1-3. Accessories

Accessory	Description	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	Call factory
Yagi Antenna (Directional)	Rugged antennas well suited for use at Remote installations. Consult with your factory Sales Representative for details.	Call factory
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
Fuse	Small, board-mounted fuse used to protect against over-current conditions.	29-1784A03
Flat-Surface Mounting Brackets & Screws	Brackets: 2″ x 3″ plates designed to be screwed onto the bottom of the unit for surface-mounting the radio.	82-1753-A01
	Screws: 6-32/1/4″ with locking adhesive. (Industry Standard MS 51957-26)	70-2620-A01
DIN Rail Mounting Bracket	Bracket used to mount the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	03-4022A02
COM2 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

2 EMBEDDED MANAGEMENT SYSTEM

Contents



2.1 INTRODUCTION

The MDS entraNET 900 is equipped with an embedded management system that is accessible through different data interfaces. These include the COM1 (serial) port, the LAN (Ethernet) port and over the wireless network. Essentially the same capabilities are available through either of these paths.

You have a choice of using three common communications tools—a computer terminal-emulator through the COM1 port, Telnet, or a Web browser through the LAN (Ethernet) port. You must know the unit IP address and the entraNET Management System password and user name to use the LAN port access.

The transceiver also supports SNMP-based management tools such as Microwave Data Systems' *NETview MS*™. *NETview MS* provides a network-wide management tool using a graphical user interface (GUI). For support of other software, a set of MIB files is available for download from the Microwave Data Systems' Web site at **www.microwavedata.com/service/technical/support/downloads/**. A brief summary of SNMP commands can be found at *SNMP Configuration* section on Page 28.

The entraNET Management System and its functions are divided in this guide into five functional groups that are listed below.

- Section 2.3, *CONFIGURING NETWORK PARAMETERS* (beginning on Page 27)
- Section 2.4, *CONFIGURING RADIO PARAMETERS* (beginning on Page 28)
- Section 2.5, *CONFIGURING THE SERIAL INTERFACES* (beginning on Page 32)
- Section 2.7, *PERFORMANCE VERIFICATION* (beginning on Page 44)
- Section 2.8, *MAINTENANCE* (beginning on Page 58)

Each of these sections has a focus that is reflected in its heading. The section you are now in will provide you with information on connecting to the entraNET Management System, how to navigate through it, and how it is structured, and how to perform some top-level configuration tasks.

NOTE: Parameter options/range, and any default value, will be displayed at the end of the field description between square brackets. [range, options or description; default]

2.1.1 Menu Structure

The following two illustrations are flowcharts that display the organization of the entraNET Management System (*i*NET MS). For this presentation, they are divided into two groups:

- Configuration Group
  (Figure 2-1 on Page 16)
- Security, Performance & Maintenance Group
  (Figure 2-2 on Page 17)

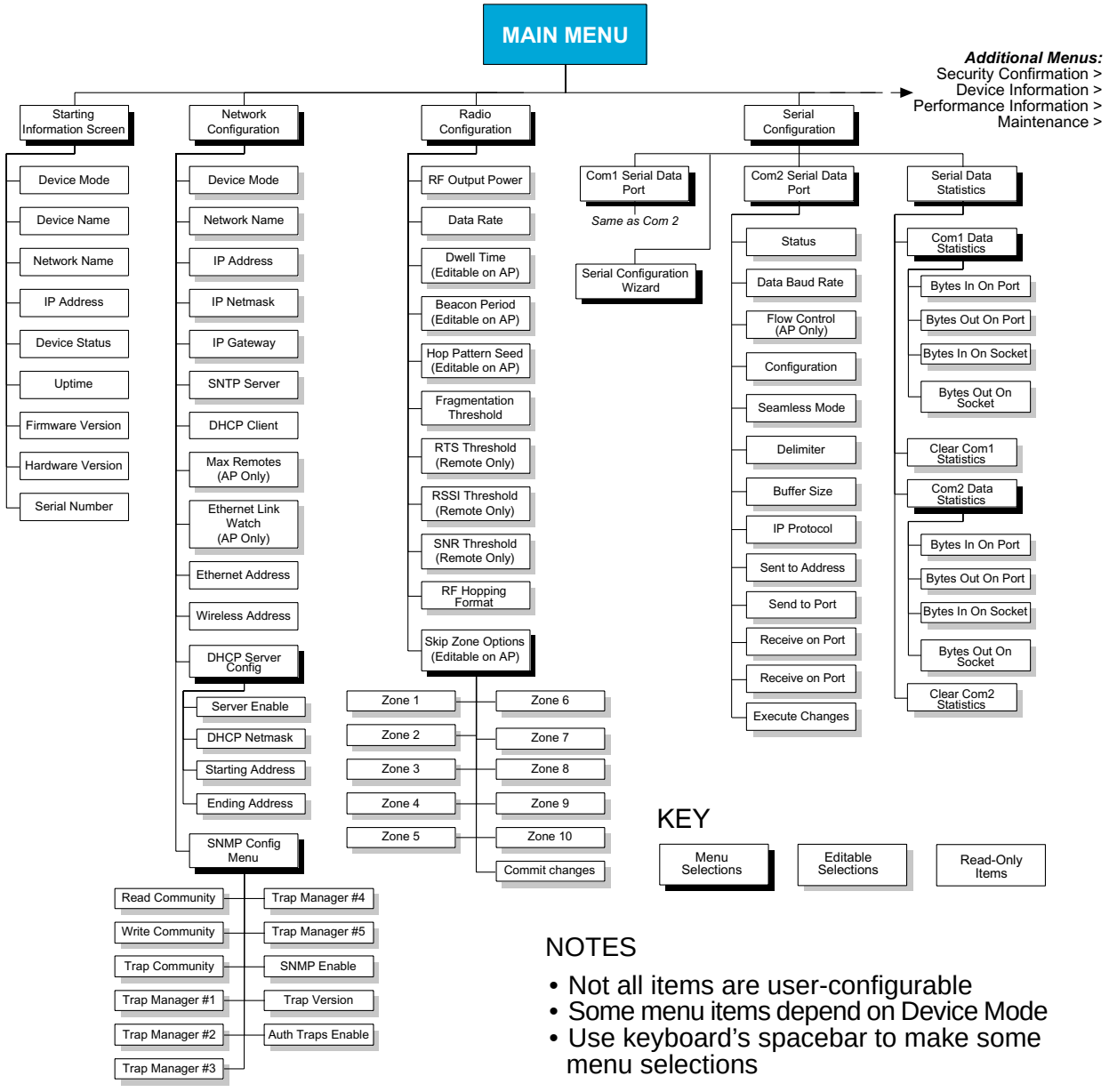
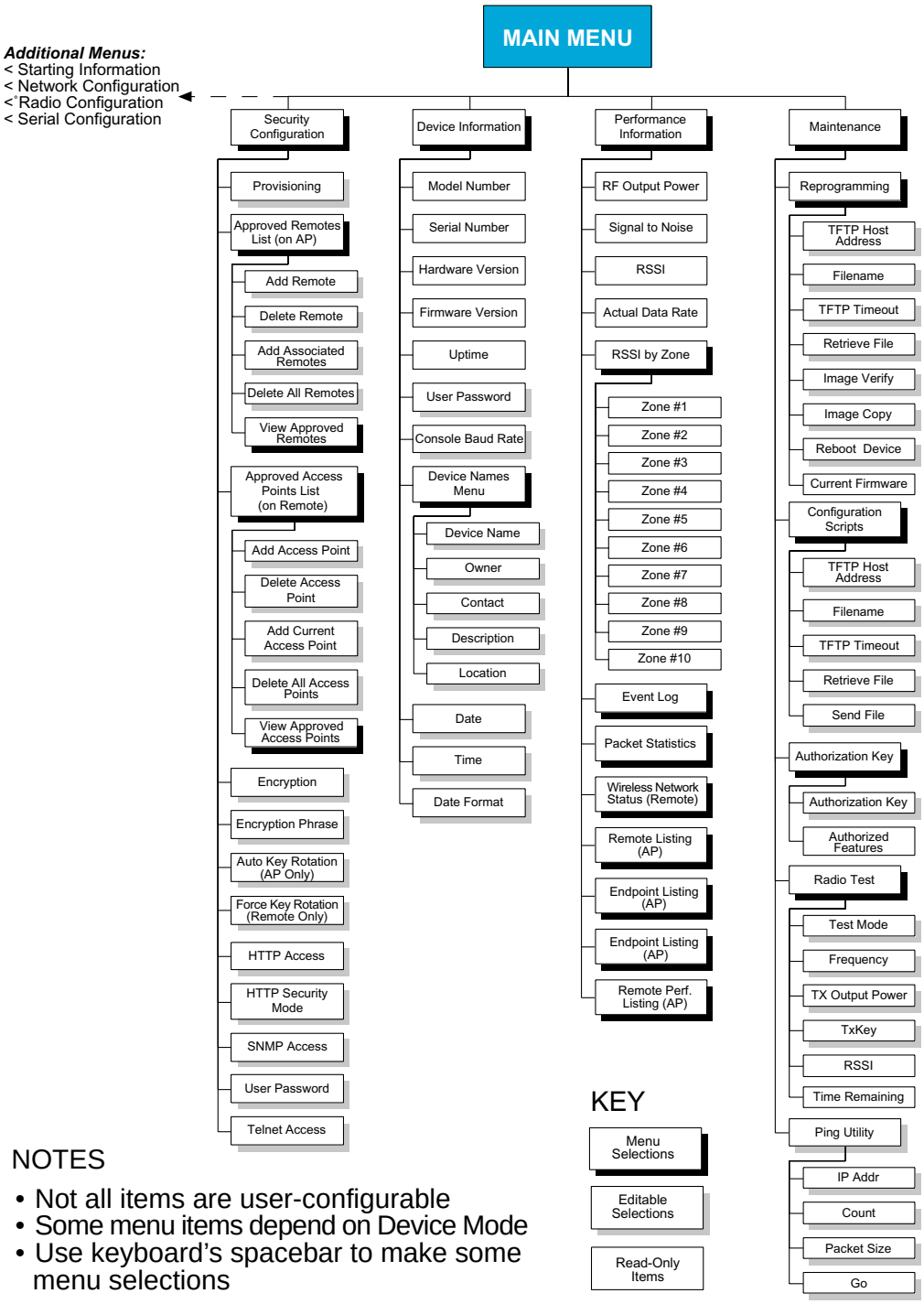


Figure 2-1. Embedded Management System Organization—Configuration Group (under revision)



NOTES

- Not all items are user-configurable
- Some menu items depend on Device Mode
- Use keyboard's spacebar to make some menu selections

Figure 2-2. Embedded Management System Organization—Security, Performance & Maintenance Groups (under revision)

2.1.2 Differences in the User Interfaces

There are slight differences in navigation, but for the most part, the content is the same. You will find a few differences in capabilities—the communications tool is driven by limitations of the access channel. Below are samples of the Starting Information Screen seen through a terminal and a Web-browser.

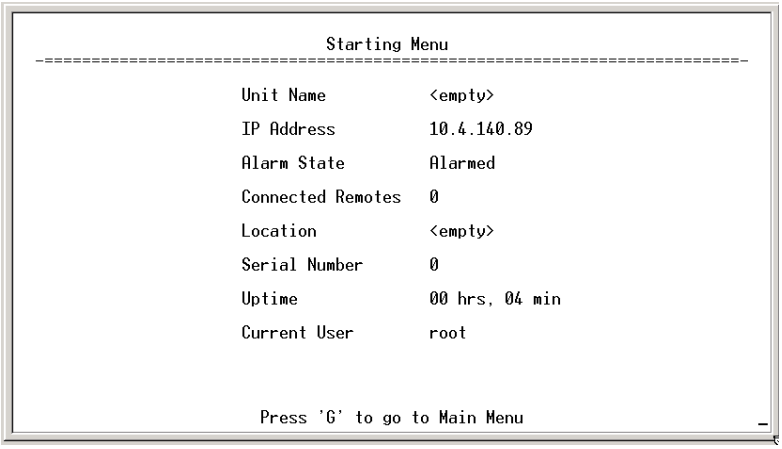


Figure 2-3. View of entraNET MS with a text-based program—(Terminal or Telnet)

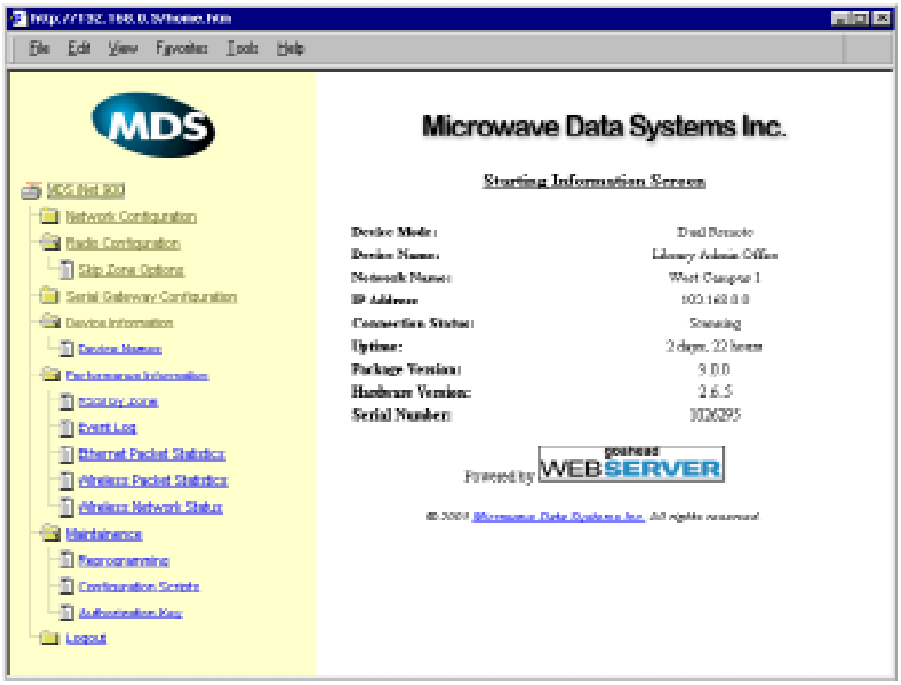


Figure 2-4. View of the entraNET MS with a Browser

2.1.3 Accessing the Embedded Management System

The menu-based management system provides access to view and configure many unit parameters and provides you with basic diagnostic and maintenance tools. There are several tools that can be used to gain access to the entraNET Management System.

- **Terminal-Emulator**—Use a terminal emulator program on your PC, such as HyperTerminal, connected directly to the MDS entraNET 900 COM1 port via a serial cable.
- **Telnet**—Text-based access to the Management System through a network connection (AP only).
- **Web Browser**—Connect to the entraNET units using a Web browser on a local PC connected directly to the transceiver's LAN port or associated network (AP only).

The following are detailed procedures for connecting to the embedded Management System.

Procedure with Terminal Emulator

a. Connect a computer's serial communications port to the transceiver's COM1 Port connector.

b. Launch a terminal emulator program, such as HyperTerminal, on the computer. Configure it to 19,200 bps data rate, 8-bit characters, no parity, one stop bit, and no flow-control. Use ANSI or VT100 emulation.

c. Press the **ENTER** key. A login screen will be displayed that will require a user name and password to access the Management System. (User = entraNET; default password = **admin**)

The radio will respond with a login screen, followed by the start-up screen similar to Figure 2-5 on Page 22.

NOTE: If the transceiver is powered-up or rebooted while connected with a terminal, you will see a series of pages of text information relating to the booting of the unit's microcomputer. Wait for the initial entraNET MS login screen before proceeding. The boot process takes approximately 30 seconds.

Procedure with Telnet (AP only)

a. Connect a personal computer's Ethernet port to the LAN Port connector on the AP transceiver using an Ethernet crossover cable or connect the AP to the network. (See Figure 3-3 on Page 81 for location.) The LAN LED will light up.

b. Start the Telnet program on your computer targeting the IP address of the transceiver to which you are connected and press the **ENTER** key.

For example, in Windows: **Start>Run>Telnet**

NOTE: Do not use the default IP address (192.168.1.1) if there are multiple transceivers on the same network set with the default address.

c. The transceiver will respond with a login screen. Enter your password and press the **ENTER** key. (Default = **admin**)

The entraNET responds with the start-up menu screen. (Figure 2-6 on Page 23)

Procedure with Web Browser (AP only)

a. Connect a personal computer's Ethernet port to the LAN Port connector on the transceiver using an Ethernet crossover cable. (See Figure 3-3 on Page 81 for location.) The LAN LED will light up.

b. Launch a Web-browser (HTTP) program, such as Microsoft's Internet Explorer™, on your computer.

c. Type in the radio's IP address. For example **192.168.1.1** and press the **ENTER** key. (Default address = **192.168.1.1**)

d. A login screen will be displayed that will require a user name and password to access the Management System. (Defaults: user = entraNET; password= **admin**)

e. The transceiver responds with the startup menu screen. (See Figure 2-6 on Page 23.)

NOTE: If the default address of 192.168.1.1 does not work, use the terminal-emulator procedure to communicate with the unit through the COM1 port. The current IP address will be displayed on the *Starting Information Screen* (Figure 2-6 on Page 23).

2.1.4 Navigating the Menus

Navigating with a Web browser is straightforward with a framed page. The primary navigation menu is permanently located in the left-hand window. The right-hand window displays the current menu item.

The text-based interface, accessible through Telnet or terminal emulator, uses a traditional multi-layered text menu system. To move further down a path in the menu tree, type the letter key to the left of the menu item. You will automatically move to the associated screen. In most cases, use the **ESCAPE** key to move back up a level.

In general, the top portion of the screen shows read-only information with no user selection letter. The bottom portion of the screen contains parameters that can be selected for further information, alteration of values, or to navigate to other menus.

When you arrive at a screen with user-controllable parameter fields, you select the menu item by keying in an associated letter. If there is a user definable value, the field will clear to the right of the menu item and you will be allowed to type in the value you wish to use. Follow this action by the **ENTER** key to save the changes. If you make a mistake or change your mind before using the **ENTER** key, 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 cases, press the keyboard's **SPACEBAR** and you will step through the available selections. After the desired option appears, press the **ENTER** key to save the selection. In some screens, several parameters may be changed and then saved by a single keystroke. The **ESCAPE** key can be used to cancel the action and restore the previous value.

In most cases, you can press the **ESCAPE** key to exit the action without implementing any changes or to navigate to the next higher level menu.

2.1.5 Logging In and Out of the Embedded Management System

Logging in via Telnet or a Web Browser

When you use Telnet or a Web browser to communicate with the transceiver, you will need to know the unit's IP address, the "User Name", and "Password" in advance.

With some Web browsers, the User Name, entraNET will be filled in. If it is blank, type in entraNET with a lowercase "i" and capitals N-E-T. The default user password is **admin** in lowercase letters.

NOTE: Passwords are case sensitive. Do not use punctuation mark characters. Use a maximum of eight characters.

Once the User Name and Password have been entered, press **ENTER**.

NOTE: It may be necessary to change your IP access to the local area network to match the one used by the MDS entraNET 900. (Defaults: IP–192.168.1.1, Netmask–255.255.0.0) You can identify or verify the transceiver's IP address using a terminal-emulator to communicate with the transceiver through the COM1 Port and then viewing the *Starting Information Screen*.

If you are accessing the entraNET MS via a browser connected to the LAN port, you will see a sign-in screen similar to the one in Figure 2-5.

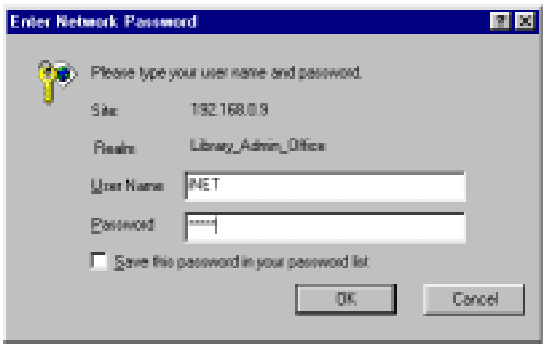


Figure 2-5. Sign-in Screen when using a Web Browser

The transceiver's Device Name is used as the "Realm." (See *Device Names Menu* on Page 27 to learn how to change this name.) This name will confirm you are connecting to the transceiver you desire.

Changing Passwords

Via Terminal Emulator or Telnet

Once you are logged in, you can go to the **Device Information Menu** and change the password (case-sensitive). Follow any changes to the password or other parameters with an **ENTER** key to save the change.

Via Web Browser

At the time of publication, it is not possible to change the password via the web browser interface. This restriction is done for security reasons—a web browser transmits messages in clear text.

Logging Out of the entraNET Management System

For security reasons, it is best to formally log-out of the entraNET Management System. If you do not formally log out, the session will be terminated within 10 minutes of your last activity with the system.

Web Browser

To logout of the entraNET MS with a Web browser, click on the "Logout" listing in the left hand frame of the browser window. The right-hand frame will change to a logout page. Follow the instructions on this Web page.

Telnet

From the Main Menu, press "Q" to quit and terminate the session. If you do not manually log out, your session will time-out after 10 minutes of no keyboard activity.

Terminal Emulator

You do not need to logout from a terminal emulator when connected to the COM1 port. You can force a logout by pressing the exclamation point (!) key to optimize the transceiver's security. (Note: This only works from the Starting Information Screen or the Main Menu Screen.)

2.2 BASIC DEVICE INFORMATION

2.2.1 Starting Information Screen

Once you have logged into the entraNET Management System, you will be presented with a screen that provides an overview of the transceiver and its current operating condition. It provides an array of vital information on the unit and its operating condition.

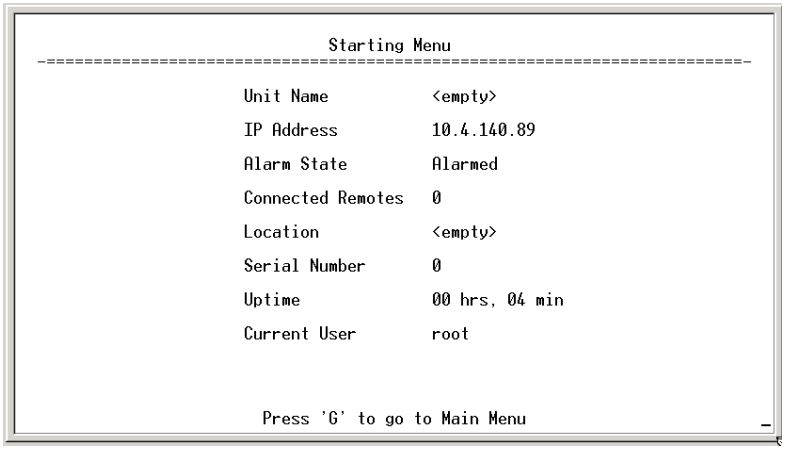


Figure 2-6. Starting Menu

- **`Device Mode`**—Current operating mode of the unit as it relates to the network.
- **`Device Name`**—This is a user-defined parameter that will appear in the heading of all pages.
  (To change it, see *Network Configuration Menu* on Page 27.)
- **`Network Name`**—The name of the network in which the unit is associated.
- **`IP Address`**—Unit's IP address [192.168.1.1]
- **`Device Status`**—Condition of transceiver's association with an Access Point.

  At the Access Point:
  - *Alarmed*—A alarming event has been logged and not cleared.
  - *Operational*—Unit operating normally.

At a Remote:

- *Scanning*—The unit is looking for an Access Point beacon signal.
- *Exp(ecting) Sync(hronization)*—The unit has found a valid beacon signal for its network.
- *Hop Sync*—The unit has changed its frequency hopping pattern to match that of the Access Point.
- *Associated* —This unit has successfully synchronized and associated with an Access Point.
- *Alarmed*—The unit is has detected one or more alarms that have not been cleared.

  NOTE: If an alarm is present when this screen is displayed, a "A)" will appear to the left of the **Device Status** field as seen in Figure 2-6. Pressing the "A" key on your keyboard will take you directly to the "Current Alarms" screen.

- **`Uptime`**—Elapsed time since the transceiver was powered-up.
- **`Firmware Version`**—Version of firmware that is currently active in the unit.
- **`Hardware Version`**— Hardware version of the transceiver printed circuit board.
- **`Serial Number`**—Make a record of this number. It must be provided to purchase Authorization Keys to upgrade unit capabilities. (See *"Authorization Keys Menu"* on Page 71.)

2.2.2 Main Menu

The next screen, the Main Menu, is the entryway to all user-controllable features. The radio's Device Name appears at the top of this and all other screens as a reminder of the unit that is currently being controlled.

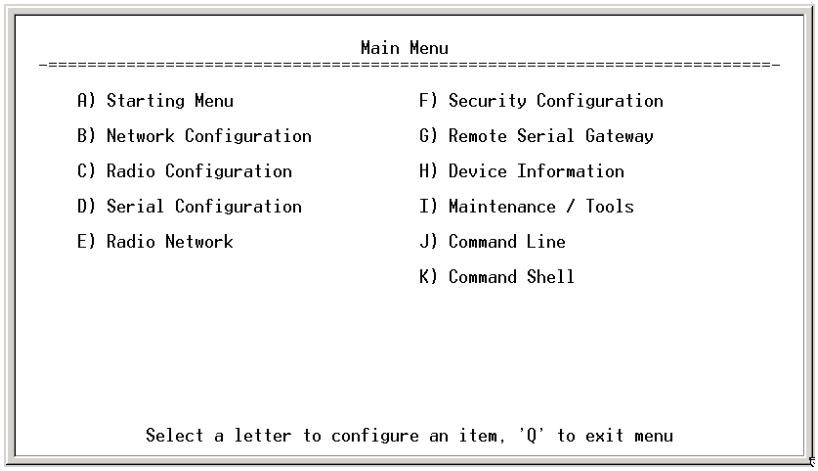


Figure 2-7. Main Menu

- **`Starting Information Screen`**—Select this item to return to the start-up screen. (See *"Starting Information Screen"* on Page 23)
- **`Network Configuration`**—Tools to configure the data network layer of the transceiver. (See *"Network Configuration Menu"* on Page 27)
- **`Radio Configuration`**—Tools to configure the wireless (radio) layer of the transceiver. (See *"Radio Configuration Menu"* on Page 29)
- **`Serial Gateway Configuration`**—Tools to configure the COM2 serial port. (See *"Serial Data Port Configuration Menu"* on Page 33)
- **`Security Configuration`**—Tools to configure the security services available with the transceiver environment. (See *"SECURITY CONFIGURATION"* on Page 42)
- **`Device Information`**—Top level user-specific and definable parameters, such as unit password. (See *"Device Information Menu"* on Page 25)
- **`Performance Information`**—Tools to measure the radio and data layer's performance of the network. (See *"Performance Information Menu"* on Page 45)
- **`Maintenance/Tools`**—Tools to use configuration files, change firmware and use Authorization Keys to change major unit capabilities. (See *"Authorization Key —Alter the unit's overall capabilities by enabling the built-in resources. (See "Authorization Keys Menu" on Page 71)"* on Page 58)

2.2.3 Configuring Basic Device Parameters

Device Information Menu

Below is the menu/screen that displays basic administrative data on the unit to which you are connected. It also provides access to some user-specific parameters such as password and device names.

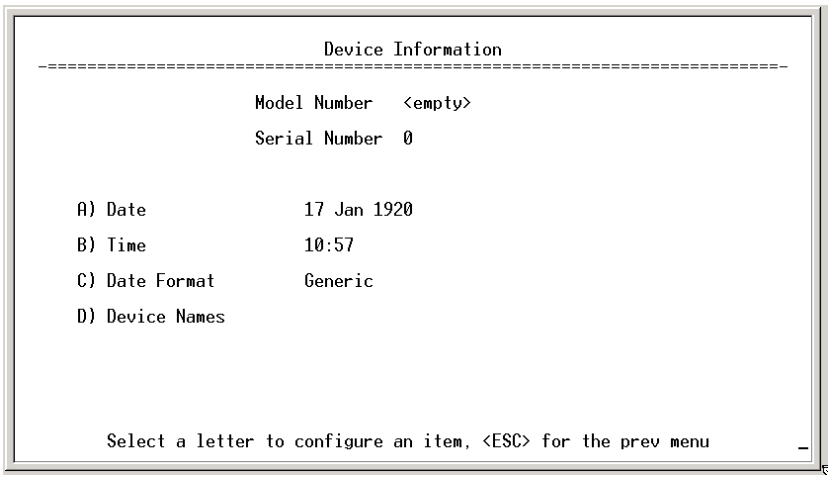


Figure 2-8. Device Information Menu

- **`Model Number`** *(Display only)*
- **`Serial Number`** *(Display only)*
- **`Hardware Version`** *(Display only)*
- **`Firmware Version`** *(Display only)*—Current firmware installed and being used by the transceiver.
- **`Uptime`** *(Display only)*—Elapsed time since powering up.
- **`User Password`**—Password for gaining access to the entraNET Management System from remote locations (over-the-air or LAN) and for changing parameters settings. Use this menu item to change the password. [admin]

  This menu item is always accessible via a terminal connected to the COM1 Port, and via Telnet if access enabled in the unit's Security Configuration Menu (Page 42).
- **`Device Names Menu`**—Fields used at user's discretion for general administrative purposes. The Device Name field is used by the transceiver as the "Realm" name for network security and in the entraNET MS screen headings. (See Figure 2-9 on Page 27)
- **`Date`**—Current date being used for the transceiver logs. User-setable. (Value lost with power failure if SNTP (Simple Network Time Protocol) server not accessible.)
- **`Time`**—Current time of day. User-setable.
  Setting: HH:MM:SS
  (Value lost with power failure if SNTP server not accessible.)
- **`Date Format`**—Select presentation format:
  - Generic = dd Mmm yyyy
  - European = dd-mm-yyyy
  - US = mm-dd-yyyy

Device Names Menu

```
Screen not found in MDS entraNET
```

Figure 2-9. Device Names Menu

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

2.3 CONFIGURING NETWORK PARAMETERS

2.3.1 Network Configuration Menu

The *Network Configuration Menu* is the home of three parameters that should be reviewed and changed as necessary before placing an transceiver in service—Device Mode, IP Address and Network Name. Screens for both the Access Point and Remote units are shown below.

```
                        Network Configuration
-=============================================================================-

                A) IP Address          10.4.140.89
                B) IP Netmask          255.255.0.0
                C) IP Gateway          10.4.1.1

                   Ethernet Address    00:00:00:00:00:00

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

Figure 2-10. Network Configuration Menu
From Access Point

- **`Network Name`** *(User Review Required)*—Name of the network of which this unit will be a part. Essential for association of Remotes to the Access Point in the entraNET network. [Not Programmed]
- **`IP Address`** *(User Review Recommended)*—Essential for connectivity to the MDS entraNET 900 MS via the LAN port and Ethernet data over the network. Enter any valid IP address that will be unique within the network. [192.168.1.1]

CAUTION: Changing this value in the transceiver while you are communicating with it over the network, will cause a loss of communication with the transceiver. Communication will need to be re-established using the new IP address.

- **`IP Netmask`**—The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled. [255.255.0.0]
- **`IP Gateway`**—The IPv4 address of the default gateway device, typically a router. This field is unnecessary if DHCP is enabled. [0.0.0.0]
- **`SNTP Server`**—Address of server from which the transceiver will automatically get the time-of-day. Without an SNTP server, the date and time must be manually set. [0.0.0.0]
- **`DHCP Server Config(uration)`**—Menu for configuration of DHCP services by the Access Point unit. DHCP provides on-the-fly IP address assignments to other LAN devices, including MDS entraNET 900 units. [Disabled]
- **`DHCP Client`**—Enabling this option forces the transceiver (AP or Remote) to obtain an IP address from any DHCP server available on the LAN. [Disabled]
- **`Ethernet Link Watch`** *(Access Point Only)*—Detects the lack of activity (no traffic) through the Ethernet port in the specified time period. If the period expires, then all Remotes are dissociated and expected to re-associate with an alternate AP. The current AP will broadcast a beacon indicating its "NOT AVAILABLE" status so Remotes that hear him do not try to associate to it. Once traffic is restored this beacon signal changes to "AVAILABLE" and Remotes are allowed to join in. [Disabled]
- **`Max(imum Allowed) Remotes`** *(Access Point Only)*—Number of Remotes permitted to be associated with (served by) this Access Point. [50]
- **`Ethernet Address`** *(Display Only)*—Hardware address of this unit's Ethernet interface.
- **`Wireless Address`** *(Display Only)*—Hardware address of the unit's wireless interface.

2.4 CONFIGURING RADIO PARAMETERS

There are two primary data layers in the MDS entraNET 900 network—radio and data. Since the data layer is dependent on the radio layer working properly, this is a good place to make sure the unit is configured as you want it to be. This is the primary radio menu, the *Radio Configuration Menu*, and a secondary menu, the *Skip Zone Options*.

2.4.1 Radio Configuration Menu

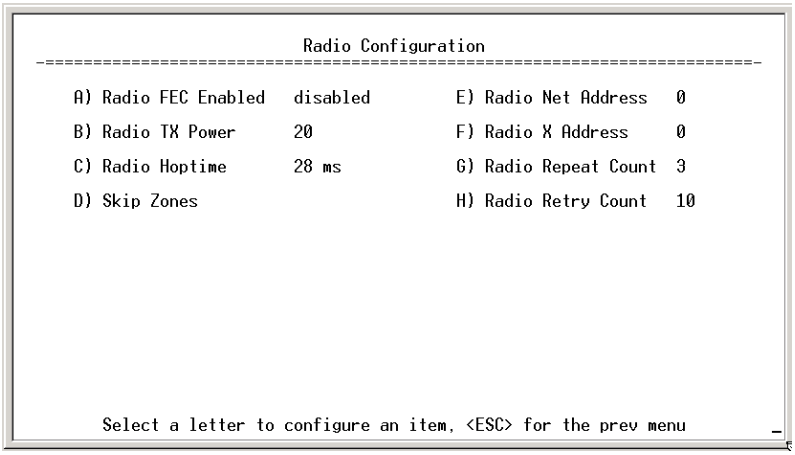


Figure 2-11. Radio Configuration Menu
From Access Point

- **RF Output Power** *(User Review Recommended)*—Set RF power output level. Displayed in dBm. Setting should reflect local regulatory limitations and losses in antenna transmission line. (See *"How Much Output Power Can be Used?"* on Page 110 for information on how to calculate this value.) [20–30; 20]
- **Data Rate** *(Remote Only)*—Over-the-air data transmission rate for this remote. Remotes can operate at different data rates when communicating with a common Access Point. 115.2 kbps data rates are possible with strong RF signal levels (> –79 dBm RSSI including a 15 dB fade margin). Data throughput will be reduced in the presence of interference due to retransmissions.

  The data rate value for Access Points is displayed as **AP.** This shows that the AP is varying the communication speed with each Remote depending on the received signal strength from each station. [115.2, AUTO; AUTO]
- **Dwell Time**—Duration of one hop on a particular frequency in the hopping pattern. **Dwell Time** should be set to 32.8 ms. (This field is only changeable on an Access Point. Remotes get their value from AP upon association.)
  [16.4, 32.8, 65.5, 131.1, 262.1 msec; 32.8]

  TIP: If a packet is being transmitted and the dwell time expires, the packet will be completed before hopping to the next frequency.
- **Beacon Period**—Amount of time between Beacon transmissions (msec).

  Available Intervals: **Fast** (52 ms), **Normal** (104 ms), **Moderate**

(208 ms), and **Slow** (508 ms). These values provide relatively quick association times where Fast is very fast (≈ 5 sec) and the other end, the largest recommended value, the 508 ms period is slow (≈ 60 sec). [Fast, Normal, Moderate Slow; Normal]

TIP: Increasing the Beacon Period will provide a *small improvement* in network data throughput. Shortening it decreases the time needed for Remotes to associate with the AP. A short period is usually only a benefit when there are mobile Remotes in the network.

- **Hop Pattern Seed** *(Access Point Only)*—A user-selectable value to be added to the hop pattern formula in an unlikely event of identical hop patterns of two co-located or nearby networks. Changing the seed value will minimize possible RF-signal collisions of transceivers. (This field is only changeable on an Access Point. Remotes read the AP's value upon association.) [1 to 65,000; 1]
- **Fragment Threshold**—Before transmitting over the air, if a packet exceeds this number of bytes, the transceiver sends the packet in multiple fragments that are reassembled before being delivered over the Ethernet interface at the receiving end. Use smaller values on high interference locations. (See *"Network Performance Notes"* on Page 54.) [(256–1600 bytes; 1600]

  TIP: In an interference-free environment this value should be large to maximize throughput. If interference exists then the value should be set to smaller values. The smaller the packet the less chance of it being interfered with at the cost of slightly reduced throughput.

- **RTS Threshold**—Number of bytes for the over-the-air RTS/CTS handshake boundary. (See *"Network Performance Notes"* on Page 54.) [0 to 1600 bytes; 500]

  TIP: Lower the **RTS Threshold** as the number of Remotes or overall over-the-air traffic increases. Using RTS/CTS is a trade-off, giving up some throughput in order to prevent collisions in a busy over-the-air network.

  The **RTS Threshold** should be enabled and set with a value smaller than the **Fragmentation Threshold** described above. RTS forces the Remotes to request permission from the AP before sending a packet. The AP sends a CTS control packet to grant permission to one Remote. All other Remotes stop transmitting for the specified amount of time.

- **RSSI Threshold**—Level (dBm) below which connection is deemed to have degraded, and an critical event is generated and logged. [0 to -120; Not Programmed]

- **`SNR Threshold`**—Value (dB) below which the wireless network connection is deemed to have degraded and an critical event is generated and logged. [0 to 40; Not Programmed]
- **`Hop Format`**—Operation compliant to country-specific restrictions into the frequency hopping algorithm. This option must be specified when the order is placed and cannot be modified in the field by the user. Authorizations at time of publication:
  - Australia: 915–928 MHz band
  - Brazil: 902-907.5 and 915-928 MHz bands
  - U.S.A. & Canada: 902–928 MHz band

  NOTE: Other country-specific configurations may be available. Check with your MDS sales representative for new additions.
- **`Skip Zones`** *(Editable at Access Point Only)*—Display of current utilization of zones. Each zone consists of eight RF channels. (See *"Skip Zone Options Menu"* on Page 31.)

Skip Zone Options Menu

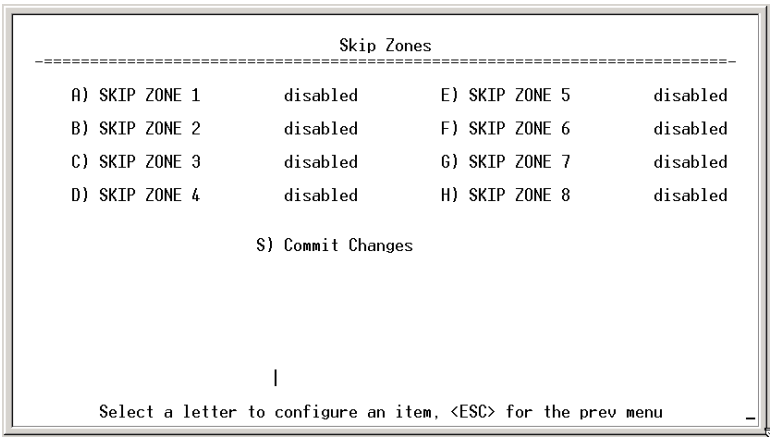


Figure 2-12. Skip Zones Menu
("Commit changes" displayed only on Access Point units)

This is a display of current utilization of 10 zones, each of eight RF operating frequencies. Zones can be toggled between **Active** and **Skipped** at Access Point units by first keying in the letter of the zone to be changed, and then pressing the spacebar to toggle between the two options for each zone. Select the **Commit Changes** menu item to implement changes. These changes will be forwarded to all units in the network through the Access Point's beacon signal.

A maximum of three zones can be skipped and still be compliant with FCC regulations.

2.5 CONFIGURING THE SERIAL INTERFACES

2.5.1 Overview

Modes

The transceiver includes an embedded terminal server that provides serial-data-encapsulation over IP. In this capacity, the *entraNET* 900 acts as a gateway between serial and IP remotes devices. Two basic scenarios come to mine, PC applications using IP to talk to remote devices, or serial PC applications talking to remote serial-devices over an IP network.

Two types of services are offered by the transceiver—TCP and UDP. TCP provides a connection-type link, and end-to-end acknowledgment of data, but with some added overhead. UDP provides a best-effort delivery service.

Most polled protocols will be best served by UDP services as the protocol itself has built-in recovery mechanisms (error-correction). UDP provides the needed multidrop operation by means of multicast addressing, where multiple remote devices will receive and process the same poll message. The serial-to-serial example which follows, shows how to provide multicast services. (See *"Point-to-Multipoint Serial-to-Serial Application Example"* on Page 39.)

On the other hand, TCP services are best suited for applications that do not have a recovery mechanism (error-correction) and most have the guaranteed delivery that TCP provides despite the extra overhead. The IP-to-Serial example shows how to do this. (See *"IP-to-Serial Application Example"* on Page 36.)

Essentially the same data services are available for both serial ports: COM1 and COM2. Note that the transceiver COM1 port is DCE and COM2 is DTE. Therefore, if the RTU to be connected is also DTE, then a null-modem cable will need to be used when connecting to COM2.

NOTE: In the discussion that follows, COM1 and COM2 will be treated alike unless noted. They provide essentially the same data services.

Configuration

There are several configuration parameters for the Remote Serial Gateway found under the *Serial Configuration Menu* of the entraNET Management System. Note that some of the parameters are not applicable to IP-to-Serial mode. After making changes to the configuration, you must use the menu's "Execute Changes" to cause the transceiver to implement the requested changes.

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

Serial Configuration Wizard

The Serial Configuration Wizard (FW≥ 3.0) available through the **Serial Data Port Configuration Menu** is recommended for configuration of serial ports. The wizard uses a step-by-step process, will eliminate possible conflicting settings, and streamline complex configurations.

2.5.2 Serial Data Port Configuration Menu

The first two menu present the identical parameter fields for each port with one exception—Flow Control. This is available only on Com2.

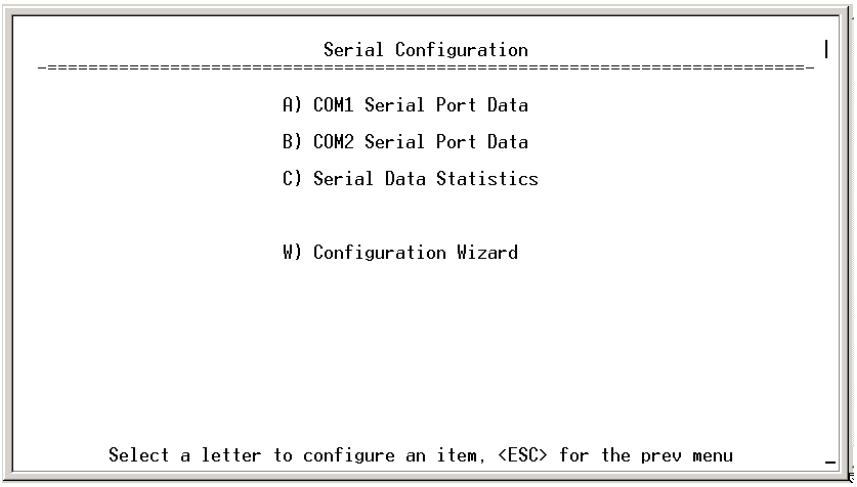


Figure 2-13. COM1/2—Serial Data Port Configuration Menu

- **`Serial Configuration Wizard`**—Tool for configuration of serial ports using a step-by-step process.
- **`Com1 Serial Data Port`**—For additional information see Page 33.
- **`Com2 Serial Data Port`**—For additional information see Page 33.
- **`Serial Data Statistics`**—Provides statistics on the serial and IP activity through the COM1 and COM2 ports. (See Page 36 for details)

Serial Data Port Configuration Screens

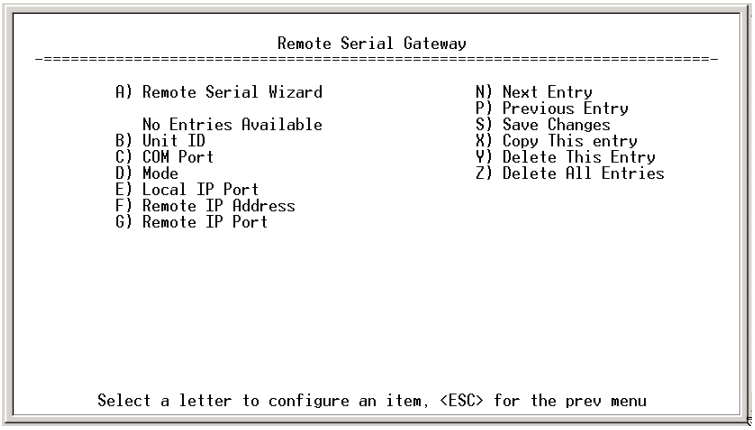


Figure 2-14. COM1/2—Serial Gateway Configuration Screen

NOTE: Setting this parameter for COM1 port to **Enable** prevents access of the entraNET Management System (MS) through this port.

However, the entraNET MS can still be accessed via Telnet or browser through the LAN port.

TIP: If you need to restore the COM1 port to support entraNET Management System services, connect a terminal to the port and enter an escape sequence to reset it the console mode. (**+++ ENTER**)

- **Status**—Enable/Disable the serial data port.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1,200–115,200; 19200]
- **Configuration**—Interface signaling parameters. Data bits, parity and stop bits.
  [7N1, 7E1, 7O1, 8N1, 8E1, 8O1; 8N1]
- **Flow Control [Com2 Only] (Access** *Point Only)*—RTS/CTS handshaking between the transceiver and connected device. [Enable, Disable; Disabled]
- **Seamless Mode**— If data buffering is Enabled, the radio will operate in seamless mode. Data bytes will be sent over the air as quickly as possible, but the receiver will buffer the data until enough bytes have arrived to cover worst case gaps in transmission. The delay introduced by data buffering may range from 22 to 44 ms, but the radio will not create any gaps in the output data stream. This mode of operation is required for protocols such as MODBUS™ that do not allow gaps in their data transmission. [Enable, Disable; Disabled]
- **Delimiter**— Number of characters that represent the end of a message (inter-character time-out). A transceiver receiving data through the serial port will send an end-of-message

signal to the remote end. MODBUS defines a “3.5-character” parameter. [0–1,000; 0]

- **Buffer Size**—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [0–100; 4]
- **IP Protocol**—TCP (Transmission Control Protocol) or UDP (User Datagram Protocol). [TCP, UDP; TCP]

  This is the type of IP port that will be offered by the transceiver serial device server. UDP requires configuration of **Send to Address** parameter. **NOTE:** TCP has guaranteed delivery, but at the expense of more overhead; UDP delivery is not guaranteed, but has less overhead.
- **Send to Address**—The IP address to be used as a destination for data received through the serial port. To reach multiple Remotes in the network, use a multicast address at the AP. Remotes in the network should have the multicast address programmed in their **Send to Address.**
  [Any legal IP address; 0.0.0.0]
- **Send to Port**—The IP port to which data packets received from the device connected to the transceiver should be sent. [Any valid IP port; COM1: 30010, COM2: 30011]
- **Receive on Port**—Receive IP data from this source and pass it through to the connected serial device. The port number must be used by the application connecting to local TCP socket. [Any valid IP port; COM1: 30010, COM2: 30011]
- **Receive on Address**—Must be configured with a valid multicast address. IP packets received with a matching destination address will be terminated at this unit
  [Any legal IP address; 0.0.0.0]

  Used only for UDP multicast purposes
- **Execute Changes**—Save and execute changes made on this screen (Shown only after changes have been entered.)

Serial Data Statistics Menu

This screen provides a summary of port activity for both serial data ports. These values will be reset to zero after a reboot cycle.

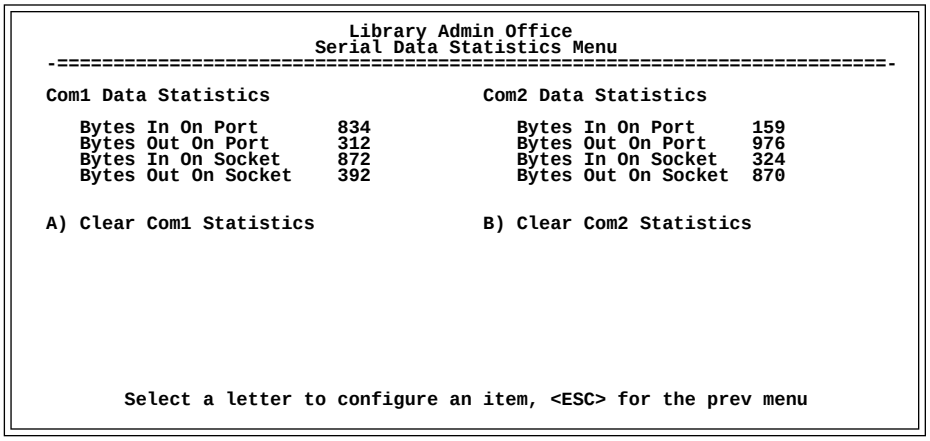


Figure 2-15. Serial Data Statistics Screen
(Both COM1 and COM2 will be shown)

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

  In general, the number of bytes **Out on Socket** should follow the number of bytes **In On Port** as all bytes received on the serial port should be transmitted out to the IP interface. The same should be true in the opposite direction, bytes **Out On Port** should follow bytes **In On Socket.**
- **Clear Com1 Statistics**—Resets counter to zero.
- **Clear Com2 Statistics**—Resets counter to zero.

2.5.3 IP-to-Serial Application Example

You have a choice to use UDP or TCP to establish communications. This will depend on the type of device you are communicating with at the other end of the IP network. In this example we will use TCP to illustrate its use.

In TCP mode, the transceiver remains in a passive mode offering a socket for connection. Once a request is received, data received in the serial port will be sent out through the IP socket and vice versa, until the connection is closed, or the link is interrupted. The TCP session has a timeout of 10 minutes. If inactive for that time, it will be closed. The

transceiver will offer again the port for connection after this time. In this mode, the entraNET 900 behaves the same, whether it is an Access Point or a Remote. (See Figure 2-16 and Table 2-1)

Establishing a Connection

From the PC, establish a TCP connection to the IP address of the Remote transceiver and to the IP port as configured above (typically 30011). A Telnet client application can be used to establish this connection. Data can now be sent between the PC and the RTU or other connected device.

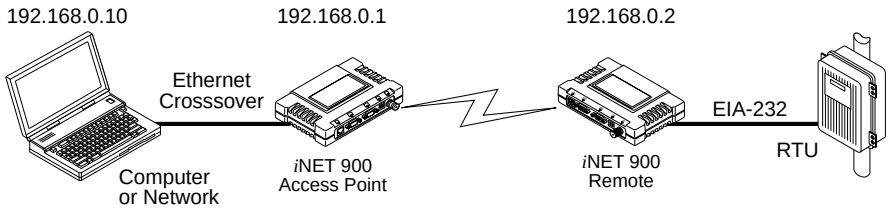


Figure 2-16. IP-to-Serial Application Diagram

Table 2-1. Serial Port Application Configuration

IP-to-Serial Connection

Unit Location	Menu Item	Setting
Access Point	None is required	None is required
Remote Unit	IP Address	192.168.0.2
	Status	Enabled
	IP Protocol	TCP
	Baud Rate	9,600 (Example)
	Flow Control	None
	Receive on Port	30011

2.5.4 Point-to-Point Serial-to-Serial Application Example

Once the transceivers are configured and the changes have been executed, they begin processing any data presented at the COM ports. Data presented at the Access Point's COM port will be packetized and sent via UDP to the Remote. Upon receiving the packet, the Remote strips the data out of the UDP packet and sends it out its COM port. Likewise, data presented at the Remote's COM port is packetized, sent to the Access Point, stripped, and sent out the Access Point's COM port. Note, this configuration does not use multicast addressing.

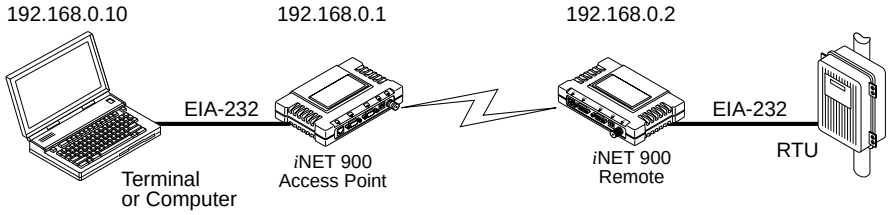


Figure 2-17. Point-to-Point Serial-to-Serial Application Diagram

Table 2-2. Serial Port Application Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point (COM2)[1]	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	Hardware (Example)
	Seamless Mode	Disabled
	Delimiter (Chars)	0
	Buffer Size	0
	IP Protocol	UDP
	Send to Address	192.168.0.2 (IP address of the entraNET Remote)
	Send to Port	30011
	Receive on Port	30011 (Not used)
	Receive on Address	0.0.0.0 (Not used)
Remote Unit (COM2)[1]	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	X-ON/X-OFF (Example)
	Seamless Mode	Disabled
	Delimiter	0 (Characters)
	Buffer Size	0 (Characters)
	IP Protocol	UDP
	Send to Address	192.168.0.1 (IP address of the *entraNET* AP)
	Send to Port	30011
	Receive on Port	30011 (Not used)
	Receive on Address	0.0.0.0 (Not used)

1. Either COM port can be used, but they must be the same ones at both ends of the link. Both COM ports can be used simultaneously for two independent data channels.

2.5.5 Point-to-Multipoint Serial-to-Serial Application Example

The operation and data flow for this mode is very similar to Point-to-Point serial-to-serial application, except that it uses multicast addressing. The primary difference is that data presented at the Access Point's COM port will be packetized and sent via UDP to all of the Remotes. Upon receiving the packet all of the Remotes strip the data out of the UDP packet and send it out their COM port. Likewise, data presented at any of the Remotes' COM ports is packetized, sent to the Access Point, stripped, and sent out the Access Point's COM port.

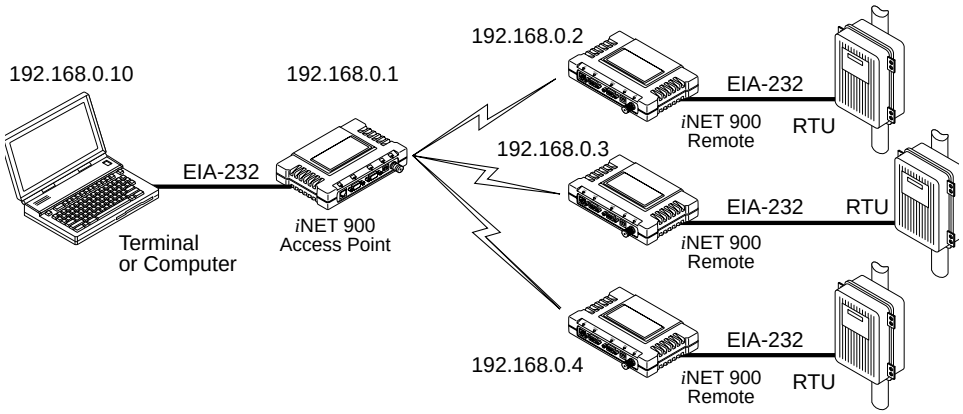


Figure 2-18. Point-to-Multipoint Serial-to-Serial Application Diagram

Table 2-3. Serial Port Application Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point (COM2)[1]	Status	Enabled
	Baud Rate	9600 (Example)
	Seamless Mode	Disabled
	Flow Control	Disabled
	IP Protocol	UDP
	Send to Address	224.254.1.1—Multicast Address[2]
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	0.0.0.0 (Not applicable)
Remote Units (COM2)[1]	Enable	Enabled
	Baud Rate	2,400 (Example)
	Seamless Mode	Disabled
	Flow Control	Hardware (Example)
	IP Protocol	UDP
	Send to Address	192.168.0.1

Table 2-3. Serial Port Application Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	224.254.1.1 — Multicast Address[2]

1. Either COM port can be used, but they must be the same ones at both ends of the link. Both COM ports can be used simultaneously for two independent data channels.
2. This address is an example only. Any Class D IP address will work.

2.5.6 Mixed Modes

Note that in this example, the TCP mode does not involve the Access Point. Thus, the transceiver in a single network can run in *both* modes at the same time. In other words, some Remotes can be configured for TCP mode while others can be configured (along with the Access Point) for UDP mode.

In this configuration, the Host PC can use both data paths to reach the RTUs. This may be helpful when a mixed collection of RTUs is present where some RTUs can operate in a broadcast form while others cannot. (See Figure 2-19 on Page 40 and Table 2-4 on Page 41)

Operation and Data Flow

- Communicate with RTU A by Telneting to Remote 1, port 30011.
- Communicate with RTU B by Telneting to Remote 2, port 30011.
- Communicate with RTUs C and D by sending and receiving data from the Access Point's COM port.
- All communication paths can be used simultaneously.

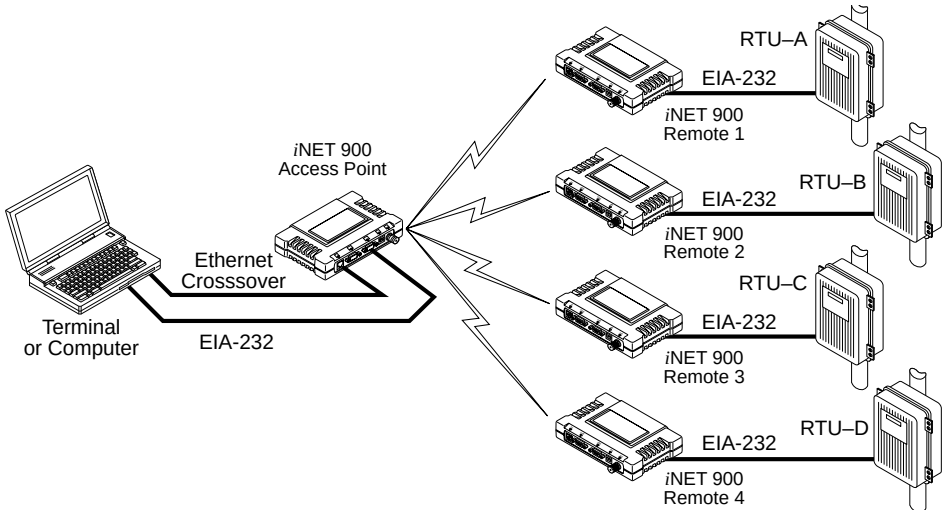


Figure 2-19. Mixed-Modes Application Diagram

Table 2-4. Serial Port Application Configuration

MDS entraNET 900 Unit Location	Menu Item	Setting
Access Point	Status	Enabled
	Baud Rate	9,600
	Flow Control	Disabled
	IP Protocol	UDP
	Send to Address	A multicast IP address such as 224.254.1.1
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	0.0.0.0 (Not Used)
Remote Units 1 & 2 (COM2)	Status	Enabled
	Baud Rate	2,400
	Flow Control	Disabled
	IP Protocol	TCP
	Receive on Port	30011
Remote Units 3 & 4 (COM2)	Status	Enabled
	Baud Rate	9,600
	Flow Control	Disabled
	IP Protocol	UDP
	Send to Address	IP address of the *entraNET* AP
	Send to Port	30011
	Receive on Port	30011
	Receive on Address	224.254.1.1 (The multicast IP address used for the AP's Send To Address above)

2.6 SECURITY CONFIGURATION

There are many options for assisting you in providing secondary security for your transceivers and the network. These options start with controlling remote access to the network via Telnet, Web Browser, and SNMP. Other areas include multiple levels of encryption and MD5-level security for HTTP connections.

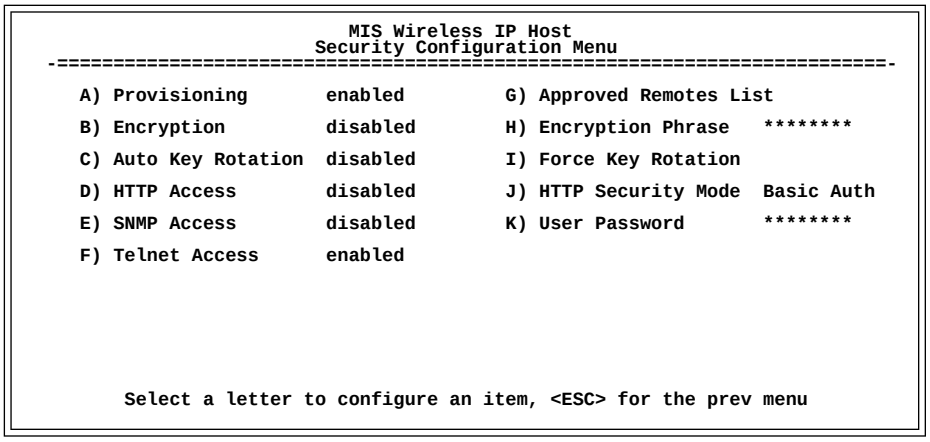


Figure 2-20. Security Configuration Menu
(Access Point Version Shown)

- **`Provisioning`**— Enable provisioning at the Remote. [Enabled/Disabled; Disabled]

  Enabling forces the entraNET 900 to check the *Approved AP List* before continuing the authorization process. In the case of a Remote, the AP must be in the *Approved Access Points List* before it accepts the beacon as valid. In the case of an AP, a Remote must be in the *Approved Remotes List* to be granted authorization. Before enabling this option, at least one entry must already exist in the *Approved List*.
- **`Encryption`**— Enable encryption of over-the-air data packets. [Enabled, Disabled; Disabled]

  Enabling forces the transceiver to use 128-bit encryption on all over-the-air messages. This option requires the Encryption Phrase to be previously configured.
- **`Auto Key Rotation`**—Enable automatic rotation of encryption keys. [Enabled, Disabled; Disabled]

  Enabling forces the transceiver to use the key rotation algorithm to generate a new encryption key after 500 kilobytes of information has been transmitted, or one hour has elapsed. Key rotation prevents reusing encryption data that could result in key-cracking, unlike standard 802.11b communications that rely on static encryption keys.
- **`HTTP Access`**—Prevents remote access through HTTP (Web browser) on Port 80 [Enabled/Disabled; Disabled]

- **SNMP Access**— Prevents remote access through SNMP commands on Port 161 [Enabled, Disabled; Enabled]
- **Telnet Access**—Prevents remote access through Telnet sessions on Port 23 [Enabled, Disabled; Enabled]
- **Approved Access Points/Remotes List (Menu)**—Go to menu providing the creation and management list of units permitted (provisioned) with which this unit will be permitted to communicate.
- **Encryption Phrase**—Phrase (text & numbers) that will be part of the encryption algorithm. [Any 30-character alphanumeric string; Blank]
- **Force Key Rotation**— It triggers an immediate key rotation of the encryption keys before the internal counters do it automatically.
- **HTTP Security Mode**—Select security mode/level of login via HTTP browser. **HTTP Access** disabled prevents access through HTTP. **HTTP Security Mode** is functional if **HTTP Access** is enabled. [Basic Auth, MD5 Digest; Basic Auth]

  Basic mode requires a password, but the actual password text is transmitted in the clear (unencrypted).

  MD5 is the most secure. MD5 Digest protects/encrypts the password but is only supported by Microsoft's *Internet Explorer*™ browser at the time of publication.

User Password—General administrative password only for this unit. Used at log-in via COM1 Port, Telnet and Web browser. [Up to 8-character alphanumeric string without spaces (case-sensitive); Default=**admin**]

TIP: For enhanced security, consider using a misspelled word. This helps protect against sophisticated hackers who may use a database of common words (e.g., dictionary file) to determine a password.

2.6.1 Approved Remotes/Access Points List Menu

This menu is the same for both Access Points and Remotes and the names change to reflect their mode. Replace “Remotes” with Access Points” in the following description.

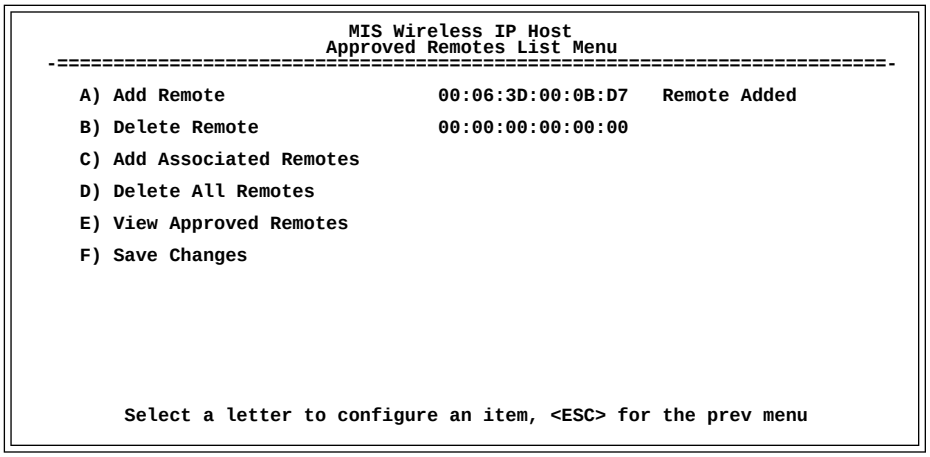


Figure 2-21. Approved Remotes List Menu

- **`Add Remote`**—Enter MAC address of Remote. [Any valid 6-octet MAC address; 00:00:00:00:00:00]
- **`Delete Remote`**—Enter MAC address of Remote.

  For security purposes, you may want to delete a stolen or deprovisioned radio.
- **`Add Associated Remotes`**—Add all currently associated remotes (1-255) to the approved remote list. Alternatively, you can enter each Remote MAC manually.
- **`Delete All Remotes`**—Remove (complete purge) of all Remotes from current list.
- **`View Approved Remotes`**—Simple listing of approved Remotes by MAC address, of radios authorized to join this AP. If a Remote is not in this list, it will not be able to associate with this AP.
- **`Save Changes`**—Save all changes made during this session with this menu. Changes will be implemented only if they are “saved” before exiting this menu.

2.7 PERFORMANCE VERIFICATION

After the basic operation of the radio has been checked, you may wish to optimize the network’s performance using some of the following suggestions. The effectiveness of these techniques will vary with the design of your system and the format of the data being sent.

There are two major areas for possible improvement—the radio and the data network. The following sections will provide you with a variety of

items to check and on many occasions, ways to correct or improve their performance.

2.7.1 Performance Information Menu

This menu/screen is one of two primary sources of information on the radio layer and shows network performance.

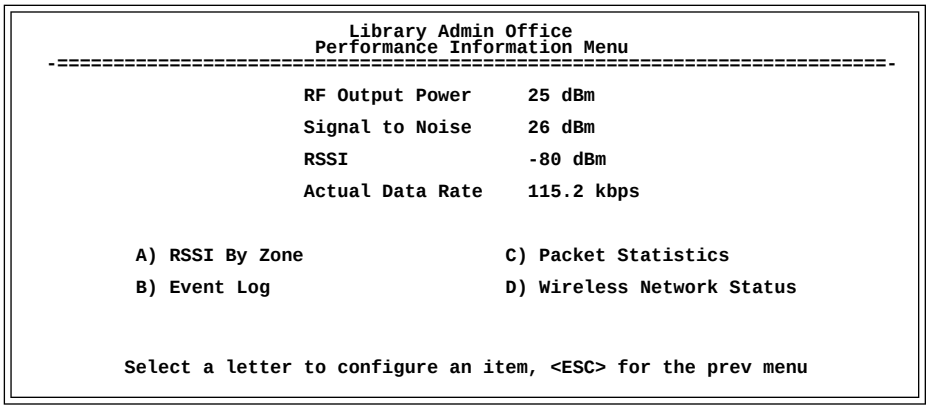


Figure 2-22. Performance Information Menu
(Remote Version Shown)

- **`RF Output Power`** *(Display only)*—Measured power output. (See *"How Much Output Power Can be Used?"* on Page 110)
- **`Signal-to-Noise`** *(Display only)*—Current running-average SNR value all active operating frequencies. (No value displayed on APs)
- **`RSSI`** *(Display only)*—Current running-average Received Signal Strength Indication for all active operating frequencies. (No value displayed on APs.)
- **Actual Data Rate**—Over-the-air transmission rate (as opposed to selected data rate) for the remote being monitored. The fastest data rates can generally be achieved with stronger signal levels.
- **`RSSI by Zone`**—Received Signal Strength Indicator by Zone. (See *"RSSI by Zone Menu (Remotes Only)"* on Page 46)
- **`Event Log`**—Access the menu for managing the unit's log of operational activities.(See *"Authorization Key—Alter the unit's overall capabilities by enabling the built-in resources. (See "Authorization Keys Menu" on Page 71)"* on Page 58)
- **`Packet Statistics`**—Multiple radio and network operating statistics. (See *"Packet Statistics Menu"* on Page 49)
- **`Wireless Network Status`** *(Displayed only at Remotes)*—Current association state and MAC address of the Access Point. (See *"Wireless Network Status (Remotes Only)"* on Page 50)
- **`Remote Listing`** *(AP Display only)*—List of basic information for all Remote units currently associated with this Access Point. (See *"Remote Listing Menu (Access Points Only)"* on Page 52)

- **`Endpoint Listing`** *(AP Display only)*—List of units accessible by this AP through associated Remote ports. (See *"Endpoint Listing Menu (Access Points Only)"* on Page 53)
- **`Remote Performance Listing`** *(AP Display only)*—(See *"Remote Performance Listing Menu (Access Points Only)"* on Page 54)

RSSI by Zone Menu *(Remotes Only)*

This screen displays the strength of RF signals received from the currently associated Access Point.

Wireless network integrity depends partially on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than –80 dBm will provide reliable communication that includes a 15 dB fade margin.

If you find there is a poor signal level on one zone, check the *Packet Statistics Menu* section on Page 49 and record the values. Then, set the questionable zone to "Skipped" in the Radio Configuration Menu (Page 29) and look for an improvement in the Packet Statistics error rates. If there is none, return the Zone to "Active."

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

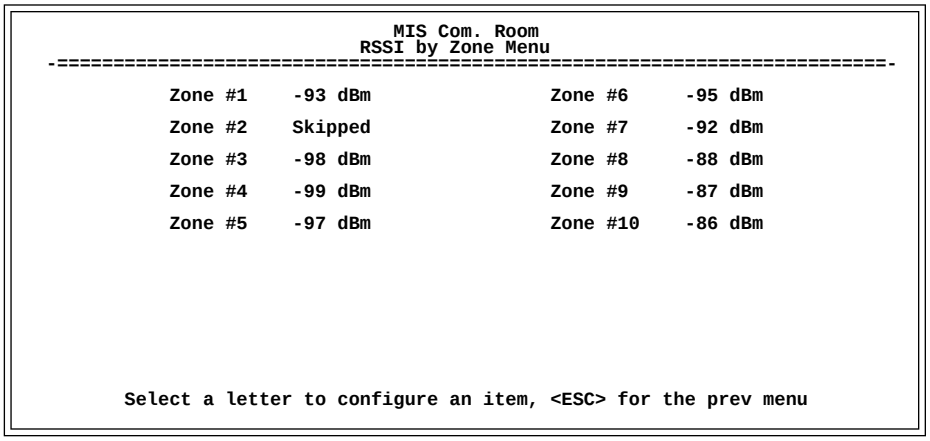


Figure 2-23. RSSI by Zone Menu

TIP: Under normal circumstances, the signal levels in each zone should be within a few decibels of each other. If you see one that is significantly lower or higher, it may be a sign of radio frequency interference from another signal source on the 900 MHz band. See *"Network Performance Notes"* on Page 54 for further information.

Event Log Menu

The transceiver's microprocessor monitors many operational parameters and logs them. Events are classified into four levels of importance, which are described in Table 2-5. Some of these events will result from a condition that prevents the normal of the unit—these are "critical" events. These will cause the unit to enter an "alarmed" state and the POWER LED to blink until the condition is corrected. All events are stored in the Events Log that can hold up to 8,000 entries**.**

Table 2-5. Event Classifications

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

Time and Date

The events stored in the Event Log are time-stamped using the time and date of the local transceiver. Remote transceivers obtain this information from the Access Point when they associate with it. The Access Point obtains the time and date from a Time Server. This server can generally be provided by a standard Windows PC server SNTP application. In the absence of the SNTP services, the user must manually enter it at the Access Point. (See *"Device Information Menu"* on Page 25 for SNTP server identification.) The manually set time and date clock is dependent on the unit's primary power. A loss of power will reset the clock to January 1, 2002 but will not affect previously stored error events.

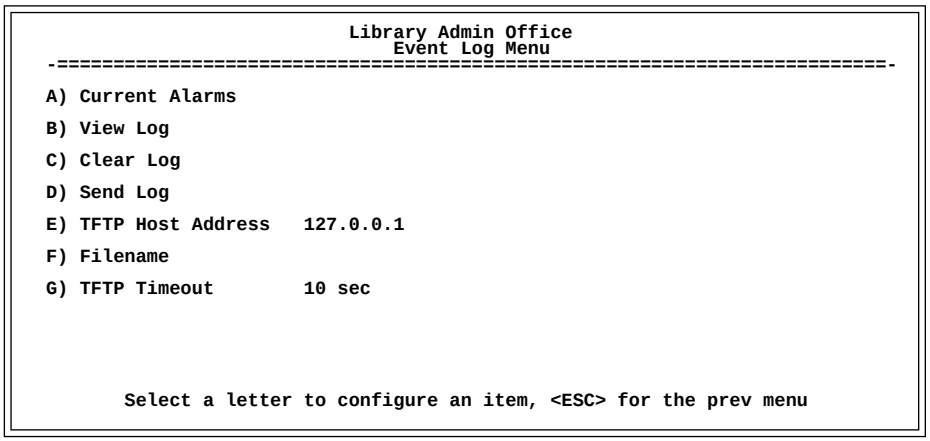


Figure 2-24. Event Log Menu

- **`Current Alarms`** *(Telnet/Terminal only)*—View list of root causes that have placed the Device Status in the alarmed state. (See *"Alarm Conditions"* on Page 92)
- **`View Log`**—View a list of events stored in the current log. Some of these events are stored in volatile memory and will be erased with a loss of power.

- **`Clear Log`**—Purges the log of all events

  TIP: Save your Event Log before choosing to clear it in order to retain potentially valuable troubleshooting information. (See *"Upgrading the Firmware"* on Page 59 for an overview on how to transfer files from the transceiver to a computer on the network using TFTP.)

- **`Send Log`** *(Telnet/Terminal only)*—Initiate TFTP transfer of the unit's event Event Log in a plain text (ASCII) file to a TFTP server at the remote location.
- **`TFTP Host Address`** *(Telnet/Terminal only)*—IP address of the computer on which the TFTP server resides.
  [Any valid IP address; 127.0.0.1]
- **`Filename`** *(Telnet/Terminal only)*—Name to be given to the Event Log file sent to the TFTP server for archiving.
  [Any 40-char alphanumeric string; Blank]

  NOTE: You may want to change it to reflect the type of log you intend to archive and/or its date.
- **`TFTP Time-out`** *(Telnet/Terminal only)*—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the *transceiver* before suspending the file transfer.
  [10 to 120 seconds; 10]

View Current Alarms

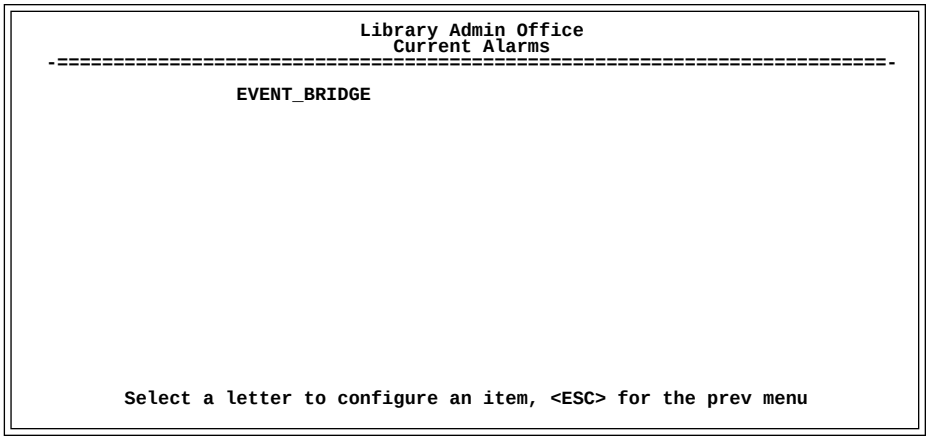


Figure 2-25. Current Alarms Screen

View Event Log

```
                          Library Admin Office
                                Event Log
  -=============================================================================-

Num    Date         Time   Description
-------------------------------------------------------------------------------
==START OF OPERATIONS LOG==
    1  28 Dec 2001  23:21  Hop Table Write Successful
    2  28 Dec 2001  23:21  Scanning Started
    3  29 Dec 2001  20:55  Received Beacon OK
    4  29 Dec 2001  20:55  Hop Table Write Successful
    5  29 Dec 2001  20:55  Expected Sync Established
    6  29 Dec 2001  20:55  Hop Sync Established
    7  29 Dec 2001  20:55  Association Established
    8  29 Dec 2001  20:56  Association Lost
    9  29 Dec 2001  20:56  Hop Table Write Successful
   10  29 Dec 2001  20:56  Scanning Started
   11  29 Dec 2001  20:57  Received Beacon OK
   12  29 Dec 2001  20:57  Hop Table Write Successful
   13  29 Dec 2001  20:57  Expected Sync Established
   14  29 Dec 2001  20:57  Hop Sync Established


  Use Up, Down, Pg-Up, Pg-Dn, Home or End to view log, <ESC> for the prev menu
```

Figure 2-26. Sample Event Log Screen

Packet Statistics Menu

```
                          Library Admin Office
                        Packet Statistics Menu
-=============================================================================-

    Wireless Packet Statistics          Ethernet Packet Statistics

       Packets received 2206               Packets received      0
       Packets sent     2177               Packets sent          2172
       Bytes received   247575             Bytes received        0
       Bytes sent       236106             Bytes sent            161877
       Packets dropped  0                  Packets dropped       0
       Receive errors   1                  Receive errors        0
       Retries          4                  Lost carrier detected 0
       Retry errors     2

       A) Clear Wireless stats             B) Clear Ethernet stats




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

Figure 2-27. Sample Packet Statistics Menu

Wireless Packet Statistics

- **`Packets received`**—Over-the-air data packets received by this unit
- **`Packets sent`**—Over-the-air data packets sent by this Remote.
- **`Bytes received`**—Over-the-air data bytes received by this Remote.
- **`Bytes sent`**—Over-the-air data bytes sent by this Remote.
- **`Packets dropped`**—Received packets dropped as a result of a lack of buffers.
- **`Receive errors`**—Packets that do not pass CRC. This may be due to transmissions corrupted by RF interference.
- **`Retries`**—Number of requests to re-send a data packet
- **`Retry errors`**—Packets discarded after exceeding five retries over-the-air.
- **`Clear Wireless stats`**—Resets the statistics counter.

Ethernet Packet Statistics

- **`Packets received`**—Packets received by the transceiver through the Ethernet port.
- **`Packets sent`**—Packets received by the transceiver through the Ethernet port.
- **`Bytes received`**—Data bytes received by this Remote.
- **`Bytes sent`**—Data bytes sent by this Remote.
- **`Packets dropped`**—Received packets dropped as a result of a lack of buffers.
- **`Receive errors`**—Packets discarded after exceeding five retries the network.
- **`Lost carrier detected`**—A count of how many times the carrier signal on the Ethernet port has been missing. This count increase significantly when the Ethernet cable is plugged in and unplugged.
- **`Clear Ethernet stats`**—Resets the statistics counter.

Wireless Network Status

(Remotes Only)

The Wireless Network Status screen provides information on a key operating process of the transceiver—the association of the Remote with the Access Point. The following is a description of how this process takes place and as monitored on the *Figure 2-28. Wireless Network Status Screen"* on page 51.

The Association Process

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

Under normal circumstances, the association process should be completed within 20 seconds after boot-up.

Remote units are always monitoring the beacon signal. If an associated Remote loses the AP's beacon for more than 20 seconds, the association process starts again.

The Wireless Network Status Screen

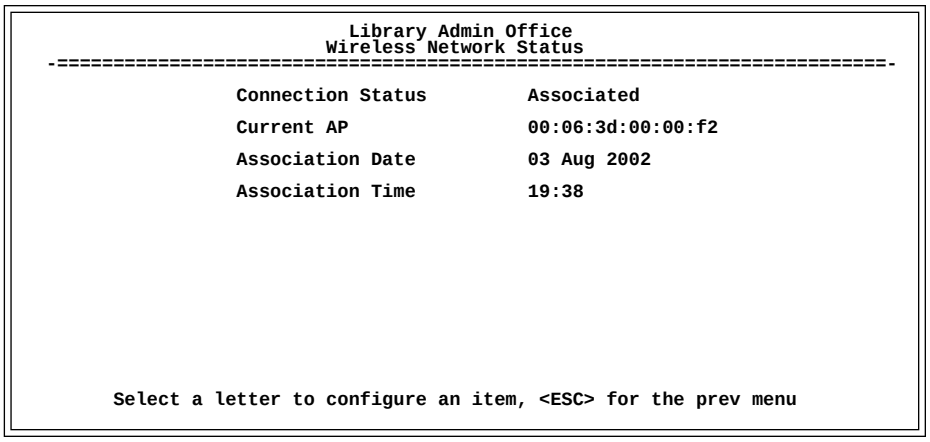


Figure 2-28. Wireless Network Status Screen

- **Connection Status**—Current state of the wireless network communication.
  - *Scanning*—The unit is looking for an Access Point beacon signal.
  - *Exp(ecting) Sync(hronization)*—The unit has found a valid beacon signal for its network.
  - *Hop Sync*—The unit has changed its frequency hopping pattern to match that of the Access Point.
  - *Associated* —This unit has successfully synchronized and associated with an Access Point. This is the normal status.
  - *Alarmed*—The unit is has detected one or more alarms that have not been cleared.
- **Current AP**—Wireless address of Access Point with which the Remote is associated.
- **Association Date**—Date of last successful association with an Access Point.
- **Association Time**—Time of day association was established on the association date.

Remote Listing Menu

(Access Points Only)

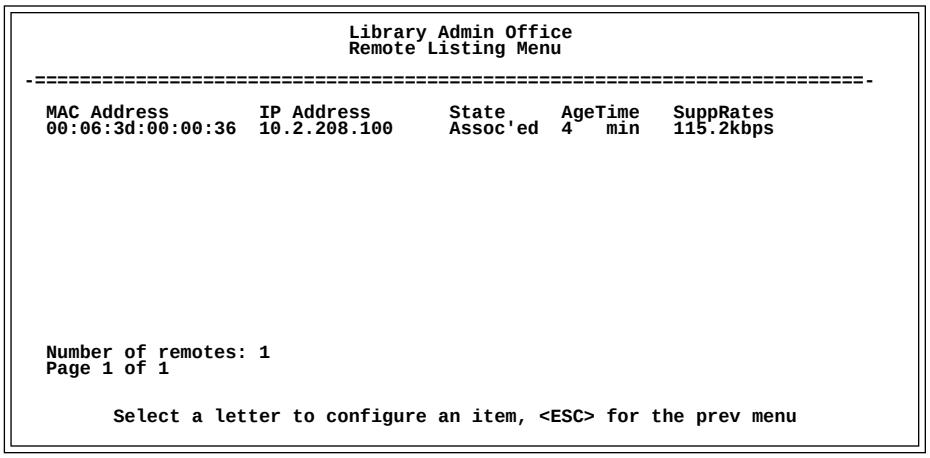


Figure 2-29. Remote Listing Menu
(List of MDS transceiver units associated with this AP)

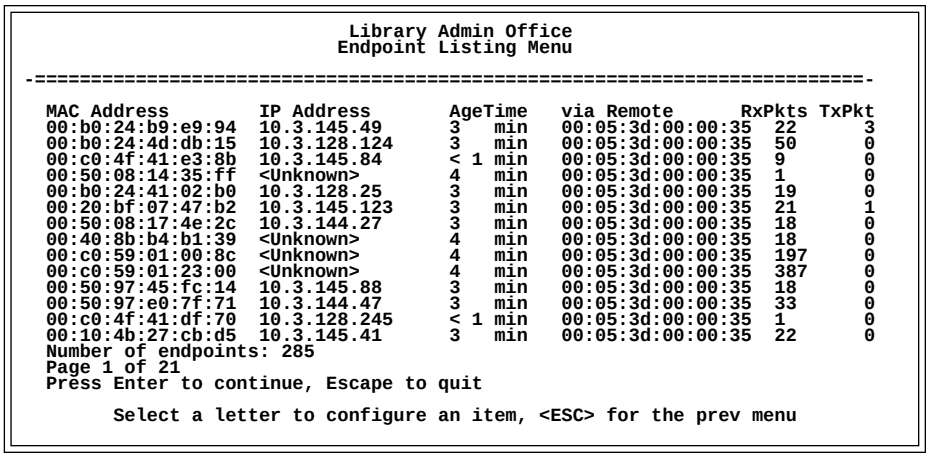
- **MAC Address**—Hardware address of Remote.
- **IP Address**—IP Address of Remote.
- **State**—Current association state of Remote.
- **AgeTime**—Time, in minutes, remaining before the device (address) will be deleted from the table.

  Each transceiver maintains a table with the addresses of the devices it communicates with. The age time countdown is restarted to 5 minutes every time a message to/from that device is detected. If no traffic with that device happens, it then "ages out" of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.
- **SuppRates**—Supported data rate by this unit.

Endpoint Listing Menu

(Access Points Only)

This list shows all of the non-entraNET 900 Ethernet devices that are known to the transceiver and is equivalent to the ARP table of IP devices.



```
                          Library Admin Office
                        Endpoint Listing Menu

-=============================================================================-

  MAC Address        IP Address       AgeTime   via Remote      RxPkts TxPkt
  00:b0:24:b9:e9:94  10.3.145.49      3   min   00:05:3d:00:00:35  22      3
  00:b0:24:4d:db:15  10.3.128.124     3   min   00:05:3d:00:00:35  50      0
  00:c0:4f:41:e3:8b  10.3.145.84      < 1 min   00:05:3d:00:00:35  9       0
  00:50:08:14:35:ff  <Unknown>        4   min   00:05:3d:00:00:35  1       0
  00:b0:24:41:02:b0  10.3.128.25      3   min   00:05:3d:00:00:35  19      0
  00:20:bf:07:47:b2  10.3.145.123     3   min   00:05:3d:00:00:35  21      1
  00:50:08:17:4e:2c  10.3.144.27      3   min   00:05:3d:00:00:35  18      0
  00:40:8b:b4:b1:39  <Unknown>        4   min   00:05:3d:00:00:35  18      0
  00:c0:59:01:00:8c  <Unknown>        4   min   00:05:3d:00:00:35  197     0
  00:c0:59:01:23:00  <Unknown>        4   min   00:05:3d:00:00:35  387     0
  00:50:97:45:fc:14  10.3.145.88      3   min   00:05:3d:00:00:35  18      0
  00:50:97:e0:7f:71  10.3.144.47      3   min   00:05:3d:00:00:35  33      0
  00:c0:4f:41:df:70  10.3.128.245     < 1 min   00:05:3d:00:00:35  1       0
  00:10:4b:27:cb:d5  10.3.145.41      3   min   00:05:3d:00:00:35  22      0
  Number of endpoints: 285
  Page 1 of 21
  Press Enter to continue, Escape to quit

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

Figure 2-30. Endpoint Listing Menu
(Lists all equipment attached to REMOTE transceivers in the network)

- **MAC Address**—Hardware address of endpoint device.
- **IP Address**—IP Address of endpoint device.
- **AgeTime**—Time, in minutes, remaining before the device (address) will be deleted from the table.

  Each transceiver maintains a table with the addresses of the devices it communicates with. The age time countdown is restarted to 5 minutes every time a message to/from that device is detected. If no traffic with that device happens, it then "ages out" of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.
- **via Remote**—Hardware address of the transceiver connected to this device.
- **RxPkts**—Over-the-air data packets received by the transceiver. and passed on to the endpoint device.
- **TxPkt**—Number of packets received from the endpoint device and passed over-the-air.

Remote Performance Listing Menu

(Access Points Only)

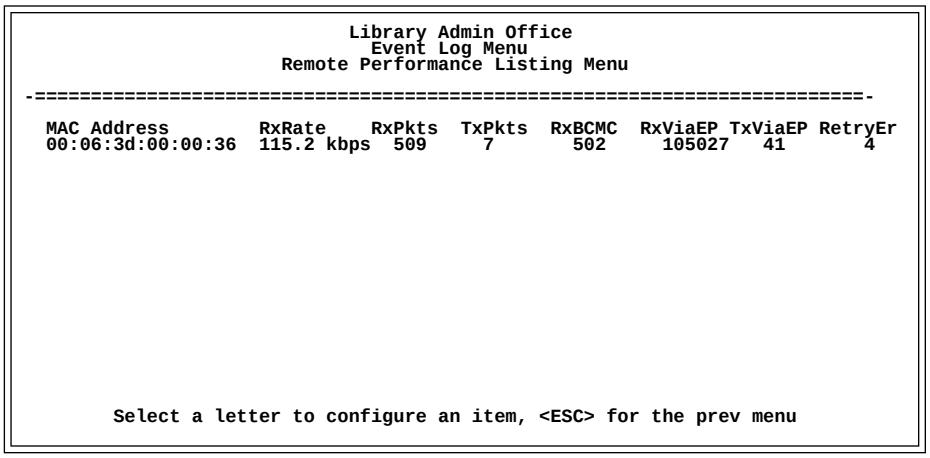


Figure 2-31. Remote Performance Listing Menu

This screen provides a unit-by-unit summary of all Remote units currently associated with this Access Point. The parameters are displayed in a column format with each line corresponding to one Remote.

- **RxRate**—Over-the-air data rate the transceiver is currently using. All units do *not* need to use the same rate.
- **RxPkts**—Over-the-air data packets received from this unit.
- **TxPkts**—Over-the-air data packets sent to this unit.
- **RxBCMC**—Total number of Broadcast and/or Multicast packets received over-the-air.
- **RxViaEP**—Packets received by the transceiver through the Ethernet port.
- **TxViaEP**—Packets sent by the transceiver through the Ethernet port.
- **RetryEr**—Packets discarded after exceeding five retries over-the-air.

2.7.2 Network Performance Notes

Principles of Network Operation

The following is a list of points that could be of value in dealing with the networking aspects of the transceiver.

1. The transceiver serves as a network bridge
    - The transceiver goes through a “listening and learning” period at start-up before it will send any packets over either of its ports. This lasts about 10 seconds after the CPU’s operating system has finished its boot cycle.

- The bridge code in the transceiver operates and makes decisions about packet forwarding just like any other bridge. The bridge code builds a list of source MAC addresses that it has seen on each of its ports. There are a few general rules that are followed when a packet is received on any port:
- If the destination address is a multicast or broadcast address, forward the packet to all other ports.
- If the destination address is not known, forward the packet to all other ports.
- If the destination address is known, forward the packet to the port that the destination is known to be on (usually the RF port).
- The bridge code uses Spanning Tree Protocol (STP) to prevent loops from being created when connecting bridges in parallel. For example, connecting two remotes to the same wired LAN could create a loop if STP was not used. Every bridge running STP sends out Bridge Protocol Data Units (BPDU's) at regular intervals so that the spanning tree can be built and maintained. BPDU's are 60-byte multicast Ethernet frames.

2. The wireless MAC has two settings that can be adjusted.

   - **Fragmentation threshold** is the threshold in bytes, which causes the MAC to fragment a packet.
   - **RTS threshold** is the threshold in bytes that causes the MAC to use RTS/CTS before sending the packet.

3. Throughput calculations must take into account all overhead.

The following is an example of the overhead at each layer for a 100-bytes of data over UDP:

- Data: 100 bytes
- UDP header: 8 bytes
- IP header: 20 bytes
- Ethernet header: 14 bytes
- 802.11 header 24 bytes
- LLC and SNAP header: 8 bytes
- FHSS header and FCS: 16 bytes

Total over-the-air frame size=190 bytes

If the frame is directed (for example: not multicast/broadcast), the 802.11 ACK frame must be accounted for:

- 14 bytes—802.11 ACK
- 30 bytes—Over-the-air ACK frame (added 16 the FHSS PHY)

If the 802.11 encapsulated Ethernet frame (NOT the UDP or Ethernet frame) exceeds the RTS threshold, then the overhead for RTS/CTS frames must also be accounted for.

- 20 bytes—802.11 RTS.
- 14 bytes—802.11 CTS.
- 66 bytes—Total Over-the-air bytes for RTS/CTS with PHY headers.

If the frame is TCP, then there is a 32-byte TCP header instead of the 8-byte UDP header.

- ARP requests, ARP replies and BPDU's will affect throughput.
- ARP requests are 60-byte Ethernet frames. 142 bytes over-the-air.
- ARP replies are 60-byte Ethernet frames. 142 bytes over-the-air.
- BPDUs are 60-byte Ethernet frames. 142 bytes over-the-air.

  Note that the overhead to put a single Ethernet frame over-the-air is 82 bytes. If RTS/CTS is invoked, it is 148 bytes. Therefore, the overhead for a minimal Ethernet frame (60 bytes) is 128% and, as such, gives the transceiver a poor small-packet performance.

If any transceiver in your entraNET network is connected to a large LAN, such as may be found in a large office complex, there may be undesired multicast/broadcast traffic over the air.

4. Station-to-Station Traffic

   - When sending frames from an endpoint connected to one transceiver to *another* endpoint with a different transceiver, the throughput will be halved at best. This is because all frames must go through the AP. Therefore, in the previous 100-byte UDP example, the number of over-the-air bytes will be 380 bytes (190 bytes x 2) if the frame has to go station-to-station.

5. Interference has a direct correlation to throughput.

   - Interference could be caused by any unnecessary traffic on the network from unrelated activities, or Radio Frequency Interference in the wireless spectrum.

Tips for Optimizing Network Performance

Here are some suggestion on things to try that may maximize throughput:

1. *AP Only:* Increment the **Dwell Time** to the maximum of 262.1 ms. This lowers the overhead since it will stay longer on a channel. The down side is that if a particular channel is interfered with it will take longer to hop to another channel.
   (**Main Menu>Radio Configuration>Dwell Time**)

2. *AP Only:* Change the **Beacon Period** to **Normal** (508 ms). This will also reduce the overhead of beacons sent out. On the down side, association time may be a little longer.
(**Main Menu>Radio Configuration>Beacon Period**)

3. Change the **Fragmentation Threshold** to the maximum of 1600. Longer packets will be sent over the air reducing overhead. On the down side, if a packet is corrupted it will take longer to be retransmitted.
(**Main Menu>Radio Configuration>Fragmentation Threshold**)

4. Increase the **RTS Threshold** to 1600. RTS mechanism is used to reserve a time slot if packets exceed this number. On the down side, a hidden-node might interfere more often than if RTS is not used.
(**Main Menu>Radio Configuration>RTS Threshold**)

5. Decreasing the **RTS Threshold,** to the 100 to 200 range, will improve throughput on a busy network. It will add small packets, but reduce collisions (and resulting re-tries) of large packets.
(**Main Menu>Radio Configuration>RTS Threshold**)

6. Use **Performance Information Menu** to check RSSI by zone.
(Remotes Only / **Main Menu>Performance Information>RSSI by Zone**)

   Readings should be close in value (±2 dB). A lower value might indicate interference. Block the zones at the Access Point that affect the Remotes. (**Main Menu>Radio Configuration>Skip Zone Option**)

7. Use **Performance Information Menu** to check for errors, retries and dropped packets. Do the same with Ethernet traffic.

   With weak signals, interference, or hidden nodes, the optimal performance may be lower due to collisions and retries.

Data Latency—TCP versus UDP Mode

The latency of data passing through a network will depend on user data message length, the overall level of traffic on the network, and the quality of the radio path.

Under ideal conditions—low traffic and good RF signal path—the latency for units operating in the TCP mode, will typically be around 5 ms in each direction. However, when UDP multicast traffic is transported, the outbound packet latency (from AP to remote) is dependent on the beacon period.

UDP multicast packet latency can be minimized by setting the **Beacon Period** to "**Fast**" (52 ms). Changing beacon rate to **Fast** will result in an average latency of 29 ms, assuming outbound packets wait for a beacon transmission 50% of the time (26ms) plus the normal packet latency (5 ms).

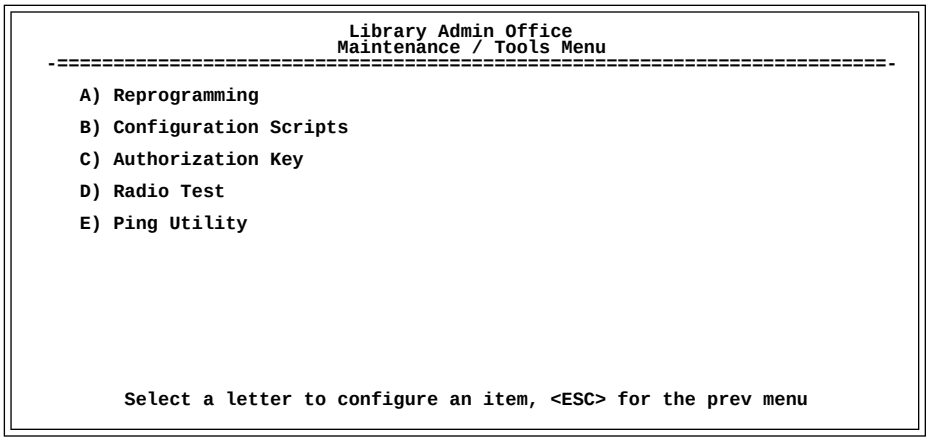
2.8 MAINTENANCE

In the normal course of operating an transceiver network, you will want to take advantage of product improvements, and to read and archive the configuration of your individual transceivers. The *Maintenance Menu* provides several tools to make this possible. This section provides detail information on how to take advantage of these services.

The three maintenance tasks are:

- Reprogramming— Managing and selecting the unit's operating system firmware resources. *(See "Reprogramming Menu"* on Page 58*)*
- Configuration Scripts—Saving and importing data files containing unit operating parameters/settings. *(See "Configuration Scripts Menu"* on Page 63*)*
- Authorization Key —Alter the unit's overall capabilities by enabling the built-in resources. (*See "Authorization Keys Menu"* on Page 71*)*
- Radio Test—A diagnostic tool for testing RF operation. (See *"Radio Test Menu"* on Page 71)
- Ping Utility—Diagnostic tool to test network connectivity. (See *"Ping Utility Menu"* on Page 73)

Figure 2-32. Maintenance Menu



2.8.1 Reprogramming Menu

The transceiver has two copies of the firmware (microprocessor code) used for the operating system and applications. One copy is "active" and the second one is standing by, ready to be used. You can upload a new

release into the inactive position and place it in service whenever you desire.

```
                          Library Admin Office
                           Reprogramming Menu
-=============================================================================-

     A) TFTP Host Address  10.4.2.1
     B) Filename           entranet-bkrf-3_1_0.ipk
     C) TFTP Timeout       120 sec
     D) Retrieve File
     E) Image Verify
     F) Image Copy
     G) Reboot Device
        Current Firmware   Image 1: 1.1.0  (active)
                           Image 2: 1.1.0


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

Figure 2-33. Reprogramming Menu
(Shown with "Image Copy" Selected)

- **`TFTP Host Address`**—IP address of the host computer from which to get the file. [Any valid IP address]
- **`Filename`**—Name of file to be received by the TFTP server. [Any 40-character alphanumeric string] Verify that this corresponds to the TFTP directory location. May require sub-directory, for example: **br\inet-bkrf-3_1_0.ipk.**
- **`TFTP Timeout`**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [10 to 120 seconds; 10]
- **`Retrieve File`**—Initiate the file transfer from the file from TFTP server. Placed into inactive firmware position in the transceiver's non-volatile memory [Y, N]
- **`Image Verify`**—Initiate the verification of the integrity of firmware file held in unit.
- **`Image Copy`**—Initiate the copying of the active firmware into the inactive image.
- **`Reboot Device`**—Initiate rebooting the transceiver. This will interrupt data traffic through this unit, and the network if performed on an Access Point. Intended to be used to toggle between firmware images.

NOTE: See *"Upgrading the Firmware"* on Page 59 for details on setting up the TFTP server.

Upgrading the Firmware

From time-to-time MDS will offer upgrades to the transceiver firmware. One version of the firmware provides core software resources for all radio models. Uploading new firmware into the unit will not alter any privileges provided by Authorization Keys and does not require the transceiver to be taken off-line until you want to operate the unit from the new firmware image in the unit.

You must use the embedded entraNET Management System for all firmware activities, including uploading from a TFTP server.

The uploads can be initiated through any of the three entraNET Management System gateways:

- **Terminal-Emulator**—Use a terminal emulator program on your PC, such as HyperTerminal, connected directly to the transceiver's COM1 port via a serial cable.
- **Telnet**—Text-based access to the Management System through a network connection.
- **Web Browser**—Connect to the transceiver using a Web browser on a local PC connected directly to the transceiver's LAN port or associated network.

Firmware images are provided free-of-charge on the MDS Web site at: **www.microwavedata.com/service/technical/support**

Installing Transceiver Firmware by TFTP

To install firmware by TFTP, the user will need:

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

If you do not know your computer's address on a Windows PC, you can use the **RUN** function from the **Start** menu and enter **winipcfg** or **ipconfig** to determine your local PC's IP address. The IP address of the radio can be found under the entraNET Management Systems' **Configuration** menu. (*See "Network Configuration Menu"* on Page 27.)

A TFTP server can be found on the MDS Web site at: **www.microwavedata.com/service/technical/support/downloads.asp**

There are several alternatives to connecting the transceiver to the server containing the firmware and TFTP server, and a computer control point. Figure 2-34 and Figure 2-35 show two variations. It is essential all of the equipment be on the same subnet.

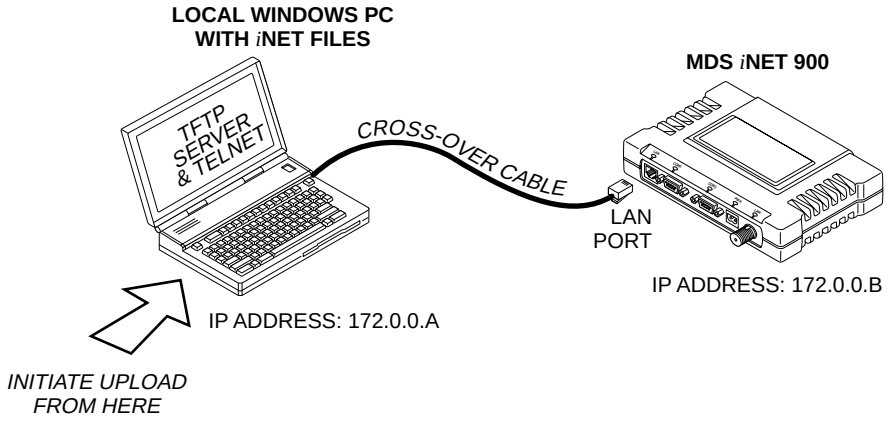


Figure 2-34. Upload Configuration—Option 1
(TFTP Server and Firmware File on Same CPU)

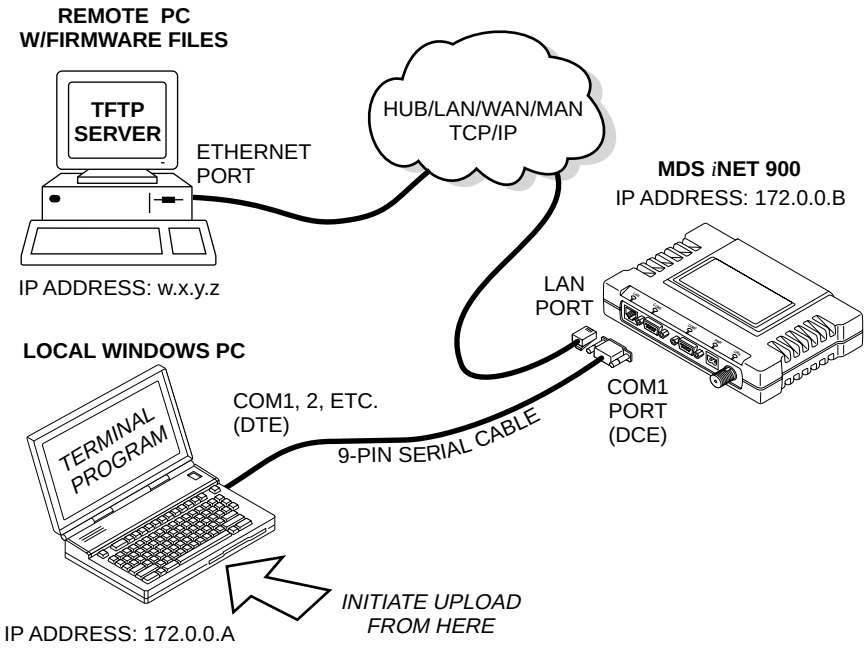


Figure 2-35. Upload Configuration—Option 2
(TFTP Server and Firmware File on Remote Server)

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

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

Upload Procedure

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

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

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

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

4. Fill in the information for the:

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

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

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

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

---

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

7. Test the transceiver for normal operation.

End of Procedure

2.8.2 Configuration Scripts Menu

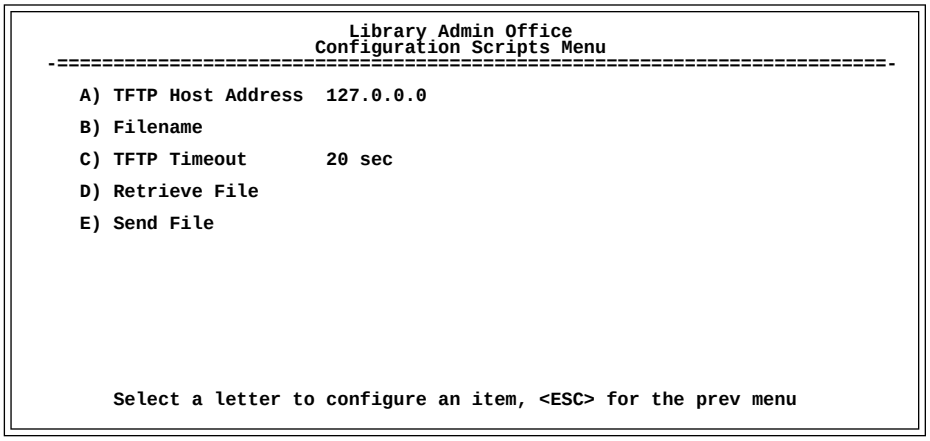


Figure 2-36. Configuration Files Menu

- **`TFTP Host Address`**—IP address of the computer on which the TFTP server resides. [Any valid IP address]
- **`Filename`**—Name of file containing this unit's configuration profile that will be transferred to the TFTP server. The configuration information will be in a plain-text ASCII format. [Any 40-character alphanumeric string] May require sub-directory, for example: **config\inet-config.txt.** (See *"Using Configuration Scripts"* on Page 64)

  NOTE: The filename field is used in identifying the desired incoming file and as the name of file being exported to the TFTP server. Before exporting the unit's configuration, you may want to name it something that reflect the unit's services or identification.
- **`TFTP Timeout`**—Time in seconds the TFTP server will wait for a packet ACK (acknowledgment) from the transceiver before suspending the file transfer. [10 to 120 seconds; 10]
- **`Retrieve File`**—Initiate the file transfer of the configuration file from TFTP server into the transceiver.
- **`Send File`**—Initiate the file transfer from the transceiver's current configuration file to TFTP server.

NOTE: See *"Upgrading the Firmware"* on Page 59 for details on setting up the TFTP server.

A brief description of configuration files

If you plan to have more than a few transceivers in your network, use the configuration file feature to configure similar units from a common set of parameters. There are over 50 user-controllable settings that can be used to optimize the network and saved into a Configuration File. However, only four essential parameters need to be reviewed and altered to use the file with another transceiver.

A Configuration File (data file) will make it easy to apply your unique settings to any transceiver(s) you wish. Configuration files will also provide you with a tool to restore parameters to a "known good" set, in the event that a parameter is improperly set and performance is affected. (See *"Using Configuration Scripts"* on Page 64 for detailed instructions and a sample configuration file.)

Using Configuration Scripts

Configuration Scripts can be created and downloaded from the transceiver that contain a wealth of information on the unit. This file can serve many purposes, not the least of which is to keep a permanent "snapshot" of the unit's configuration at a point in time. These files can also be used to view the setup of a unit without needing to connect to it. Examining archival files can be a useful source of information during troubleshooting.

In the next few sections you will learn about the contents of the file and, how to use it as a template for configuring multiple transceivers with the same profile. Ultimately, standardized files can be uploaded into the transceiver to speed up the installation process.

Configuration Files can also be uploaded into a transceiver to restore the settings of a unit using a previously saved configuration of the unit. This is particularly convenient after finishing a test using some experimental settings.

Sample of an Exported Configuration File

The following is a sample of a typical configuration file as produced by a transceiver that contains over 150 parameters; many of which are user editable. The presentation has been slightly altered to allow notes to appear below associated parameter lines. Some of the values used in the calibration of the unit's built-in test equipment have been deleted to reduce space. This presentation is offered as a guide to the type of information contained in the file. See *"Editing Configuration Files"* on Page 70 for further information.

NOTE: The parameter names and the data values from the Exported Configuration File are shown in bolded text. Any description will be found below in an indented paragraph. Descriptions for parameters that are functionally identical to both COM1 & COM2 are not repeated.

Beginning of Configuration File

; MDS entraNET

; Created 00-03-2002 6:59:41

IP Address: 192.168.1.1

The IPv4 address of this unit. This field is unnecessary if DHCP is enabled.

NOTE: Changing the IP value via the network will cause a loss of communication with other devices unaware of the new address.

IP Netmask: 255.255.255.0

The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled.

IP Gateway: 0.0.0.0

The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled.

Ethernet Address: 00:06:3D:00:00:5D

The physical Ethernet MAC (Media Access Controller) address of the device. This value is set by the factory and cannot be changed.

Wireless Address: 00:06:3D:00:00:5C

The physical wireless MAC (Media Access Controller) address of the device. This value is set by the factory and cannot be changed.

Model Number: 900

The model number of this unit. This value is set by the factory and cannot be changed.

Serial Number: 1026295

The serial number of this unit. This value is set by the factory and cannot be changed.

Unit Name: Library Admin Office

A name for this unit. It appears at the top of every menu screen.

Owner: Hilltop College MIS

The name of the owner of this unit.

Contact: MIS Dept. X232

The contact person regarding this unit.

Description: Link to Campus Server

A brief general description of this unit.

Location: Hollister Bldg. RM450

The location of this unit.

Com1 Port Config: 8N1

Configuration of character size, type of parity, and number of stop bits to be used.

Com2 Port Config: 8N1

Configuration of character size, type of parity, and number of stop bits to be used

Max Remotes Allowed: 50

The maximum number of remotes allowed to connect to this Access Point.

Device Mode: Access Point

Configures the unit to act as a Remote or an Access Point. The Access Point option is not allowed unless the unit is specifically ordered as such, or an Authorization Key has been purchased to allow it.

Dwell Time: 32.8

The amount of time the unit spends at any given frequency in its hopping pattern. This field is only changeable by an Access Point. Remotes read the Masters value upon association.

Hop Pattern: 1

RSSH Calibration: 235

RSSL Calibration: 190

Freq Calibration: 8402

Network Name: West Campus Net

The name of the network this unit belongs to. The unit will only communicate with devices having identical *Network Names*.

Date Format: Generic

Specifies the format of the date.

- Generic = dd Mmm yyyy
- European = dd-mm-yyyy
- US = mm-dd-yyyy

Console Baud: 19200

The baud rate of the serial menu console. Default value is 19200 bps.

Company Name: MDS

Version Name: 06-1234567

Product Name: entraNET

Beacon Period: Normal

The amount of time in milliseconds between beacon transmissions by the AP.

Data Rate: 115.2 kbps

The selected over-the-air data rate. A lower data rate generally allows more distance between the unit and its Access Point.

RF Output Power Setpoint: 30

The desired amount of RF output power, measured in dBm.

Power Cal Table DAC1: 98

21 additional values follow; do not alter

Active Boot Image: 0

Tx Coefficient1: 0

31 additional values follow; do not alter

Rx Coefficient1: 0

14 additional values follow; do not alter

Skipped Hop Zone1: Active

Skipped Hop Zone2: Skip

Skipped Hop Zone3: Active

Skipped Hop Zone4: Active

Skipped Hop Zone5: Active

Skipped Hop Zone6: Active

Skipped Hop Zone7: Active

Skipped Hop Zone8: Active

Skipped Hop Zone9: Active

Skipped Hop Zone10: Active

Firmware TFTP Host IP: 63.249.227.105

Address of the TFTP Host from which firmware images are downloaded

Firmware TFTP Filename: entraNET-krf-3_0_0.ipk

Eventlog TFTP Host IP: 192.168.1.3

Address of TFTP Host to which to send the event log

Eventlog TFTP Filename:

Config Script TFTP Host IP: 192.168.1.33

Address of TFTP Host to which to send the event log

Config Script TFTP Filename: entraNET_config.txt

Fragmentation Threshold: 1600

Maximum packet size allowed before fragmentation occurs

RTS Threshold: 500

Number of bytes for the RTS/CTS handshake boundary

RSSI Threshold: 0

RSSI value at that the connection is deemed “degraded”

SNR Threshold: 0

SNR value at that the connection is deemed “degraded”

SNMP Read Community: public

Community string for read access using SNMPv1

SNMP Write Community: private

Community string for write access using SNMPv1

SNMP Trap Community: public

Community string sent with traps using SNMPv1

SNMP Trap Manager #1: 0.0.0.0

IP Address of a SNMP manager to which traps will be sent

SNMP Trap Manager #2: 0.0.0.0

SNMP Trap Manager #3: 0.0.0.0

SNMP Trap Manager #4: 0.0.0.0

SNMP Trap Manager #5: 0.0.0.0

Auth trap enable: disabled

Setting to enable SNMP authentication traps

Trap Version: v1 Traps

Selects which SNMP trap format

Package 1 Version: 1.1.0

Indicates the version of firmware in Image 1

Package 2 Version: 1.1.0

TFTP Timeout: 20

Com1 Serial Data Enable: disabled

Setting to enable COM1 data mode

Com1 Serial Data Mode: UDP

IP Protocol for COM1 data mode

Com1 Serial Data Baud Rate: 9600

Baud rate for COM1 data mode

Com1 Serial Data Tx IP Address: 0.0.0.0

COM1 data will be sent to this IP address

Com1 Serial Data Tx IP Port: 0

COM1 data will be sent to this IP port

Com1 Serial Data Rx IP Port: 0

COM1 data will be received on this IP port

Com2 Serial Data Enable: enabled

Com2 Serial Data Mode: UDP

Com2 Serial Data Baud Rate: 9600

Com2 Serial Data Tx IP Address: 169.254.10.2

Com2 Serial Data Tx IP Port: 0

Com2 Serial Data Rx IP Port: 0

Com1 Serial Data Rx IP Address: 0.0.0.0

COM1 data will be received on this IP address

Com2 Serial Data Rx IP Address: 169.254.0.2

Com2 Serial Data Flow Control: disabled

Setting to enable hardware flow control (RTS/CTS) in COM2 data mode

SNTP Server IP: 0.0.0.0

The IPv4 address of NTP/SNTP Time Server

Com1 Serial Data Seamless Mode: enabled

Setting to enable seamless mode for COM1 data mode

Com2 Serial Data Seamless Mode: enabled

Com1 Serial Data Delimiter Chars: 4

Minimum number of characters which will be considered a gap in seamless mode for COM1

Com2 Serial Data Delimiter Chars: 4

Com1 Serial Data Buffer Size: 20

Number of output characters which will be buffered in seamless mode for COM1

Com2 Serial Data Buffer Size: 20

RF Frequency Hopping Format: USA/CANADA

(Read Only) The frequency-hopping rules the radio is configured to operate under

SNMP Enable: disabled

Enable/Disable SNMP Agent

Hop Protocol: 1

Frequency hopping protocol version

DHCP Server Enable: disabled

Enable/Disable DHCP Server Daemon

DHCP Netmask: 255.255.255.0

The IP Address to be used as the DHCP Netmask

DHCP Start Address: 192.168.0.11

The IP Address to be used as the starting address

DHCP End Address: 192.168.0.22

The IP Address to be used as the ending address

Approved Remotes List Enable: disabled

Setting to enable the Approved Remotes List

Encryption Enable: disabled

Setting to enable over-the-air data encryption

HTTP Enable: enabled

Setting to enable the HTTP interface

Telnet Enable: enabled

Setting to enable the Telnet interface

HTTP MD5 Authentication: disabled

Setting to enable MD5 Digest Authentication

Automatic Key Rotation: disabled

Setting to enable Automatic Key Rotation

Approved APs List Enable: disabled

Setting to enable the Approved Access Points List

Watch-Link-Status Flag @ AP: disabled

A flag that controls whether the Remotes care about the AP's Ethernet Link Status

Network Name Hash Enable: disabled

A flag that controls whether MD5 hashing is applied to the network name

End of Configuration File

Editing Configuration Files

Once a Remote unit's operation is fine-tuned, use the *Configuration Scripts Menu* on Page 63 to save a copy of the configuration in a PC. Once the file is saved in the PC it can be used as a source to generate modified copies adjusted to match other devices. The configuration files can be modified using a text editor or an automated process. (Not provide by MDS).

We recommend that you review and update the following parameters for each individual unit. Other parameters may also be changed.

Table 2-6. Common User-Alterable Parameters

Field	Comment	Range
IP Address	Unique for each individual radio	Any legal IP address
IP Gateway	May change for different groups or locations	Any legal IP address
Unit Name	Should reflect a specific device. This information will appear in entraNET Management System headings	Any 20-character alphanumeric string
Location	Used only as reference for network administration	Any 40-character alphanumeric string
System Mode	The application of the parameter in this field is dependent on the authorized options stored in the unit's permanent memory. The mode must be compatible with any previously installed Authorization Keys.	"Access Point" "Dual Remote" "Serial Remote" "Ethernet Remote" NOTE: These are case-sensitive.
Network Name	Used to identify different groups or locations	Any 15-character alphanumeric string

Each resulting file should be saved with a different name. We recommend using directories and file names that reflect the location of the unit to facilitate its identification.

Editing Rules

- You may include only parameters you want to change.
- Change only the parameter values.
- Capitalization counts in some field parameters. (Example: System Mode)
- Comment Fields
    a. Edit, or delete anything on each line to the right of the comment delineator, the semicolon (;).
    b. Comments can be of any length, but must be on the same line as the parameter, or on a new line that begins with a semicolon character.
    c. Comments after parameters included in files exported from a transceiver do not need to be present in your customized files.

2.8.3 Authorization Keys Menu

```
                          Library Admin Office
                          Authorization Key Menu
-=============================================================================-
   A) Authorization Key


   Authorized Features
      Access Point             enabled
      Dual Remote              enabled
      Remote Serial Gateway    enabled
      Remote Ethernet Bridge   enabled
      MDS NETview MS           enabled


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

Figure 2-37. Authorization Key Menu

- **`Authorization Key`**—Initiate the entering of an Authorization Key into the transceiver's non-volatile memory.
- **`Authorized Features`**—List of authorized features.

  In addition to the four transceiver configurations fields, is the **MDS NETview MS** access control. *NETview MS* is designed to help users monitor system performance, configure network elements, detect faults and correct problems in the convenience of an office setting or at any other point in the network.

2.8.4 Radio Test Menu

This area provides several useful tools for installers and maintainers. You can manually key the transceiver to make measurements of antenna

performance. (See *"Antenna Direction Optimization"* on Page 97 for details.

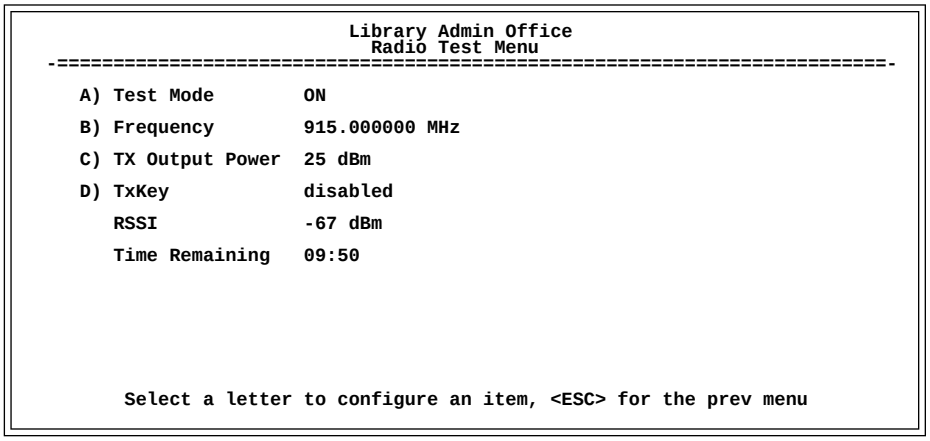


Figure 2-38. Radio Test Menu
Shown with Test Mode Enabled

NOTE : Use of the test mode will disrupt traffic through this unit. If the unit is the Access Point, it will disrupt traffic through the entire network.

Test Mode function is automatically limited to 10 minutes and *should only be used to measure transmit power*. It may also be manually reset to continue with the testing or turned off.

- **`Test Mode`**—Controls access to the transceiver's suite of tools. [(ON, OFF; OFF]
- **`Frequency`**—Set radio operating frequency during the testing period to a single frequency. [915.0000 MHz]
- **`TX Output Power`**—Temporarily overrides the power level setting in the Radio Configuration Menu. [20]
- **`TxKey`**—Manually key the radio transmitter for power measurements. [Enable, Disable; Disable]
- **`RSSI`**—Incoming received signal strength on frequency entered in the frequency parameter on this screen (–dBm).

  This RSSI measurement is updated more frequently than the RSSI by Zone display of the Performance Information menu.

2.8.5 Ping Utility Menu

```
                          Library Admin Office
                           Ping Utility Menu
-=============================================================================-

   A) IP Addr            192.168.1.1
   B) Count              4
   C) Packet Size        32
   D) Go

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

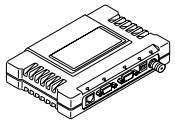
Figure 2-39. Ping Utility Menu

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

  Screen will be replaced with detailed report of PING activity. Press any key after viewing the results to return to this menu.

3 TABLETOP EVALUATION AND TEST SETUP

Contents



3.1 OVERVIEW

It is convenient to set up a tabletop network that can be used to verify the basic operation of the transceivers and give you a chance to experiment with network designs, configurations or network equipment in a convenient location. This test can be performed with any number of radios.

NOTE: It is important to use a "Network Name" that is different from any currently in use in your area during the testing period. This will eliminate unnecessary disruption of traffic on the existing network while you become familiar with the transceiver or evaluate variations of unit operating parameters.

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.

3.2 STEP 1—INSTALL THE ANTENNA CABLING

Figure 3-1 is a drawing of the tabletop arrangement. Connect the antenna ports of each transceiver as shown. This will provide stable radio communications between each unit while preventing interference to nearby electronic equipment from a large number of co-located units.

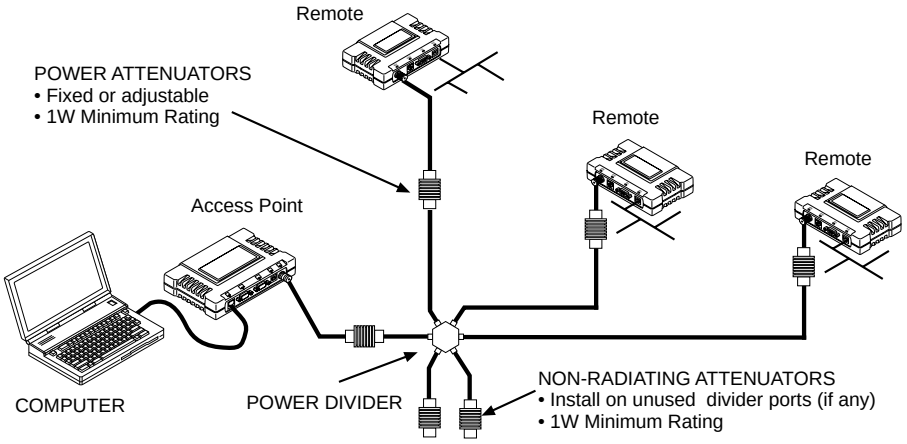


Figure 3-1. Typical setup for tabletop-testing of radios

NOTE: It is very important to use attenuation between all units in the test setup. The amount of attenuation required will depend on the number of units being tested and the desired signal strength (RSSI) at each transceiver during the test. In no case should a signal greater than –50 dBm be applied to any transceiver in the test setup. An RF power output level of +20 dBm is recommended. (See *"Radio Configuration Menu"* on Page 29.)

3.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER

The primary power at the transceiver's power connector must be within 10.5–30 Vdc and be capable of continuously providing a minimum of 8 Watts. (Typical power consumptions are: 760 mA @ 10.5 Vdc, 580 mA @ 13.8 Vdc, and 267 mA @ 30 Vdc.) A 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 as shown in Figure 3-2 with the positive lead (+) on the left.

NOTE: It will take about 30 seconds for the transceiver to power up and be ready for operation.

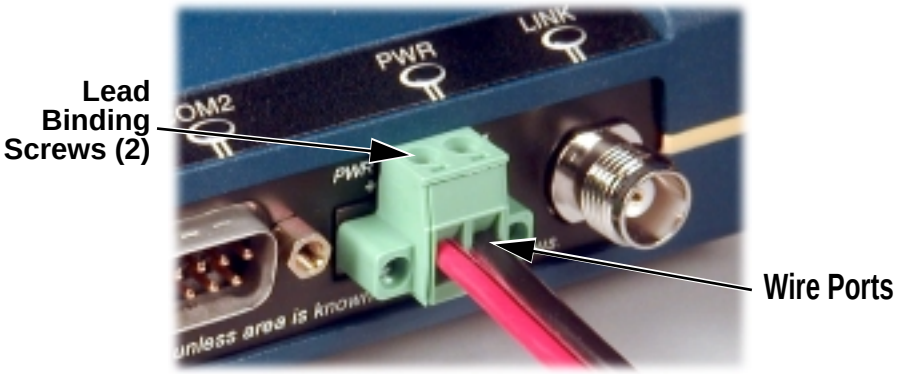


Figure 3-2. Power Connector, Polarity: Left +, Right –

CAUTION
POSSIBLE EQUIPMENT

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

3.4 STEP 3—CONNECT PC TO THE MDS TRANSCEIVER

Connect a PC's Ethernet port to the LAN port using an Ethernet cross-over cable. The LAN LED should light. Alternately, you can use a serial cable to connect to the COM1 port. (Figure 3-3 on Page 81)

3.5 STEP 4—REVIEW THE TRANSCEIVER'S CONFIGURATION

3.5.1 Getting Started

Start with the Access Point and log-in. It should be the first unit to be set up as the Remotes are dependent on its beacon signal to achieve the "associated" state.

Login credentials (all lower case):

Username: **root**

Password: **zonukh4x**

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

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

3.5.2 Procedure

The following is a summary of the configuration procedure that must be done on each unit in the system. Key parameters are highlighted on the embedded Management System flowchart on Figure 3-4 on Page 83, *Management System Menu Flowchart (*abbreviated). A lists of parameters can found in two tables: Table 4-5 on Page 92 and Table 4-7 on Page 95. Detailed information on using the Management System can be found in *INTRODUCTION* on Page 15 in this manual.

NOTE: The Management System supports the use of "configuration files" to aid in uniformly configuring multiple transceivers. These are detailed in *Using Configuration Scripts* on Page 64.

3.5.3 Basic Configuration Defaults

Table 3-1 provides a selection of key transceiver 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 103 for hookup.)

NOTE: Access to the entraNET's Management System and changes to some parameters, are controlled by password when accessing by means of a Web browser or Telnet.

Table 3-1. Basic Configuration Defaults (AP)

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

A unique IP address and subnet are required to access the browser-based entraNET Management System through the LAN port.

Table 3-2. Basic Configuration Defaults (Remote)

Item	Mgt. System Location	Default	Values/Range
Payload			
Radio			
Remote IP Address			
Unit ID			
Mode			
Local IP Port			
Remote IP Port			
Network Name	**Main Menu> Network Configuration> Network Name**	"Not Programmed"	• 1–15 alphanumeric characters • Case-sensitive; can be mixed case
IP Address	**Main Menu> Network Configuration> IP Address**	192.168.1.1	Contact your network administrator

Table 3-2. Basic Configuration Defaults (Remote) *(Continued)*

Item	Mgt. System Location	Default	Values/Range
Subnet Mask			
Net Address			
RF Output Power	**Main Menu> Radio Configuration> RF Power Output**	+30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watts)
Unit Password	**Main Menu> Device Information> User Password**	admin (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case

3.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT

Connect a local area network to the LAN port or serial devices to the COM1 (DCE) or COM2 (DTE) ports. Make sure your transceivers are capable of supporting your devices. (See *Table 1-1 . MDS entraNET 900 Models and Data Interface Services*, on page 5 for a summary of model capabilities.) The LAN port will support any Ethernet-compatible equipment. This includes devices that use the Internet Protocol (IP).

NOTE: The COM1 port also provides access to the transceiver's Management System. If you use the COM1 port for normal data services, you may find it convenient to use the LAN port for access to the entraNET Management System.

Figure 3-3 shows the default functions and services for the interface connectors.

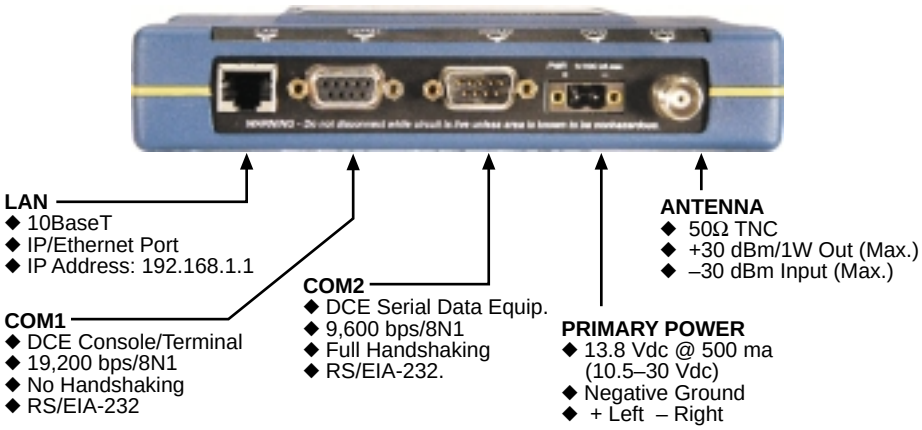


Figure 3-3. Transceiver (AP) Interface Default Configuration & Functions

3.7 STEP 6—CHECK FOR NORMAL OPERATION

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

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

- PWR—Lit continuously
- LINK—on or blinking intermittently
- LAN—On or blinks intermittently

Table 3-3 provides details on the LED functions.

Table 3-3. Transceiver LED Functions

LED Label	Activity	Indication
LAN	ON	LAN detected
	Blinking	Data TX/RX
	OFF	LAN not detected
COM1 (MGT System)	Blinking	Data TX/RX
	OFF	No data activity
COM2	Blinking	Data TX/RX
	OFF	No data activity
PWR	ON	Primary power (DC) present
	Blinking	Unit in “Alarmed” state
	OFF	Primary power (DC) absent
LINK (Access Point)	ON	Default state
	Blinking	Data Tx/Rx
LINK (Remote Gateway)	ON	Associated to AP
	Blinking	Data Tx/Rx
	OFF	Not associated with AP

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

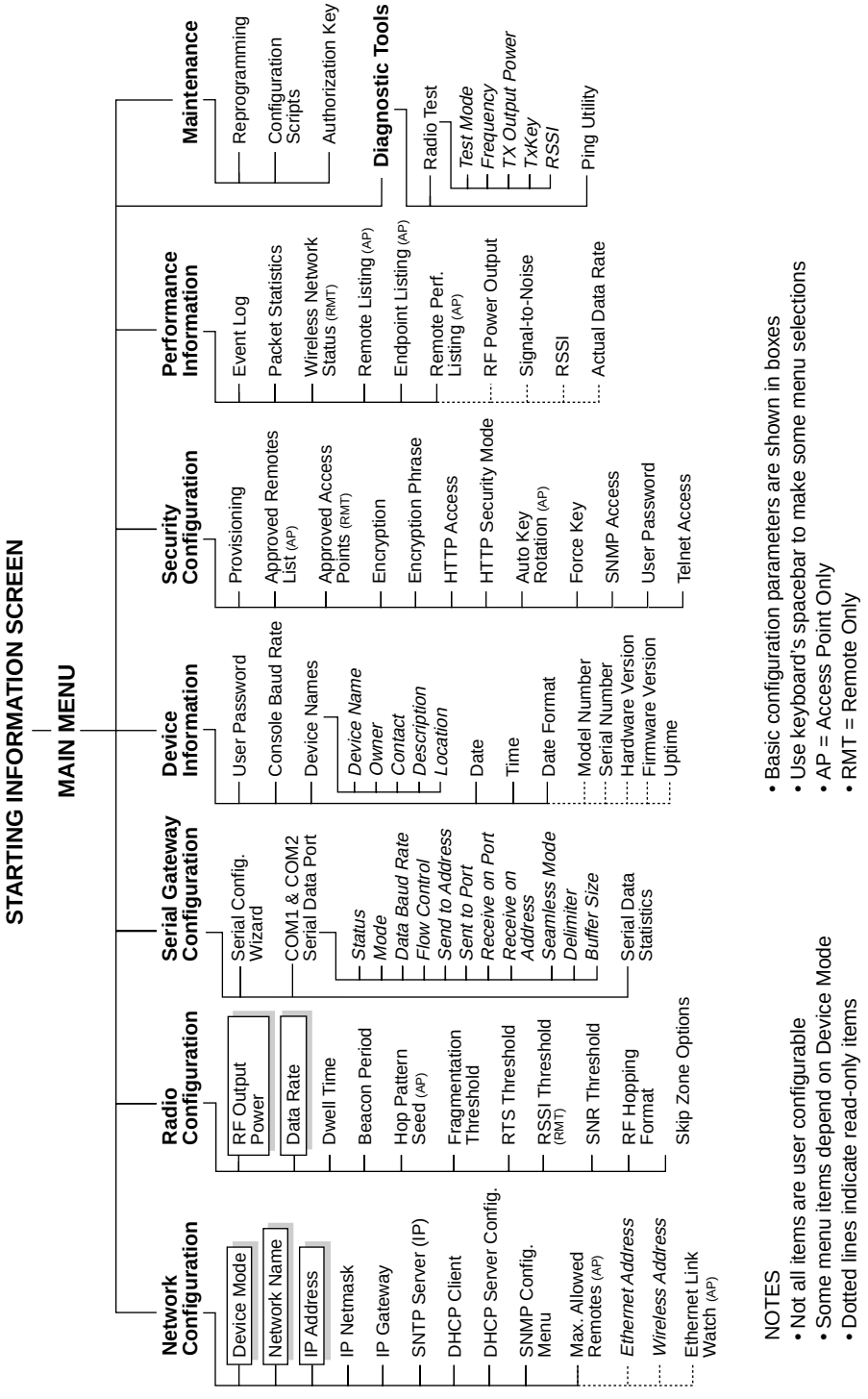
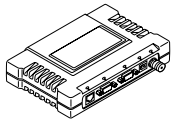
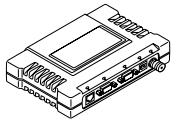


Figure 3-4. *entraNET* Management System Menu Flowchart
(Security, Performance & Maintenance Menus are abbreviated. See Figure 2-2 on Page 17 for details for these areas.)



4 TROUBLESHOOTING & RADIO MEASUREMENTS

Contents



4.1 TROUBLESHOOTING

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

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

Multiple Communication Layers

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

Unit Configuration

There are over 50 user-configurable parameters in the entraNET Management System. Do not overlook the possibility that human-error may be the cause of the problem. With so many possible things to look at and change, a parameter may be incorrectly set, and then what was changed is forgotten.

To help you avoid these problems, we recommend creating an archive of the transceiver's profile when your installation is complete in a Configuration File. This file can be reloaded into the transceiver to restore the unit to the factory defaults or your unique profile. For details on creating and archiving Configuration Files,

See *"Using Configuration Scripts"* on Page 64.

Factory Assistance

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

4.1.1 Interpreting the Front Panel LEDs

An important set of troubleshooting tools are the LED status indicators on the front panel of case. They should be the first thing to check whenever a problem is suspected. Table 3-3 on Page 82 describes the function of each status LED. Table 4-1 below provides suggestions for

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

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

Symptom	Problem/Recommended System Checks
PWR LED does not turn on.	a. Voltage too low—Check for the proper supply voltage at the power connector. (10.5–30 Vdc) b. Indefinite Problem—Cycle the power and wait (≈ 30 seconds) for the unit to reboot. Then, recheck for normal operation.
LINK LED does not turn on.	a. Network Name of Remote not identical to desired Access Point—Verify that the system has a unique Network Name. b. Not yet associated with an Access Point with the same Network Name. Check the "Status" of the unit's process of associating with the Access Point. Use the entraNET Management System. c. Poor Antenna System—Check the antenna, feedline and connectors. Reflected power should be less than 10% of the forward power reading (SWR 2:1 or lower).
PWR LED is blinking.	a. Blinking indicates an alarm condition exists. b. View Current Alarms and Event Log and correct the problem if possible. (See *"Using Logged Operation Events"* on Page 92) c. Blinking will continue until the source of the alarm is corrected, for example, a valid IP address is entered, etc.
LAN LED does not turn on.	a. Verify the Ethernet cable is connect at both ends. b. Verify that the appropriate type of Ethernet cable is used: straight-through, or crossover.

4.1.2 Troubleshooting Using the Embedded Management System

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

Table 4-2. Basic Troubleshooting with the entraNET MS

Symptom	Problem/Recommended System Checks
Remote does not associate; stays in HOPSYNC	a. Verify the AP has sufficiently large number in the "Max Remotes" parameter of the Network Configuration Menu. b. Verify the correct MAC address is listed in the "Approved Remotes List" or "Approved Access Points List" of the Security Configuration menu.
Serial data is slow with UDP multicast traffic	a. Change Beacon Period to FAST. (Radio Configuration Menu)

Table 4-2. Basic Troubleshooting with the entraNET MS

Symptom	Problem/Recommended System Checks
Cannot access the entraNET MS through COM1	a. Connect to unit via Telnet or Web browser b. Disable the serial mode for COM1 (Serial Gateway Configuration>Com1 Serial Data Port>Status>Disabled) or, if you know the unit's data configuration a. Connect to COM 1 via a terminal set to VT100 and the port's data baud rate. b. Type "+++ [ENTER]" c. Change the terminal's baud rate to match the transceiver's Console Baud Rate. d. Type "+++ [ENTER]"
Display on terminal/Telnet screen garbled	a. Verify the terminal/terminal emulator or Telnet application is set to VT100
Cannot pass IP data to WAN.	a. Verify your IP settings. b. Use the PING command to test communication with transceivers in the local radio system. c. If successful with local PING, attempt to PING an IP unit attached to a radio. d. If successful with the LAN PINGs, try connecting to a known unit in the WAN.
Wireless Retries too high.	Possible Radio Frequency Interference— a. If omnidirectional antennas are used, consider changing to directional antennas. This will often limit interference to and from other stations. b. Try skipping some zones where persistent interference is known or suspected. c. The installation of a filter in the antenna feedline may be necessary. Consult the factory for further assistance.
Password forgotten.	a. Connect to the transceivertransceiver using a terminal through the COM1 Port. b. Call MDS. Get a password-resetting Authorization Key. c. Enter the Authorization Key at the login prompt as a password.

The following is a summary of how several screens in the entraNET Management System can be used as diagnostic tools. For information on how to connect to the entraNET Management System See *"STEP 3—CONNECT PC TO THE MDS TRANSCEIVER"* on Page 78.

Starting Information Screen

(See *Starting Information Screen* on Page 23)

The entraNET MS's "home page" provides some valuable bits of data. Probably the most important is the "Device Status" field. This one item will tell you if the unit is showing signs of life.

If the *Device Status* field says "associated," then look in the network areas beginning with network data statistics. If it displays some other

message, such as *Scanning*, *Hop Sync* or *Alarmed*, you will need to determine why it is in this state.

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

Table 4-3. Device Status[1]

Scanning	The unit is looking for an Access Point beacon signal. If this is a Remote, *Associated* means that the unit is associated with an Access Point
Hop Sync	The unit has found a valid beacon signal for its network and has changed its frequency hopping pattern to match that of the AP.
Associated	This unit has successfully synchronized and is "associated" with an Access Point. This is the normal operating state.
Alarmed	The unit is has detected one or more alarms that have not been cleared.

1. Only available in the *Startup Information Screen* at Remotes.

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

If the unit is in an "Alarmed" state and not able to associate with an Access Point unit, then there may be problem with the wireless network layer. Call in a radio technician to deal with wireless issues. Refer the technician to the *RADIO MEASUREMENTS* on Page 96 for information on antenna system checks.

Packet Statistics Menu

(See Packet Statistics Menu on Page 49)

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

Wireless Packet Statistics

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

Ethernet Packet Statistics

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

The most significant fields are the *Packets Dropped*, *Retries*, *Retry Errors*, *Receive Errors* and *Lost Carrier Detected*. If the data values are more than 10% of their sent and received counterparts, or the *Lost Carrier Detected* value is greater than a few dozen, there may be trouble with radio-frequency interference or a radio link of marginal strength. Look over the *RSSI by Zone Screen's* values (Page 46) for zones that are more than a couple of dBs (decibels) below the average level, and for signal level values that are likely to provide marginal service. For example, the average level is less than –85 dBm during normal conditions with a data rate of 115.2 kbps.

If the RSSI levels in each zone are within a few decibels (dB) of each other, but less than –85 dBm, then a check should be made of the aiming of the antenna system and for a satisfactory SWR. Call in a radio technician to deal with wireless issues. Refer the technician to the *RADIO MEASUREMENTS* on Page 96 for information on antenna system checks.

NOTE: For a data rate of 115.2 kbps, the average signal level should be –77 dBm or stronger.

Serial Port Statistics Menu

(See Serial Data Statistics Menu on Page 36)

This screen provides top-level information on data exchanges between the unit's serial ports and the network through the wireless and the Ethernet (data) layers. These include:

- Bytes In On Port *xxx*
- Bytes Out On Port *xxx*
- Bytes In On Socket *xxx*
- Bytes Out On Socket *xxx*

You can use this screen as a barometer of port activity at the data and IP levels.

Diagnostic Tools

(See MAINTENANCE on Page 58)

The radio's Maintenance menu contains two tools that are especially useful to network technicians—the Radio Test Menu and the Ping Utility. The Radio Test selection allows for testing RF operation, while the Ping Utility can be used to verify reachability to pieces of equipment connected to the network. This includes *entraNET* 900 transceivers as well as user-supplied Ethernet devices.

4.1.3 Using Logged Operation Events

(See Event Log Menu on Page 47)

The transceiver's microprocessor monitors many operational parameters and logs them as various classes of "events". If the event is one that affects performance, it is an "alarmed". There are also normal or routine events such as those marking the rebooting of the system, implementation of parameter changes and external access to the entraNET Management System. Informational events are stored in temporary (RAM) memory that will be lost in the absence of primary power, and Alarms will be stored in permanent memory (Flash memory) until cleared by user request. Table 2-5 summarizes these classifications.

Table 4-4. Event Classifications

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

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

4.1.4 Alarm Conditions

(See View Current Alarms on Page 48)

Most events, classified as "critical", will make the POWER LED blink, and will inhibit normal operation of the transceiver. The LED will remain blinking until the corrective action has been completed

Table 4-5. Alarm Conditions (Alphabetical Order)

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_ADC	ADC output Railed	adcInput(3)
EVENT_BRIDGE	Network Interface /Error	networkInterface(17)
EVENT_ETH_LINK_AP*	AP Ethernet Link Disconnected	apEthLinkLost(19)
EVENT_FLASH_TEST	Flash Test Failed	-
EVENT_FPGA	FPGA communication Failed	fpgaCommunication(2)
EVENT_FREQ_CAL	Frequency Not Calibrated	frequencyCal(7)
EVENT_INIT_ERR	Initialization Error	initializationError(18)
EVENT_IPADDR*	IP Address Invalid	ipAddressNotSet(4)
EVENT_IPMASK*	IP Mask Invalid	ipNetmaskNotSet(5)

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

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_MAC	MAC communication Failed	macCommunication(1)
EVENT_MACADDR	MAC Address Invalid	noMacAddress(6)
EVENT_NETNAME*	Netname Invalid	invalidNetname(12)
EVENT_PLL_LOCK	PLL Not locked	pllLock(10)
EVENT_POWER_CAL	Power Calibrated/Not Calibrated	powerCal(8)
EVENT_POWER_HIGH	RF Power Control Saturated High	rfPowerHigh(13)
EVENT_POWER_LOW	RF Power Control Saturated Low	rfPowerLow(14)
EVENT_RSSI*	RSSI Exceeds threshold	rssi(11)
EVENT_RSSI_CAL	RSSI Not Calibrated	rssiCal(9)
EVENT_SYSTEM_ERROR*	System Error Cleared; Please Reboot	systemError(16)

*Condition may be corrected by user and alarm cleared.

4.1.5 Correcting Alarm Conditions

(See View Event Log on Page 49)

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

Table 4-6. Correcting Alarm Conditions (Alphabetical Order)

Event Log Entry	Generating Condition	Clearing Condition or Action
ADC Failure	The ADC always reads the same value (either high or low limit)	Contact MDS Technical Services for assistance
AP Ethernet Link	Monitor will check state of Ethernet link and set alarm if it finds the link down	Ethernet link is re-established
Bridge Down	When the Bridge fails to be initialized	Contact MDS Technical Services for assistance
Flash Test Failed	Internal check indicates corruption of Flash memory	Contact MDS Technical Services for assistance
FPGA Failure	Communication lost to the FPGA	Contact MDS Technical Services for assistance
General System Error	Internal checks suggest unit is not functioning properly	Reboot the transceiver
Initialization Error	Unit fails to complete boot cycle	Contact MDS Technical Services for assistance

Table 4-6. Correcting Alarm Conditions (Alphabetical Order) *(Continued)*

Event Log Entry	Generating Condition	Clearing Condition or Action
Invalid IP Address	The IP address is either 0.0.0.0 or 127.0.0.1	IP address is programmed to something other than 0.0.0.0 or 127.0.0.1 by the user
MAC Failure	The monitor task reads the LinkStatus from the MAC every second. If the MAC does not reply 10 consecutive times (regardless of what the result is) the CPU assumes the transceiver has lost communication to the MAC.	Contact MDS Technical Services for assistance
Network Interface Error	Unit does not recognize the LAN interface	Contact MDS Technical Services for assistance
Network Name Not Programmed	Network name is “Not Programmed”	Change Network Name to something other than “Not Programmed”
PLL Out-of-Lock	The FPGA reports a synthesizer out-of-lock condition when monitored by the CPU.	Contact MDS Technical Services for assistance.
Power Control Railed High	Power control can no longer compensate and reaches the high rail	Contact MDS Technical Services for assistance
Power Control Railed Low	Power control can no longer compensate and reaches the low rail	Contact MDS Technical Services for assistance
RSSI Exceeds Threshold	The running-average RSSI level is weaker (more negative) than the user-defined value.	Check aiming of the directional antenna used at the Remote; or raise the threshold level to a stronger (less-negative) value.

4.1.6 Logged Non-Critical Events

(See View Event Log on Page 49)

The following events allow the transceiver to continue operation and do not make the POWER LED blink. Each is reported through an SNMP

trap. The left hand column, “Event Log Entry” is what will be shown in the Event Log.

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

Event Log Entry	Severity	SNMP Trap
Association Attempt Success/Failed	MAJOR	assocTryFail(60)
Association Lost - AP Hop Parameter Changed	MINOR	apParmChange(44)
Association Lost - AP's Ethernet Link Down	MAJOR	apEthLinkDown(55)
Association Lost - Local IP Address Changed	MAJOR	ipAddrChanged(59)
Association Lost - Local Network Name Changed	MAJOR	netnameChanged(58)
Association Lost/Established	MAJOR	associated(43)
Auth Demo Mode Expired -- Rebooted Radio/Enabled	MAJOR	authDemoMode(53)
Auth Key Entered - Key Valid/Key Invalid	MAJOR	keyEntered(54)
Bit Error Rate Below threshold/Above threshold	INFORM	ber(42)
Console Access Locked for 5 Min	MAJOR	consoleLockdown(63)
Console User Logged Out/Logged In	MAJOR	consoleLogin(62)
Country/SkipZone Mismatch	INFORM	countrySkipZoneMismatch(50)
Current AP is No Longer Approved	MAJOR	apNotApproved(57)
Desired AP IP Addr Mismatch	INFORM	desiredAPIPMismatch(51)
Expected Sync Lost/Established	INFORM	expectedSync(38)
Hop Sync Lost/Established	INFORM	hopSync(39)
Hop Table Generated/Generation Failed	INFORM	hopTableWrite(40)
HTTP Access Locked for 5 Min	MAJOR	httpLockdown(65)
HTTP User Logged Out/Logged In	MAJOR	httpLogin(49)
Log Cleared	INFORM	eventLogCleared(52)
Max Beacon Wait Time Exceeded	MAJOR	noBeacons(56)
Received Beacon - AP is Blacklisted	INFORM	rxBeaconFromBlacklistAP(37)
Received Beacon - Netname Does Not Match	INFORM	rxBeaconWrongNetworkName(36)
Received Beacon - Valid/Errored	INFORM	rxBeaconErrored(35)
Rem Ethernet Link Connected/Disconnected	MAJOR	remEthLinkLost(61)

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

Event Log Entry	Severity	SNMP Trap
Reprogramming Complete	INFORM	reprogComplete(46)
Reprogramming Failed	MAJOR	reprogFailed(47)
Reprogramming Started	INFORM	reprogStarted(45)
Scanning Started	INFORM	startScan(34)
SNR Within threshold/Below threshold	INFORM	snr(41)
System Bootup (power on)	INFORM	systemBoot(32)
Telnet Access Locked for 5 Min	MAJOR	telnetLockdown(64)
Telnet User Logged Out/Logged In	MAJOR	telnetLogin(48)
User Selected Reboot	MAJOR	systemReboot(33)

4.2 RADIO MEASUREMENTS

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

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

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

4.2.1 Antenna System SWR and Transmitter Power Output

Introduction

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

The SWR of the antenna system should be checked before the radio is put into regular service. For accurate readings, a wattmeter suited to 1000 MHz measurements is required. One unit meeting this criteria is the Bird Model 43™ directional wattmeter with a 5J element installed.

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

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

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

Procedure

1. Place a directional wattmeter between the ANTENNA connector and the antennas system.

2. Place the transceiver into the Radio Test Mode.
   (Main Menu>Maintenance Menu>Radio Test>Test Mode>Y>ON)

   NOTE: The Test Mode has a 10-minute timer, after which it will return the transceiver to normal operation. The Radio Test Mode can be terminated manually.

3. Set the transmitter power to 30 dBm.
   (Main Menu>Maintenance Menu>Radio Test>Test Mode>
   Tx Power Output)

   NOTE: The Radio Test Mode RF power setting will not affect the output level during normal operation.

4. Key the transceiver.
   (Main Menu>Maintenance Menu>Radio Test>Test Mode>
   TxKey> Enable)

   User the spacebar to key and unkey the transmitter ON and OFF. (Enable/Disable)

5. Measure the forward and reflected power into the antenna system and calculate the SWR and power output level. The output should agree with the programmed value.

   (Main Menu>Radio Configuration>RF Power Output)

6. Turn off Radio Test Mode at the Access Point and Remote.
   (Main Menu>Maintenance Menu>Radio Test>Test Mode>Disable)

   End of procedure

4.2.2 Antenna Direction Optimization

Introduction

The wireless network integrity depends, in a large part, on stable radio signal levels being received at each end of a data link. In general, signal

levels stronger than –77 dBm will provide the basis for reliable communication that includes a 15 dB fade margin. As the distance between the Access Point and Remotes increases, the influence of terrain, foliage and man-made obstructions become more influential and the use of directional antennas at Remote locations becomes necessary. Directional antennas usually require some fine-tuning of their bearing to optimize the received signal strength. The transceiver has a built-in received signal strength indicator (RSSI) that can be used to tell you when the antenna is in a position that provides the optimum received signal.

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

The measurement and antenna alignment process will usually take 10 or more minutes at each transceiver.

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

Procedure

1. Verify the Remote is associated with an Access Point unit. Observe the condition of the LINK LED.
   LINK LED = On or Blinking

   This will indicate that you have an adequate signal level for the measurements and it is safe to proceed.

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

   This information will be used later.

3. Clear the *Wireless Packets Statistics* history.

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

4. Read the RSSI level at the Remote.
   (Main Menu>Performance Information>RSSI by Zone)

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

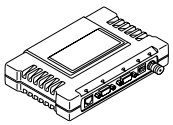
   Watch the RSSI indication for several seconds after making each adjustment so that the RSSI accurately reflects any change in the link signal strength.

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

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

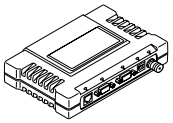
   If the RSSI peak results in an increase in the *Wireless Packets Dropped* and *Received Error*, the antenna may be aimed at an undesired signal source. Try a different antenna orientation.

End of procedure



5 PLANNING AN MDS entraNET 900 RADIO NETWORK

Contents



5.1 INSTALLATION

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

5.1.1 General Requirements

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

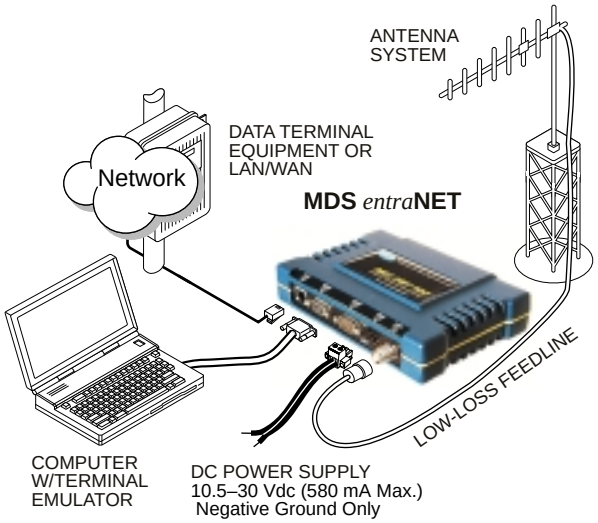


Figure 5-1. Typical Installation with a tower-mounted antenna
(Connect user data equipment to any compatible LAN or COM Port)

Unit Dimensions

Figure 5-2 shows the dimensions of the transceiver case and its mounting holes, and Figure 5-3 on Page 105, the dimensions for mounting with MDS-supplied brackets. If possible, choose a mounting location that provides easy access to the connectors on the end of the radio and an unobstructed view of the LED status indicators.

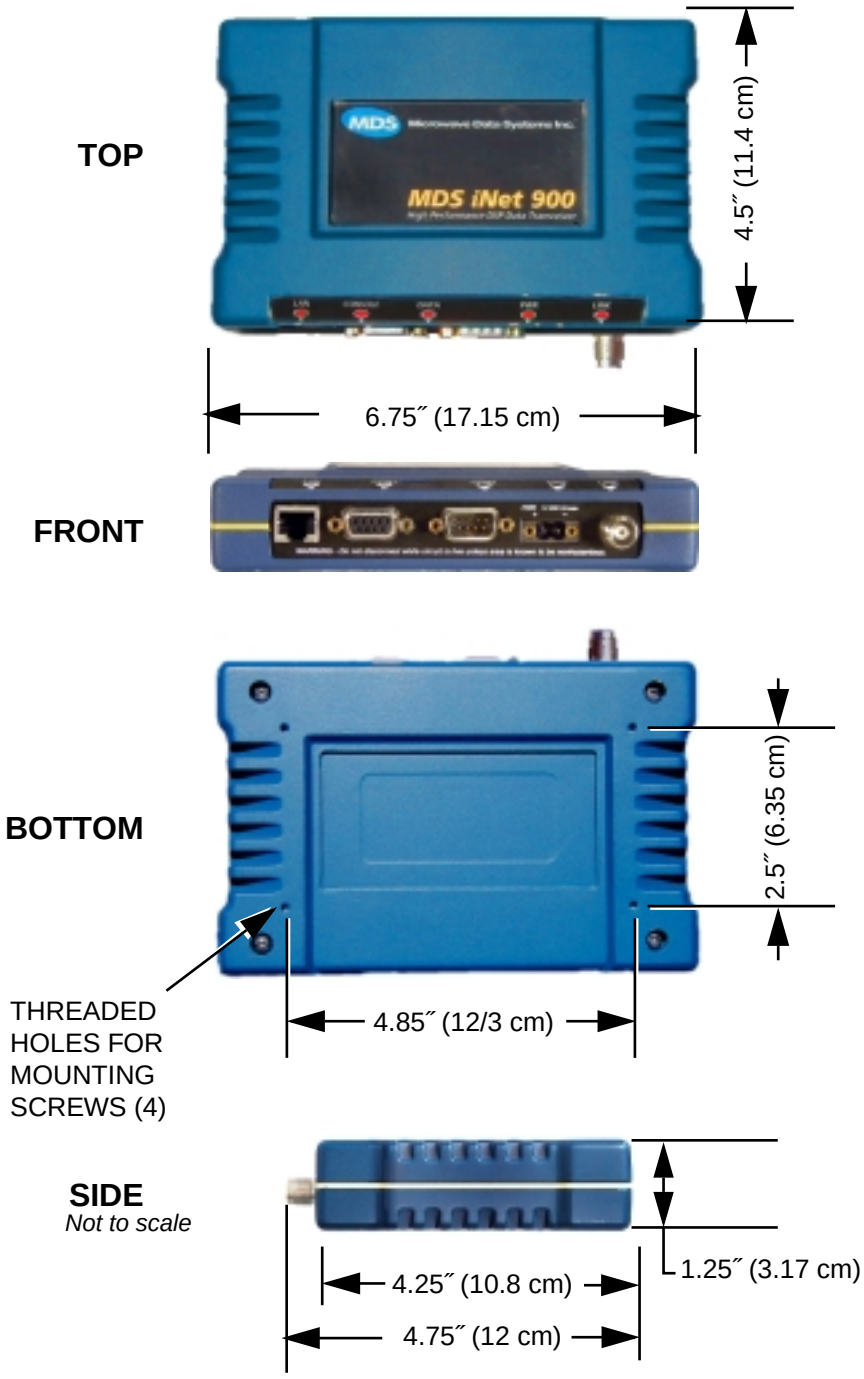


Figure 5-2. Transceiver Dimensions

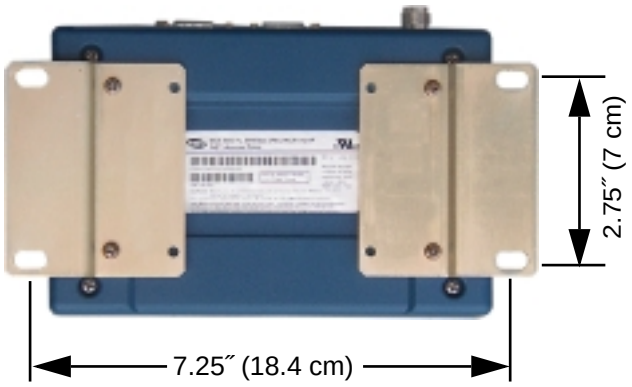


Figure 5-3. Mounting Brackets Dimensions

5.1.2 Site Selection

Suitable sites should provide:

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

These requirements can be quickly determined in most cases. A possible exception is the last item—verifying that an unobstructed transmission path exists. Radio signals travel primarily by line-of-sight, and obstructions between the sending and receiving stations will affect system performance. If you are not familiar with the effects of terrain and other obstructions on radio transmission, the discussion below will provide helpful background.

5.1.3 Terrain and Signal Strength

While the license-free 900 MHz band offers many advantages for data transmission services, signal propagation is affected by attenuation from obstructions such as terrain, foliage or buildings in the transmission path.

A line-of-sight transmission path between the central transceiver and its associated transceiver site(s) is highly desirable and provides the most reliable communications link.

Much depends on the minimum signal strength that can be tolerated in a given system. Although the exact figure will differ from one system to another, a Received Signal Strength Indication (RSSI) of –77 dBm or stronger will provide acceptable performance in many systems. While the equipment will work at lower-strength signals, signals stronger than – 77 dBm provide a “fade margin” of 15 dB to account for variations in

signal strength that may occur from time-to-time. RSSI can be measured with a terminal connected to the COM1 Port or with a HTTP browser to the LAN (Ethernet) connector. (See *"Antenna Direction Optimization"* on Page 97 for details.)

5.1.4 Antenna & Feedline Selection

Antennas

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

In general, an omnidirectional antenna (Figure 5-4) is used at the Access Point station site. This provides equal coverage to all of the Remote Gateway sites.

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

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

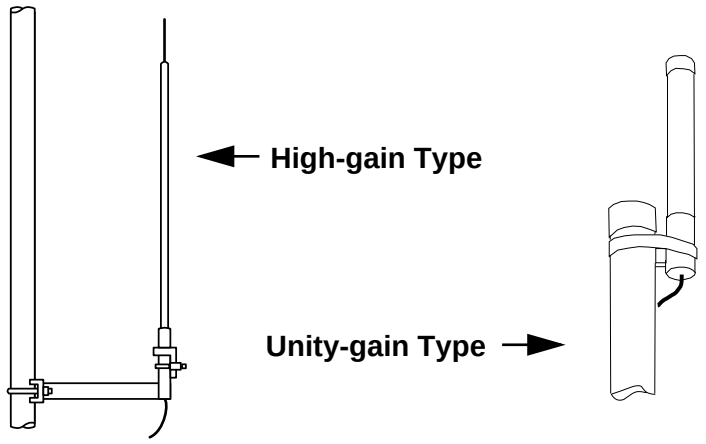


Figure 5-4. Typical Omnidirectional Antennas

At Remote Gateway sites and units in point-to-point LANs, a directional Yagi (Figure 5-5) antenna is generally recommended to minimize interference to and from other users. Antennas are available from a number of manufacturers.

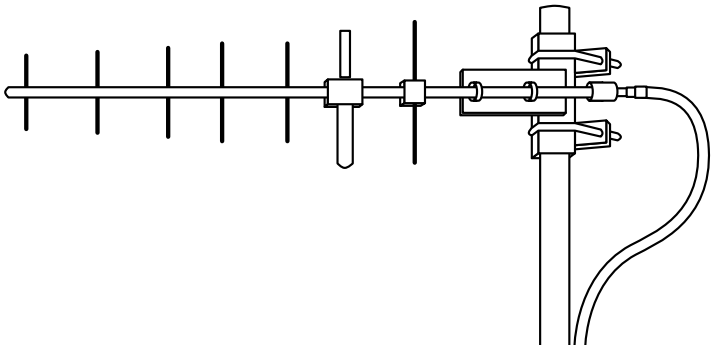


Figure 5-5. Typical Yagi antenna (mounted to mast)

Feedlines

The choice of feedline used with the antenna should be carefully considered. Poor-quality coaxial cables should be avoided, as they will degrade system performance for both transmission and reception. The cable should be kept as short as possible to minimize signal loss.

For cable runs of less than 20 feet (6 meters), or for short range transmission, an inexpensive type such as Type RG-8A/U may be acceptable. Otherwise, we recommend using a low-loss cable type suited for 900 MHz, such as Heliax®.

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

Table 5-1. Length vs. loss in coaxial cables at 900 MHz

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

Table 5-2 outlines the minimum lengths of RG-214 coaxial cable that must be used with common MDS omnidirectional antennas in order *to maintain compliance with FCC maximum limit of +36 dBm*.

Table 5-2. Minimum Feedline Length versus Antenna Gain

Antenna Gain (dBd)	Antenna Gain (dBi)	Minimum Feedline Length (Loss in dB)	Power Level @ Minimum Length
Unity (0 dB)	2.15 dBi	3 meters (1.0 dB)	+31.15 dBi
3 dBd	5.15 dBi	3 meters (1.0 dB)	+34.15 dBi
5 dBd	7.15 dBi	3.1 meters (1.2 dB)	+35.95 dBi

5.1.5 Conducting a Site Survey

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

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

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

With the hand-held antenna positioned near the proposed mounting spot, a technician can check for synchronization with the Access Point station (shown by a lit LINK LED on the front panel) and measure the reported RSSI value. (See *"Antenna Direction Optimization"* on Page 97 for details.) If adequate signal strength cannot be obtained, it may be necessary to mount the station antennas higher, use higher gain antennas, select a different site or consider installing a repeater station. To prepare the equipment for an on-the-air test, follow the general installation procedures given in this guide and become familiar with the operating instructions found in the *CHAPTER-4 TROUBLESHOOTING & RADIO MEASUREMENTS* section Page 85.

5.1.6 A Word About Radio Interference

The transceivers share the radio-frequency spectrum with other 900 MHz services and other Part 15 (unlicensed) devices in the USA. As such, near 100% error-free communications may not be achieved in a given location, and some level of interference should be expected. However, the radio's flexible design and hopping techniques should allow adequate performance as long as care is taken in choosing station loca-

tion, configuration of radio parameters and software/protocol techniques.

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

1. Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.

2. Use a directional antenna at remote sites whenever possible. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, that minimizes interference to (and from) stations located outside the pattern.

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

   Another approach is to use a bandpass filter to attenuate all signals outside the 900 MHz band.

4. Multiple Access Point units can co-exist in proximity to each other with only very minor interference. Each network name has a different hop pattern. (See *"Protected Network Operation through Multiple Access Points"* on Page 8.) Additional isolation can be achieved by using separate directional antennas with as much vertical or horizontal separation as is practical.

5. If constant interference is present in a particular frequency zone (collection of 8 RF channels), it may be necessary to "skip" that zone from the radio's hopping pattern. The radio includes built-in software to help users identify and remove blocked frequency zones from its hopping pattern. (See *"Skip Zone Options Menu"* on Page 31 for more information.)

6. If interference problems persist even after skipping some zones, try reducing the length of data streams. Groups of short data streams have a better chance of getting through in the presence of interference than do long streams.

7. The power output of all radios in a system should be set for the lowest level necessary for reliable communications. This lessens the chance of causing unnecessary interference to nearby systems.

If you are not familiar with these interference-control techniques, contact your MDS sales or Technical Support Department for more information.

5.1.7 How Much Output Power Can be Used?

The transceiver is normally supplied from the factory set for a nominal +30 dBm (1 Watt) RF power output setting; this is the maximum transmitter output power allowed under FCC rules. The power must be *decreased* from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

NOTE: In some countries, the maximum allowable RF output may be limited to less than 1 watt (For example, 100 mW /+20 dBm). Be sure to check for and comply with the requirements for your area.

Calculating System Gain

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

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

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

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

For convenience, Table 5-3 lists several antenna system gains and shows the maximum allowable power setting of the radio. Note that a gain of 6 dB or less entitles you to operate the radio at full power output –30 dBm (1 Watt).

Table 5-3. Antenna system gain vs. power output setting (USA)

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (in dBm)	EIRP (in dBm)
6 (or less)	30	36
8	28	36
10	26	36
12	24	36
14	22	36
16	20	36

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

† Feedline loss varies by cable type and length. To determine the loss for common lengths of feedline, see Table 5-1 on Page 107.

For assistance in the conversion of dBm to Watts, please see *dBm-WATTS-VOLTS CONVERSION CHART* on Page 112.

5.2 dBm-WATTS-VOLTS CONVERSION CHART

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

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

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

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

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

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

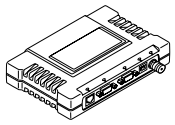
dBm	µV	Po
-65	128	
-66	115	
-67	100	
-68	90	
-69	80	
-70	71	.1nW
-71	65	
-72	58	
-73	50	
-74	45	
-75	40	
-76	35	
-77	32	
-78	29	
-79	25	
-80	22.5	.01nW
-81	20.0	
-82	18.0	
-83	16.0	
-84	11.1	
-85	12.9	
-86	11.5	
-87	10.0	
-88	9.0	
-89	8.0	
-90	7.1	.001nW
-91	6.1	
-92	5.75	
-93	5.0	
-94	4.5	
-95	4.0	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

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

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

6 TECHNICAL REFERENCE

Contents



6.1 REMOTE TRANSCEIVER COMMAND REFERENCE

6.1.1 Command Description

The following commands are used to set the configuration and operating parameters for the MDS entraNET radio...They can be issued from a console terminal connected as shown in Section...

HELP

Lists the commands available through the console interface.

HELP DUMP TOR RADIO

LOGIN AUTH BOOT DATE

COM1 CONSOLE PAYLOAD OEM

REG POWER WAKE TREND

ENCRYPT REPROG H2H VER

DEVICE CONFIG CONFIGTAB IMAGE

DUMP

Lists the current value of all variables.

TOR

Syntax: TOR [optional arguments as follows]...

<COMMAND> command string to send to TOR

PASS=<choices>

0 ;COM2passthroughto/fromTORLCPdataportDISABLED

1 ;COM1 passthrough to/from TOR diagnostic port

2 ;COM2 passthrough to/from TOR LCP data port

REPROG=<choices>

0 ;reprogram tor with image for currently executing OIB image.

1 ;reprogram tor with image 1

2 ;reprogarm tor with image 2

CMD=<0|1> dump command line format

RADIO

Syntax: RADIO [optional arguments as follows]...

ADDR=<integer> Current Radio Network Address

MAC=<integer> Current Radio MAC Address

SYNC=<integer> Current state of Radio Sync

CMD=<0|1> dump command line format

LOGIN

Syntax: LOGIN [optional arguments as follows]...

<PASS> Login securely; prompt username + password and echo '*' when inputting password.

ADMIN=<string> Administrator console login password.

DIST=<string> Distributor console login password.

NONE=<string> User Read-only login.

FACT=<string>

ENG=<string>

AUTH

Syntax: AUTH [optional arguments as follows]...

<CODE=>

ELI_NOT_BLUNET ;1: ELI; 0: BLUNET

MAC_UNIT_MASTER ;1: MASTER; 0: REMOTE

RS232_NOT_4XX ;1: RS232; 0: RS485

ETHERNET_ENABLE ;1:ETHERNETENABLED;0:DISABLED

NETWKMGMT_ENABLE ;1: NETWORK MANAGEMENT ENABLED; 0: DISABLED

CMD=<0|1> dump command line format

BOOT

Syntax: BOOT [optional arguments as follows]...

RUN=<choices>

RESET ;goto Reset Vector

APP1 ;Application Image 1

APP2 ;Application Image 2

CMD=<0|1> dump command line format

DATE

Syntax: DATE [optional arguments as follows]...

<DATE> Current real time clock date.

FORM=<choices>

US ;US Date Format

EUROPE ;Europe Date Format

GENERIC ;Generic Date Format

TIME=<string> Current system time-of-day in military format

CMD=<0|1> dump command line format

COM1

Syntax: COM1 [optional arguments as follows]...

MODE=<choices>

CMDL ;Console port in Command-line mode

DATA ;Console port in transparent data mode

DLINK ;Console port in DLINK remote diagnostic mode.

CMD=<0|1> dump command line format

CONSOLE

Syntax: CONSOLE [optional arguments as follows]...

BAUD=<choices>

Data Rate of Console Port (COM1):

1200 ;1200 bps
2400 ;2400 bps
4800 ;4800 bps
9600 ;9600 bps
19200 ;19200 bps
38400 ;38400 bps
57600 ;57600 bps
115200 ;115200 bps

CBITS=<choices>

Number of Bits that form one character (byte):

7 ;7 character bits

8 ;8 character bits

9 ;9 character bits

PAR=<choices>

NONE ;no parity

ODD ;odd parity

EVEN ;even parity

SBITS=<choices>

1 ;1 stop bit

2 ;2 stop bits

CMD=<0|1> dump command line format

PAYLOAD (Serial)

Syntax: PAYLOAD [optional arguments as follows]...

<untagged index>

COM1 ;COM1 port

COM2 ;COM2 port

BAUD=<choices>

1200 ;1200 bps

2400 ;2400 bps

4800 ;4800 bps

9600 ;9600 bps

19200 ;19200 bps

38400 ;38400 bps

57600 ;57600 bps

115200 ;115200 bps

230400 ;230400 bps

CBITS=<choices>

7 ;7 character bits

8 ;8 character bits

9 ;9 character bits

EN=<choices>

OFF ;Payload data disabled on port

ON ;Payload data enabled on port

PAR=<choices>

NONE ;no parity bit

ODD ;Odd Parity

EVEN ;Even Parity

SBITS=<choices>

1 ;1 stop bit

2 ;2 stop bit

CMD=<0|1> dump command line format

COM1 port

COM2 port

OEM

Syntax: OEM [optional arguments as follows]...

COMP=<string> Name of company selling the radio.

MODEL=<string> Model number given to the radio

PROD=<string> Product Name given to the radio

SREV=<string> Software ID.

CMD=<0|1> dump command line format

REG

Syntax: REG [optional arguments as follows]...

REG=<0|1> Whether the device (remote) has registered with a master

CA=<integer> Master-assigned connection address (mac address) after registration

MASTER=<integer> serial number of registered master

PROT=<integer> agreed protocl version for H2H after registration w/ master

REFRESH=<integer> registration refresh period - determined from Age Out time provided by Master at registration

SAF=<choices>

OFF ;Store and Forward Disabled

ON ;Store and Forward Enabled

LOWPOWER ;Store and Froward w/ Low Power Enabled

SHUTDOWN=<0|1> Agreement with master whether disconnect sent when shutting down - yes/no

SLEEP=<choices>

NONE ;Sleep Disabled on Network

XPARENT ;Transparent Sleep Only on Network

SIMPLE ;Simple Sleep Supported on Network

TIWAKE ;Traffic Indication w/ Wake on Data at Master

TINOWAKE ;Traffic Indication w/o Wake on Data at Master

SLEEPIND=<integer> Master-assigned sleep TIM index after registration

TYPE=<integer> RegMasterType - type of master accepting registration

CMD=<0|1> dump command line format

POWER

Syntax: POWER [optional arguments as follows]...

CNTRL=<choices>

DTR ;DTR controls power mode

PERM ;Power mode is permanent until explicitly wake up b

y master or local data.

PERIOD ;Wake-up is periodically

MODE=<choices>

NORM ;Normal low power mode

SLEEP ;Sleep mode

SHUT ;Shutdown mode

PWKTIME=<integer> This determines the period of wake-up when power mode control is periodic wake-up.

PHGTIME=<integer> This determines how long the remotes hang out after awaken before going back to sleep.

CMD=<0|1> dump command line format

WAKE

Syntax: WAKE [optional arguments as follows]...

LDATA=<0|1> When in sleep mode this enable whether remote can wake on local data/console or not.

MDATA=<0|1> When in sleep mode this enable whether remote can wake on data at master.

CMD=<0|1> dump command line format

TREND

Syntax: TREND [optional arguments as follows]...

<TREND> Writing to this register invokes a request to return trending data at the next non-intrusive opportunity.

CMD=<0|1> dump command line format

ENCRYPT

Syntax: ENCRYPT [optional arguments as follows]...

EN=<0|1> Enable encryption of payload Data

PHRASE=<string> Encryption Pass Phrase

MASTKEY=<string of bytmaster key

KEYIDX=<integer> current key

KEY0=<string of bytes>key 0

KEY1=<string of bytes>key 1

KEY2=<string of bytes>key 2

KEY3=<string of bytes>key 3

IV=<integer> current IV

CMD=<0|1> dump command line format

REPROG

Syntax: REPROG [optional arguments as follows]...

START=<hex> Start address of Flash reprogramming process.

SIZE=<hex> Number of reprogramming bytes to be downloaded.

H2H

Syntax: H2H [optional arguments as follows]...

PROT=<choices>

LCP_ONLY ;LCP, no network or H2H layer

H2H_ONLY ;H2H but no Network layer

H2H_NETWORK ;Full H2H/Network protocol

CMD=<0|1> dump command line format

VER

Syntax: VER [optional arguments as follows]...

IMAGE=<integer> Currently active image: 1 or 2

SREV=<string> Current Software Version number. xx.yy.zz

SWID=<string> Current Software ID text. 06-nnnnAnn

XSREV=<string> Current Radio Software Version number. xx.yy.zz

H2H=<integer> Host to Host protocol version number.

HREV=<string> OIB Board Hardware Revision

XHREV=<string> OEM Radio Board Hardware Revision.

CMD=<0|1> dump command line format

DEVICE

Syntax: DEVICE [optional arguments as follows]...

UNIT=<integer> This is the remote unit ID which is used for Host to Host interface as well as DLINK remote diagnostic messages.

SNUM=<integer> OIB Board Serial Number.

OWNER=<string> Owner can program any information (as 1 string).

UPTIME=<string> Current system uptime.

XSNUM=<integer> OEM Radio Board Serial Number

CMD=<0|1> dump command line format

CONFIG

Syntax: CONFIG [optional arguments as follows]...

ELI=<string> Product configurator string.

CMD=<0|1> dump command line format

CONFIGTAB

Syntax: CONFIGTAB [optional arguments as follows]...

VER=<integer> Config Table Version

CMD=<0|1> dump command line format

IMAGE

Syntax123

: IMAGE [optional arguments as follows]...

<untagged index>

APP1 ;Application Image 1

APP2 ;Application Image 2

SREV=<string> Software Version number. (xx.yy.zz). Not supported

SWID=<string> Software ID text. (06-nnnnAnn). Not supported

XSREV=<string> Display TOR radio software version. Not supported.

CMD=<0|1> dump command line format

Application Image 1

Application Image 2

6.2 DATA INTERFACE CONNECTORS

(Pubs Note: There will be separate sections for the AP and Remote in the final book. Presently, only the AP is covered.)

Three data interface connectors are provided on the face of the Access Point transceiver. The first, the LAN Port, is an RJ-45 connector. The other two use two DB-9 interface connectors that use the RS-232 (EIA-232) signaling standard. Note that the connector for COM1 Port is DCE (Female DB-9) and the COM2 Port is DTE (male DB-9).

CAUTION
RADIO FREQUENCY INTERFERENCE POTENTIAL

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

6.2.1 LAN Port

The LAN Port is used to connect the radio to an Ethernet network. The transceiver will provide a data link to an Internet Protocol-based (IP) data network through the radio network's Access Point station. Each transceiver in the network must have a unique IP address for the network to function properly.

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

The connector uses the standard Ethernet RJ-45 cables and wiring. For custom-made cables, use the pinout information below.

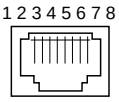


Figure 6-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

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

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

6.2.2 COM1 Port

To connect a PC to the transceiver's COM1 port use a DB-9M to DB-9F cross-over cable. This cable may also be purchased from a computer retail store or mail-order company. For custom interface cables, use the pinout information in Figure 6-2 and Table 6-2.

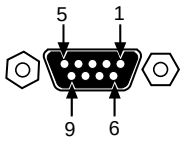


Figure 6-2. COM1 Port (DCE)
(Viewed from the outside of the unit.)

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

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

6.2.3 COM2 Port

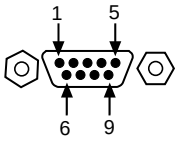


Figure 6-3. COM2 Port (DTE)
Viewed from the outside of the radio

Table 6-3. COM2 Port, DB-9M/EIA-232 Interface

Pin	Functions	DTE
1	Data Carrier Detect (DCD)	In]<—
2	Receive Data (RXD)	In]<—
3	Transmit Data (TXD)	Out]—>
4	Data Terminal Ready (DTR)	Out]—>
5	Signal Ground (GND)	
6	Data Set Ready (DSR)	In]<—
7	Request-to-Send (RTS)	Out]—>
8	Clear-to-Send (CTS)	In]<—
9	Unused	

6.3 TECHNICAL SPECIFICATIONS

GENERAL

Temperature Range:	–40° C to +70° C (–40° F to 158° F)
Humidity:	95% at +40° C (104° F); non-condensing
Primary Power:	6–30 Vdc (13.8 Vdc Nominal)
Supply Current (typical):	(8 Watts Maximum @ 1 Watt RF Output)
Transmit:	28 mA @ 13.8 Vdc
Receive:	100 mA @ 13.8 Vdc
Sleep:	<7 mA @ 13.8 Vdc
MTBF:	35 Years (Telcordia Method 1, Case 3)
Size (Excluding mtg. hardware):	1.5" x 6" x 4" (H x W x D) 3.8 x 15.2 x 10.2 cm
Weight:	0.9 kg / 2 lb (AP) 0.0 kg/0 lb (Remote)
Case:	Cast Aluminum
Boot Time:	≈ 30 sec
Time Required to Associate with Access Point:	≈ 20 sec

APPROVALS/HOMOLOGATION

:

- FCC Part 15.247 (Pending)
- Industry Canada RSS-210 and RSS-139 (Pending)
- UL/CSA Class 1, Div. 2; Groups A, B, C and D hazardous locations (Pending)
- Contact MDS for information on availability and governmental approvals in other countries

EMBEDDED MANAGEMENT SYSTEM

Access Point:	• HTTP (Embedded Web server) • Text-based menu on COM1 serial port • Telnet
Remote Radios:	• Command line via COM1 port

DATA CHARACTERISTICS

PORTS (AP):

Ethernet:

Interface Connectors:	RJ-45 Standard
Data Rate:	10BaseT

COM1, COM2:

Signaling Standard:	EIA-232/V.24
Interface Connectors:	RJ-45
Interface:	COM1: DCE / COM2: DTE

Data Rate:	1200–115,200 bps asynchronous
Data Latency:	< 10 ms typical

PORTS (Remote):

Ethernet:

Interface Connectors:	RJ-45 Standard
Data Rate:	10BaseT

COM1, COM2:

Signaling Standard:	EIA-232/V.24
Interface Connectors:	DB-9
Interface:	COM1: DCE / COM2: DTE
Data Rate:	1200–115,200 bps asynchronous
Data Latency:	< 10 ms typical

PROTOCOLS:

- CSMA/CA Wireless Protocol with Collision Avoidance (802.11)
- IEEE 802.11 CSMA/CD (Wireless)
- IEEE 802.3 (Ethernet)
- IP/Ethernet (ICMP, UDP, TCP, ARP)
- Clear-channel mode for serial async multidrop protocols including: Modbus, DNP.3, Bisync, BSAP, DF1, TotalFlow, Poll Select

RADIO CHARACTERISTICS

GENERAL:

Frequency Range:	902–928 MHz ISM Band
Frequency Hopping Range:	Ten user-configurable 2.5 MHz-wide zones, each containing 8 frequencies
Hop Pattern:	Based on network name
Frequency Stability:	20 ppm

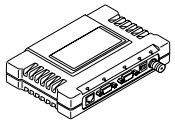
TRANSMITTER:

Power Output (at antenna connector):	0.1 to 1.0 watt (+20 dBm to +30 dBm) ±1.0 dB, *set by user*
Duty Cycle:	Continuous
Modulation Type:	Binary CPFSK
Output Impedance:	50 Ohms
Spurious:	–67 dBc
Occupied Bandwidth:	200 kHz

RECEIVER:

Type:	Double conversion superheterodyne
Sensitivity:	–108 dBm @ 106 kbps < $1x10^{-6}$ BER
Intermodulation:	59 dB Minimum (EIA)

Desensitization:	70 dB
Spurious:	60 dB



7 GLOSSARY OF TERMS AND ABBREVIATIONS

If you are new to wireless IP/Ethernet systems, some of the terms used in this guide may be unfamiliar. The following glossary explains many of these terms and will prove helpful in understanding the operation of the transceiver.

Access Point (AP)—The transceiver in the network that provides synchronization information to one or more associated Remote units. AP units may be configured for either the Access Point (master) or Remote services. (See *"Network Configuration Menu"* on Page 27.)

Active Scanning—See *Passive Scanning*

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

AP—See *Access Point*

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

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

Bit—The smallest unit of digital data, often represented by a one or a zero. Eight bits (plus start, stop, and parity bits) usually comprise a byte.

Bits-per-second—See *BPS*.

BPDU—Bridge Protocol Data Units

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

Byte—A string of digital data usually made up of eight data bits and start, stop and parity bits.

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

Data Circuit-terminating Equipment—See *DCE*.

Data Communications Equipment—See *DCE*.

Data Terminal Equipment—See *DTE*.

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

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

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

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

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

DHCP (Dynamic Host Configuration Protocol)—An Internet standard that allows a client (i.e. any computer or network device) to obtain an IP address from a server on the network. This allows network administrators to avoid the tedious process of manually configuring and managing IP addresses for a large number of users and devices. When a network device powers on, if it is configured to use DHCP, it will contact a DHCP server on the network and request an IP address. The DHCP server will provide an address from a pool of addresses allocated by the network administrator. The network device may use this address on a "time lease" basis or indefinitely depending on the policy set by the network administrator. The DHCP server can restrict allocation of IP addresses based on security policies. An MDS NET 900 access point may be configured by the system administrator to act as a DHCP server if one is not available on the wired network.

Digital Signal Processing—See *DSP*.

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

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

Encapsulation—Process in by which, a complete data packet, such as Modbus frame or any other polled asynchronous protocol frame, is placed in the data portion of another protocol frame (in this case IP) to be transported over a network. Typically this action is done at the receiving end, before being sent as an IP packet to a network. A similar re-

versed process is applied at the other end of the network extracting the data from the IP envelope, resulting in the original packet in the original protocol.

Endpoint—IP address of data equipment connected to the ports of the radio.

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

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

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

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

Frequency Zone—The transceiver uses up to 80 discrete channels in the 902 to 928 MHz spectrum. A group of 8 channels is referred to as a zone; in total there are 10 zones.

Hardware Flow Control—An transceiver feature used to prevent data buffer overruns when handling high-speed data from the connected data communications device. When the buffer approaches overflow, the radio drops the clear-to-send (CTS) line, that instructs the connected device to delay further transmission until CTS again returns to the high state.

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

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

HTTP—Hypertext Transfer Protocol

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

access point, the new access point tells the old access point, using IAPP, that the station has left and is now located on the new access point.

ICMP—Internet Control Message Protocol

IEEE—Institute of Electrical and Electronic Engineers

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

LAN—Local Area Network

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

MAS—Multiple Address System. A radio system where a central master station communicates with several remote stations for the purpose of gathering telemetry data. Figure 1-2 on Page 6 shows an example of an MAS system.

MAC—Media Access Controller

MCU—Microcontroller Unit. This is the processor responsible for controlling system start-up, synthesizer loading, hop timing, and key-up control.

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

Microcontroller Unit—See *MCU*.

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

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

through the access points' territory. In order to do this, the station employs roaming and Mobile IP.

Mode—*See Device Mode.*

MTBF—Mean-Time Between Failures

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

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

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

Passive Scanning—Scanning is a process used by stations to detect other access points on network to which it may connect if it needs to roam. Passive scanning is a slower process in which it listens for information offered by the access points on a regular basis. Active scanning is a faster process in which the station sends out probe message to which the access points respond. Passive scanning can be done while maintaining the current network connectivity. Active scanning affects the RF configuration of the radio and therefore, at least temporarily, disconnects the station from the access point.

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

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

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

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

Portability refers to the ability of a transceiver to connect to an access point from multiple locations without the need to reconfigure the network settings. For example, a transceiver located in one place and con-

nected to an access point can be turned off, moved to another place, turned back on, and when the right information is entered can immediately reconnect to the access point without user intervention.

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

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

Remote Terminal Unit—See *RTU*.

RFI—Radio Frequency Interference

Roaming—An station's ability to automatically switch its wireless connection between various MDS NET 900 access points as the need arises. A station may roam from one access point to another because the signal strength or quality of the current access point has degraded below what another access point can provide. When two access points are co-located for redundancy, roaming allows the stations to switch between the access points to provide a robust network. Roaming may also be employed in conjunction with Portability where the station has been moved beyond the range of the original access point to which it was connected. As the station comes in range of a new access point, it will switch its connection to the stronger signal. Roaming refers to a station's logical, not necessarily physical, move between access points within a specific network and IP subnet.

RSSI—Received Signal Strength Indicator

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

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

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

SNMP—Simple Network Management Protocol

SNR—Signal-to-Noise Ratio. A measurement of relative received signal quality. High ratios will likely result in better signal detection and performance.

SNTP—Simple Network Time Protocol

STP—Spanning Tree Protocol

Standing-Wave Ratio—See *SWR*.

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

TCP—Transmission Control Protocol

TFTP—Trivial File Transfer Protocol

UDP—User Datagram Protocol

Zone—See *Frequency Zone*.