

SIMREX Corporation

DataMover ESS

DataMover™ ESS
DataMover™ ESS-II



Wireless IP/Ethernet Transceiver

DataMover ESS-II Firmware Release 1
DataMover ESS Firmware Release 6.2.1

SIMREX MAN.ESS-01, Rev. F1
MAY 2006

QUICK-START INSTRUCTIONS

INSTALLATION SUMMARY

Step 1 – Mount the Transceiver

Step 2 – Install the Antenna

Step 3 – Measure & Connect Primary Power (10.5–30 Vdc)

Step 4 – Review the transceiver's Configuration

Device Mode—Access Point, or Remote (Default)

Network Name—Unique name for each radio network.

Required for Remotes to associate with Access Point.

IP Address—Must be a unique number to allow for IP access through the Ethernet Port.

NOTE: A unique IP address is essential to access the browser-based Management System.

RF Output Power—Adjust as necessary for regulatory compliance. (Default = 1 Watt / +30 dBm)

Password—Used for remote access and some Management System features. (Default = admin)

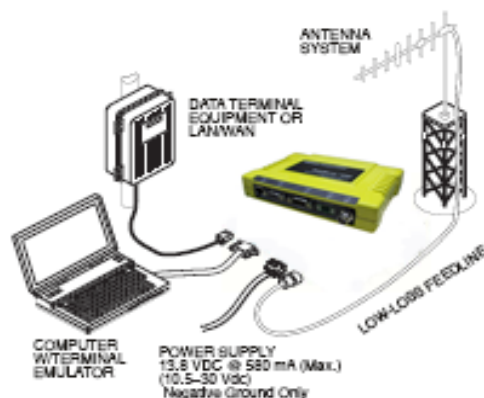
Step 5 – Connect the Data Equipment

Connect the data equipment to data port(s):

- LAN—10BaseT Ethernet-compatible equipment:
Ethernet Hub (Straight-Through Cable); Ethernet Node (Crossover)
- COM2—Serial, RS/EIA-232 compatible equipment
- COM1—Management System (Default); Serial (Alternate)

Step 6 – Check for Normal Operation

- Observe the transceiver LED status panel for the proper indications. In a normally operating system, the following LED indications will be seen within 30 seconds of power-up:
PWR—Lights continuously LAN—On or blinks intermittently LINK— On or blinks intermittently (Remotes: if associated)
- Use PING command to test basic data link integrity between Access Point and Remotes.
- If the PING command is successful, connect the RTU/data equipment to the data port and verify normal operation.
- If the LINK LED on Remotes is not on after 20 to 30 seconds, the unit has failed to associate with the Access Point. It may be necessary to reposition or redirect the radio's antenna for better reception/signal strength.
- Check connected data equipment for normal operation



TYPICAL INSTALLATION

BASIC CONFIGURATION DEFAULTS

The Management System can be accessed through the COM1 Port using a terminal session on a PC. The basic items listed below, along with many other parameters & tools can be accessed through this method. HTTP, Telnet access, and changing some parameters are controlled by password.

ITEM	MGT SYSTEM MENU	DEFAULT	VALUES/RANGE
Device Mode	Network Configuration	Remote	• Remote • Access Point
Unit Password	Device Information	admin (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case
Network Name	Network Configuration	"Not Programmed"	• 1–16 alphanumeric characters • Case-sensitive; can be mixed case
IP Address	Network Configuration	192.168.1.1	Contact your Network Administrator
RF Output Power	Radio Configuration	+30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watt)

Detailed instructions for setting transceiver parameters are contained in Section 3 of this manual.

TABLE OF CONTENTS

1 PRODUCT OVERVIEW AND APPLICATIONS 1

1.1	PRODUCT DESCRIPTION.....	3
1.1.1	Model Offerings	5
1.1.2	Differences Between ESS and ESS-II	6
1.2	APPLICATIONS	6
1.2.1	Wireless LAN	6
1.2.2	Point-to-Point LAN Extension	7
1.2.3	Backhaul for Serial Radio Networks	7
1.2.4	Multiple Protocols and/or Services	8
1.2.5	Wireless LAN with Mixed Services	9
1.2.6	Upgrading Older Wireless Network with Serial Interfaces	10
1.2.7	High-Speed Mobile Data	10
1.3	NETWORK DESIGN CONSIDERATIONS.....	11
1.3.1	Extending Network Coverage with Repeaters	11
1.3.2	Protected Network Operation using Multiple Access Points	13
1.3.3	Collocating Multiple Radio Networks	13
1.4	SIMREX CYBER SECURITY SUITE	14
1.5	ACCESSORIES	16

2 TABLETOP EVALUATION AND TEST SETUP 19

2.1	OVERVIEW.....	21
2.2	STEP 1—INSTALL THE ANTENNA CABLING	21
2.3	STEP 2—MEASURE & CONNECT THE PRIMARY POWER.....	22
2.4	STEP 3—CONNECT PC TO THE TRANSCEIVER	22
2.5	STEP 4—REVIEW TRANSCEIVER CONFIGURATION	23
2.5.1	Getting Started	23
2.5.2	Procedure	23

SIMREX CORPORATION

2.5.3 Basic Configuration Defaults	23
2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT	24
2.7 STEP 6—CHECK FOR NORMAL OPERATION	25

3 EMBEDDED MANAGEMENT SYSTEM 27

3.1 MS INTRODUCTION	29
3.1.1 Differences in the User Interfaces	29
3.2 ACCESSING THE MENU SYSTEM	31
3.2.1 Methods of Control	32
3.2.2 PC Connection & Log In Procedures	32
3.2.3 Navigating the Menus	37
3.3 BASIC DEVICE INFORMATION	38
3.3.1 Starting Information Screen	38
3.3.2 Main Menu	39
3.3.3 Configuring Basic Device Parameters	40
3.4 CONFIGURING NETWORK PARAMETERS	42
3.4.1 Network Configuration Menu	42
3.4.2 IP Address Configuration Menu	44
3.4.3 Ethernet Port Configuration Menu	45
3.4.4 DHCP Server Configuration	46
3.4.5 SNMP Agent Configuration	48
3.5 RADIO CONFIGURATION.....	50
3.5.1 Radio Configuration Menu	50
3.5.2 Mobile Data Configuration	57
3.6 CONFIGURING THE SERIAL INTERFACES.....	60
3.6.1 Overview	60
3.6.2 Serial Data Port Configuration Menu	63
3.6.3 Configuring for UDP Mode	64
3.6.4 Configuring for TCP Mode	67
3.6.5 Configuring for PPP Mode	70
3.6.6 IP-to-Serial Application Example	71
3.6.7 Point-to-Point Serial-to-Serial Application Example	72
3.6.8 Point-to-Multipoint Serial-to-Serial Application Example	73
3.6.9 Mixed Modes	75
3.7 CYBER SECURITY CONFIGURATION	77
3.7.1 Device Security	77

3.7.2	Wireless Security	79
3.7.3	RADIUS Authentication	81
3.7.4	RADIUS Configuration	82
3.7.5	Certificate Management (Remote transceivers only)	83
3.8	PERFORMANCE VERIFICATION	84
3.8.1	Performance Information Menu	84
3.8.2	Network Performance Notes	95
3.9	MAINTENANCE	99
3.9.1	Reprogramming Menu	100
3.9.2	Configuration Scripts Menu	105
3.9.3	Authorization Keys Menu	114
3.9.4	Auto-Upgrade/Remote-Reboot Menu	114
3.9.5	Radio Test Menu	115
3.9.6	Ping Utility Menu	117
3.9.7	Reset to Factory Defaults	117
4	TROUBLESHOOTING AND RADIO MEASUREMENTS	119
4.1	TROUBLESHOOTING	121
4.1.1	Interpreting the Front Panel LEDs	121
4.1.2	Troubleshooting Using the Embedded Management System	122
4.1.3	Using Logged Operation Events	126
4.1.4	Alarm Conditions	126
4.1.5	Correcting Alarm Conditions	128
4.1.6	Logged Events	129
4.2	RADIO (RF) MEASUREMENTS	131
4.2.1	Antenna System SWR and Transmitter Power Output	132
4.2.2	Antenna Aiming	133
5	PLANNING A RADIO NETWORK	135
5.1	INSTALLATION PLANNING	137
5.1.1	General Requirements	137
5.1.2	Site Selection	139
5.1.3	Terrain and Signal Strength	139
5.1.4	Antenna & Feedline Selection	140
5.1.5	How Much Output Power Can be Used?	143
5.1.6	Conducting a Site Survey	143
5.1.7	A Word About Radio Interference	144
5.2	dBm-WATTS-VOLTS CONVERSION CHART	147

6 TECHNICAL REFERENCE 149

6.1 DATA INTERFACE CONNECTORS	151
6.1.1 LAN Port	151
6.1.2 COM1 Port	152
6.1.3 COM2 Port	152
6.2 FUSE REPLACEMENT PROCEDURE	153
6.3 TECHNICAL SPECIFICATIONS.....	154
6.4 CHANNEL HOP TABLE.....	157
6.5 SNMP USAGE NOTES.....	159
6.5.1 Overview	159

7 GLOSSARY OF TERMS & ABBREVIATIONS 165**Copyright Notice**

This publication is protected by U.S.A. copyright law. Copyright 2006, SIMREX Corporation. All rights reserved.

ISO 9001 Registration

SIMREX Corporation DataMover products adheres to the internationally-accepted ISO 9001 quality system standard.

To our Customers

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

What Products are Covered in this Manual?

This manual covers two members of the SIMREX DataMover ESS Transceiver Series, both of which are designed to be operated under the FCC's Part 15 license-free rules. The ESS radio is a Frequency Hopping Spread Spectrum (FHSS) transceiver that operates at data speeds of 256 and 512 kbps.

The ESS-II is a similar design, but it is certified under the Digital Transmission System (DTS) provisions of FCC Part 15 and can operate at data speeds of 512 or 1024 kbps. Operational differences between these two models are identified, as necessary, in this manual.

NOTE: DataMover ESS and DataMover ESS-II transceivers are *not* over-the-air compatible.

Other DataMover ESS Documentation

Installation Guide—The associated DataMover ESS Installation Guide, P/N MAN.ESS-INSTALL, is provided with the transceiver and is limited to essential information needed for installers. The installation guide assumes some guidance to installers will be provided by the readers of this manual. This includes such things as antenna selection, 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 updated information is available on the SIMREX Web site at www.simrex.com.

About SIMREX Corporation

For almost 2 decades, SIMREX Corporation's wireless products have been providing wireless networking solutions with applications in SCADA, telemetry, telecommunications, mobile data and online transaction markets. SIMREX Corporation provides licensed and unlicensed solutions, installed worldwide.

The majority of SIMREX DataMover radios deployed are still installed and performing within our customers' wireless networks. That's because our DataMover products are designed and manufactured according to ISO 9001 control guidelines and meet stringent global quality standards.

Thanks to our durable products and comprehensive solutions, SIMREX is a 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. SIMREX is also at the forefront of wireless communications for private and public infrastructure and online transaction processing. Now is an exciting time for SIMREX 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 SIMREX. We'll always put the performance of your network above all. Visit us at www.simrex.com for more information.

OPERATIONAL & SAFETY NOTICES

RF Exposure



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

UL/CSA Notice

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

The transceiver has been recognized for use in these hazardous locations by two independent agencies —Underwriters Laboratories (UL) and the Canadian Standards Association (CSA). The UL certification for the transceiver is as a Recognized Component for use in these hazardous locations, in accordance with UL Standard 1604. The CSA Certification is in accordance with CSA STD C22.2 No. 213-M1987.

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

SIMREX CORPORATION

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

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

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

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

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



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

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

FCC Part 15 Notices

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

Part 15 rules also require that the Effective Isotropic Radiated Power (EIRP) from an DataMover ESS installation not exceed 36 dBm. Refer to [Antenna & Feedline Selection on Page 140](#) for more information.

Industry Canada RSS Notices

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

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

This device has been designed to operate with the antennas listed below, and having a maximum gain of 12 dB. Antennas not included in this list or having a gain greater than 12 dB are strictly prohibited for use with this device. The required antenna impedance is 50 ohms. Refer to [Table 5-3 on Page 146](#) for a list of antennas acceptable for use with this transceiver.

Manual Revision and Accuracy

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

Environmental Information

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



1 PRODUCT OVERVIEW AND APPLICATIONS

Contents

1.1	PRODUCT DESCRIPTION	3
1.1.1	Model Offerings	5
1.1.2	Differences Between ESS and ESS-II	6
1.2	APPLICATIONS.....	6
1.2.1	Wireless LAN	6
1.2.2	Point-to-Point LAN Extension	7
1.2.3	Backhaul for Serial Radio Networks	7
1.2.4	Multiple Protocols and/or Services	8
1.2.5	Wireless LAN with Mixed Services	9
1.2.6	Upgrading Older Wireless Network with Serial Interfaces	10
1.2.7	High-Speed Mobile Data	10
1.3	NETWORK DESIGN CONSIDERATIONS	11
1.3.1	Extending Network Coverage with Repeaters	11
1.3.2	Protected Network Operation using Multiple Access Points	13
1.3.3	Collocating Multiple Radio Networks	13
1.4	SIMREX CYBER SECURITY SUITE.....	14
1.5	ACCESSORIES.....	16



1.1 PRODUCT DESCRIPTION

The SIMREX DataMover ESS transceiver provides an easy-to-install wireless local area network (WLAN) service with long range and secure operation. It supports both Ethernet *and* serial data interface options at over-the-air data speeds of up to 1 Mbps (ESS-II) and 512 kbps (ESS).

NOTE: For information on the DataMover ESS ENI, which provides expanded gateway and protocol conversion capabilities not found in the DataMover ESS (DF1 to EIP, and MODBUS to MODBUS TCP conversions), refer to the SIMREX *ESS/ENI Supplement*.



Figure 1-1. The SIMREX DataMover ESS Transceiver

Rugged Packaging

The transceiver is housed in a compact and rugged cast-aluminum case that need only be protected from direct exposure to the weather. It contains a single printed circuit board with all necessary components for radio operation and data communications. The only user-serviceable component inside the case is a fuse on the DC power input line.

Simple Installation

Most installations employ an omni-directional antenna at the Access Point (AP) location and a directional antenna at each Remote unit. The antenna is a vital link in the system and must be chosen and installed correctly. Consult [INSTALLATION PLANNING on Page 138](#) for guidance on choosing suitable installation sites and antennas.

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

Secure Operation

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

Remember, security is not a one-step process that can simply be turned on and forgotten. It must be practiced and enforced at multiple levels, 24 hours-a-day and 7 days-a-week. See “[SIMREX CYBER SECURITY SUITE](#)” on Page 14 for more information about the transceiver’s security tools.

Robust Radio Operation

The transceiver is designed for frequency-hopping spread-spectrum operation in the license-free 900 MHz Industrial, Scientific, and Medical (ISM) band. It can provide reliable communications at distances up to 25 miles (40 km) over favorable terrain, even in the presence of weak signals or interference. Frequency hopping allows the transceiver to avoid interference from other transmitters in the same band, and provides frequency diversity for more reliable transmission. The over-the-air MAC increases reliability by adding retries to failed messages.

The DataMover ESS-II transceiver, which is certified to operate under DTS rules (hopping not required), also hops in order to achieve the same benefits that are realized with the DataMover ESS transceiver which is certified under FHSS rules.

Flexible Services

Users with a mixture of equipment having Ethernet and serial data interfaces can choose to use one or two of the user-configurable serial ports through the use of a Remote Dual Gateway. This flexibility allows the transceiver to provide services in data networks that are being migrated from legacy serial/EIA-232-based hardware to the faster and more easily interfaced Ethernet world.

Flexible Management

Configuration, commissioning, troubleshooting and other maintenance activities can be done locally or remotely. Four different modes of access are available: local RS-232 console, local or remote IP access (via Telnet or SSH), web browser (HTTP, HTTPS, and SNMP (v1/v2/v3)). The text-based interface (RS-232 console Telnet and SSH) is implemented in the form of easy-to-follow menus, and the terminal server configuration includes a wizard to help you set up the units correctly.

Transceiver Features

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

- Long Range—Up to 25 miles (40 km) in line-of-sight conditions. Repeater stations may be used to extend the operational range. (Refer to [TECHNICAL SPECIFICATIONS](#) on Page 154 for more detailed information on range.)
- Industrial-Grade Product—Extended temperature range for trouble-free operation in extreme environments
- Robust Radio Communications—Designed to operate in dense, high-interference environments
- Robust Network Security—Prevents common attack schemes and hardware from gaining access or control of network. Common attack events logged and reported by alarms.

- High Speed—1 Mbps (ESS-II) is 100-times faster than 9.6 kbps radios. (ESS transceiver speed is 512 kbps).
- Plug-and-Play Connectivity—Ethernet bridge configuration option requires minimal setup
- Serial Ports—Gateway for serial-based equipment to IP/Ethernet networks with embedded terminal server. Site-to-site configurations are also possible.
- Single hardware package provides configuration as Access Point or Remote

1.1.1 Model Offerings

The transceiver comes in two primary models—Access Point and Remote. Three types of Remote Gateways are available—the Ethernet Bridge, the Serial Gateway, and the Dual Gateway supporting both IP/Ethernet and serial services. [Table 1-1](#) summarizes the different interface abilities for each type.

A unit can be configured by the owner to operate as an Access Point or as a Remote with some restrictions. Only the Dual Gateway Remote units can be reconfigured as an Access Point. Ethernet Bridge and a Serial Gateway Remotes cannot be reconfigured as Access Point unless they are first upgraded to Dual Gateway type. This is accomplished with an “Authorization Key” purchased from the factory. Each one of these individual software keys is associated with the serial number of the corresponding unit.

Table 1-1. Transceiver Models and Data Interface Services

Model	Type	LAN ¹	COM1 ¹	COM2
Access Point ³	N/A	Yes	Yes	Yes
Remote...	Ethernet Bridge ²	Yes	No	No
	Serial Gateway ²	No	Yes	Yes
	Dual Gateway ³	Yes	Yes	Yes

NOTES

1. Provides access to the embedded Management System on all units.
2. Can be upgraded to Dual Gateway with an Authorization Key.
3. Can be configured as an Access Point or Dual Gateway through the embedded Management System.

1.1.2 Differences Between ESS and ESS-II

The ESS and ESS-II Transceivers, while similar in many respects, do have some key differences. The main differences are summarized in [Table 1-2](#):

Table 1-2. Transceiver Differences (ESS vs. ESS-II)

Characteristic	ESS	ESS-II
Data Rate	256/512 kbps	512 kbps/1 Mbps
FCC Certification Type	FHSS	DTS
Encryption	RC4-128	AES-128
Channel size	316.5 kHz	600 kHz
Channel operation	Zones	Channels
Firmware	Specific for ESS	Specific for ESS-II

NOTE: The DataMover ESS and DataMover ESS-II transceivers are *not* over-the-air compatible.

1.2 APPLICATIONS

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

1.2.1 Wireless LAN

The wireless LAN is the most common application of the transceiver. It consists of a central control station (Access Point) and one or more associated Remote units, as shown in [Figure 1-2 on Page 7](#). A LAN provides communications between a central WAN/LAN and remote Ethernet segments. The operation of the radio system is transparent to the computer equipment connected to the transceiver.

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

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

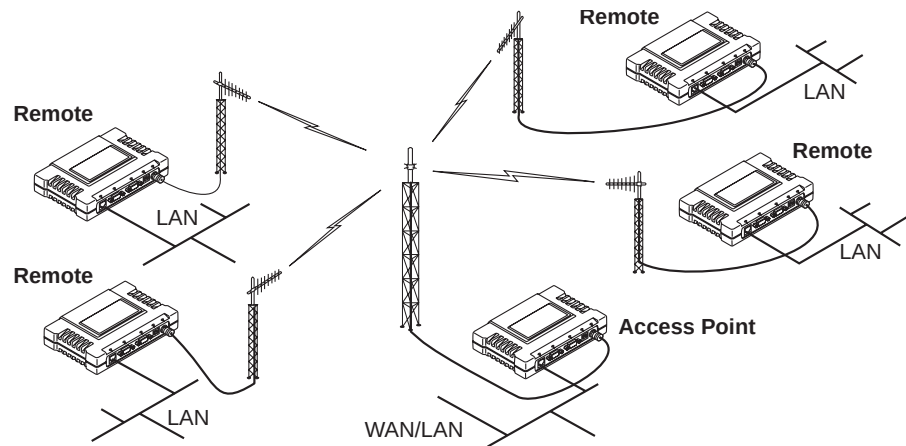


Figure 1-2. Typical Wireless LAN

1.2.2 Point-to-Point LAN Extension

A point-to-point configuration (Figure 1-3) is a simple arrangement consisting of an Access Point and a Remote unit. This provides a communications link for the transfer of data between two locations.

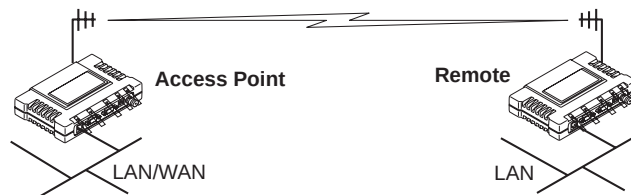


Figure 1-3. Typical Point-to-Point Link

1.2.3 Backhaul for Serial Radio Networks

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

A Remote transceiver using one serial port for the data stream, and the other for network-wide diagnostics can support operational radio networks built with SIMREX serial-based radios, such as DataMover Transparent, DataMover SS and others. In the case of radios using a single port for data and diagnostics, the capabilities are doubled. The data streams are delivered to an IP socket in an application, or in serial format using the Access Point.

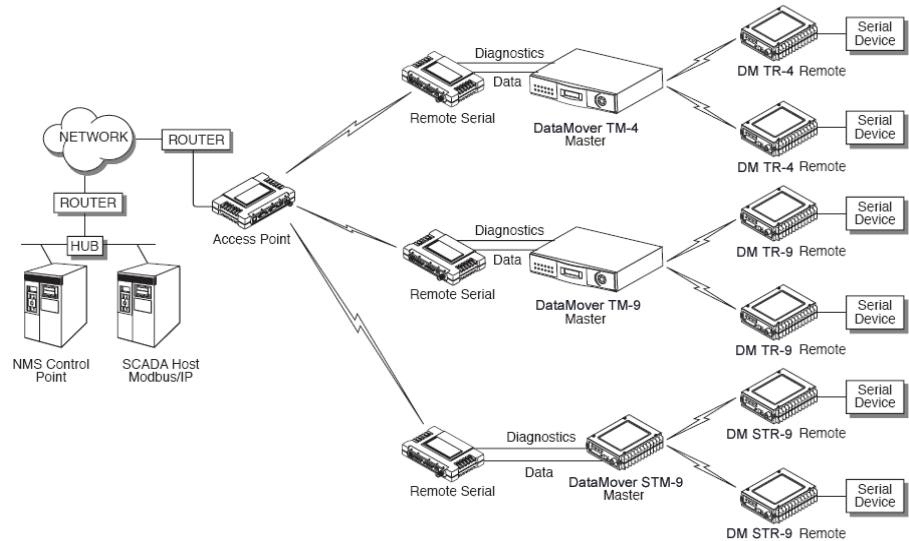


Figure 1-4. Backhaul Network

1.2.4 Multiple Protocols and/or Services

Prior to the DataMover ESS, two radios were often used to service two different types of devices (typically connected to different SCADA hosts). An ESS or ESS-II radio provides this functionality with a single remote radio. Each of the two serial ports 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 1-5 on Page 8](#).

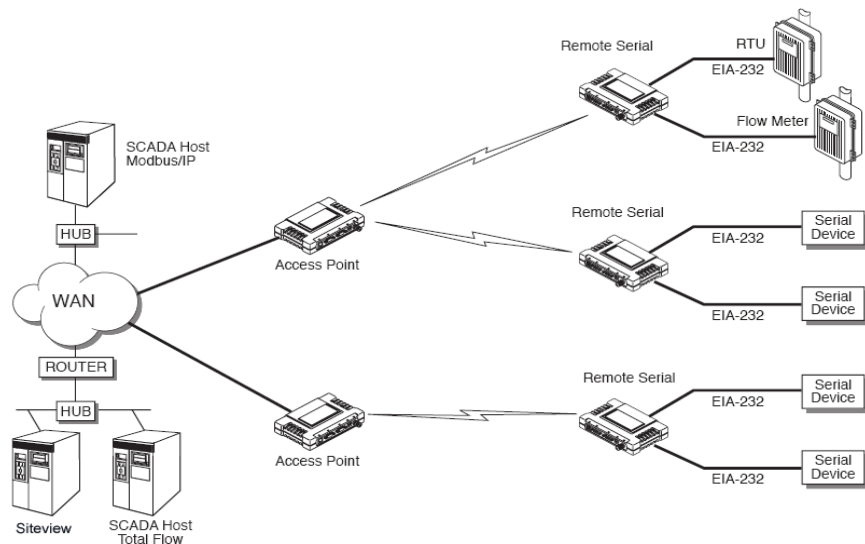


Figure 1-5. Multiple Protocol Network

By using a single radio, the cost of deployment is cut in half. Beyond requiring only one radio instead of two, the biggest cost reduction comes

from using half of the required infrastructure at the remote site: one antenna, one feedline, one lightning protector and ancillary hardware. Other cost reductions come from the system as a whole, such as reduced management requirements. And above all, the potential for future applications that run over Ethernet and IP, such as video for remote surveillance.

1.2.5 Wireless LAN with Mixed Services

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

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

IP-based devices that may be used with the transceiver include a new breed of more powerful Remote Terminal Units (RTUs) and Programmable Logic Controllers (PLCs). These, as well as other devices, may be used in applications ranging from SCADA/telemetry monitoring, web-based video, security monitoring, and voice over IP. [Figure 1-6](#) shows a typical wireless IP network.

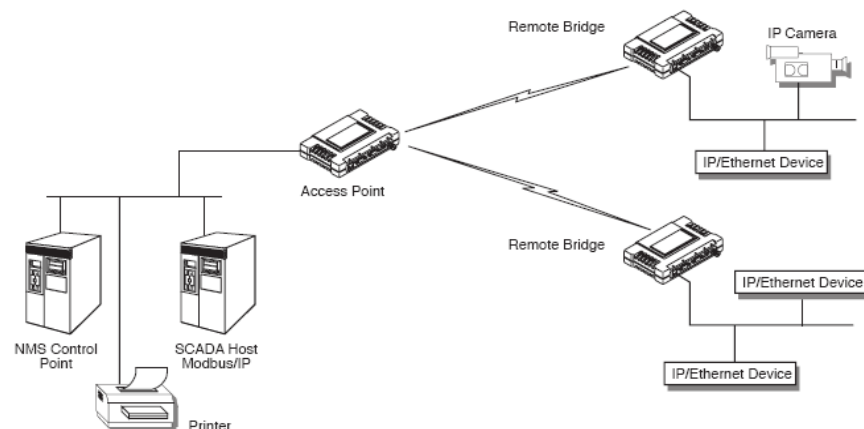


Figure 1-6. Extended-Range LAN with Mixed Applications

1.2.6 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 sold by SIMREX Corporation. There are several ways that these systems can benefit from incorporating ESS equipment. The chief advantages are interface flexibility (serial and Ethernet in one unit), and higher data throughput. By taking advantage of its built-in serial and Ethernet interfaces, the transceiver is well suited to replace leased lines, dial-up lines, or existing MAS 900 MHz data transceivers.

Replacing Legacy Wireless Products

In most cases, legacy radio transceivers supporting serial-interface equipment can be replaced with ESS transceivers. Legacy equipment can be connected to the transceiver 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).

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

Supplement legacy wireless network with IP services

The ESS 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 UDP and connection-orientated TCP.

In the UDP mode, the transceiver supports point-to-multipoint serial-port to serial-port connectivity. In the TCP mode, it supports point-to-point Ethernet/IP to serial port connectivity.

For further details on the transceiver's Serial Gateway interface modes, see [“CONFIGURING THE SERIAL INTERFACES” on Page 61](#).

1.2.7 High-Speed Mobile Data

The ESS radios support high-speed data communications in a mobile environment. Remote radios roam between different access points, providing seamless transitions and continuous coverage. For additional information on configuring a mobile network, refer to [Mobile Data Configuration on Page 58](#).

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. It introduces some additional end-to-end transmission delay but provides longer-range connectivity.

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

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

Although the range between transceivers can be up to 40 km (25 miles) over favorable terrain, it is possible to extend the range considerably by connecting two units together at one site in a “back-to-back” fashion to form a repeater, as shown in Figure 1-7. This arrangement should be used whenever the objective is to utilize the maximum range between stations. In this case, using high-gain Yagi antennas at each location will provide more reliable communications than their counterparts—omnidirectional antennas.

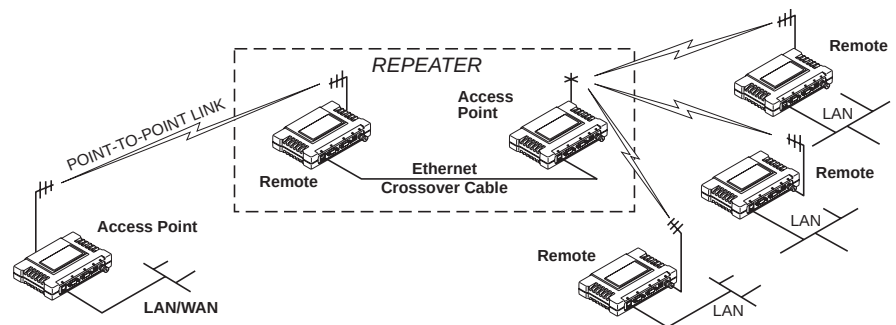


Figure 1-7. Typical LAN with a Repeater Link

Overview

Two transceivers may be connected “back-to-back” through the LAN Ports to form a repeater station. (The cable must be a “cross-over” Ethernet cable for this to work). This configuration is sometimes required in a network that includes a distant Remote that would otherwise be unable to communicate directly with the Access Point station due to distance or terrain.

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

by the repeater station antennas. A detailed discussion on the effects of terrain is given in [Section 5.1.2, Site Selection \(beginning on Page 140\)](#).

The following paragraphs contain specific requirements for repeater systems.

Antennas

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

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

Network Name

The two radios that are wired together at the repeater site *must* have different network names. To set or view the network names, see [“STEP 3—CONNECT PC TO THE TRANSCEIVER” on Page 22](#) for details.

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

A wireless network can be extended through the use of an alternate arrangement using the Access Point as a repeater to re-transmit the signals of all stations in the network. The repeater is a standard transceiver configured as an Access Point, and operating in Store and Forward mode. (See [Figure 1-8](#).)

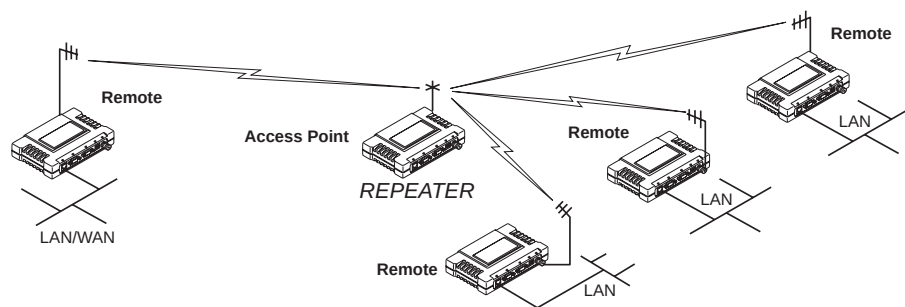


Figure 1-8. Typical network with store-and-forward repeater

As with the conventional repeater described in Option 1 above, the location of a store and forward repeater is also important. A site must be chosen that allows good communication with *both* the Access Point and the outlying Remote site. This can be on the top of a hill, building, or other elevated terrain from which all sites can be “seen” by the repeater

station antenna. A detailed discussion on the effects of terrain is given in [Section 5.1.2, Site Selection](#) (beginning on Page 140)

1.3.2 Protected Network Operation using Multiple Access Points

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

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

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

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

1.3.3 Collocating Multiple Radio Networks

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

The Network Name and the association process

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

Multiple APs with the same Network Name should be used with care. Using the same Network Name in multiple APs may result in Remotes

associating with undesired APs and preventing data exchange from occurring as planned.

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

**Co-Location for
Multiple Networks**

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

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

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

When multiple radio networks operate in close physical proximity to other wireless networks, individual units may not operate reliably under weak signal conditions and may be influenced by strong radio signals in adjacent bands. This radio frequency interference cannot be predicted with certainty, and can only be determined by experimentation. If you need to co-locate two units, start by using the largest possible vertical antenna separation between the two AP antennas on the same support structure. If that does not work, consult with your factory representative about other techniques for controlling radio frequency interference between the radios. (See ["A Word About Radio Interference"](#) on [Page 145](#) for more details.)

1.4 SIMREX CYBER SECURITY SUITE

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

The transceiver is capable of dealing with many common security issues. [Table 1-3](#) profiles security risks and how the transceiver provides a solution for minimizing vulnerability.

Table 1-3. Security Risk Management

Security Vulnerability	SIMREX Cyber Security Solution
Unauthorized access to the backbone network through a foreign remote radio	• 802.1x RADIUS authentication • Approved Remotes List (local) Only those remotes included in the AP list will associate
"Rogue" AP, where a foreign AP takes control of some or all remote radios and thus remote devices	• 802.1x RADIUS authentication • Approved AP List A remote will only associate to those AP included in its local authorized list of AP
Dictionary attacks, where a hacker runs a program that sequentially tries to break a password.	• Failed-login lockdown After 3 tries, the transceiver ignores login requests for 5 minutes. Critical event reports (traps) are generated as well.
Denial of service, where Remote radios could be reconfigured with bad parameters bringing the network down.	• Remote login with SSH or HTTPS • Local console login • Disabled HTTP & Telnet to allow only local management services
Airsnort and other war-driving hackers in parking lots, etc.	• 900 MHz operation is not interoperable with standard 802.11b wireless cards • The transceiver cannot be put in a promiscuous mode • Proprietary data framing
Eavesdropping, intercepting messages	• AES-128 encryption (ESS-II) • RC4-128 encryption (ESS)
Key cracking software	• Automatic Rotating Key algorithm
Replaying messages	• Automatic Rotating Key algorithm

Table 1-3. Security Risk Management

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

1.5 ACCESSORIES

The transceiver can be used with one or more of the accessories listed in [Table 1-4](#). Contact the factory for ordering details.

Table 1-4. Accessories

Accessory	Description	SIMREX 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	ESS-PWR-KIT
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.	ESS-ADPT-TNCM-NF
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.	CAB.ESS-TNC-36N (3FT./1M) CAB.ESS-TNC-72N (6FT./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 $\approx$ 3 ft./1M)	CAB.ESS-RJ45X
2-Pin Power Plug	Mates with power connector on transceiver. Screw terminals provided for wires, threaded locking screws to prevent accidental disconnect.	ESS-CONN-2P

Table 1-4. Accessories (Continued)

Accessory	Description	SIMREX Part No.
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 $\approx$ 3 ft./1M)	CAB.ESS-RJ45S
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).	CAB.ESS-DB25M-9F-6 (6 ft./1.8m) CAB.ESS-DB25M-9F-15 (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.	CAB.ESS-DB9M-9F-6
Fuse	Small, board-mounted fuse used to protect against over-current conditions.	ESS-FUSE-2A
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.	ESS-MNT-BRKT
	Screws: 6-32/1/4" with locking adhesive. (Industry Standard MS 51957-26)	MS6-32-ESS
DIN Rail Mounting Bracket	Bracket used to mount the transceiver to standard 35 mm DIN rails commonly found in equipment cabinets and panels.	ESS-DIN-BRKT
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.)	CAB.ESS-DB25F-DB9M
SIMREX DataMover NMS Software	PC-based network management system for new-generation SIMREX transceivers. Allows radio control and diagnostics in a hierarchical map perspective.	ESS-NETMGR
Bandpass Filter	Antenna system filter that helps eliminate interference from nearby paging transmitters.	ESS-FLTR-A2
Ethernet Surge Suppressor	Surge suppressor for protection of Ethernet port against lightning.	ESS-SURGE-RJ





2 TABLETOP EVALUATION AND TEST SETUP

Contents

2.1 OVERVIEW	21
2.2 STEP 1—INSTALL THE ANTENNA CABLING	21
2.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER.	22
2.4 STEP 3—CONNECT PC TO THE TRANSCEIVER	22
2.5 STEP 4—REVIEW TRANSCEIVER CONFIGURATION	23
2.5.1 Getting Started	23
2.5.2 Procedure	23
2.5.3 Basic Configuration Defaults	23
2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT	24
2.7 STEP 6—CHECK FOR NORMAL OPERATION	25



2.1 OVERVIEW

It is best 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.

When you are satisfied that the network is functioning properly in a bench setting, field installation can be performed. Complete information for field installation, including mounting dimensions and antenna selection, is provided in [INSTALLATION PLANNING on Page 138](#)

For the following evaluation, one of the transceivers in the network must be set to Access Point service (**Device Mode = Access Point**) for proper operation.

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.

2.2 STEP 1—INSTALL THE ANTENNA CABLING

[Figure 2-1](#) 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.

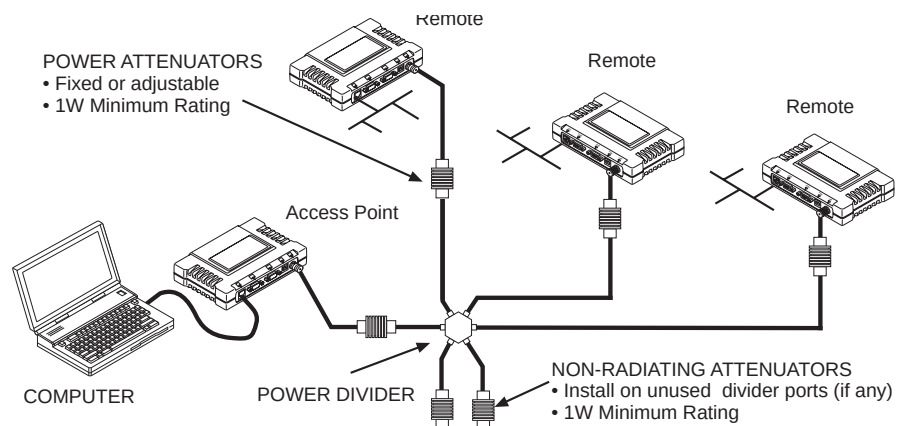


Figure 2-1. Typical setup for tabletop-testing of radios

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 51.)

2.3 STEP 2—MEASURE & CONNECT THE PRIMARY POWER

The primary power at the transceiver’s power connector must be within 10–30 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 2-2 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 2-2. Power Connector, Polarity: Left +, Right –

CAUTION

POSSIBLE
EQUIPMENT
DAMAGE

The transceiver must only be used 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.

2.4 STEP 3—CONNECT PC TO THE TRANSCEIVER

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

2.5 STEP 4—REVIEW TRANSCEIVER CONFIGURATION

2.5.1 Getting Started

Start by logging into the Access Point. Set up the Access Point first because the Remotes are dependent on its beacon signal to achieve the “associated” state.

NOTE: Transceivers are shipped from the factory set to the “Remote” mode unless they are marked differently.

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

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

2.5.2 Procedure

The following is a summary of the configuration procedure that must be done on each unit in the system. Key parameters are shown on the Embedded Management System overview ([Figure 3-1 on Page 30](#)). A lists of parameters can found in two tables: [Table 4-5 on Page 128](#) and [Table 4-7 on Page 131](#). Detailed information on using the Management System can be found in [MS INTRODUCTION on Page 30](#).

NOTE: The Management System supports the use of “configuration files” to aid in uniformly configuring multiple units. These are detailed in [Using Configuration Scripts on Page 107](#).

2.5.3 Basic Configuration Defaults

[Table 2-1](#) provides a selection of key operating parameters, their range, and default values. All of these are accessible through a terminal emulator connected to the COM1 serial port or through a Web browser connected to the LAN Port. (See [Figure 5-1 on Page 138](#) for hookup.)

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

Table 2-1. Basic Configuration Defaults

Item	Menu Location	Default	Values/Range
Device Mode ¹	Main Menu>> Network Configuration>> Device Mode	Marked on unit's ID label	• Access Point • Dual Remote • Serial Gateway • Ethernet Bridge
Network Name	Main Menu>> Network Configuration>> Network Name	"Not Programmed"	• 1–15 alphanumeric characters • Case-sensitive; can be mixed case
IP Address	Main Menu>> Network Configuration>> IP Address	192.168.1.1	Contact your network administrator
RF Output Power	Main Menu>> Radio Configuration>> RF Output Power	30 dBm (1.0 Watt)	20–30 dBm @ 50Ω (0.1–1.0 Watts)
Unit Password	Main Menu>> Device Information>> User Password	admin (lower case)	• 1–8 alphanumeric characters • Case-sensitive; can be mixed case

1. Ethernet Bridge and Serial Gateway will not be displayed if a superior mode is authorized for this unit.

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

2.6 STEP 5—CONNECT LAN AND/OR SERIAL EQUIPMENT

Connect a local area network to the LAN port or serial devices to the COM1 (DCE) or COM2 (DTE) ports. Make sure your transceivers are capable of supporting your devices. (See [Table 1-1 . Transceiver 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: If you configure COM1 for payload data service while you are plugged into it, you will not be able to access the management system. Alternate methods for accessing the management system are: use Telnet or the web browser through the Ethernet port; use Telnet or the web browser through the antenna port (remote management).

[Figure 2-3 on Page 25](#) shows the default functions and services for the interface connectors.

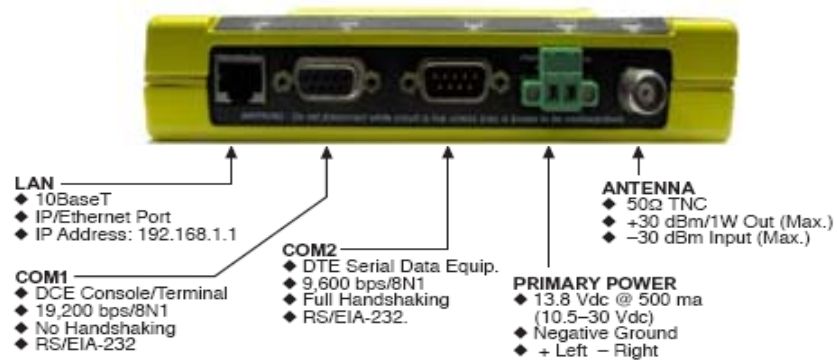


Figure 2-3. Interface Connectors, Functions & Defaults

2.7 STEP 6—CHECK FOR NORMAL OPERATION

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

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

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

Table 2-2 provides details on the LED functions.

Table 2-2. Transceiver LED Functions

LED Label	Activity	Indication
LAN	ON	LAN detected
	Blinking	Data TX/RX
	OFF	LAN not detected, or excessive traffic present
COM1 (MGT System)	Blinking	Data TX/RX
	OFF	No data activity
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

Table 2-2. Transceiver LED Functions (Continued)

LED Label	Activity	Indication
LINK (Access Point)	ON	Default state
	Blinking	Data Tx/Rx
	OFF	Traffic exceeds the capacity of the radio network
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.

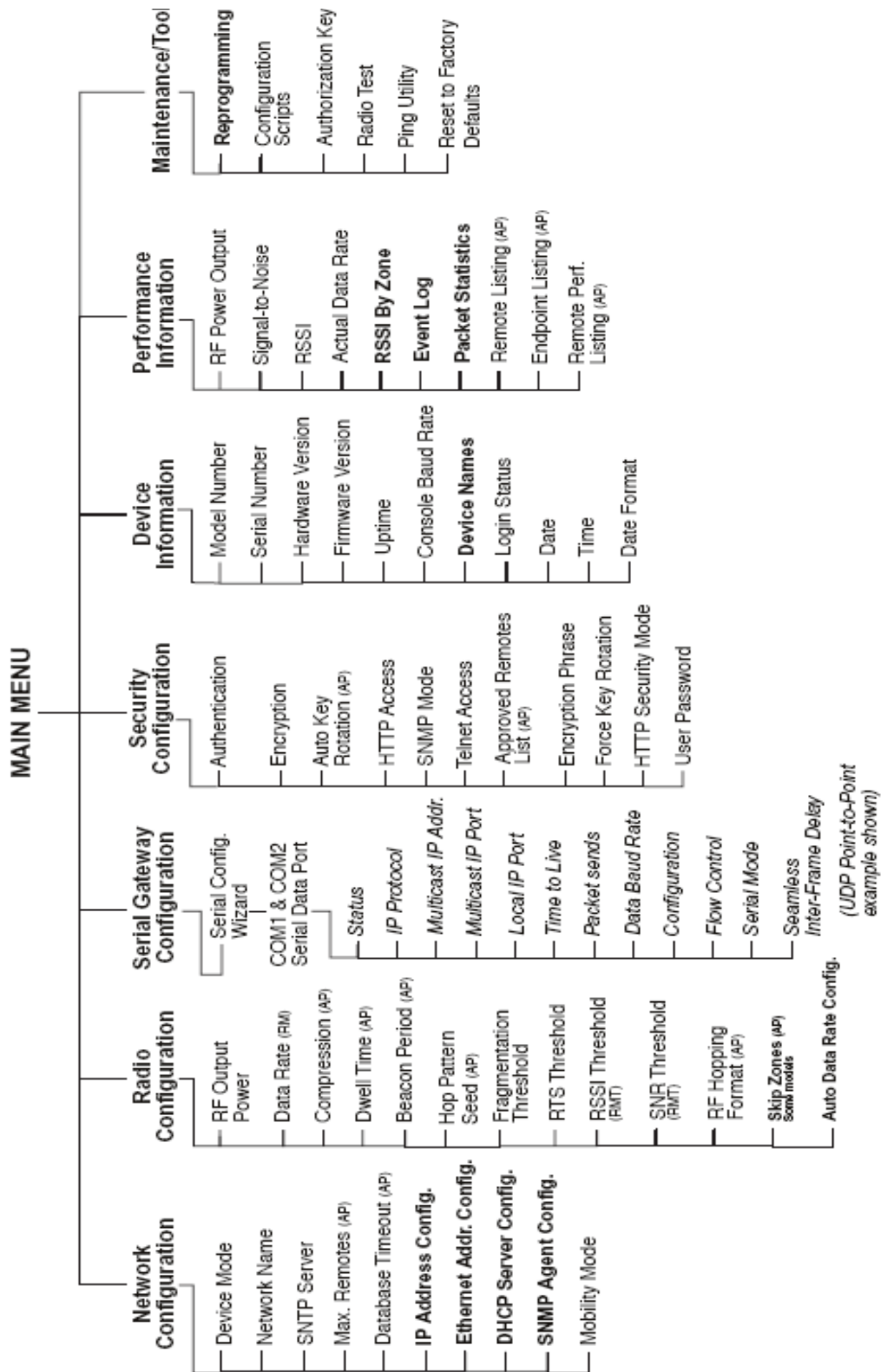


3 EMBEDDED MANAGEMENT SYSTEM

Contents

3.1 MS INTRODUCTION.....	29
3.1.1 Differences in the User Interfaces	29
3.2 ACCESSING THE MENU SYSTEM	31
3.2.1 Methods of Control	32
3.2.2 PC Connection & Log In Procedures	32
3.2.3 Navigating the Menus	37
3.3 BASIC DEVICE INFORMATION.....	38
3.3.1 Starting Information Screen	38
3.3.2 Main Menu	39
3.3.3 Configuring Basic Device Parameters	40
3.4 CONFIGURING NETWORK PARAMETERS	42
3.4.1 Network Configuration Menu	42
3.4.2 IP Address Configuration Menu	44
3.4.3 Ethernet Port Configuration Menu	45
3.4.4 DHCP Server Configuration	46
3.4.5 SNMP Agent Configuration	48
3.5 RADIO CONFIGURATION	50
3.5.1 Radio Configuration Menu	50
3.5.2 Mobile Data Configuration	57
3.6 CONFIGURING THE SERIAL INTERFACES.....	60
3.6.1 Overview	60
3.6.2 Serial Data Port Configuration Menu	63
3.6.3 Configuring for UDP Mode	64
3.6.4 Configuring for TCP Mode	67
3.6.5 Configuring for PPP Mode	70
3.6.6 IP-to-Serial Application Example	71
3.6.7 Point-to-Point Serial-to-Serial Application Example	72
3.6.8 Point-to-Multipoint Serial-to-Serial Application Example	73
3.6.9 Mixed Modes	75
3.7 CYBER SECURITY CONFIGURATION	77
3.7.1 Device Security	77

- 3.7.2 Wireless Security 79
- 3.7.3 RADIUS Authentication 81
- 3.7.4 RADIUS Configuration 82
- 3.7.5 Certificate Management (Remote transceivers only) 83
- 3.8 PERFORMANCE VERIFICATION..... 84
- 3.8.1 Performance Information Menu 84
- 3.8.2 Network Performance Notes 95
- 3.9 MAINTENANCE 99
- 3.9.1 Reprogramming Menu 100
- 3.9.2 Configuration Scripts Menu 105
- 3.9.3 Authorization Keys Menu 114
- 3.9.4 Auto-Upgrade/Remote-Reboot Menu 114
- 3.9.5 Radio Test Menu 115
- 3.9.6 Ping Utility Menu 117
- 3.9.7 Reset to Factory Defaults 117

**NOTES**

- Chart shows top-level view only. Details are given on the following pages.
- Not all items are user-configurable
- Some menu items depend on the Device Mode selected
- Bolded items indicate a menu selection
- Spacebar used to make some menu selections
- AP = Access Point Only
- RM = Remote Only

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

3.1 MS INTRODUCTION

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

For SNMP management, the transceiver is compatible with SIMREX *D-View* software. Refer to SIMREX publication MAN.D-VIEW for more information on this tool. For support of other SNMP software, a set of MIB files is available for download from the SIMREX Web site at www.simrex.com. A brief summary of SNMP commands can be found at [SNMP Agent Configuration](#) section on Page 49 of this manual.

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

- [Section 3.3, BASIC DEVICE INFORMATION](#) (beginning on Page 38)
- [Section 3.4, CONFIGURING NETWORK PARAMETERS](#) (beginning on Page 42)
- [Section 3.5, RADIO CONFIGURATION](#) (beginning on Page 51)
- [Section 3.6, CONFIGURING THE SERIAL INTERFACES](#) (beginning on Page 61)
- [Section 3.7, CYBER SECURITY CONFIGURATION](#) (beginning on Page 78)
- [Section 3.8, PERFORMANCE VERIFICATION](#) (beginning on Page 85)
- [Section 3.9, MAINTENANCE](#) (beginning on Page 100)

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

3.1.1 Differences in the User Interfaces

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

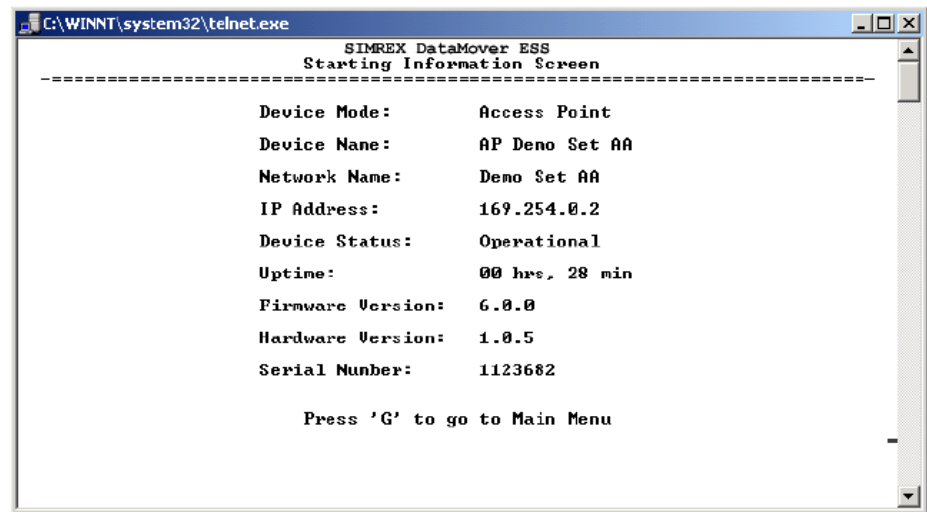


Figure 3-1. View of MS with a text-based program—
(Terminal Emulator shown—Telnet has similar menu structure)

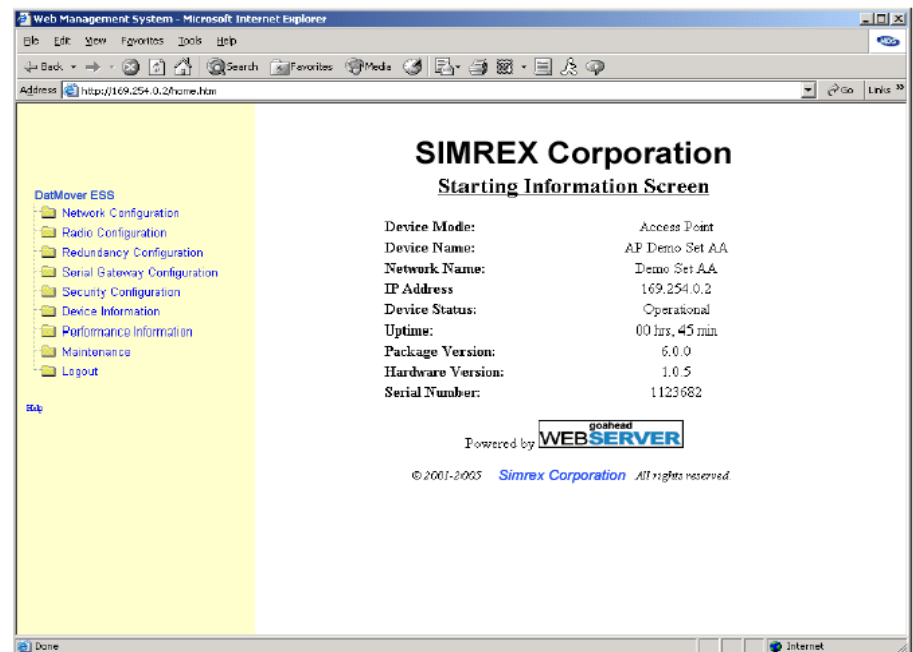


Figure 3-2. View of the MS with a Browser
(Selections at left provide links to the various menus)

3.2 ACCESSING THE MENU SYSTEM

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

3.2.1 Methods of Control

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

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

- * Telnet, SSH and Web Browser sessions require the use of a *straight-through* or *crossover* Ethernet cable, depending on whether the PC-to-radio connection is made directly, or through a network. For direct connection, a **crossover** cable is required; For connection via a network, a **straight-through** type is needed.

Cable type can be identified as follows: Hold the two cable ends side-by-side and in the same plug orientation (*i.e.*, both locking tabs up or down). Now look at the individual wire colors on each plug. If the wires on both plugs are ordered in the same sequence from left to right, the cable is a straight-through type. If they are not in the same order, it *may* be a crossover cable, or it may be wired for some other application. Refer to [DATA INTERFACE CONNECTORS on Page 151](#) for detailed pinout information.

3.2.2 PC Connection & Log In Procedures

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

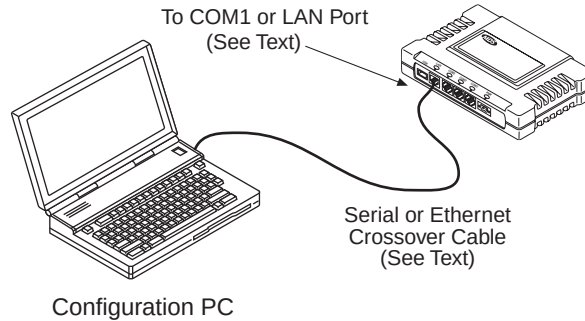


Figure 3-3. PC Configuration Setup

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

1. Connect a serial communications cable between the PC and the unit's COM 1 port. If necessary, a cable may be constructed for this purpose as shown in [Figure 3-4](#).

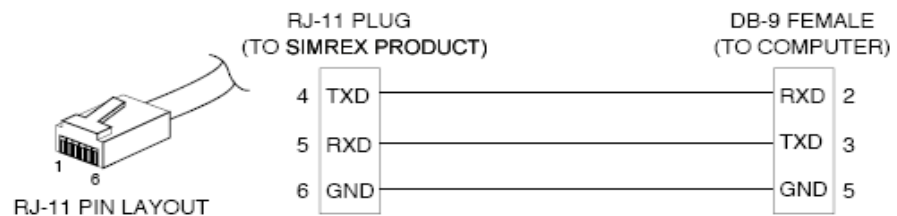


Figure 3-4. Serial Communications Cable (RJ-11 to DB-9)
(Maximum Recommended Cable Length 50 Feet/15 meters)

2. Launch a terminal emulation program such as HyperTerminal and configure the program with the following settings:
 - 19,200 bps data rate
 - 8 data bits, no parity
 - One stop bit, and no flow-control
 - Use ANSI or VT100 emulation.

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

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

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

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

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

The unit responds with the Starting Information Screen ([Figure 3-5](#)). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

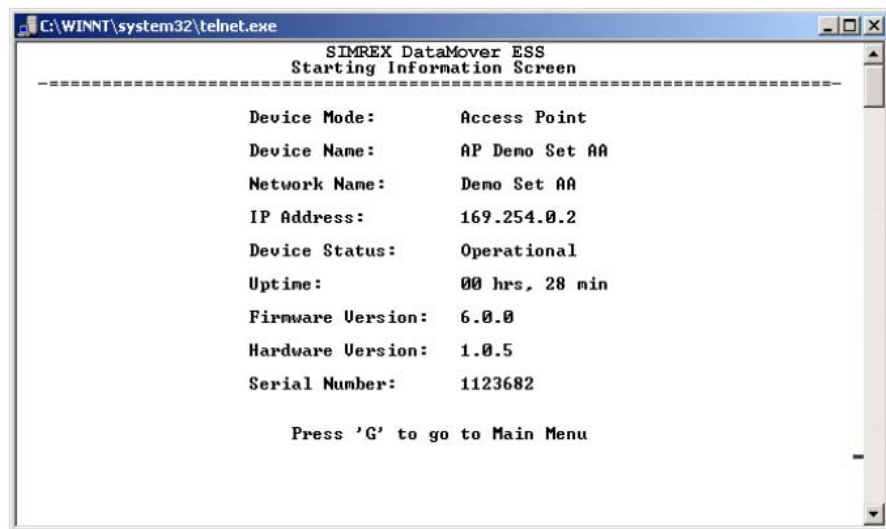


Figure 3-5. Starting Information Screen—Local Console Session
(Telnet has similar menu structure)

Starting a Telnet Session

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

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

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

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

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

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

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

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

The unit responds with a Starting Information Screen (see [Figure 3-5](#)). From here, you can review basic information about the unit or press **G** to proceed to the Main Menu.

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

Starting a Web Browser Session

NOTE: Web access requires that you know the IP address of the unit you are connecting to. If you do not know the address, start a Local Console session (see [Starting a Local Console Session \(Recommended for first-time log-in\)](#) on Page 33) and access the *Starting Information Screen*. The IP address is displayed on this screen.

1. Connect a PC to the unit's LAN port, either directly or via a network. If connecting directly, use an Ethernet *crossover* cable; if connecting via a network, use a *straight-through* cable. The LAN LED lights to indicate an active connection.
2. Launch a Web-browser session on your computer (*i.e.*, Internet Explorer, Netscape Navigator, etc.).

3. Type in the unit's IP address and press **ENTER**.
4. A log-in screen is displayed (**Figure 3-6**) where you enter a user name and password to access the unit's menu system. Note that the default entries are made in *lower case*. (Default User Name: **DataMover**; Default Password: **admin**)

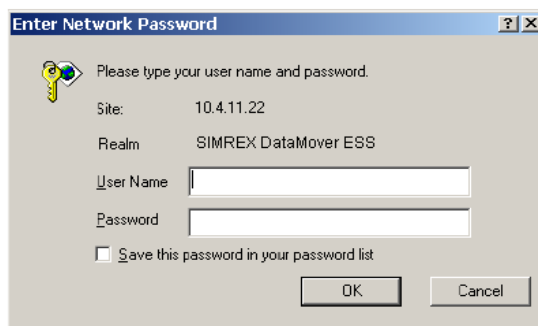


Figure 3-6. Log-in Screen when using a Web Browser

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

5. Click **OK**. The unit responds with a startup menu screen similar to that shown in **Figure 3-7**. From here, you can review basic information about the unit or click on one of the menu items at the left side of the screen.

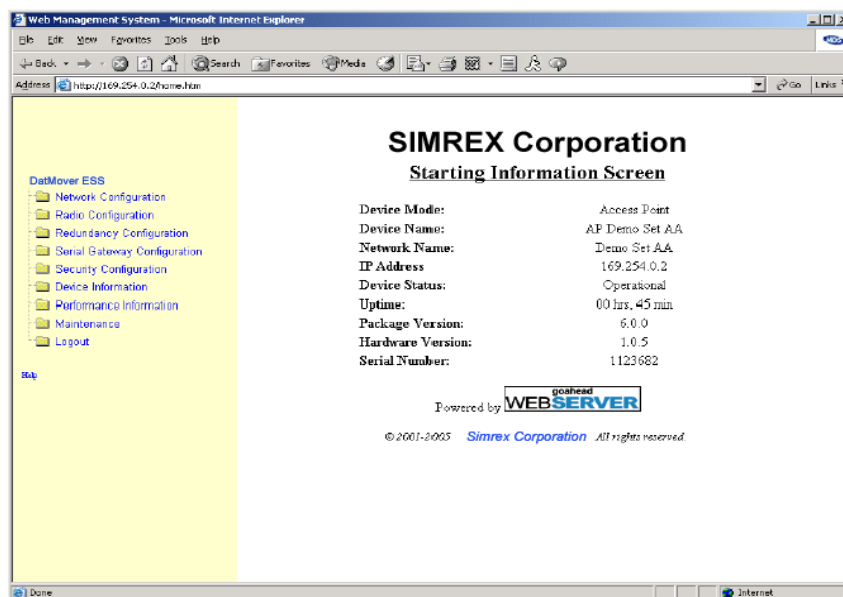


Figure 3-7. Starting Information Screen—Web Browser Example

3.2.3 Navigating the Menus

Via Terminal Telnet or SSH Sessions

Recommended for first-time log-in

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

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

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

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

Logging Out Via Terminal Emulator or Telnet

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

Navigating via Web Browser

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

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

Logging Out Via Web Browser

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

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

3.3 BASIC DEVICE INFORMATION

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

3.3.1 Starting Information Screen

Once you have logged into the Management System, 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 and operating conditions.

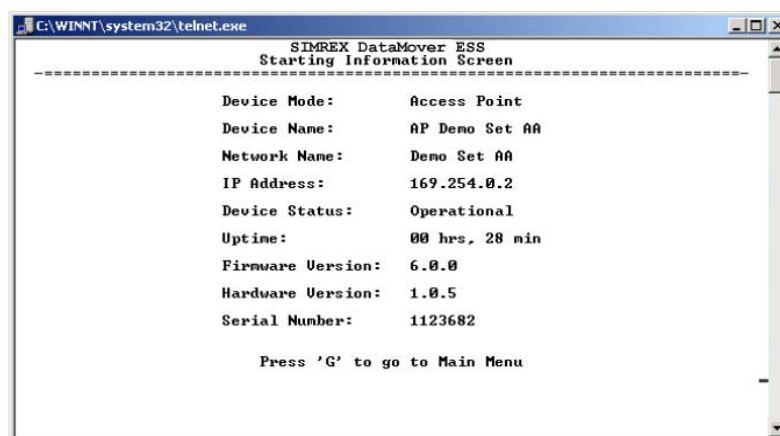


Figure 3-8. Starting Information Screen

- **Device Mode**—Current operating mode of the unit as it relates to the radio 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 42.](#))
- **Network Name**—The name of the radio network in which the unit is associated.
- **IP Address**—Unit's IP address [192.168.1.1]
- **Device Status**—Condition of the unit's association with an Access Point.

At the Access Point:

- *Alarmed*—A alarm 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 has detected one or more alarms that have not been cleared.

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

- **Uptime**—Elapsed time since the transceiver was powered-up.
- **Firmware Version**—Version of firmware that is currently active in the unit.
- **Hardware Version**—Hardware version of the transceiver’s printed circuit board.
- **Serial Number**—Make a record of this number. It must be provided to purchase Authorization Keys to upgrade unit capabilities. (See [“Authorization Keys Menu” on Page 115.](#))

3.3.2 Main Menu

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

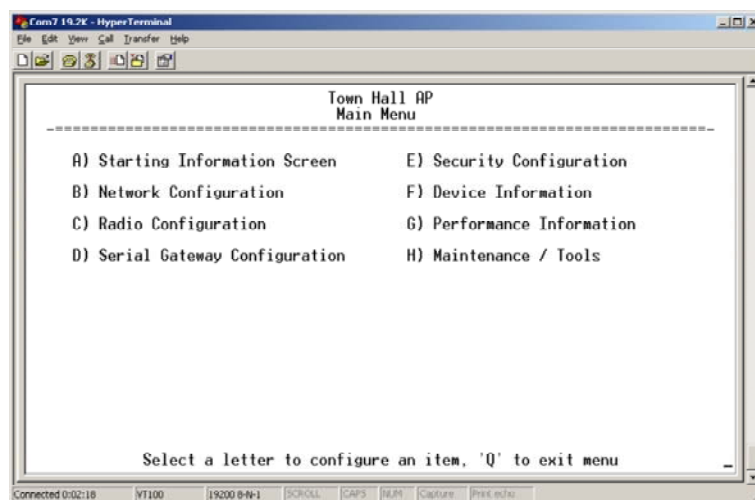


Figure 3-9. Main Menu

- **Starting Information Screen**—Select this item to return to the start-up screen. (See “[Starting Information Screen](#)” on Page 38)
- **Network Configuration**—Tools to configure the data network layer of the transceiver. (See “[Network Configuration Menu](#)” on Page 42)
- **Radio Configuration**—Tools to configure the wireless (radio) layer of the transceiver. (See “[Radio Configuration Menu](#)” on Page 51)
- **Serial Gateway Configuration**—Tools to configure the two serial ports. (See “[Serial Data Port Configuration Menu](#)” on Page 64)
- **Security Configuration**—Tools to configure the security services available with the transceiver’s environment. (See “[SIMREX CYBER SECURITY SUITE](#)” on Page 14)
- **Device Information**—Top level user-specific and definable parameters, such as unit password. (See “[Device Information](#)” on Page 40)
- **Performance Information**—Tools to measure the radio and data layer’s performance of the radio network. (See “[Performance Information Menu](#)” on Page 85)
- **Maintenance/Tools**—Tools to use configuration files, change firmware and use Authorization Keys to change major unit capabilities. (See “[Authorization Keys Menu](#)” on Page 115)

3.3.3 Configuring Basic Device Parameters

Device Information

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 device names.

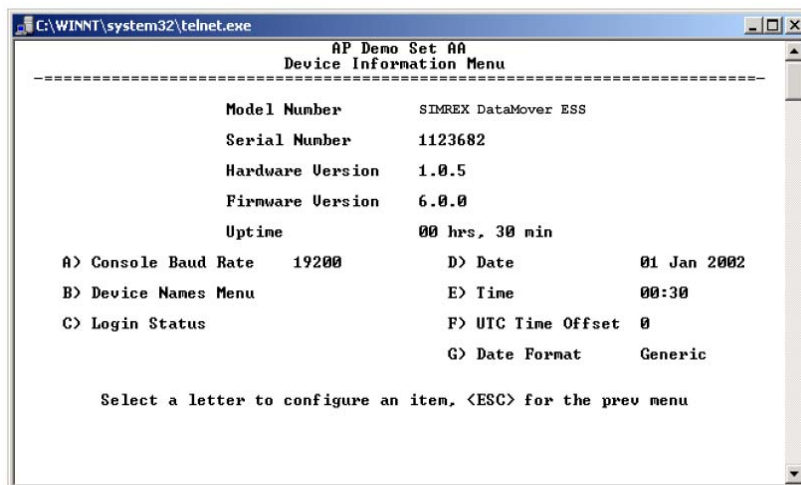


Figure 3-10. Device Information Menu

- **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.
- **Console Baud Rate**—Used to set/display data communications rate (in bits-per-second) between a connected console terminal and the radio. [19200]
- **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 MS screen headings. (See [Figure 3-11 on Page 41](#))
- **Date**—Current date being used for the transceiver logs. User-settable. (Value lost with power failure if SNTP (Simple Network Time Protocol) server not accessible.)
- **Time**—Current time of day. User-settable.
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

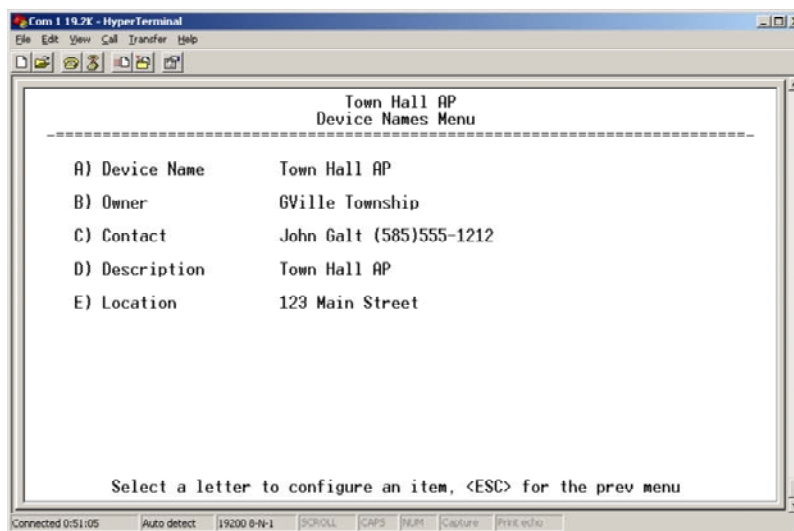


Figure 3-11. Device Names Menu

- **Device Name**—Device Name, used by the transceiver as the "Realm" name for network login (web browser only) 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.

3.4 CONFIGURING NETWORK PARAMETERS

3.4.1 Network Configuration Menu

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

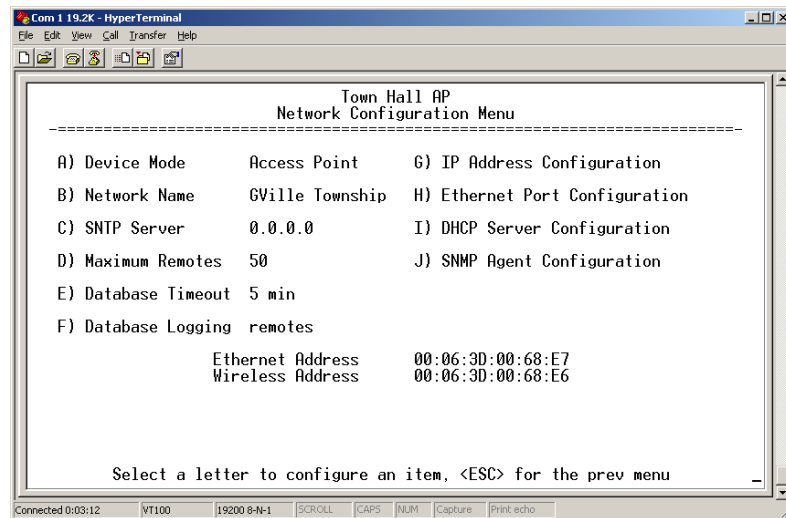


Figure 3-12. Network Configuration Menu
From Access Point

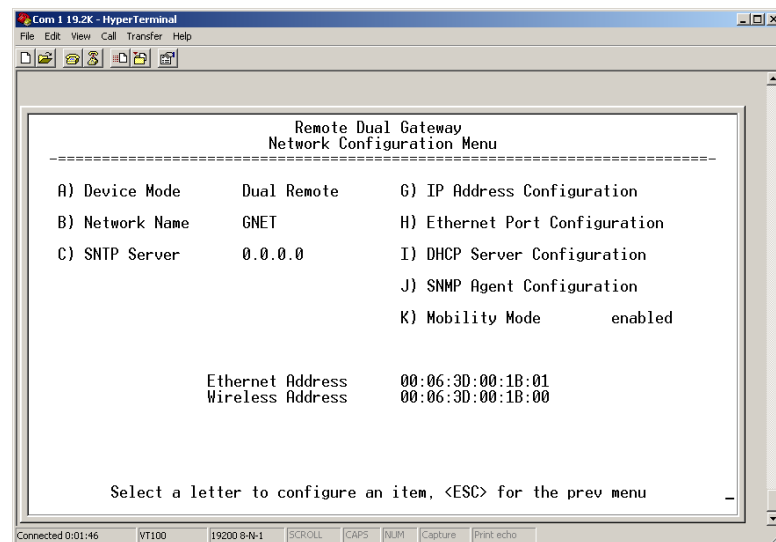


Figure 3-13. Network Configuration Menu
From Remote Unit

- **Device Mode** (*User Review Recommended*)—Either Access Point or a variation of a Remote. [**Remote**]
- **Network Name** (*User Review Required*)—Name of the radio network of which this unit will be a part. Essential for association of Remotes to the Access Point in the network. [**Not Programmed**]

TIP: For enhanced security, consider using misspelled words, a combination of letters and numbers, and a combination of upper and lower case letters. Also, the Network Name should be at least nine characters long. This helps protect against sophisticated hackers who may use a database of common words (for example, dictionary attacks) to determine the Network Name.

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

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

- **IP Address Configuration**—Presents a menu for configuring the local static IP address of the transceiver. Detailed explanations are provided in the section titled [IP Address Configuration Menu on Page 45](#)
- **Ethernet Port Configuration**—Presents a menu for defining the status of the Ethernet port (enabled or disabled), the Ethernet rate limit, link hardware watch (enabled/disabled), and the Ethernet link poll address. Detailed explanations of this menu are contained in [Ethernet Port Configuration Menu on Page 46](#)
- **DHCP Server Configuration**—Menu for configuration of DHCP services by the Access Point unit. DHCP provides “on-the-fly” IP address assignments to other LAN devices, including SIMREX DataMover ESS units. [Disabled]
- **SNMP Config Menu**—SNMP configuration parameters.
- **Mobility Mode**—Used to configure whether the transceiver is enabled or disabled for mobility operation. *Note that this selection may appear on both Access Point and Remote menus, but it only takes effect when set on Remotes.* Additional settings and information for mobility operation are contained in [Mobile Data Configuration on Page 58](#). [enabled, disabled; disabled].
- **Maximum Remotes (AP Only)**—Number of Remotes permitted to be associated with (served by) this Access Point. [50]
- **Database Timeout (AP Only)**—This sets the database “age time” ([Remote Listing Menu \(Access Points Only\) on Page 93](#)) to determine when a remote is declared as unavailable. The timer may be set from 0 to 255 minutes and resets each time a message is received from a remote. [0–255 minutes; 5 minutes]

- **Database Logging** (*AP Only*)—Determines which types of devices will be reported as “added” or “deleted” from the AP’s database (See [Section 3.8.1, Performance Information Menu \(beginning on Page 85\)](#)). In the case of deletions, this information is triggered by a timer expiration as described in the item above. Available selections are: **Remote**, **All** (endpoints and remotes), or **Disabled**.
- **Ethernet Address** (*Display Only*)—Hardware address of this unit’s Ethernet interface.
- **Wireless Address** (*Display Only*)—Hardware address of the unit’s wireless interface.

3.4.2 IP Address Configuration Menu

The radios use a local IP address to support remote management and serial device services. The IP address of a radio can be set as a *static IP address* or as a *dynamic IP address*. When static IP addressing is used, the user must manually configure the IP address and other parameters. When dynamic addressing is used, the radio uses a DHCP Client process to obtain an IP address from a DHCP Server, along with other parameters such as a *net mask* and a *default gateway*.

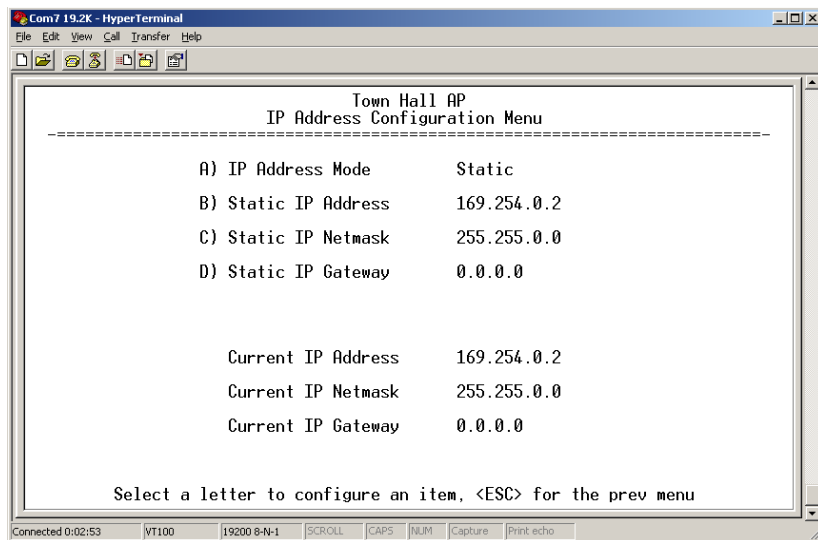


Figure 3-14. IP Address Configuration Menu

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

- **IP Address Mode**—Defines the source of the IP address of this device. [Static, Dynamic; Static]
- **Dynamic Mode**—Enabling this option forces the transceiver (AP or Remote) to obtain an IP address from any DHCP server available on the LAN. Dynamic Mode is also known as *DHCP Client* mode. [Disabled]
- **Static IP Address** (*User Review Recommended*)—Essential for connectivity to the transceiver's MS via the LAN port and to send Ethernet data over the network. Enter any valid IP address that will be unique within the network. [192.168.1.1]
This field is unnecessary if DHCP is enabled. [255.255.0.0]

Static IP Netmask—The IPv4 local subnet mask. This field is unnecessary if DHCP is enabled. [255.255.0.0]

- **Static IP Gateway**—The IPv4 address of the network gateway device, typically a router. This field is unnecessary if DHCP is enabled. [0.0.0.0]

The lower three lines of the screen show the actual addressing at the transceiver whether it was obtained from static configuration or from a DHCP server.

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

3.4.3 Ethernet Port Configuration Menu

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

NOTE: The DataMover ESS Ethernet port supports 10BaseT connections only. This should not present a problem because most hubs/switches auto-switch between 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

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

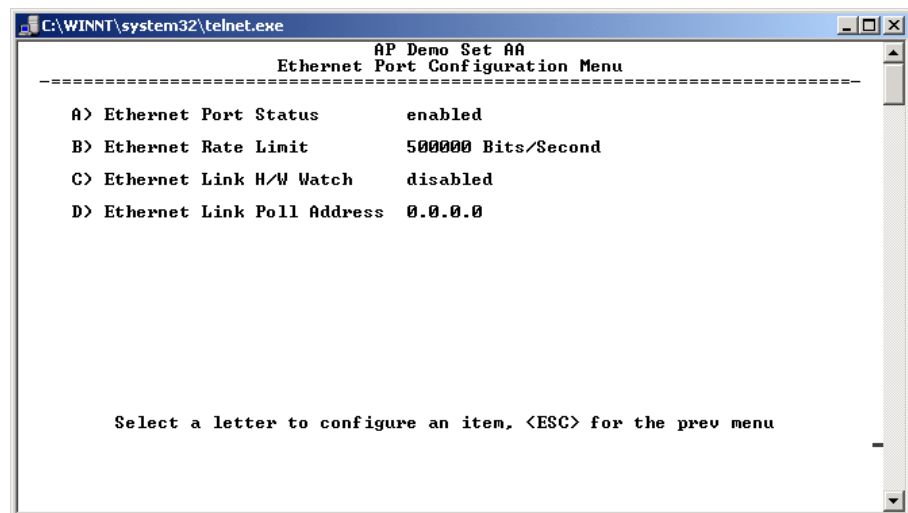


Figure 3-15. Ethernet Port Configuration Menu

- **Ethernet Port Status**—Allows enabling/disabling Ethernet traffic for security purposes. Setting it to **Follows Link Status** enables the port if there is a connection established with the AP, but disables it otherwise. [AP: **Enabled, Disabled; Enabled**]
[Remote: **Always On, Follow Radio Link, Disabled; Always On**]
- **Ethernet Rate Limit**—The transceiver will send alarms (SNMP traps) when the rate reaches 50%, 75%, and 100% to help identify potential problems with traffic.
- **Ethernet Link (H/W) Watch** (*AP Only*)—Detects the lack of an Ethernet connection to the LAN port at the electrical level (link integrity). The current AP will broadcast a beacon signal indicating its “NOT AVAILABLE” status so Remotes that hear it do not try to associate to it. Once the Ethernet connection is restored, this beacon signal changes to “AVAILABLE” and Remotes are allowed to join in. [**Disabled**]
- **Ethernet Link Poll Address** (*AP Only*)—When an IP address is provided, the Access Point pings the remote IP device every 2 minutes to test the integrity of the backhaul link. If this link is not available, the AP will advertise its “NOT AVAILABLE” status in the beacon signal so Remotes do not try to associate to it. Once the IP address is reachable, this beacon signal changes to “AVAILABLE” and Remotes are allowed to join in. 0.0.0.0 disables this function. Any other valid IP address enables it. [**0.0.0.0**]

3.4.4 DHCP Server Configuration

A transceiver can provide automatic IP address assignments to other IP devices in the network by providing DHCP (Dynamic Host Configuration Protocol) services. This service eliminates setting individual device IP address on Remotes in the network, but it still requires thoughtful

planning of the IP address range. One drawback to network-wide automatic IP address assignments is that SNMP services may become inaccessible as they are dependent on fixed IP addresses.

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

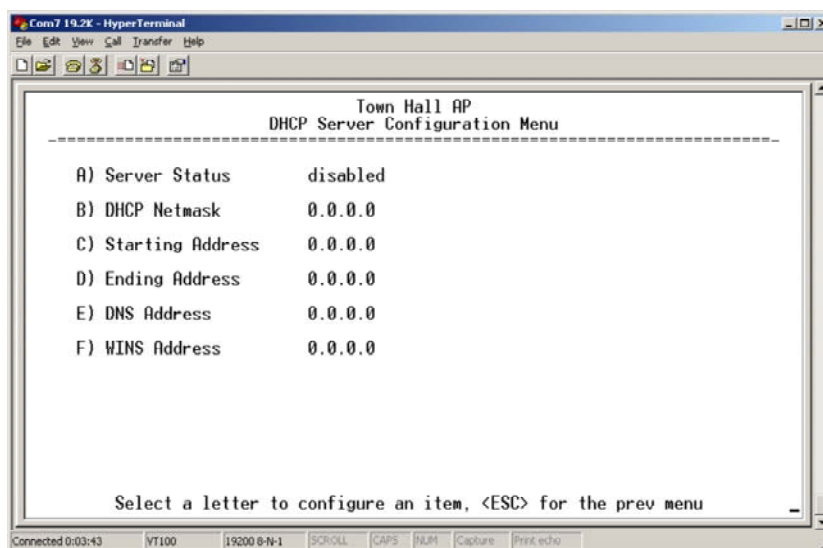


Figure 3-16. DHCP Server Configuration Menu

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

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

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

- **Restart DHCP Server**—Selecting this option forces the transceiver to start servicing DHCP requests using the Starting Address. Payload data will not be interrupted but may experience some delays as new addresses are distributed.

3.4.5 SNMP Agent Configuration

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

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

- **msdreg.mib**—SIMREX sub-tree registrations
- **mds_comm.mib**—SIMREX Common MIB definitions for objects and events which are common to the entire product family
- **inet_reg.mib**—SIMREX sub-tree registrations
- **inettrv1.mib**—SNMPv1 enterprise-specific traps
- **inettrv2.mib**—SNMPv2 enterprise-specific traps
- **inet_comm.mib**—MIB definitions for objects and events which are common to the entire ESS Series
- **inet_ap.mib**—MIB definitions for objects and events for an Access Point transceiver
- **inet_sta.mib**—Definitions for objects and events for a Remote radio
- **inet_sec.mib**—For security management of the radio system. SNMPv3 allows read/write operation. SNMPv1/2 allows only for read-only access.

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

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

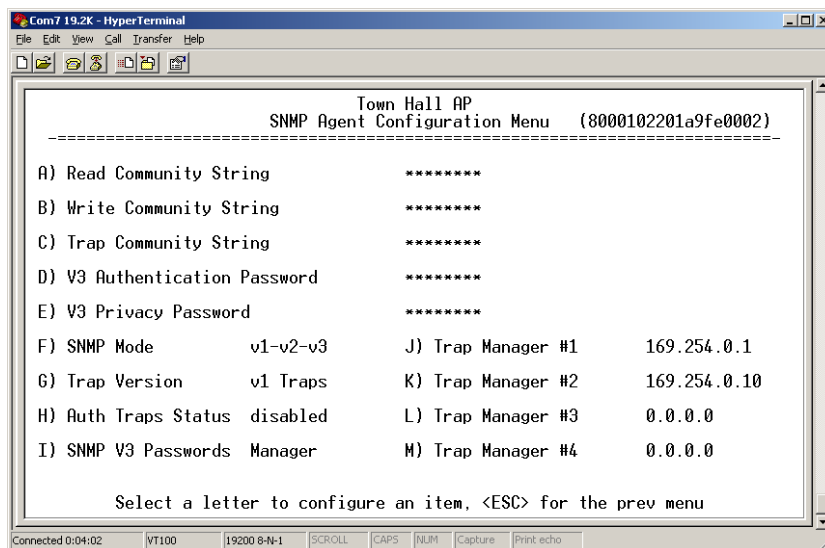


Figure 3-17. SNMP Server Configuration Menu
From Access Point

This menu provides configuration and control of vital SNMP functions.

- **Read Community String**—SNMP community name with SNMPv1/SNMPv2c read access. This string can be up to 30 alpha-numeric characters.
- **Write Community String**—SNMP community name with SNMPv1/SNMPv2c write access. This string can be up to 30 alpha-numeric characters.
- **Trap Community String**—SNMP community name with SNMPv1/SNMPv2c trap access. This string can be up to 30 alpha-numeric characters.
- **V3 Authentication Password**—Authentication password stored in flash memory. This is used when the Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for Authentication (currently, only MD5 is supported). This string can be up to 30 alpha-numeric characters.
- **V3 Privacy Password**—Privacy password stored in flash memory. Used when the SNMP Agent is managing passwords locally (or initially for all cases on reboot). This is the SNMPv3 password used for privacy (DES encryption). This string can be between 8 and 30 alpha-numeric characters.
- **SNMP Mode**—This specifies the mode of operation of the radio's SNMP Agent. The choices are: disabled, v1_only, v2_only, v3_only, v1-v2, and v1-v2-v3. If the mode is disabled, the Agent does not respond to any SNMP traffic. If the mode is v1_only, v2_only, or v3_only, the Agent responds only to that version of SNMP traffic. If the mode is v1-v2, or v1-v2-v3, the Agent responds to the specified version of SNMP traffic.
[v1-v2-v3]

- **Trap Version**—This specifies what version of SNMP will be used to encode the outgoing traps. The choices are v1_traps, v2_traps, and v3_traps. When v3_traps are selected, v2-style traps are sent, but with a v3 header. [v1 Traps, v2 Traps, v3 Traps]
- **Auth Traps Status**—Indicates whether or not traps will be generated for login events to the transceiver. [Disabled/Enabled; Disabled]
- **SNMP V3 Passwords**—Determines whether v3 passwords are managed locally or via an SNMP Manager. The different behaviors of the Agent depending on the mode selected, are described in **SNMP Mode** above.
- **Trap Manager #1-#4**— Table of up to 4 locations on the network that traps are sent to. [Any standard IP address]

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

3.5 RADIO CONFIGURATION

There are two primary data layers in the transceiver network—radio and data. Since the data layer is dependent on the radio layer working properly, configuration of the radio items should be reviewed and set before proceeding. This section explains the *Radio Configuration Menu*, (Figure 3-18 for AP, Figure 3-19 for Remote). The Configuration Menu is followed a secondary menu, the *Skip Zone Options*.

3.5.1 Radio Configuration Menu

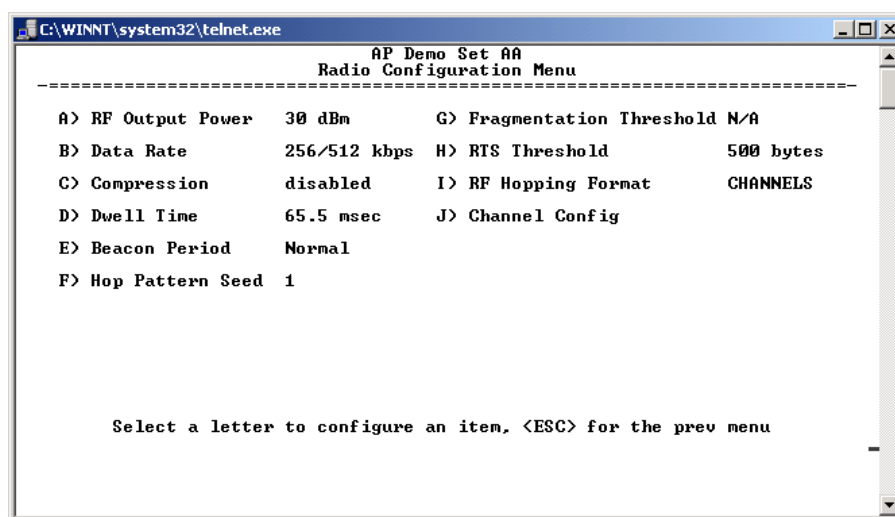


Figure 3-18. Radio Configuration Menu From ESS Access Point
(ESS-II data rate selection is 512/1024 kbps)

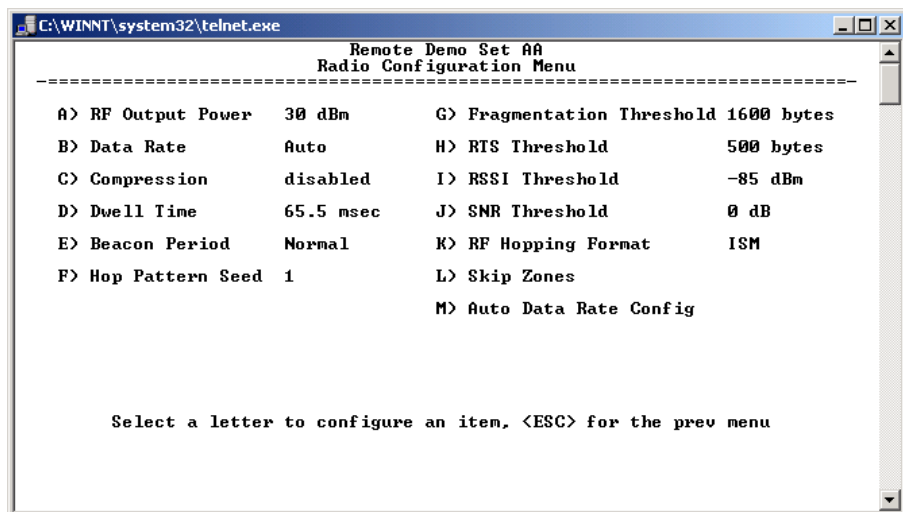


Figure 3-19. Radio Configuration Menu
From Remote Unit

- **RF Output Power** (*User Review Recommended*)—Sets/displays 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 144](#) for information on how to calculate this value.)
[20–30; 20]
- **Data Rate** (*Remote Only. AP fixed is at 256/512 kbps for ESS; 512/1024 kbps for ESS-II.*)—Shows the over-the-air data rate setting for the Remote radio. Remotes can operate at one of two data rates when communicating with an AP; 256 kbps or 512 kbps (512 kbps or 1 Mbps for ESS-II). 512 kbps data rates (1 Mbps for ESS-II) are possible with strong RF signal levels, typically stronger than –77 dBm RSSI including a 15 dB fade margin.

When the data rate is set to **AUTO**, the remote radio is able to change speeds based on the signal quality criteria set in the Auto Data Rate submenu described later in this section (see [Page 55](#)).
[256, 512, AUTO; AUTO]

- **Compression** (*AP Only*)—Enabling this option uses LZO compression algorithm for over-the-air data. Varying levels of data reduction are achieved depending on the nature of the information. Text files are typically the most compressible, whereas binary files are the least compressible. On average, a 30% increase in throughput can be achieved with compression enabled.

- **Dwell Time**—Duration (in milliseconds) of one hop on a particular frequency in the hopping pattern. (This field is only changeable on an Access Point. Remotes get their value from AP upon association.)

[ESS: 16.4, 32.8, 65.5, 131.1, 262.1; 32.8]

[ESS-II: 8.2, 16.4, 32.8, 65.5, 131.1; 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 (in msec).

Available Intervals: **Normal** (104 ms), **Fast** (52 ms), **Faster** (26 ms), **Slow** (508 ms), **Moderate** (208 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). [**Normal, Fast, Faster, Slow, Moderate; 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 beacon period is usually only a benefit when there are mobile Remotes in the network.

- **Hop Pattern Seed**—A user-selectable value to be added to the hop pattern formula. This is done in the unlikely event that identical hop patterns are used with two collocated or nearby networks. Changing the seed value will minimize the potential for RF-signal collisions in these situations. (This field is only changeable on an Access Point. Remotes read the AP's value upon association.) [0 to 255; 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. Only even numbers are acceptable entries for this parameter. Over-the-air data fragmentation is not supported on AP units. (See “[Network Performance Notes](#)” on Page 96 for additional information.) [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 96.) [0 to 1600 bytes; 500]

NOTE: While the transceiver accepts RTS Threshold values below 100, the lowest value that works is 100.

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 wait for the specified amount of time before transmitting.

- **RSSI Threshold (for alarm)**—Level (dBm) below which the received signal strength is deemed to have degraded, and a critical event (alarm) is generated and logged. Under these conditions, the PWR lamp flashes, and a trap is sent to the trap manager if SNMP is enabled and set properly. [0 to -120; -90]
- **SNR Threshold (for alarm)**—Value (dB) below which the signal-to-noise ratio is deemed to have degraded and a critical event is generated and logged. Under these conditions, the PWR lamp flashes, and a trap is sent to the trap manager if SNMP is enabled and set properly. [0 to 40; Not Programmed]
- **RF Hopping Format**—Operation must be compliant with country-specific restrictions for the frequency band used. This option must be specified when the order is placed and cannot be modified in the field by the user. The available formats are:
 - **ISM:** 902–928 MHz band
 - **GSM:** 915–928 MHz band
 - **SPLIT:** 902-907.5 and 915-928 MHz bands
 - **CHANNELS:** 902–928 MHz, selectable hopping, from 1 to 80 channels. This selection is available only on ESS-II or specially provisioned ESS units.

NOTE: When using **CHANNELS** mode, all radios (AP and Remotes) must be set to use the same channels in order to establish a link. If this is not done, the radios will not connect.

NOTE: ESS-II operates only in the **CHANNELS** mode, with selectable hopping from 1 to 75 channels.

- **Channel Config**—Brings up a submenu ([Figure 3-20](#)) that displays.

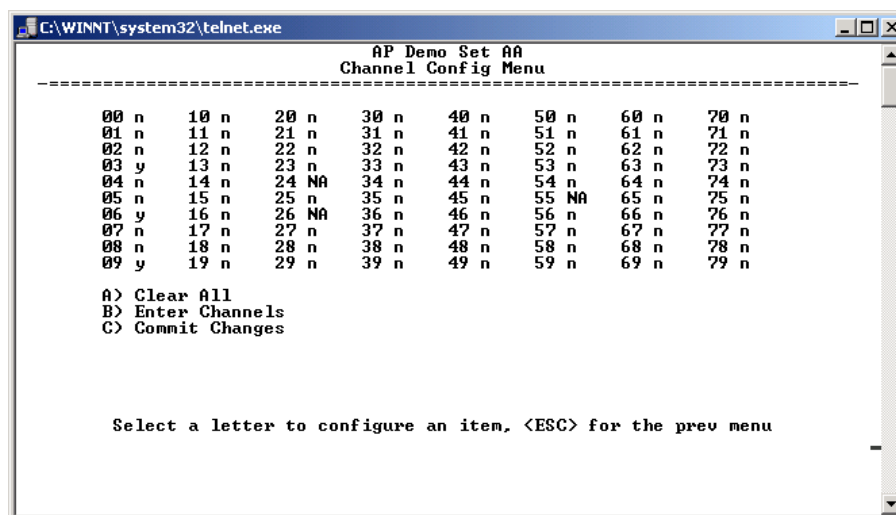


Figure 3-20. Channel Config Submenu
(In the default configuration, all channels are disabled)

Key to channel indicators:

n (no) = Radio channel is not used

y (yes) = Radio channel is used

NA (not available) = Radio channel is not available

- **Clear All**—This command clears all entries in the Channel Config Menu, resetting the available channels to “no usage.” Channels that are not available for use will appear with a notation of or **NA**. These channels are not available because of pre-existing conditions, and are not user-configurable.
- **Enter Channels**—This allows selection of the channels used for frequency hopping operation. *The selection of particular channels will result in an indication of y. Be aware that these channels do not become active until the **Commit Changes** selection is invoked.*
- **Commit Changes**—This re-boots the radio and loads the active channels into the frequency list for frequency hopping operation.

Radio Configuration Menu descriptions, continued...

- **Auto Data Rate Configuration**—This selection brings up a submenu as shown in [Figure 3-21](#). For the settings in this submenu to have any effect, the Data Rate menu item (Page 52) must be set to **AUTO**.

The Auto Data Rate Configuration submenu is typically for use in environments where signal quality is variable, and you wish to maintain the highest possible over-the-air data rate as conditions change.

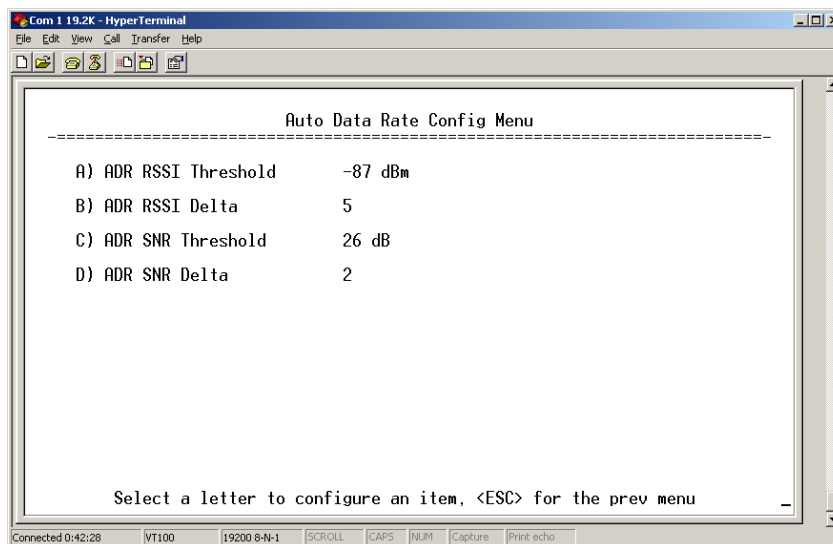


Figure 3-21. Auto Data Rate Submenu

NOTE: In the description below, “high speed” refers to 512 kbps for the ESS radio and 1 Mbps for the ESS-II radio.

“Standard speed” refers to 256 kbps for the ESS radio and 512 kbps for the ESS-II.

The Auto Data Rate Configuration submenu consists of two threshold settings, each accompanied by a “delta” (amount of change) setting. Using the example of [Figure 3-21](#), assume the current RSSI is -87 dBm. An RSSI reduction of more than 5 dBm (more negative RSSI number) would cause a data rate change from high speed to standard speed. Once the data speed has changed to standard speed, an RSSI *increase* to the level of -82 dBm would be required for the radio to switch back to high speed. This provides an operational “window” or hysteresis range over which the data speed stays constant despite minor changes in signal strength.

The SNR (signal-to-noise ratio) threshold and delta operate in the same manner described above, with the exception that the units are expressed in relative dB instead of dBm. In the example of [Figure 3-21](#), a drop of 2 dB from a level of 26 dB would result in a data rate change from high speed to standard speed. For the radio to return to high speed, the SNR would need to increase to 28 dB. (*See Glossary for definition of SNR.*)

RSSI or SNR figures alone mean little when determining signal quality. Both parameters must be considered to get a true understanding of signal quality. For example, a strong, but noisy signal would likely be less

useful than a weak signal with low noise levels. Proper use of the threshold and delta settings will result in smoother, more reliable performance from your wireless link.

Figure 3-21 shows the default values for RSSI and SNR parameters but these may be changed to optimize performance in your environment. In properly designed systems, experience has shown that RSSI levels between -50 dBm and -90 dBm provide reliable operation, provided the signal-to-noise ratio is 17 dB or above. Tailoring the thresholds with these baseline values in mind, can provide improved performance in your system.

The selections on the Auto Data Rate menu are as follows:

- **ADR RSSI Threshold**—A specified received signal strength value, which, if exceeded by the range of the **RSSI Delta** setting, causes a data rate change in the transceiver. [-50 to -100; -87 dBm]
- **ADR RSSI Delta**—A user-specified *difference* from the **RSSI Threshold** figure which, if exceeded, causes a data rate change in the transceiver. [0-10; 5]
- **ADR SNR Threshold**—A user-specified signal-to-noise ratio, which, if exceeded by the range of the **SNR Delta** setting, causes a data rate change in the transceiver. [10-30; 26]
- **ADR SNR Delta**—A user-specified *difference* from the **SNR Threshold** figure which, if exceeded, causes a data rate change in the transceiver. [0-10; 2]

Radio Configuration Menu descriptions, continued...

- **Skip Zones** (*Does not apply to ESS-II. Editable at AP Only.*)—This selection brings up a submenu (Figure 3-22) that displays the current utilization of zones. Each zone consists of eight RF channels. In some instances there may be a part of the spectrum used by another system, that results in “continuous” or “persistent” interference to your system. To alleviate this form of interference, the transceiver may be programmed to “block out” affected portions of the spectrum using the Skip Zones Menu.

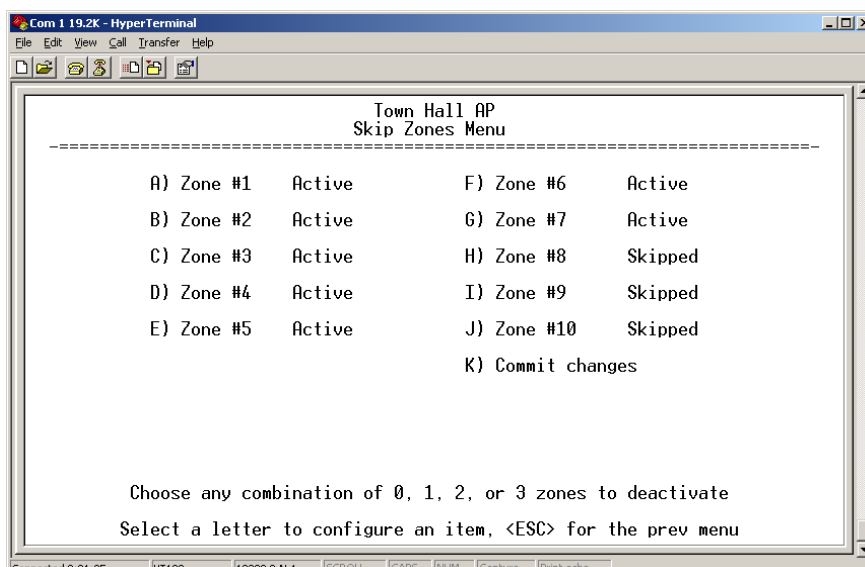


Figure 3-22. Skip Zone Options Submenu
("Commit changes" displayed only on Access Point radios)

Figure 3-22 displays the utilization of 10 zones, each having 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.

3.5.2 Mobile Data Configuration

Because a mobile environment is more demanding than fixed-site operation, additional considerations must be made at the time of configuration. These key points should be considered for all mobile installations:

- Use middleware—The use of middleware in the mobile laptops is highly recommended for better operation of a mobile data system. SIMREX provides middleware from one of the vendors available in the market. Contact your SIMREX representative for details.
- Plan your network coverage—Deploy Access Points so that they provide overlapping coverage to each other. Access Points must use the same network name to enable roaming
- Set the Remote radios to the lower speed (256 kbps for ESS, 512 kbps for ESS-II) to optimize coverage
- Configure the Remote radios for mobile operation—Enable the

mobility function using the Remote radio's Network Configuration Menu (see [Figure 3-23](#)). Although a menu selection appears in the Access Point's Network Configuration menu, this setting cannot be changed. When you enable the Remote radio's Mobility Mode option, the radio scans for an alternate AP if the RSSI is at or below the RSSI threshold defined in the Radio Configuration screen (see [Figure 3-24](#)).

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

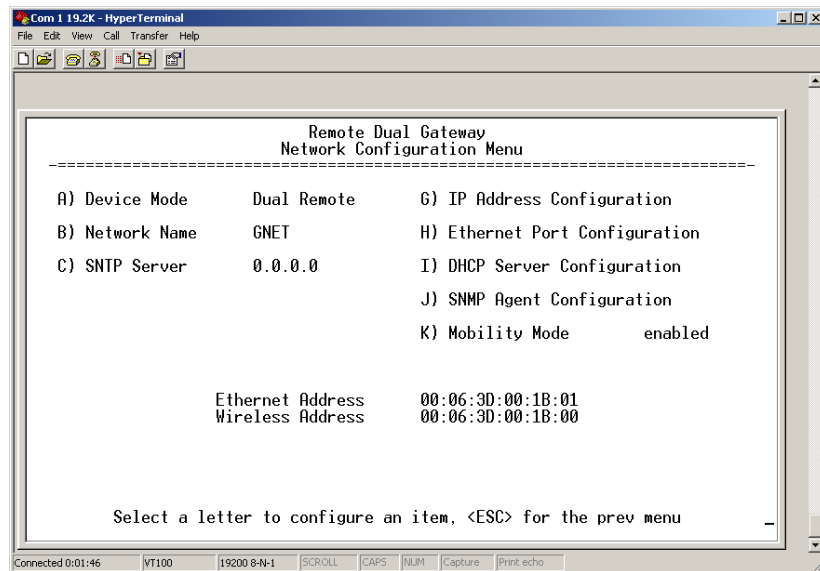


Figure 3-23. Enabling Mobility at Remote Radio

After association is lost with an AP, and scanning for an alternate AP is started, the former AP is placed on a “blacklist” for 10 seconds, to avoid linking back to the same AP. If no alternate AP is found, a link is eventually made to the same AP as before. This is why it is important to design a system with sufficient overlapping coverage by multiple APs.

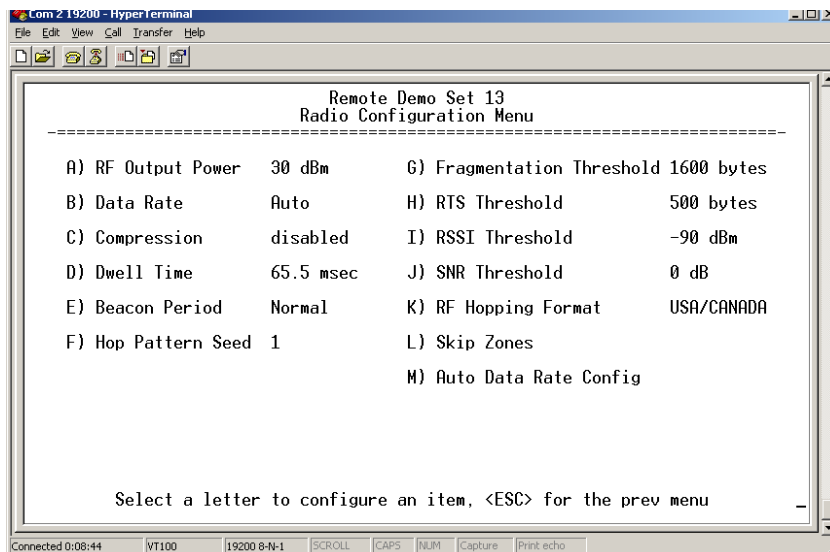


Figure 3-24. Radio Configuration Menu—Remote

Other parameter settings that should be reviewed for Mobility Mode:

- **Compression [AP; disabled]**—Disable radio compression. Data compression is best performed by the middleware running on the mobile laptop PC. Gains in efficiency are made because middleware compresses data at a higher stack level, and it aggregates multiple data frames and streams into a single packet. Compression at the radio level, although highly efficient, works at the individual packet level.
- **Dwell Time [Set to the minimum value]**—This setting controls the amount of time that the unit spends on each frequency between hops. Although overall throughput appears to decrease by this setting the effects of multipath fading are minimized through frequency diversity.
- **Beacon Period [Set to the fastest value]**—This parameter defines the interval at which the Access Point transmits a synchronization beacon to all remotes. A faster setting minimizes resynchronization times when remote radios roam between access points or in highly interrupted coverage areas (dense buildings, for example).
- **Fragmentation Threshold [remote; 256]**—Set to a small value. This parameter defines the size of the message packets transmitted over the wireless media. These fragments are reconstructed into the original packet before delivery to the external device at the remote end of the link. In a mobile environment with rapidly changing conditions, setting this value to a minimum value improves the probability of packets being sent complete on the first try.

- **RTS Threshold [AP; 0 -1600 bytes]**—Enable RTS flow at a small value. This setting is a wireless equivalent to RTS/CTS flow control in a wired communications circuit. This mechanism prevents packet collisions caused by the “Hidden Node” scenario, in which remotes can’t hear each other before transmitting. When this value is set below 100 or above 1500, it is effectively disabled.

3.6 CONFIGURING THE SERIAL INTERFACES

3.6.1 Overview

The transceiver includes an embedded serial device server that provides transparent encapsulation over IP. In this capacity, it acts as a gateway between serial and IP remote devices. Two common scenarios are PC applications using IP to talk to remote devices, and serial PC applications talking to remote serial devices over an IP network.

Essentially the same data services are available for both serial ports: COM1 and COM2. Note that the transceiver’s 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.

Com1 Port—*Dual Purpose Capability*

The COM1 port is used as a local console connection point and to pass serial data with an external device. Setting the COM1 port status to **Enable** prevents access to the Management System (MS) through this port. However, the MS can still be accessed via the LAN port using Telnet or a web browser.

To restore the COM1 port to support Management System services, connect a terminal to the port, select the proper baud rate (19,200 is default), and enter an escape sequence (+++) to reset it to the console mode.

TCP vs. UDP

Both types of IP services are used by the transceiver embedded serial device server—TCP and UDP. TCP provides a connection-oriented link with end-to-end acknowledgment of data, but with some added overhead. UDP provides a connectionless best-effort delivery service with no acknowledgment.

Most polled protocols will be best served by UDP service as the protocol itself has built-in error recovery mechanisms. UDP provides the needed multidrop operation by means of multicast addressing.

On the other hand, TCP services are best suited for applications that do not have a recovery mechanism (error-correction) and must 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 72.](#))

Serial Encapsulation

Transparent encapsulation, or IP tunneling, provides a mechanism to encapsulate serial data into an IP envelope. Basically, all the bytes received through the serial port are put into the data portion of a TCP or UDP packet (TCP or UDP are user configurable options). In the same manner, all data bytes received in a TCP or UDP packet are output through the serial port.

When data is received by the radio through the serial port it is buffered until the packet is received completely. There are two events that signal an end-of-packet to the radio: a period of time since the last byte was received, or a number of bytes that exceed the buffer size. Both of these triggers are user configurable.

One radio can perform serial data encapsulation (IP-to-Serial) and talk to a PC. Two radios (or one radio and a terminal server) can be used together to provide a serial-to-serial channel.

TCP Client vs. TCP Server

On a TCP session there is a server side and a client side. The server is always waiting for requests from clients. The transceiver can be configured to act as either a server or a client.

The client mode attempts to establish a connection to a server (typically running on a PC) whenever it receives data on the serial port.

There is also a Client/Server mode where a connection is established in either the client or server modes. An incoming “keep alive” timer and outgoing counter

UDP Multicast

IP provides a mechanism to do a limited broadcast to a specific group of devices. This is known as “multicast addressing.” Many IP routers, hubs and switches support this functionality.

Multicast addressing requires the use of a specific branch of IP addresses set apart by the Internet Assigned Numbers Authority (IANA) for this purpose.

UDP multicast is generally used to transport polling protocols typically used in SCADA applications where multiple remote devices will receive and process the same poll message.

As part of the Multicast implementation, the radio sends IGMP membership reports and IGMP queries, and responds to membership queries. It defaults to V2 membership reports, but responds to both V1 and V2 queries.

You must configure the multicasted serial port as the target for the multicast data (for example, multipoint-to-multipoint mode, or point-to-multipoint mode where the inbound data is multicast). This restriction is because a host that only sends data to a multicast address (for example, point-to-multipoint mode where the ESS acts as a point) will not join the group to receive multicast data because the host's inbound data is directed unicast data.

The serial-to-serial example which follows shows how to provide multicast services. (See [“Point-to-Multipoint Serial-to-Serial Application Example” on Page 74.](#))

PPP

External devices can connect to the transceiver using PPP (Point-to-Point Protocol). The transceiver works as a server and assigns an IP address to the device that connects through this interface.

To gain access to the transceiver from a PC even if the network is down, a modem may be connected to one of the transceiver's COM ports that has been configured with PPP.

Data Buffering

Data buffering is always active regardless of the selected mode. When Seamless mode is selected, a buffer size of 256 bytes is used. When custom mode is selected, the size options are: 16, 32, 64, 128, and 256 bytes. The Inter-Frame Delay is settable in either Seamless or Custom modes.

Implementing Configuration Changes

There are several configuration parameters for the Serial Gateway found under the *Serial Configuration Menu* of the Management System. After making changes to the configuration, you must use the menu's "Commit Changes" to assert the changes.

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

Serial Configuration Wizard

The Serial Configuration Wizard available through the **Serial Gateway 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.

The wizard can be bypassed by selecting option **B) View Current Settings** and adjusting the individual settings of the appropriate parameter

3.6.2 Serial Data Port Configuration Menu

The first two menu items present the identical parameter fields for each port with one exception—Flow Control. This is available only on COM2.

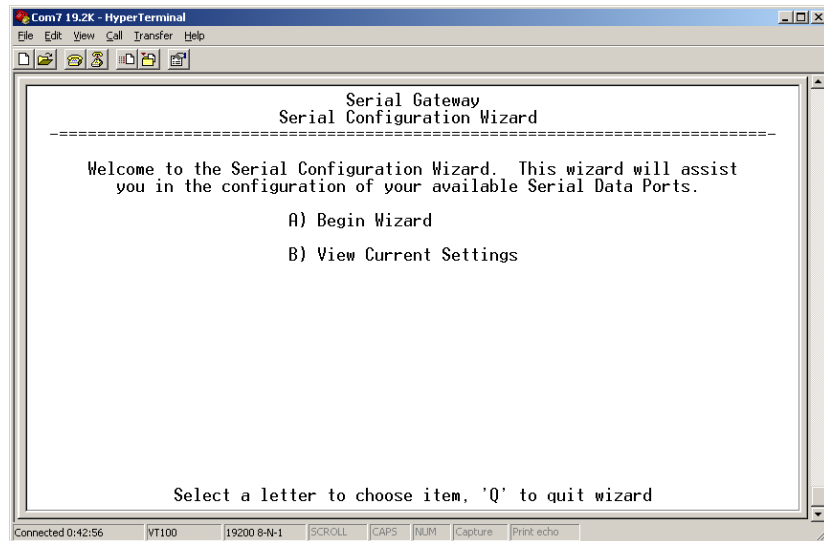


Figure 3-25. Serial Configuration Wizard

- **Begin Wizard**—Tool for configuration of serial ports using a step-by-step process.
- **View Current Settings**—Displays all settable options. Depending on the selected IP protocol.

3.6.3 Configuring for UDP Mode

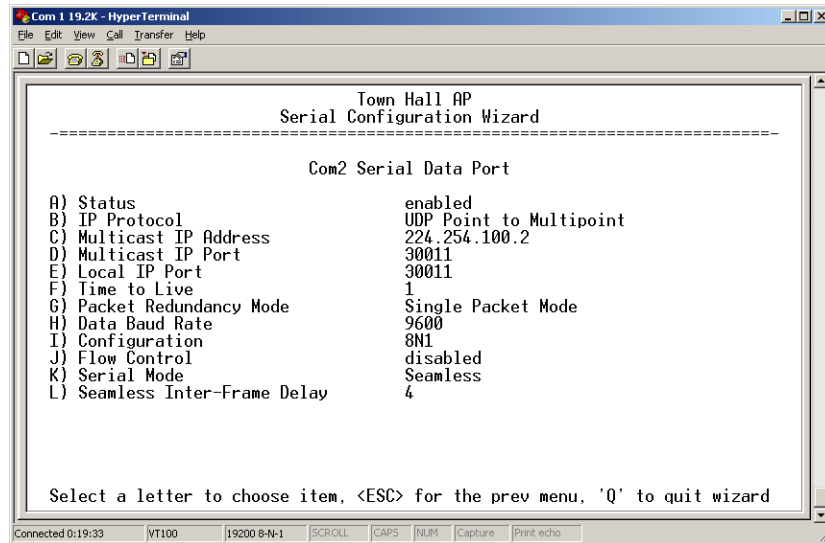


Figure 3-26. UDP Point-to-Multipoint Menu

UDP point-to-multipoint to send a copy of the same packet to multiple destinations, such as in a polling protocol.

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—Point to Multipoint [TCP, UDP PPP; TCP]. This is the type of IP port that will be offered by the transceiver's serial device server.
- **Multicast IP Address** (used instead of **Local IP Address** when using UDP Point-to-Multipoint.)— Must be configured with a valid Class D IP address (224.0.0.0–239.255.255.255). IP packets received with a matching destination address will be processed by this unit [Any legal IP address; 0.0.0.0].
- **Multicast IP Port** (used instead of **Local IP Port** when using UDP Point-to-Multipoint.)—This port number must match the number used by the application connecting to local TCP or UDP socket. [1-64,000; COM1: 30010, COM2: 30011]
- **Local IP 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 or UDP socket. [Any valid IP port; COM1: 30010, COM2: 30011]
- **Time to Live (TTL)**—An IP parameter defining the number of hops that the packet is allowed to traverse. Every router in the path will decrement this counter by one.

- **Packet Redundancy Mode**— For proper operation, all radios' Serial Packet Redundancy mode must match (Single Packet mode vs. Packet Repeat mode). This is because a transceiver, when in Packet Repeat mode, sends 12 extra characters (sequence numbers, etc.) to control the delivery of the repeated data. Misconfigurations can result in undesired operation.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1,200–115,200; 19200]
- **Configuration**—Formatting of data bytes. Data bits, parity and stop bits [7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 8N1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1].
- **Flow Control [Com2 Only]**—RTS/CTS handshaking between the transceiver and the connected device. [Enable, Disable; Disabled]
- **Serial Mode**—When seamless mode is selected 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 permits operation with protocols such as MODBUS™ that do not allow gaps in their data transmission. [Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). UDP packet sizes are delimited and sent out based on the Seamless Inter-Frame Delay only when receiving data through the serial port. MODBUS defines a “3.5-character” parameter. [1–65,535; 4]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

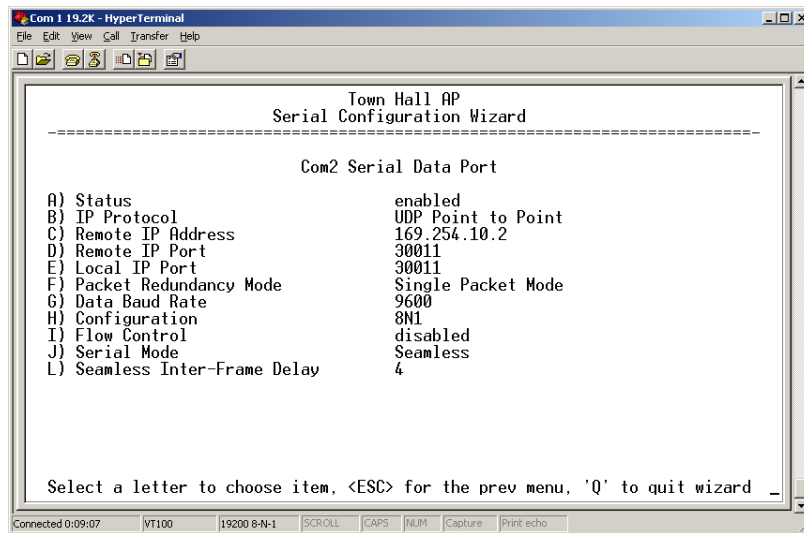


Figure 3-27. UDP Point-to-Point Menu

Use UDP point-to-point configuration to send information to a single device.

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—UDP Point-to-Point. This is the type of IP port that will be offered by the transceiver's serial device server. [TCP, UDP, PPP; TCP]
- **Remote IP Address**—Data received through the serial port is sent to this IP address. To reach multiple Remotes in the network, use UDP Point-to-Multipoint. [Any legal IP address; 0.0.0.0]
- **Remote IP Port**—The destination IP port for data packets received through the serial port on the transceiver. [1–64,000; COM1: 30010, COM2: 30011]
- **Local IP Port**—Port number where data is received and passed through to the serial port. This port number must be used by the application connecting to this transceiver. [1–64,000; COM1: 30010, COM2: 30011]
- **Packet Redundancy Mode**— For proper operation, all radios' Serial Packet Redundancy mode must match (Single Packet mode vs. Packet Repeat mode). This is because a transceiver, when in Packet Repeat mode, sends 12 extra characters (sequence numbers, etc.) to control the delivery of the repeated data. Misconfigurations can result in undesired operation.
- **Data Baud Rate**—Data rate (payload) for the COM port in bits-per-second. [1,200–115,200; 19200]
- **Configuration**—Formatting of data bytes. Data bits, parity and stop bits [7N1, 7E1, 7O1, 8N1, 8E1, 8O1, 8N1, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1].

- **Flow Control (COM2 only)**—RTS/CTS handshaking between the transceiver and the connected device.
[Enable, Disable; Disabled]
- **Serial Mode**— When seamless mode is selected, 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 MOD-BUS™ that do not allow gaps in their data transmission.
[Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MOD-BUS defines a “3.5-character” parameter. [1–65,535; 4]
- **Custom Data Buffer Size (Custom Packet Mode only)**—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port.
[16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

3.6.4 Configuring for TCP Mode

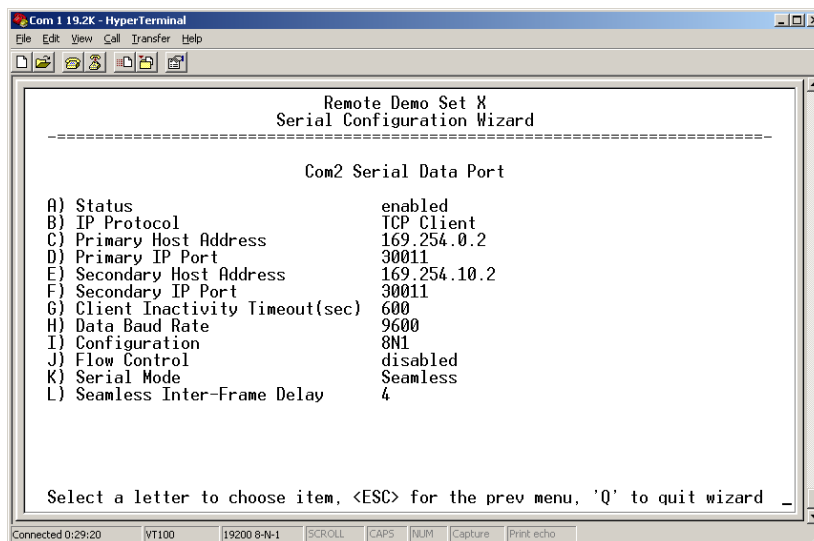


Figure 3-28. TCP Client Menu (Remote)

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—TCP Client. This is the type of IP port that will be offered by the transceiver’s serial device server. [TCP, UDP, PPP; TCP]
- **Primary Host Address**—The IP address to be used as a destination for data received through the serial port.
[Any legal IP address; 0.0.0.0]

- **Primary IP Port**—The destination IP port for data packets received through the serial port on the transceiver.
[Any valid IP port; COM1: 30010, COM2: 30011]
- **Secondary Host Address**—The IP address to be used as a destination for data received through the serial port in case the primary host address is not available.
[Any legal IP address; 0.0.0.0]
- **Secondary IP Port**—The destination IP port for data packets received through the serial port on the transceiver used along with the secondary host address above.
[Any valid IP port; COM1: 30010, COM2: 30011]
- **Outgoing Connection's Inactivity Timeout**—Amount of time (in seconds) that they transceiver will wait for data before terminating the TCP session. [0–600; 600]
- **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, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1].
- **Flow Control [Com2 Only]**—RTS/CTS handshaking between the transceiver and the connected device.
[Enable, Disable; Disabled]
- **Serial 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™ and some variants which do not allow gaps in their data transmission.
[Seamless, Custom; Seamless]
- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a “3.5-character” parameter.
[1–65,535; 4]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port.
[16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

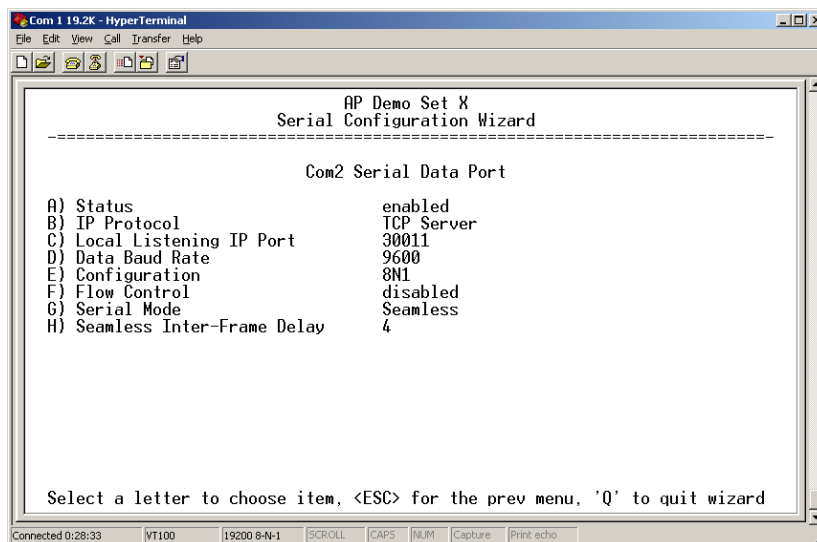


Figure 3-29. TCP Server Menu (AP)

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—TCP Server. This is the type of IP port that will be offered by the transceiver's serial device server.
[TCP, UDP, PPP; TCP]
- **Local Listening IP 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 or UDP socket.
[Any valid IP port; COM1: 30010, COM2: 30011]
- **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, 7N2, 7E2, 7O2, 8N2, 8E2, 8O2; 8N1].
- **Flow Control** (COM2 only)—RTS/CTS handshaking between the transceiver and the connected device.
[Enable, Disable; Disabled]
- **Serial 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™ and some variants which do not allow gaps in their data transmission.
[Seamless, Custom; Seamless]

- **Seamless Inter-Frame Delay**— Number of characters that represent the end of a message (inter-character time-out). MOD-BUS defines a “3.5-character” parameter. [1-65,535; 4]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [16, 32, 64, 128, 256; 32]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

3.6.5 Configuring for PPP Mode

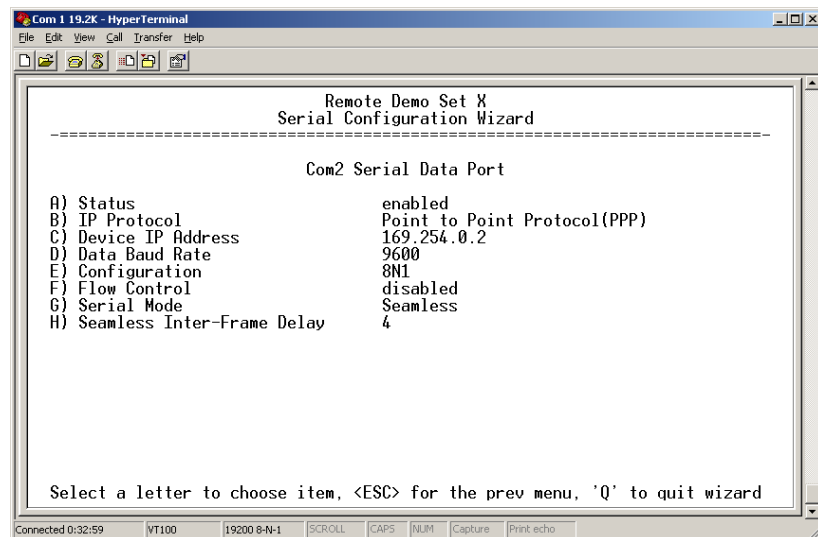


Figure 3-30. PPP Menu

- **Status**—Enable/Disable the serial data port.
- **IP Protocol**—PPP. This is the type of IP port that will be offered by the transceiver’s serial device server. [TCP, UDP, PPP; TCP]
- **Device IP Address**—IP address that will be assigned to the dialing device once the connection is established. [0.0.0.0]
- **Data Baud**—The baud rate of the serial port of the transceiver to which the external device is connected. [1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200; 19200]
- **Configuration**—Byte format of the serial port [7N1, 7E1, 7O1, 7N2, 7E2, 7O2, 8N1, 8O1, 8N2, 8E2, 8O2; 8N1]
- **Flow Control (COM2 only)**—RTS/CTS handshaking between the transceiver and the connected device. [Enable, Disable; Disabled]
- **Serial Mode**—When seamless mode is selected, 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 buffer-

ing 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. [**Seamless, Custom; Seamless**]

- **Seamless Inter-Frame Delay**—Number of characters that represent the end of a message (inter-character time-out). MODBUS defines a “3.5-character” parameter. [**1–65,535; 4**]
- **Custom Data Buffer Size** (Custom Packet Mode only)—Maximum amount of characters, that the Remote end will buffer locally before starting to transmit data through the serial port. [**16, 32, 64, 128, 256; 32**]
- **Commit Changes and Exit Wizard**—Save and execute changes made on this screen (Shown only after changes have been entered.)

A PPP session shows the following possible states:

- **Sending LCP Requests**—The PPP server is querying for any clients that need to connect.
- **Link Established**—A successful PPP connection has been negotiated and an IP address is assigned.
- **Port not Enabled**—The serial port is disabled.

3.6.6 IP-to-Serial Application Example

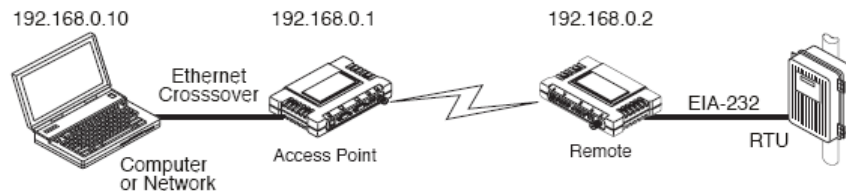
You have a choice to use UDP or TCP to establish communications. This will depend on the type of device you are communicating with at the other end of the IP network. In this example we will use TCP to illustrate its use.

In TCP mode, the transceiver remains in a passive mode offering a socket for connection. Once a request is received, data received at the serial port will be sent out through the IP socket and vice versa, until the connection is closed, or the link is interrupted. In this mode, the transceiver behaves the same, whether it is an Access Point or a Remote. (See [Figure 3-31](#) and [Table 3-1](#))

NOTE: The TCP session has a timeout of 10 minutes (600 seconds). If inactive for that time, it will be closed. The transceiver will offer the port again for connection after this time expires.

Establishing a Connection

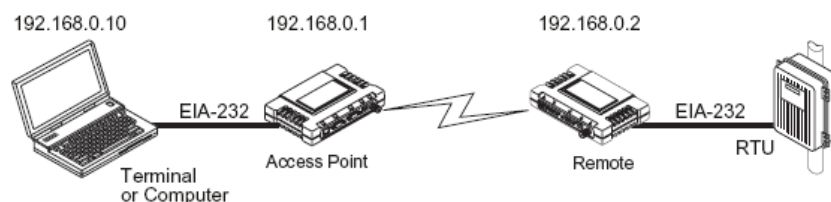
From the PC, establish a TCP connection to the IP address of the Remote transceiver and to the IP port as configured above (30010—COM1, 30011—COM2). A Telnet client application can be used to establish this connection. Data can now be sent between the PC and the RTU or other connected device.

**Figure 3-31. IP-to-Serial Application Diagram****Table 3-1. Serial Port Application Configuration**
IP-to-Serial Connection

Transceiver 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
	Local IP Port	30011

3.6.7 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 3-32. Point-to-Point Serial-to-Serial Application Diagram****Table 3-2. Serial Port Application Configuration**

Transceiver Location	Menu Item	Setting
Access Point (COM2) ¹	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	Hardware (Example)
	Serial Mode	Seamless

Table 3-2. Serial Port Application Configuration (Continued)

Transceiver Location	Menu Item	Setting
Remote Unit (COM2) ¹	SIFD	4
	IP Protocol	UDP
	Remote IP Address	192.168.0.2 (IP address of the Remote radio)
	Remote IP Port	30011
	Local IP Port	30011
	Status	Enabled
	Data Baud Rate	9,600 (Example)
	Flow Control	X-ON/X-OFF (Example)
	Serial Mode	Seamless
	SIFD	4 (Characters)
	IP Protocol	UDP
	Remote IP Address	192.168.0.1 (IP address of the AP)
	Remote IP Port	30011
	Local IP Port	30011

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.

3.6.8 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 (see [Figure 3-33](#), [Table 3-3](#), [Figure 3-34](#), and [Figure 3-35 on Page 76](#)).

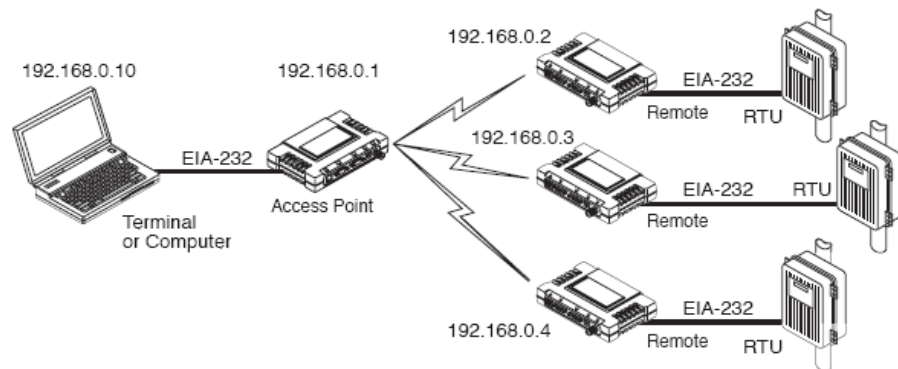


Figure 3-33. Point-to-Multipoint Serial-to-Serial Application Diagram

Table 3-3. Serial Port Application Configuration

Transceiver Location	Menu Item	Setting
Access Point (COM2) ¹	Status	Enabled
	Baud Rate	9600 (Example)
	Serial Mode	Custom
	Flow Control	Disabled
	IP Protocol	UDP
	Remote IP Address	224.254.1.1— Multicast Address ²
	Remote IP Port	30011
	Local IP Port	30011
Remote Units (COM2) ¹	Enable	Enabled
	Baud Rate	2,400 (Example)
	Serial Mode	Custom
	Flow Control	Hardware (Example)
	IP Protocol	UDP
	Remote IP Address	192.168.0.1
	Remote IP Port	30011
	Local IP Port	30011
	Local Multicast 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 (224.0.0.0–239.255.255.255) will work.

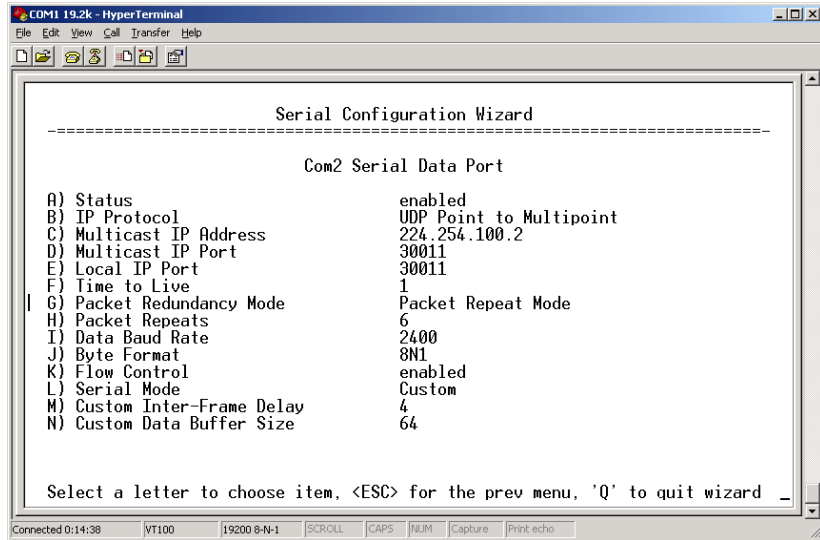


Figure 3-34. Access Point Serial Port Configuration

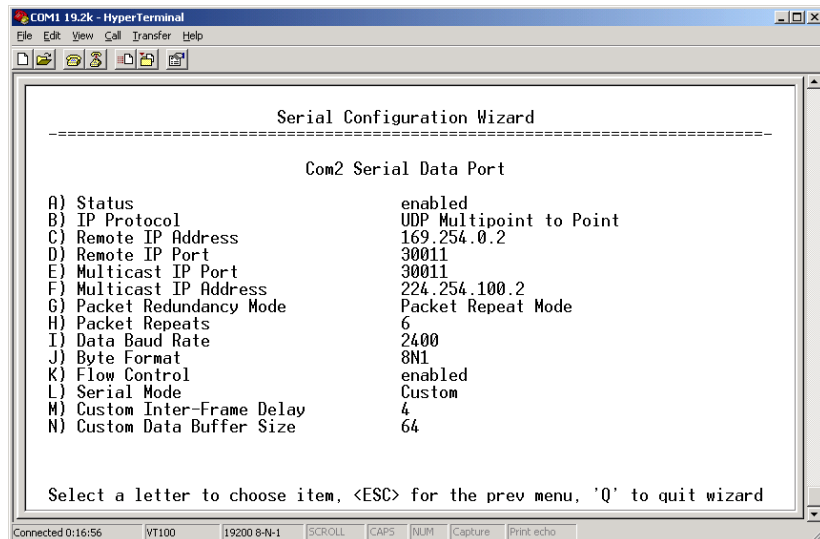


Figure 3-35. Remote Radio Serial Port Configuration

3.6.9 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 3-36 on Page 77](#) and [Table 3-4 on Page 77](#)).

Operation and Data Flow

- Communicate with RTU A by Telnetting to Remote 1, port 30011.
- Communicate with RTU B by Telnetting 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.

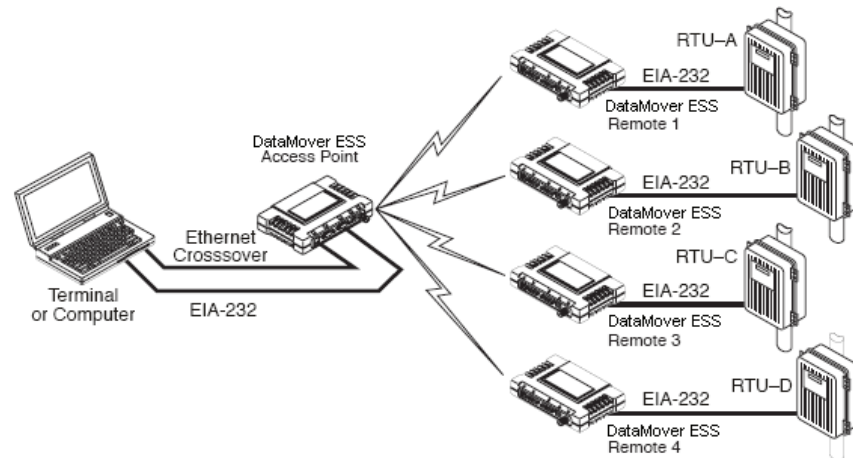


Figure 3-36. Mixed-Modes Application Diagram

Table 3-4. Serial Port Application Configuration

Transceiver 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 AP

Table 3-4. Serial Port Application Configuration (Continued)

Transceiver Location	Menu Item	Setting
	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)

3.7 CYBER SECURITY CONFIGURATION

The cyber security features of the transceiver are grouped into three general areas: controlling access to the radio itself for configuration and management purpose (Device Security), controlling how and when radios communicate with each other, as well as how data traffic is handled (Wireless Security) and a special section dealing with authentication and authorization using a central server (RADIUS Configuration). [Figure 3-37](#) shows the Security Configuration Menu, which is the entry point for these categories.

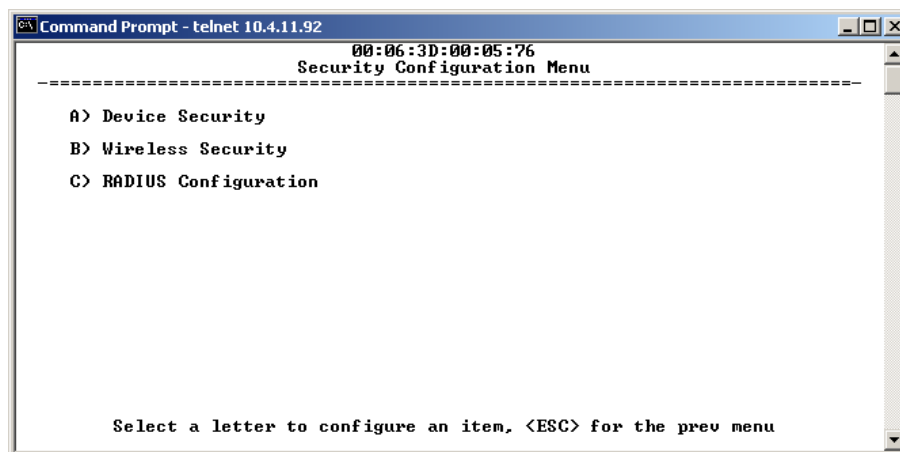


Figure 3-37. Security Configuration Menu
(Access Point Version Shown)

3.7.1 Device Security

This group of features controls how the radios can be accessed either locally or remotely for configuration and management.

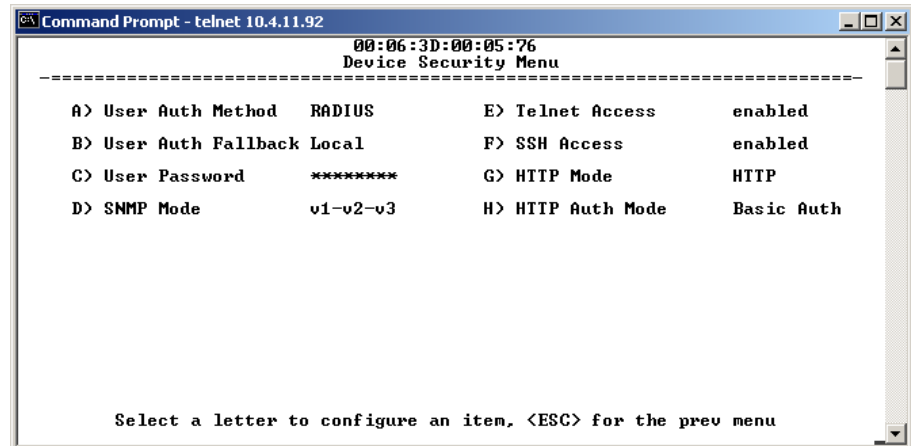


Figure 3-38. Device Security Menu

- **User Auth Method**— Defines whether username and password is verified locally or via a central server. [**Local**, **RADIUS**; **Local**]
- **User Auth Fallback**— Defines the alternate authentication mode in case the authentication server is not available. [**Local**, **None**; **Local**]
- **User Password**—Local password for this unit. Used at log-in via COM1 Port, Telnet, SSH and Web browser. [**Up to 8 alphanumeric characters without spaces (case-sensitive)**; **admin**]

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

- **SNMP Mode**—This specifies the mode of operation of the radio's SNMP Agent. If the mode is disabled, the Agent does not respond to any SNMP traffic. If the mode is v1_only, v2_only, or v3_only, the Agent responds only to that version of SNMP traffic. If the mode is v1-v2, or v1-v2-v3, the Agent responds to the specified version of SNMP traffic. [**disabled**, **v1_only**, **v2_only**, **v3_only**, **v1-v2**, **v1-v2-v3**; **v1-v2-v3**]
- **Telnet Access**—Controls remote access through Telnet sessions on Port 23 [**Enabled**, **Disabled**; **Enabled**]
- **SSH Access**— Controls remote access through SSH (Secure Shell) sessions on Port 22 [**Enabled**, **Disabled**; **Enabled**]
- **HTTP Mode**— Controls remote access through HTTP sessions on Ports 80 and 443. Selecting **HTTPS** forces secure connections to Port 443. When **HTTP Mode** is disabled, access through HTTP or HTTPS is not allowed. [**Disabled**, **HTTP**, **HTTPS**; **HTTP**]

- **HTTP Auth Mode**—Selects the method of HTTP log-in authentication. This parameter functions only when **HTTP** is selected in the previous menu item. Although the **Basic Auth** mode requests a password, the actual password text is transmitted in the clear (unencrypted). [**Basic Auth**, **MD5 Digest**; **Basic Auth**]

3.7.2 Wireless Security

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

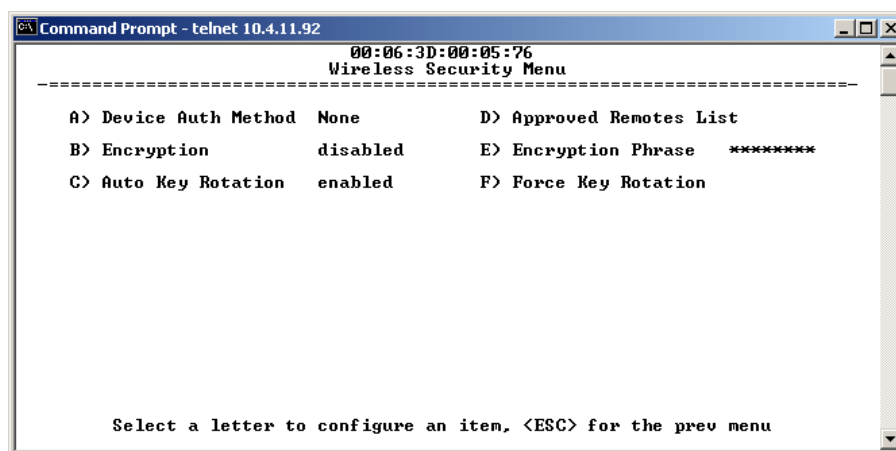


Figure 3-39. Wireless Security Menu

- **Device Auth Method**—Controls whether device authentication is executed locally, via a central server, or not at all. Selecting **Local** uses the Approved Remotes List described later in this manual. [**None**, **Local**, **RADIUS**; **None**]
- **Encryption**—When enabled, it forces the transceiver to use AES-128 encryption (RC4-128 on ESS) on all over-the-air messages. This option requires the Encryption Phrase to be previously configured. Both the AP and the Remote radios must use the same encryption phrase. (Some units may not be authorized to use encryption. “[See “Authorization Keys Menu” on Page 115](#)” for additional details.) [**Enabled**, **Disabled**; **Disabled**]
- **Auto Key Rotation**—When enabled, it 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. [**Enabled**, **Disabled**; **Disabled**]
- **Approved Access Points/Remotes List**—Displays a menu to manage the list of other radios with which this unit will be permitted to communicate.

- **Encryption Phrase**—Phrase (text & numbers) that will be used by the encryption algorithm.
[8 to 29 alphanumeric characters; Blank]
- **Force Key Rotation**— It triggers an immediate key rotation of the encryption keys before the internal counters do it automatically.

Local Authentication—Approved Remotes/Access Points List Submenu

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

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

NOTE: The limit for Remotes (in an Access Point radio) is 255. The limit for Access Points (in a Remote radio) is 104.

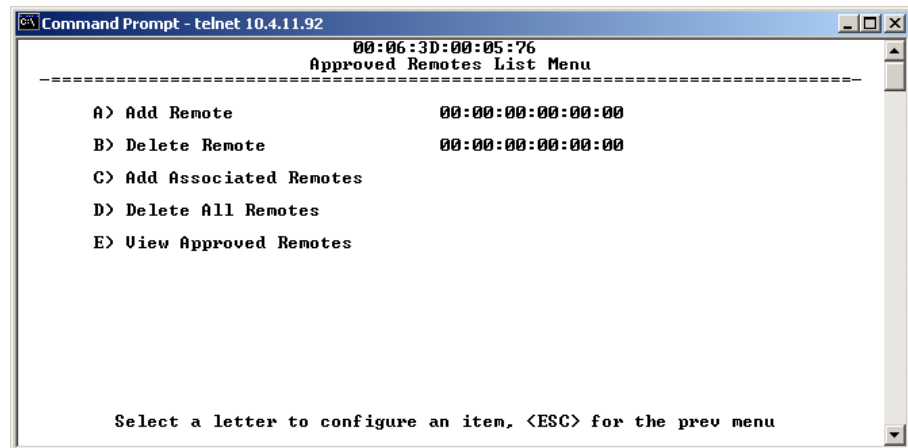


Figure 3-40. Approved Remotes List Menu

- **Add Remote**—Enter MAC address of Remote.
[Any valid 6-digit hexadecimal 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 from this list.
- **Add Associated Remotes**—Add all currently associated remotes 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**—Saves all changes made during the session with this menu. Changes are implemented only if they are “saved” before exiting this menu.

3.7.3 RADIUS Authentication

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

Operation of Device Authentication

Device authentication forces the radio to authenticate before allowing user traffic to traverse the wireless network. When Device Security is configured to use RADIUS as the Authentication Method, Remote radios need three types of certificates: public (client), private, and root (Certificate Authority). These files are unique to each Remote radio and need to first be created at the server and then installed into each unit via TFTP. The certificate files must be in DER format.

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

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

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

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

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

Operation of User Authentication

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

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

3.7.4 RADIUS Configuration

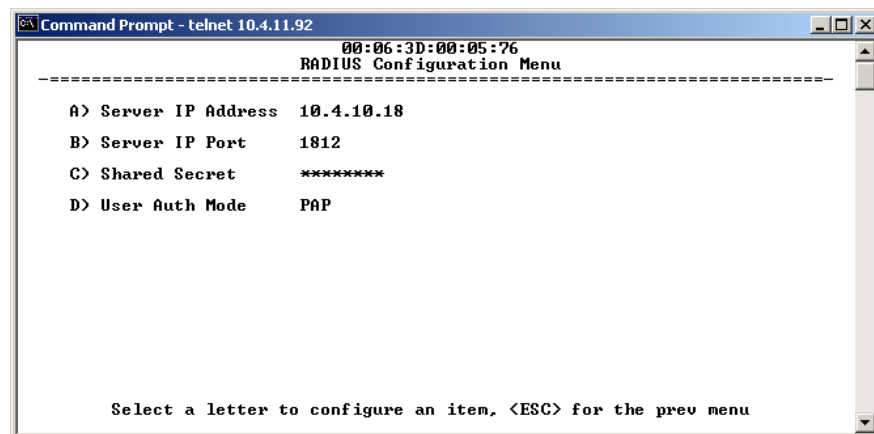


Figure 3-41. RADIUS Configuration Menu

- **Server IP Address**—Used to set/display address of the Server where the RADIUS application resides.
- **Server IP port**—1812 is the standard port for authentication (RFC 2865, June 2000) and should not be changed unless instructed to do so by an administrator.
- **Shared Secret**—User authentication and Device authentication require a common shared secret to complete a RADIUS transaction. This entry must match the string used to configure the appropriate files on the RADIUS Server.
- **User Auth Mode**—Should be set to PAP or CHAP depending on the configuration of the server.

NOTE: CHAP is the more secure mode when compared to PAP. PAP may display the login password in log files at the RADIUS Server. CHAP will encrypt the login password.

NOTE: The security password may not exceed 40 characters in length.

3.7.5 Certificate Management *(Remote transceivers only)*

Use Certificate generation software to generate certificate files and then install these files into each Remote unit via TFTP. The certificate files must be in DER format. The Common Name (CN) field in the public certificate file must match the serial number of the unit it will be installed in.

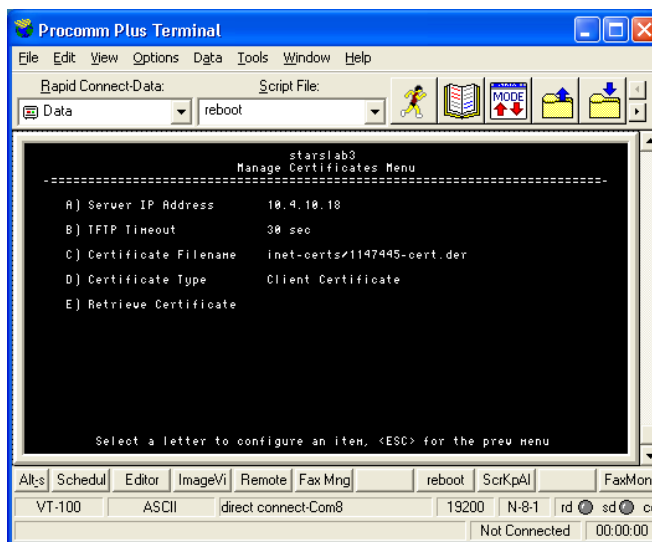


Figure 3-42. Manage Certificates Menu

(NOTE: The appearance of this screen differs from the others because a different terminal program was used; Menu content is the same regardless of program.)

- **Server IP Address**—the IP address of the Server where the RADIUS application resides.
- **TFTP Timeout** should be set appropriately according to the layout of the network.

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

- **Certificate Filename**—Used to specify the filename of the certificate file residing on the TFTP server.
- **Certificate Type**—Selects one of the three file types mentioned above. [Root Certificate, Client Certificate, Private Key Certificate; Root Certificate]
- **Retrieve Certificate**—Initiates the retrieval of the certificate file from the storage location. A successful installation issues a **Complete** status message.

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

3.8 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.

3.8.1 Performance Information Menu

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

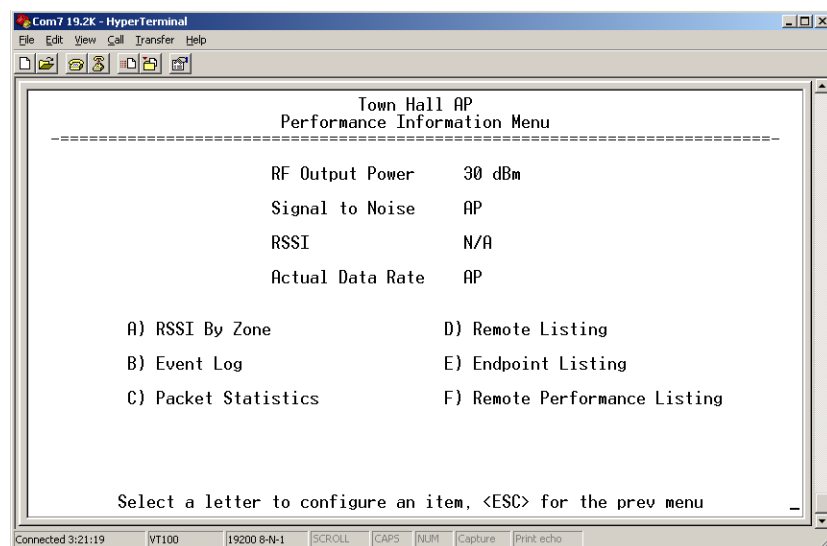


Figure 3-43. Performance Information Menu
(AP Version Shown)

- **RF Output Power** (*Display only*)—Measured power output.
(See [“How Much Output Power Can be Used?”](#) on Page 144)
- **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** (*Display only*)—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 86)

- **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. \(See “Authorization Keys Menu” on Page 115\)”](#) on Page 101)
- **Packet Statistics**—Multiple radio and network operating statistics. (See [“Packet Statistics Menu”](#) on Page 90)
- **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 92)
- **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 93)
- **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 94)
- **Remote Performance Listing** *(AP Display only)*—(See [“Remote Performance Listing Menu \(Access Points Only\)”](#) on Page 95)

RSSI by Zone Menu *(Remotes Only)*

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

Network integrity depends in large part 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 90 and record the values. Then, set the questionable zone to “Skipped” in the Radio Configuration Menu (Page 51) 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 Management System.

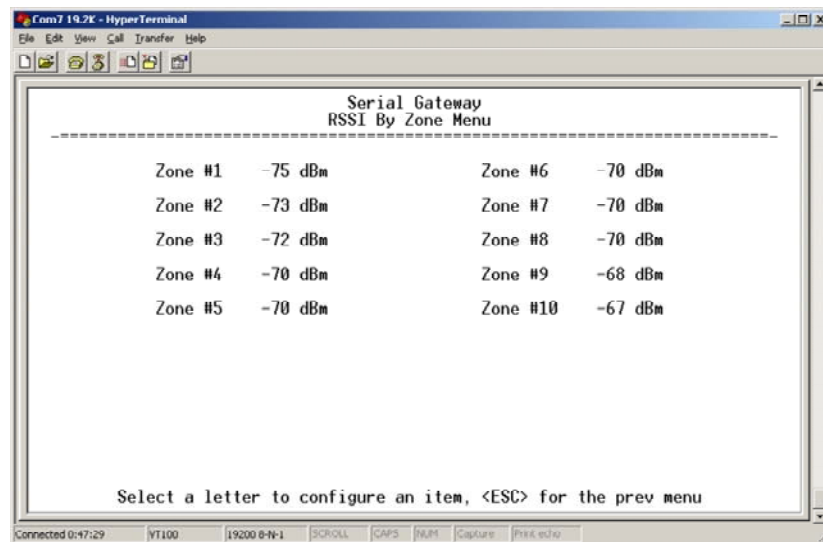


Figure 3-44. RSSI by Zone Menu

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 96](#) 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 3-5](#). 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 PWR LED to blink until the condition is corrected. All events are stored in the Event Log that can hold up to 8,000 entries.

Table 3-5. 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 locally connected device. Remote units obtain this information from the Access Point when they associate with it. The Access Point obtains the time and date from a Time Server. This server can generally be provided by a standard Windows PC server SNTP application. In the absence of the SNTP services, the user must manually enter it at the

Access Point. (See “[Device Information](#)” on Page 40 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.

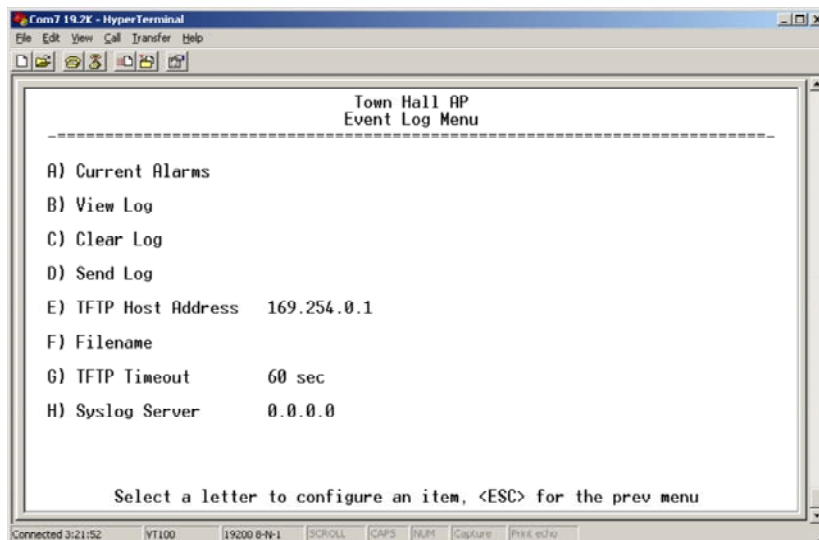


Figure 3-45. Event Log Menu

- **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 127)
- **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. The events are numbered for easier identification and navigation.
- **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 102 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. This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions. [Any valid IP address; 127.0.0.1]

- **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 the filename 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]
- **Syslog Server**—IP address to which alarms are sent using the syslog message format. [Any valid IP address; 0.0.0.0]

View Current Alarms

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

An alarm condition is different from a log event in the sense that an alarm is persistent in nature. That is, an alarm condition remains as an alarm until it has been cleared by correcting the cause (see [Table 4-6 on Page 129](#) for corrective action).

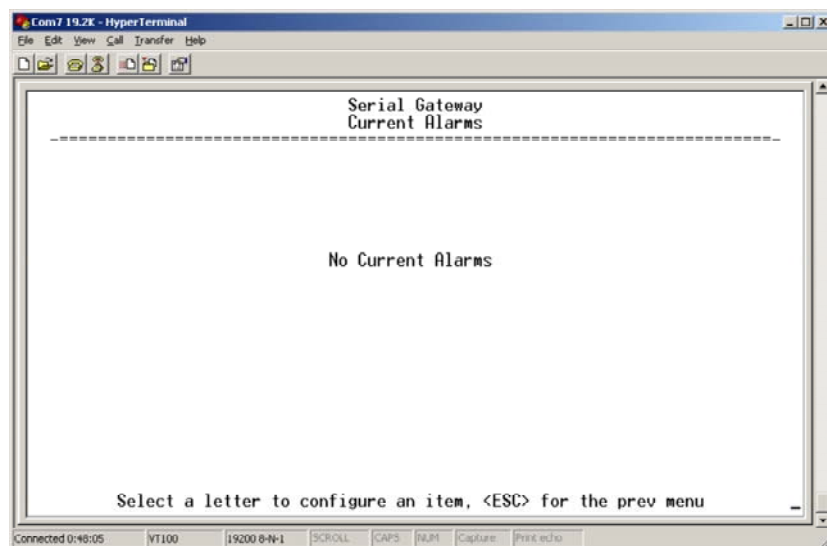


Figure 3-46. Current Alarms Screen

See [Table 4-4 on Page 127](#) for event classifications.

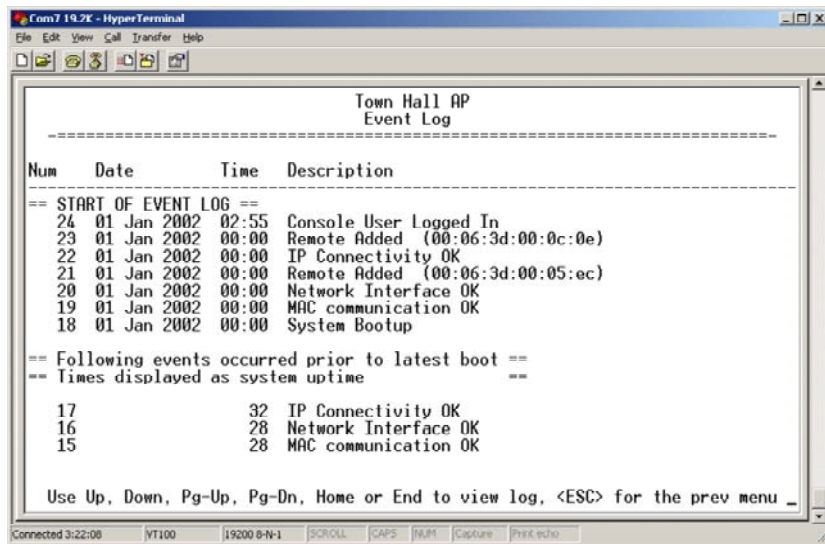


Figure 3-47. Sample Event Log Screen

Packet Statistics Menu

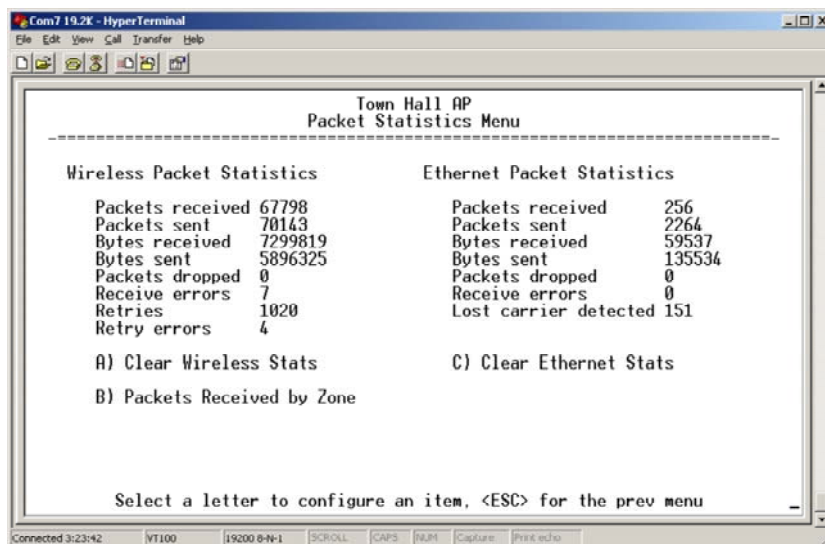


Figure 3-48. Sample Packet Statistics Menu

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**—To-be-transmitted packets dropped as a result of a lack of buffers in the RF outbound queue.
- **Receive errors**—Packets that do not pass CRC. This may be due to transmissions corrupted by RF interference.

Ethernet Packet Statistics

- **Retries**—Number of requests to re-send a data packet before it is acknowledged. If the packet was not acknowledged, this counter is not incremented.
- **Retry errors**—Packets discarded after exceeding seven retries over-the-air.
- **Clear Wireless stats**—Resets the statistics counter.
- **Packets received**—Packets received by the transceiver through the Ethernet port.
- **Packets sent**—Packets transmitted by the transceiver through the Ethernet port.
- **Bytes received**—Data bytes received by this Remote through its LAN port.
- **Bytes sent**—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 collisions in the Ethernet LAN.
- **Lost carrier detected**—A count of the number of packets that the unit attempted to send out the Ethernet port when the carrier signal of the Ethernet was not present. (No carrier present could be due to a loose connection, bad or wrong cable, or equipment failure at the other end of the Ethernet cable.)
- **Clear Ethernet stats**—Resets the statistics counter.

Packets Received by Zone

This screen, shown in [Figure 3-49](#), presents a breakdown of wireless packet statistics by-zone. All zones should report similar numbers. If one or more zones report lower numbers than the others (2% reduction), the specific zone is probably experiencing interference. An improvement can be realized by blocking this zone (see **Main Menu>>Radio Configuration>>Skip Zone Option**).

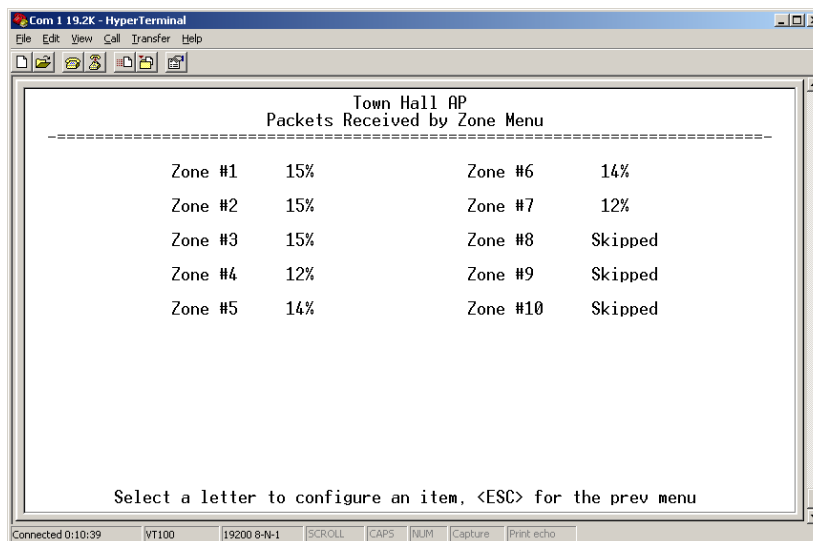


Figure 3-49. Packets Received By Zone Menu

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 3-50. Wireless Network Status Screen](#) on page 92.

The Transceiver's Association Process

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

Under normal circumstances, the association process should be completed within 20 seconds after boot-up. This time can vary depending on the beacon period setting at the AP. See **Beacon Period** description in [Section 3.5.1, Radio Configuration Menu](#) (beginning on Page 51).

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 (Remote only)

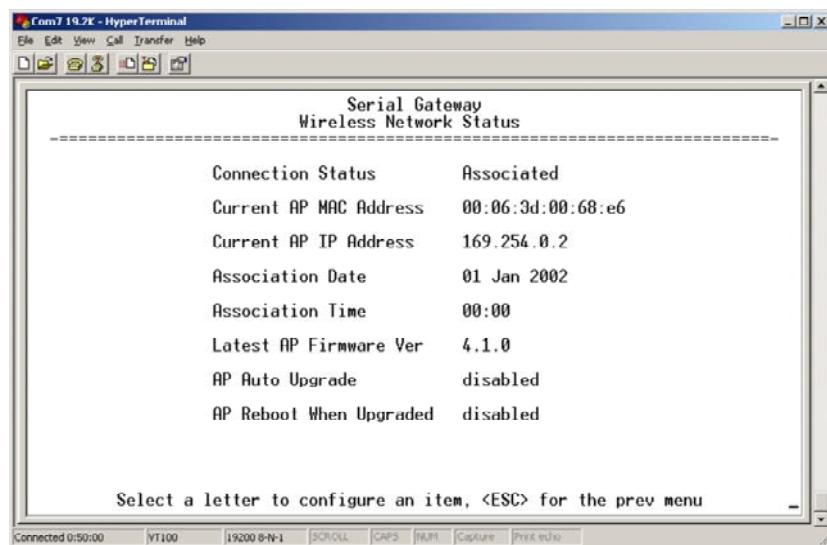


Figure 3-50. Wireless Network Status Screen

- **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.
- *Connected* —The unit has established a radio (RF) connection with the Access Point, but has not obtained cyber-security clearance to pass data.
- *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 Mac Address**—Wireless address of Access Point with which the Remote is associated.
- **Current AP IP Address**—IP 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.
- **Latest AP Firmware Version**—
- **AP Auto Upgrade**—
- **AP Reboot when Upgraded**—

Remote Listing Menu (*Access Points Only*)

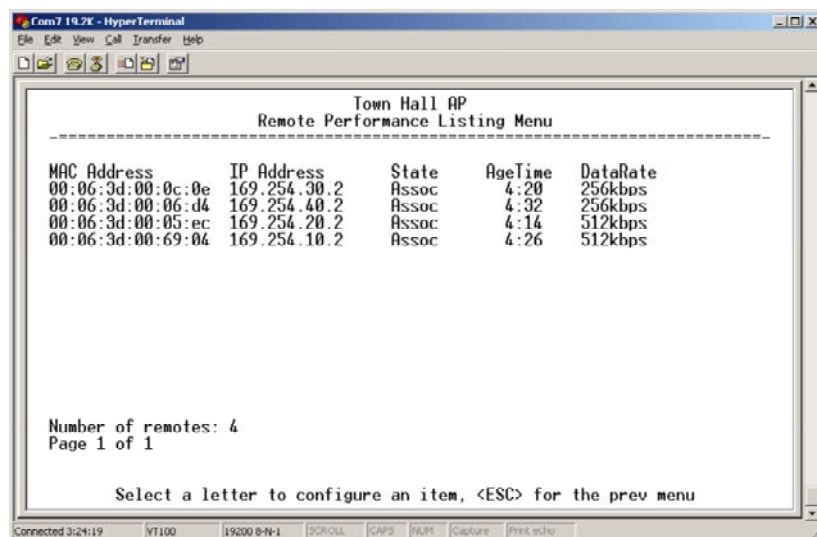


Figure 3-51. Remote Listing Menu
(List of transceivers associated with this AP)

- **MAC Address**—Hardware address of the Remote transceiver.
- **IP Address**—IP Address of the Remote transceiver.

- **State**—Current association state of the Remote transceiver.
- **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 is exchanged with that device, it then “ages out” of the table. When traffic is detected it is included again in the table. This optimizes memory space utilization.

- **DataRate**—Supported data rate by this unit.

Endpoint Listing Menu (Access Points Only)

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

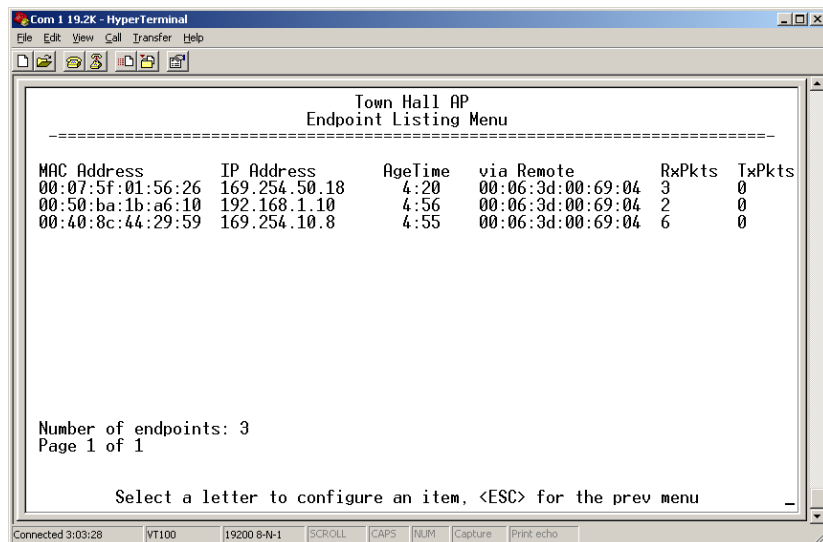


Figure 3-52. Endpoint Listing Menu
(Lists all equipment attached to REMOTE transceivers in the network)

- **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 AP maintains a table with the addresses of the remote radios it communicates with. The age-time countdown is restarted to 5 minutes every time a message to/from that remote is detected. If no traffic is exchanged with that remote, 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 radio 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)

MAC Address	RxRate	RxPkts	TxPkts	RxBCMC	RxViaEP	TxViaEP	RetryErrs
00:06:3d:00:0c:0e	256 kbps	67566	67563	4	0	0	0
00:06:3d:00:06:d4	256 kbps	5	3	3	0	0	0
00:06:3d:00:05:ec	512 kbps	13	10	5	0	0	0
00:06:3d:00:69:04	512 kbps	7	3	5	0	0	0

Number of remotes: 4
Page 1 of 1

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

Figure 3-53. Remote Performance Listing Menu for ESS AP
(ESS-II will show RxRate as 512 kbps or 1024 kbps)

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 radio is currently using. All transceivers 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.

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.

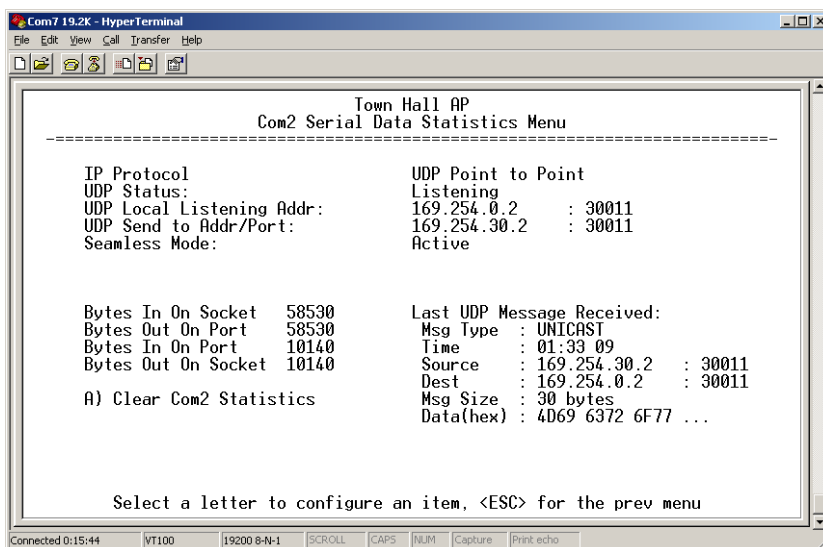


Figure 3-54. Serial Data Statistics Screen
(Both COM1 and COM2 will be shown)

- **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.

3.8.2 Network Performance Notes

Principles of Network Operation

The following is a list of points that are useful for dealing with the networking aspects of the transceiver.

1. The transceiver acts as a bridge.

- If any radio in your 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. As a bridge, the radios transmit this type of frame.
- The radio goes through a listening and learning period at start-up before it will send any packets over either of its ports. This is 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 remotes.
- If the destination address is not known, forward the packet to all remotes.
- If the destination address is known, forward the packet to the port that the destination is known to be on (usually the RF port).
- The bridge code uses Spanning Tree Protocol (STP) to prevent loops from being created when connecting bridges in parallel. For example, connecting two remotes to the same wired LAN could create a loop if STP was not used. Every bridge running STP sends out Bridge Protocol Data Units (BPDUs) at regular intervals so that the spanning tree can be built and maintained. BPDUs are 60-byte multicast Ethernet frames.

2. Distance affects throughput. Because of timers and other components of the protocol, there is a maximum distance limit of 40 miles for reliable operation. After this, although data still flows, the throughput will start to drop and latency will increase, due to additional retries between the radios. Repeater stations may be used to extend this range.
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
- PHY 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 (including 16 PHY bytes)

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 BPDUs 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.

4. Station-to-Station traffic reduces throughput

- 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 and thus are transmitted twice over the same radio system. 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 other hand, 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 other hand, a hidden-node might interfere more often than if RTS was not used.
(Main Menu>>Radio Configuration>>RTS Threshold)

Decreasing the **RTS Threshold**, to the 100 to 200 range, may 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)

5. Activate compression on the Radio Configuration Menu (**Compression enabled**).
6. Use the **Performance Information Menu** to check the packets received by zone. (Remotes Only: Main Menu>>Performance Information>>Packet Statistics>>Packets Received by Zone)

Readings should be close in value. A significantly lower value (2% reduction) probably indicates interference. Performance can be improved by blocking the affected zones at the Access Point. (Main Menu>>Radio Configuration>>Skip Zone Option)

7. Use the **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 31 ms, assuming outbound packets wait for a beacon transmission 50% of the time (26ms) plus the normal packet latency (5 ms).

Data Compression

Enabling this option uses an LZO compression algorithm for over-the-air data. Varying levels of data reduction are achieved depending on the nature of the data. Text files are typically the most compressible, whereas binary files are the least compressible. On average, a 30% increase in throughput can be achieved with compression enabled.

Compression is used on data packets of 100 bytes or more, including Ethernet, IP, and TCP/UDP headers.

Packets-per-Second (PPS)

The ESS radio has a limit of 70 PPS. Consider this restriction when planning your network, especially when smaller packets are expected to make up the majority of the traffic as is the case with VoIP (Voice over IP).

3.9 MAINTENANCE

In the normal course of operating a wireless network, you will want to take advantage of product improvements, and to read and archive the configuration of your individual transceivers using the *Maintenance Menu*. This section provides detail information on how to take advantage of these services.

The maintenance tasks are:

- **Reprogramming**— Managing and selecting the unit's operating system firmware resources. (See [“Reprogramming Menu” on Page 101](#))

- **Configuration Scripts**—Saving and importing data files containing unit operating parameters/settings. (See “[Configuration Scripts Menu](#)” on Page 106)
- **Authorization Key**—Alter the unit’s overall capabilities by enabling the built-in resources. (See “[Authorization Keys Menu](#)” on Page 115)
- **Auto-Upgrade/Remote-Reboot**—Configure when remotes retrieve new firmware versions from the associated AP, and whether or not they reboot to the new firmware after receiving the new firmware. (See “[Auto-Upgrade/Remote-Reboot Menu](#)” on Page 115)
- **Radio Test**—A diagnostic tool for testing RF operation. (See “[Radio Test Menu](#)” on Page 116)
- **Ping Utility**—Diagnostic tool to test network connectivity. (See “[Ping Utility Menu](#)” on Page 118)

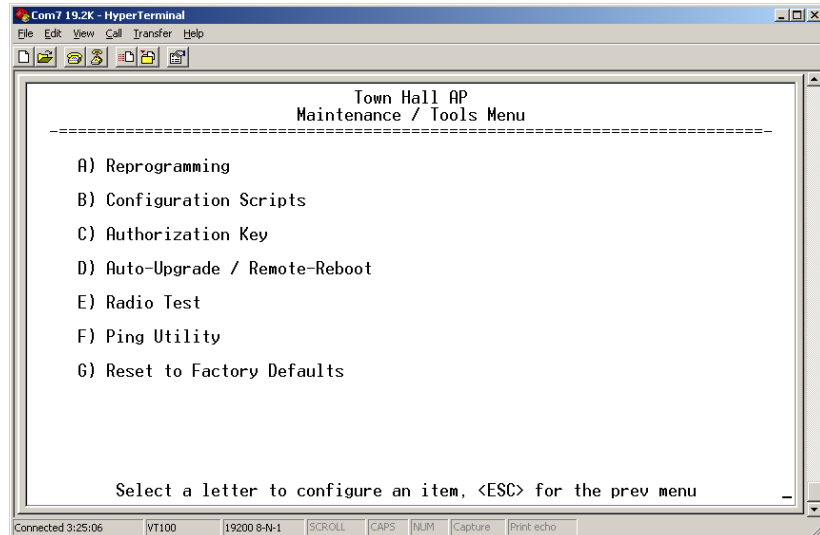


Figure 3-55. Maintenance Menu

3.9.1 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 load new firmware into the inactive position and place it in service whenever you desire.

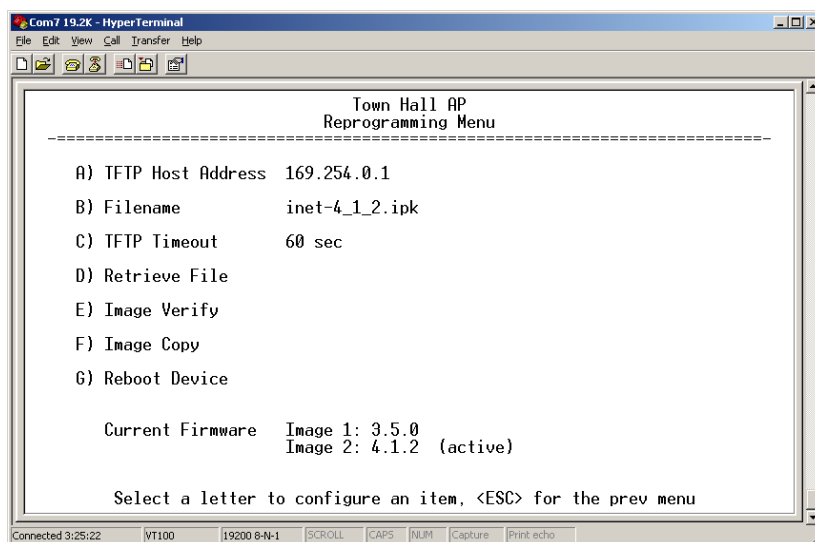


Figure 3-56. Reprogramming Menu
(Shown with “Image Copy” Selected)

- **TFTP Host Address**—IP address of the host computer from which to get the file. [Any valid IP address] This same IP address is used in other screens/functions (reprogramming, logging, etc.). Changing it here also changes it for other screens/functions.
- **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: \firmwarelessless-4_4_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. [2 to 60 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 102 for details on setting up the TFTP server.

Upgrading the Firmware

From time-to-time SIMREX offers upgrades to the transceiver firmware. One version of the firmware provides core software resources for

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

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

File transfers can be initiated through any of the three 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 radio's LAN port or associated network.

Firmware images are provided free-of-charge on the SIMREX web site at: www.simrex.com

SIMREX ESS firmware may *not* be installed in SIMREX ESS-II radios, or vice-versa.

Installing New Firmware by TFTP

To install firmware by TFTP, you will need:

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

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 Management Systems' **Configuration** menu.

(See "[Network Configuration Menu](#)" on Page 42.)

There are several alternatives to connecting the transceiver for firmware upgrade. [Figure 3-57](#) and [Figure 3-58](#) show two variations. It is essential all of the equipment be on the same subnet.

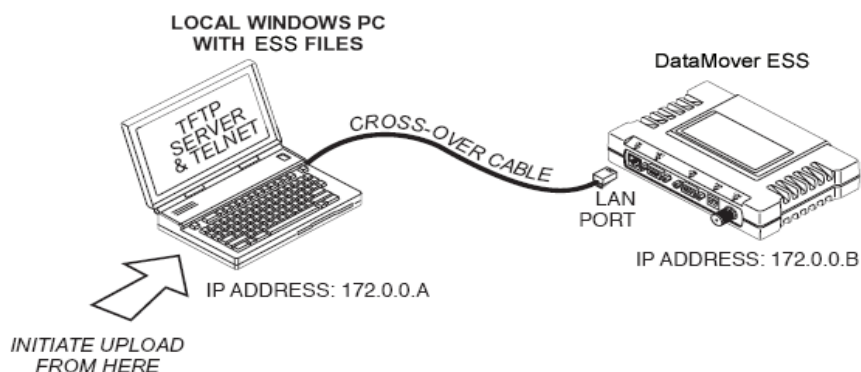


Figure 3-57. Firmware Upgrade Setup—Option 1
(TFTP Server and Firmware File on Same CPU)

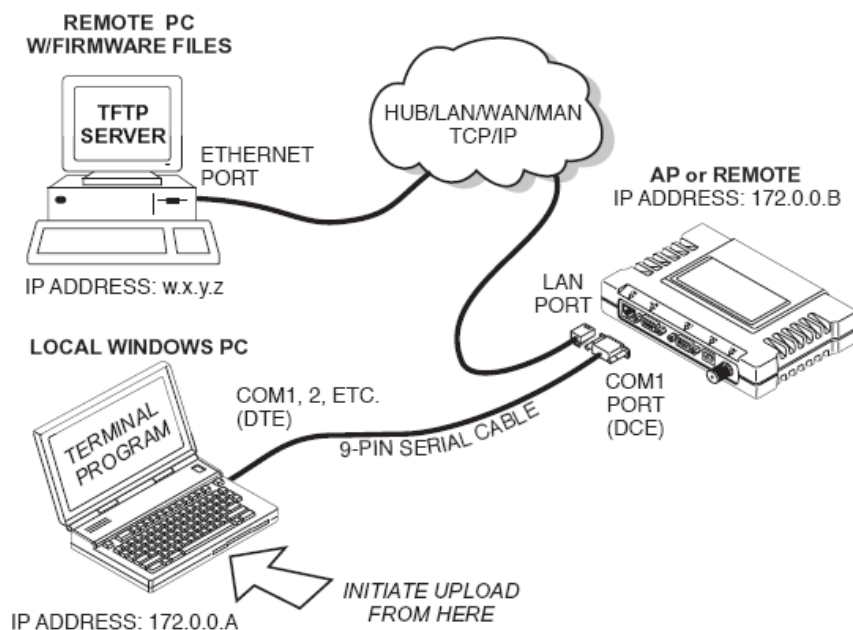


Figure 3-58. Firmware Upgrade Setup—Option 2
(TFTP Server and Firmware File on Remote Server)

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

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

Upgrade Procedure

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

1. Launch a TFTP server on a PC connected either directly or via a LAN to the Ethernet port (LAN) of the radio. Point the server towards the directory containing the firmware image file.
2. Connect to the Management System by whichever means is convenient: Browser or Telnet via the LAN, or Terminal emulator via the COM1 port.
3. Go to the MS Reprogramming Menu.
(Main Menu>>Maintenance Menu>>Reprogramming Menu)
4. Fill in the information for the:
 - **TFTP Host Address**—IP Address of server (host computer) running TFTP server.
 - **Retrieve File**—Name of file (**filename.ipk**) to be pulled from the TFTP server holding the firmware file.
5. Pull the firmware file through the TFTP server into the transceiver.
(Main Menu>>Maintenance Menu>>Reprogramming Menu>>Retrieve File)

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

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

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

NOTE: When upgrading to firmware 6.0.0 or later, the unit creates internal files following the first reboot. This one-time process delays the response of the HTTP interface for 5-10 minutes. If DC power is cycled (turned off and back on) during this process, the files will have to be created again. It is recommended that you wait until this 5-10 minute process is complete before verifying operation of HTTP, HTTPS, or SSH.

7. Test the transceiver for normal operation.

End of Procedure

Error Messages During File Transfers

It is possible to encounter errors during a file transfer. In most cases errors can be quickly corrected by referring to [Table 3-6](#).

Table 3-6. Common Errors During TFTP Transfer

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

3.9.2 Configuration Scripts Menu

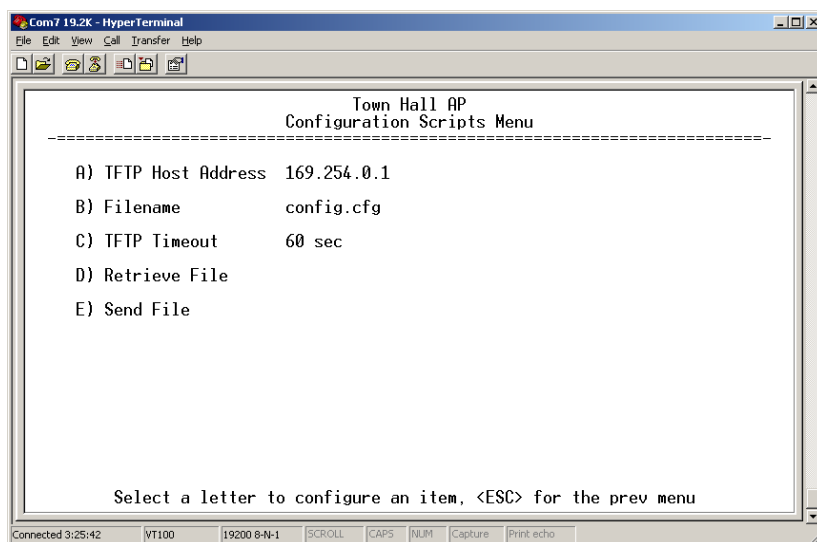


Figure 3-59. Configuration Files Menu

- **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: `configless-config.txt`. (See [“Using Configuration Scripts” on Page 107](#))

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 102](#) for details on setting up the TFTP server.

A Brief Description of Configuration Files

If you plan to have more than a few radios 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 radio(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 107](#) 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 containing 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 113](#) 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

; SIMREX DataMover ESS

; 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 IT

The name of the owner of this unit.

Contact: IT 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: SIMREX

Version Name: 06-1234567

Product Name: DataMover ESS

Beacon Period: Normal

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

Data Rate: 512 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: inet-4_4_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: inet_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

Enables 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 106](#) 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 provided by SIMREX).

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

Table 3-7. Common User-Alterable Parameters

Field	Comment	Range
IP Address	Unique for each individual radio	Any legal IP address
IP Gateway	May change for different groups or locations	Any legal IP address
Unit Name	Should reflect a specific device. This information will appear in Management System headings	Any 20-character alphanumeric string
Location	Used only as reference for network administration	Any 40-character alphanumeric string
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 in files exported from a transceiver do not need to be present in your customized files.

3.9.3 Authorization Keys Menu

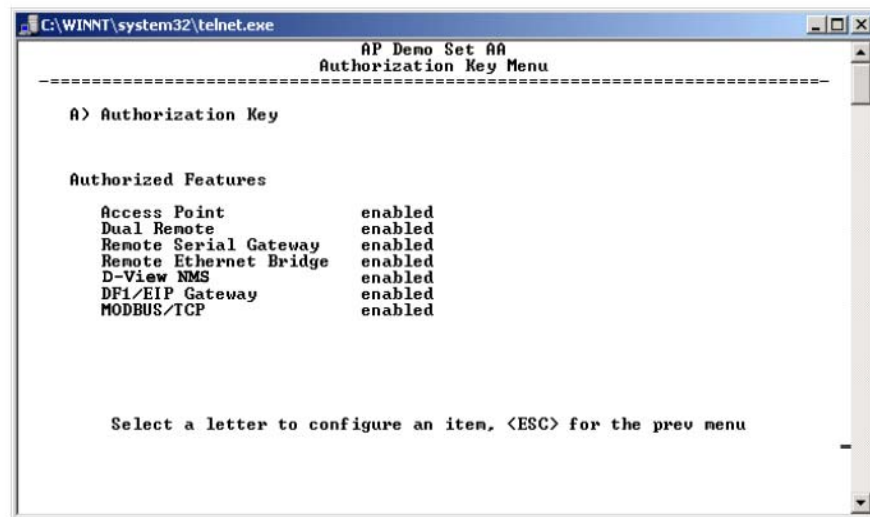


Figure 3-60. Authorization Key Menu

- **Authorization Key**—Initiate the entering of an Authorization Key into the transceiver's non-volatile memory.
- **Authorized Features**—List of authorized features available for use [enabled, disabled].

DataMover ESS-II radios will show an additional selection called **Encryption** under Authorized Features.

3.9.4 Auto-Upgrade/Remote-Reboot Menu

NOTE: This menu is only available when SIMREX D-View NMS key is enabled.

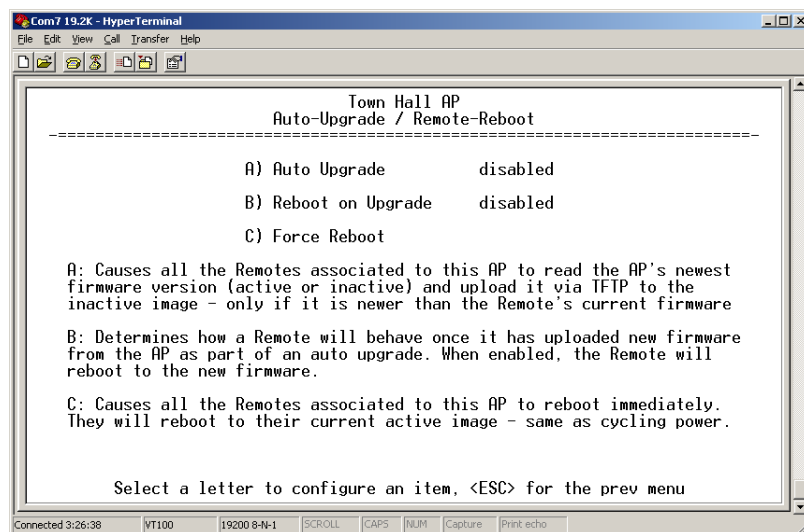


Figure 3-61. Auto-Upgrade / Remote Reboot Menu

- **Auto Upgrade**—Causes all of the Remotes associated to this AP to read the AP's newest firmware version (active or inactive) and upload it via TFTP to the inactive image, but only if it is newer than the Remote's current firmware.
- **Reboot on Upgrade**—Determines how a Remote will behave once it has uploaded new firmware from the AP as part of an auto-upgrade. When enabled, the Remote will reboot to the new firmware.
- **Force Reboot**—Causes all of the Remotes associated to this AP to reboot immediately. They will reboot to their current active image—the same as if the power were re-cycled.

NOTE: To use the Auto Upgrade/Reboot feature, both the AP and Remotes must already be running version 4.4.0 or newer firmware.

Exception: If the AP has already been upgraded to version 4.4.0 and the Remote is still at 3.5.0 or older, you can upgrade the Remote by using the AP as a file server. This method allows for only one remote to be upgraded at a time. Instructions for this method are given below.

Firmware Upgrade (with AP Acting as a File Server)

An AP running firmware version 4.4.0 (or newer) may be used as a file server to upgrade Remotes running older firmware (3.5.0 or earlier). Follow the steps below to perform the upgrade:

1. At the Reprogramming Menu (Page 102), Enter the AP's IP Address in the TFTP Server field.
2. Enter **upgrade_from_ap.ipk** in the Filename field.

NOTE: The filename is case sensitive.

3. Perform the firmware download.

3.9.5 Radio Test Menu

This area provides several useful tools for installers and maintainers. You can manually key the radio transmitter to make measurements of antenna performance. (See [“Antenna Aiming” on Page 134](#) for details.)

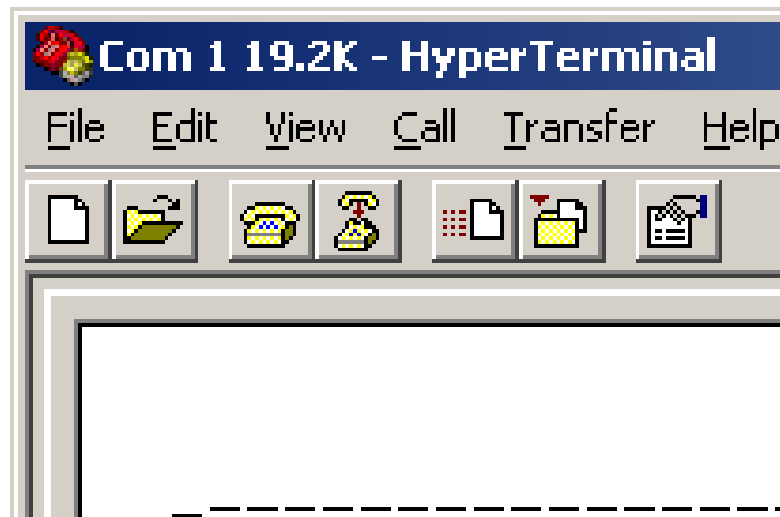


Figure 3-62. Radio Test Menu
Shown with Test Mode set to ON

NOTE : Use of the Test Mode will disrupt traffic through the radio. If the unit is an Access Point, it will disrupt traffic through the *entire* network.

Test Mode function is automatically limited to 10 minutes and *should only be used for brief measurement of 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.

3.9.6 Ping Utility Menu

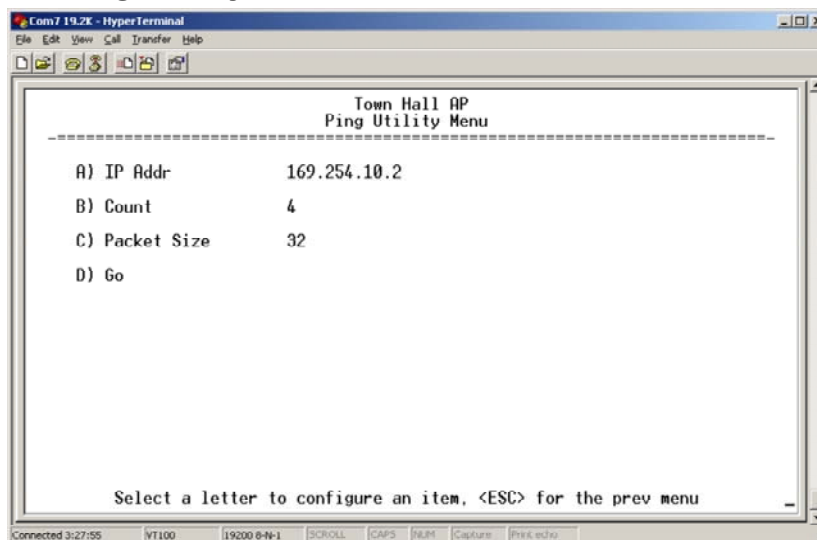


Figure 3-63. Ping Utility Menu

- **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.

3.9.7 Reset to Factory Defaults

To reset all transceiver parameters back to the factory defaults, including the password, you must enter a special code (authorization key) provided by the factory in place of the user name at the time of login.

This procedure is useful when several parameters have been modified, and there is no track of changes. It causes the transceiver to return to a known state.

Password Reset

As part of the reset action the transceiver's password is reverted to the default value of **admin**. As a security measure, this event causes all radio parameters to return to the factory default settings, including zone skipping (as applicable), baud rate settings, network name, security phrase, etc.



4 TROUBLESHOOTING & RADIO MEASUREMENTS

Contents

4.1 TROUBLESHOOTING	121
4.1.1 Interpreting the Front Panel LEDs	121
4.1.2 Troubleshooting Using the Embedded Management System ..	122
4.1.3 Using Logged Operation Events	126
4.1.4 Alarm Conditions	126
4.1.5 Correcting Alarm Conditions	128
4.1.6 Logged Events	129
4.2 RADIO (RF) MEASUREMENTS.....	131
4.2.1 Antenna System SWR and Transmitter Power Output	132
4.2.2 Antenna Aiming	133



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 Management System. Do not overlook the possibility that human error may be the cause of the problem. With so many possible parameters to look at and change, a parameter may be incorrectly set, and then what was changed is forgotten.

To help avoid these problems, we recommend creating an archive of the transceiver's profile when your installation is complete in a Configuration File. This file can be reloaded into the transceiver to restore the unit to the factory defaults or your unique profile. For details on creating and archiving Configuration Files, [see “Using Configuration Scripts” on Page 107](#).

Factory Assistance

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

4.1.1 Interpreting the Front Panel LEDs

An important set of troubleshooting tools are the LED status indicators on the front panel of case. You should check them first whenever a problem is suspected. [Table 2-2 on Page 25](#) describes the function of each status LED. [Table 4-1](#) below provides suggestions for resolving

common system difficulties using the LEDs, and [Table 4-2](#) provides other simple techniques.

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

Symptom	Problem/Recommended System Checks
PWR LED does not turn on	- Voltage too low—Check for the proper supply voltage at the power connector. (10–30 Vdc) - Indefinite Problem—Cycle the power and wait ($\approx$ 30 seconds) for the unit to reboot. Then, recheck for normal operation.
LINK LED does not turn on	- Network Name of Remote not identical to desired Access Point—Verify that the system has a unique Network Name. - Not yet associated with an Access Point with the same Network Name. Check the “Status” of the unit’s process of associating with the Access Point. Use the Management System. - 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	- Blinking indicates an alarm condition exists. - View Current Alarms and Event Log and correct the problem if possible. (See “Using Logged Operation Events” on Page 127) - 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	- Verify the Ethernet cable is connect at both ends. - Verify that the appropriate type of Ethernet cable is used: straight-through, or crossover.
LAN LED lights, but turns off after some time	Verify traffic in LAN. Typically, the radio should not be placed in high traffic enterprise LANs, as the it will not be able to pass this level of traffic. If needed, use routers to filter traffic.

4.1.2 Troubleshooting Using the Embedded Management System

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

Table 4-2. Basic Troubleshooting Using the Management System

Symptom	Problem/Recommended System Checks
Remote does not associate; stays in HOPSYNC	- Verify the AP has sufficiently large number in the "Max Remotes" parameter of the Network Configuration Menu. - 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	Change Beacon Period to FAST. (Radio Configuration Menu)
Cannot access the MS through COM1	- Connect to unit via Telnet or Web browser - Disable the serial mode for COM1 (Serial Gateway Configuration>>Com1 Serial Data Port>>Status>>Disabled) or, if you know the unit's data configuration: - Connect to COM 1 via a terminal set to VT100 and the port's data baud rate. - Type +++ - Change the terminal's baud rate to match the transceiver's Console Baud Rate. - Type +++
Display on terminal/Telnet screen garbled	Verify the terminal/terminal emulator or Telnet application is set to VT100
Cannot pass IP data to WAN.	- Verify your IP settings. - Use the PING command to test communication with the transceivers in the local radio system. - If successful with local PING, attempt to PING an IP unit attached to a transceiver. - If successful with the LAN PINGS, try connecting to a known unit in the WAN.
Wireless Retries too high.	Possible Radio Frequency Interference— - If omnidirectional antennas are used, consider changing to directional antennas. This will often limit interference to and from other stations. - Try skipping some zones where persistent interference is known or suspected. - The installation of a filter in the antenna feedline may be necessary. Consult the factory for further assistance.
Password forgotten.	- Connect to the transceiver using a terminal through the COM1 Port. - Obtain a password-resetting Authorization Key from your factory representative. - Enter the Authorization Key at the login prompt as a password.
Packet Repeat Mode troubles (extra characters in data, data not delivered)	Verify that all radios in the network have their Packet Redundancy Mode set to the same selection (Single Packet vs. Packet Repeat Mode).

The following is a summary of how several screens in the Management System can be used as diagnostic tools. For information on how to connect to the Management System See [“STEP 3—CONNECT PC TO THE TRANSCEIVER” on Page 22.](#)

Starting Information Screen

(See [Starting Information Screen on Page 38](#))

The Management System’s “homepage” provides some valuable bits of data. One of the most important is the “Device Status” field. This item 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 Status¹

Scanning	The unit is looking for an Access Point beacon signal. If this is a Remote radio, <i>Associated</i> means that this 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.
Connected	The unit has established a radio (RF) connection with the Access Point, but has not obtained cyber-security clearance to pass data.
Associated	This unit has successfully synchronized and is “associated” with an Access Point. This is the normal operating state.
Alarmed	The unit is has detected one or more alarms that have not been cleared.

1. Available in the *Startup Information Screen* or the *Wireless Status Screen* at the 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 \(RF\) MEASUREMENTS on Page 132](#) for information on antenna system checks.

Packet Statistics Menu

(See [Packet Statistics Menu on Page 90](#))

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

Wireless Packet Statistics

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

Ethernet Packet Statistics

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

The most significant fields are the *Packets Dropped*, *Retries*, *Retry Errors*, *Receive Errors* and *Lost Carrier Detected*. If the data values are more than 10% of their sent and received counterparts, or the *Lost Carrier Detected* value is greater than a few dozen, there may be trouble with radio-frequency interference or a radio link of marginal strength. Review the *RSSI by Zone Screen*'s values ([Page 86](#)) for zones that are more than 2 dB (decibels) below the average level, and for signal level values that are likely to provide marginal service. For example, an average level is less than -85 dBm during normal conditions with a data rate of 256 kbps.

If the RSSI levels in each zone are within a few dB of each other, but less than -85 dBm, then a check should be made of the aiming of the antenna system and for a satisfactory SWR. Refer to [RADIO \(RF\) MEASUREMENTS on Page 132](#) for information on antenna system checks.

NOTE: For a data rate of 512 kbps (1 Mbps for ESS-II), the average signal level should be -77 dBm or stronger with no interference.

Serial Port Statistics Menu

(See [Serial Data Statistics Menu on Page 96](#))

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 indicator of port activity at the data and IP levels.

Diagnostic Tools

(See [MAINTENANCE on Page 100](#))

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

4.1.3 Using Logged Operation Events

(See [Event Log Menu on Page 87](#))

The transceiver's microprocessor monitors many operational parameters and logs them as various classes of "events". If the event is one that affects performance, it is an "alarmed". There are also normal or routine events such as those marking the rebooting of the system, implementation of parameter changes and external access to the Management System. Informational events are stored in temporary (RAM) memory that will be lost in the absence of primary power, and Alarms will be stored in permanent memory (Flash memory) until cleared by user request. [Table 3-5](#) 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 89](#))

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

Table 4-5. Alarm Conditions (Alphabetical Order)

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_50_LIMIT	Crossed 50% of Eth Port Rate Limit	rateLimit50(20)
EVENT_75_LIMIT	Crossed 75% of Eth Port Rate Limit	rateLimit75(21)
EVENT_100_LIMIT	Crossed 100% of Eth Port Rate Limit	rateLimit100(22)
EVENT_ADC	ADC output Railed	adcInput(3)
EVENT_AP_NN_CHANGED	Network Name changed at the AP	apNetNameChanged(74)
EVENT_BRIDGE	Network Interface /Error	networkInterface(17)
EVENT_NO_CHAN_CNT	Mismatch in Channel count at AP/REM	ChanCnt(71)
EVENT_NO_CHAN	Using Channel hopping but no channels selected	NoChan(23)
EVENT_COMPRESS	Compression setting changed	compressionChanged(76)
EVENT_ENDPOINT	Endpoint Added/Removed (AP only)	eventEndpoint(67)
EVENT_ETH_LINK_AP*	AP Ethernet Link Disconnected	apEthLinkLost(19)
EVENT_FLASH_TEST	Flash Test Failed	-
EVENT_FPGA	FPGA communication Failed	fpgaCommunication(2)
EVENT_FREQ_CAL	Frequency Not Calibrated	frequencyCal(7)
EVENT_INIT_ERR	Initialization Error	initializationError(18)
EVENT_IPADDR*	IP Address Invalid	ipAddressNotSet(4)
EVENT_IP_CONN(OK)		ipConnectivityOK(75)
EVENT_IPMASK*	IP Mask Invalid	ipNetmaskNotSet(5)
EVENT_LAN_PORT		lanPortStatus(78)
EVENT_MAC	MAC communication Failed	macCommunication(1)
EVENT_MACADDR	MAC Address Invalid	noMacAddress(6)
EVENT_NETNAME*	Netname Invalid	invalidNetname(12)
EVENT_PLL_LOCK	PLL Not locked	pllLock(10)
EVENT_POWER_CAL	Power Calibrated/Not Calibrated	powerCal(8)
EVENT_POWER_HIGH	RF Power Control Saturated High	rfPowerHigh(13)
EVENT_POWER_LOW	RF Power Control Saturated Low	rfPowerLow(14)

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

Alarm Condition Reported	Event Log Entry	SNMP Trap
EVENT_REMOTE	Remote Added/ Removed (AP only)	eventRemote(66)
EVENT_REPETITIVE	The previous event is occurring repetitively	
EVENT_ROUTE_ADD	Manual entry added to Routing table	routeAdded(68)
EVENT_ROUTE_DEL	Manual entry deleted from Routing table	routeDeleted(69)
EVENT_RSSI*	RSSI Exceeds threshold	rsssi(11)
EVENT_RSSI_CAL	RSSI Not Calibrated	rsssiCal(9)
EVENT_SDB_ERR	Internal Remote/Endpoint database error (AP only)	sdbError(80)
EVENT_SINREM_SWITCH	Eth/Serial mode switch in a Single Remote	sinRemSwitch(70)
EVENT_SYSTEM_ERROR*	System Error Cleared; Please Reboot	systemError(16)
EVENT_TFTP_CONN	TFTP connectivity achieved	tftpConnection(73)
EVENT_TFTP_ERR	Attempted TFTP connection failed	tftpConnFailed(79)

* Condition may be corrected by user and alarm cleared.

4.1.5 Correcting Alarm Conditions

(See [View Event Log on Page 90](#))

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

Table 4-6. Correcting Alarm Conditions—Alphabetical Order

Event Log Entry	Generating Condition	Clearing Condition or Action
ADC Failure	The ADC always reads the same value (either high or low limit)	Contact factory Technical Services for assistance
AP Ethernet Link	Monitor will check state of Ethernet link and set alarm if it finds the link down	Ethernet link is re-established
Bridge Down	When the Bridge fails to be initialized	Contact factory Technical Services for assistance
Flash Test Failed	Internal check indicates corruption of Flash memory	Contact factory Technical Services for assistance
FPGA Failure	Communication lost to the FPGA	Contact factory Technical Services for assistance

Table 4-6. Correcting Alarm Conditions—Alphabetical Order

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

4.1.6 Logged Events

(See [View Event Log on Page 90](#))

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

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

Table 4-7. Non-Critical Events—Alphabetical Order

Event Log Entry	Severity	Description
Association Attempt Success/Failed	MAJOR	Self explanatory
Association Lost - AP Hop Parameter Changed	MINOR	Self explanatory
Association Lost - AP's Ethernet Link Down	MAJOR	Self explanatory
Association Lost - Local IP Address Changed	MAJOR	Self explanatory
Association Lost - Local Network Name Changed	MAJOR	Self explanatory
Association Lost/Established	MAJOR	Self explanatory
Auth Demo Mode Expired -- Rebooted Radio/Enabled	MAJOR	Self explanatory
Auth Key Entered - Key Valid/Key Invalid	MAJOR	Self explanatory
Bit Error Rate Below threshold/Above threshold	INFORM	Self explanatory
Console Access Locked for 5 Min	MAJOR	Self explanatory
Console User Logged Out/Logged In	MAJOR	Self explanatory
Country/SkipZone Mismatch	INFORM	Self explanatory
Current AP No Longer Approved	MAJOR	May occur during the Scanning process at a remote. Indicates that the received beacon came from an AP which is not in the “Approved AP” list. This may be caused by some remotes hearing multiple AP's. This event is expected behavior.
Decryption Error/Decryption OK		A decryption error is logged when an encryption phrase mismatch has occurred. A mismatch is declared after five consecutive errors over a 40-second window. When the error has cleared, DECRYPT OK will appear.
Desired AP IP Addr Mismatch	INFORM	Self explanatory
ETH Rate		Indicates heavy bursts of traffic on the unit's Ethernet port (LAN). This is expected behavior, resulting from the network configuration.
Ethernet Port Enabled/Disabled	INFORM	Self explanatory
Expected Sync Lost/Established	INFORM	Self explanatory
Hop Sync Lost/Established	INFORM	Self explanatory

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

Event Log Entry	Severity	Description
Hop Table Generated/Generation Failed	INFORM	Self explanatory
HTTP Access Locked for 5 Min	MAJOR	Self explanatory
HTTP User Logged Out/Logged In	MAJOR	httpLogin(49)
Log Cleared	INFORM	Self explanatory
MAC Param Changed		Caused by remotes running in auto data rate mode. Every time the link conditions cause a data rate change, the remote's MAC changes to the new rate and forwards a signal to the AP. This indicates link quality is changing and causing the data rate to adjust accordingly.
Max Beacon Wait Time Exceeded	MAJOR	Self explanatory
Received Beacon - AP is Blacklisted	INFORM	Self explanatory
Received Beacon - Netname Does Not Match	INFORM	Self explanatory
Received Beacon - Valid/Errored	INFORM	Self explanatory
Rem Ethernet Link Connected/Disconnected	MAJOR	Self explanatory
Reprogramming Complete	INFORM	Self explanatory
Reprogramming Failed	MAJOR	Self explanatory
Reprogramming Started	INFORM	Self explanatory
Scanning Started	INFORM	Self explanatory
SNR Within threshold/Below threshold	INFORM	Self explanatory
System Bootup (power on)	INFORM	Self explanatory
Telnet Access Locked for 5 Min	MAJOR	Self explanatory
Telnet User Logged Out/Logged In	MAJOR	Self explanatory
User Selected Reboot	MAJOR	Self explanatory

4.2 RADIO (RF) MEASUREMENTS

There are several measurements that are a good practice to perform during the initial installation. They 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 ($\approx 2:1$ 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 using the menu sequence below:
(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 radio to normal operation. The Radio Test Mode can be terminated manually by selecting **OFF** on the menu or temporarily disconnecting the radio's DC power.

3. Set the transmit power to 30 dBm. (This setting does not affect the output level during normal operation—only during Test Mode.)
(Main Menu>>Maintenance Menu>>Radio Test>>Test Mode>>Tx Power Output)
4. Key the transmitter.
(Main Menu>>Maintenance Menu>>Radio Test>>Test Mode>>TxKey>>Enable)

Use the PC's spacebar to key and unkey the transmitter ON and OFF. (Enable/Disable)
5. Measure the forward and reflected power into the antenna system and calculate the SWR and power output level. The output should agree with the programmed value.

(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 Aiming

Introduction

The radio network integrity depends, in a large part, on stable radio signal levels being received at each end of a data link. In general, signal levels stronger than -77 dBm (-80 dBm for ESS-II) provides the basis for reliable communication that includes a 15 dB fade margin. As the distance between the Access Point and Remotes increases, the influence of terrain, foliage and man-made obstructions become more influential and the use of directional antennas at Remote locations becomes necessary. Directional antennas usually require some fine-tuning of their bearing to optimize the received signal strength. The transceiver has a built-in received signal strength indicator (RSSI) that can be used to tell you when the antenna is in a position that provides the optimum received signal.

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

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

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

Procedure

1. Verify the Remote transceiver is associated with an Access Point unit by observing the condition of the LINK LED (**LINK LED = On or Blinking**). This indicates that you have an adequate signal level for the measurements and it is safe to proceed.
2. View and record the *Wireless Packets Dropped* and *Received Error* rates.
(Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

This information will be used later.

3. Clear the *Wireless Packets Statistics* history.
(Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics>>Clear Wireless Stats)\
4. Read the RSSI level at the Remote.
(Main Menu>>Performance Information>>RSSI by Zone)
5. Optimize RSSI (less negative is better) by slowly adjusting the direction of the antenna.

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

6. View the *Wireless Packets Dropped* and *Received Error* rates at the point of maximum RSSI level. They should be the same or lower than the previous reading.
(Main Menu>>Performance Information>>Packet Statistics>>Wireless Packet Statistics)

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

End of procedure



5 PLANNING A RADIO NETWORK

Contents

5.1	INSTALLATION PLANNING	137
5.1.1	General Requirements	137
5.1.2	Site Selection	139
5.1.3	Terrain and Signal Strength	139
5.1.4	Antenna & Feedline Selection	140
5.1.5	How Much Output Power Can be Used?	143
5.1.6	Conducting a Site Survey	143
5.1.7	A Word About Radio Interference	144
5.2	dBm-WATTS-VOLTS CONVERSION CHART	147



5.1 INSTALLATION PLANNING

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

5.1.1 General Requirements

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

NOTE: The ESS network port supports 10BaseT connections, but does not support 100BaseT connections. This should not present a problem because most hubs/switches auto-switch between 10BaseT and 100BaseT connections. Confirm that your hub/switch is capable of auto-switching data rates.

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

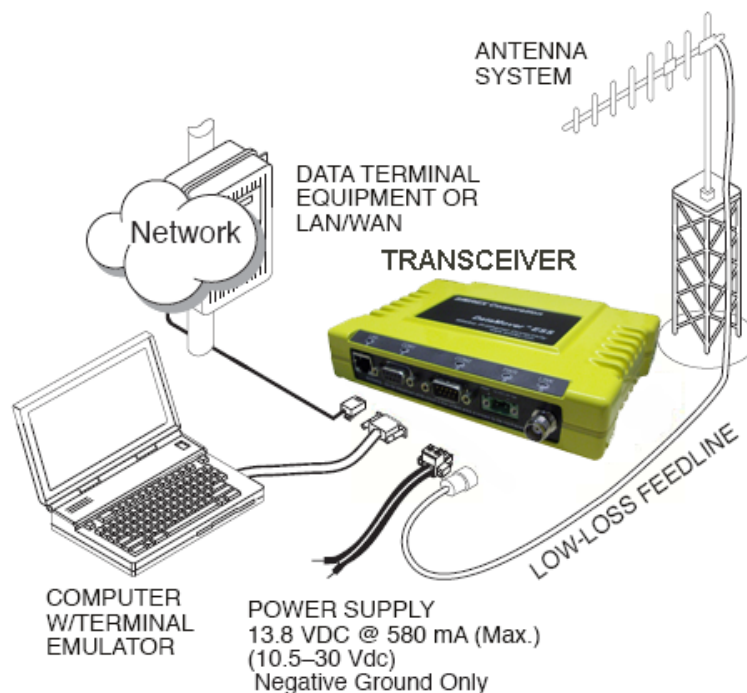


Figure 5-1. Typical Installation with a Tower-Mounted Antenna
(Connect user data equipment to any compatible LAN or COM Port)

Unit Dimensions

[Figure 5-2](#) shows the dimensions of the transceiver case and its mounting holes, and [Figure 5-3 on Page 140](#), the dimensions for mounting with factory-supplied brackets. If possible, choose a mounting

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

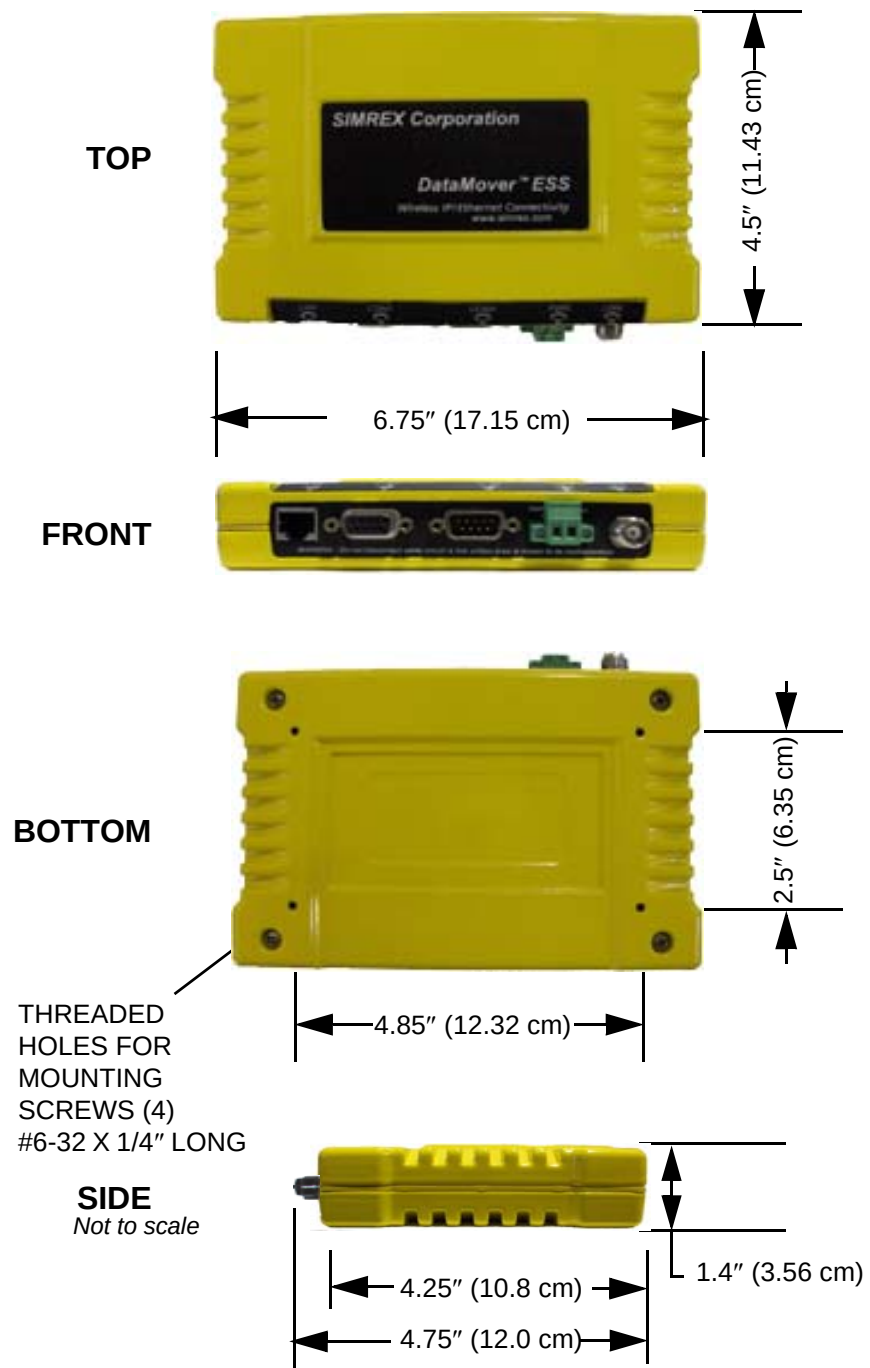


Figure 5-2. Transceiver Dimensions



Figure 5-3. Mounting Bracket Dimensions

5.1.2 Site Selection

Suitable sites should provide:

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

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

5.1.3 Terrain and Signal Strength

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

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

Much depends on the minimum signal strength that can be tolerated in a given system. Although the exact figure will differ from one system to another, a Received Signal Strength Indication (RSSI) of -77 dBm (-80 dBm for ESS-II) or stronger will provide acceptable performance in many systems. While the equipment will work at lower-strength signals, signals stronger than -77 dBm provide a “fade margin” of 15 dB to

account for variations in signal strength that may occur from time-to-time. RSSI can be measured with a terminal connected to the COM1 Port or with a HTTP browser to the LAN (Ethernet) connector. (See “[Antenna Aiming](#)” on Page 134 for details.)

5.1.4 Antenna & Feedline Selection

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

This text that follows is designed to aid the professional installer in the proper methods of maintaining compliance with FCC Part 15 limits and the +36 dBm or 4 watts peak E.I.R.P limit.

Antennas

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

In general, an omnidirectional antenna ([Figure 5-4](#)) is used at the Access 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 factory representative for details.

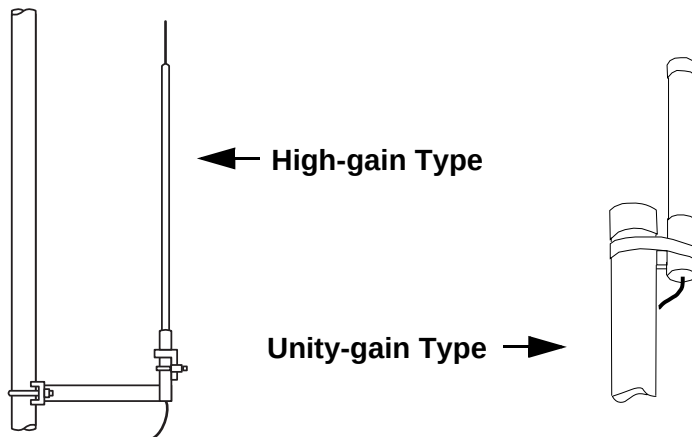


Figure 5-4. Typical Omnidirectional Antennas

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.

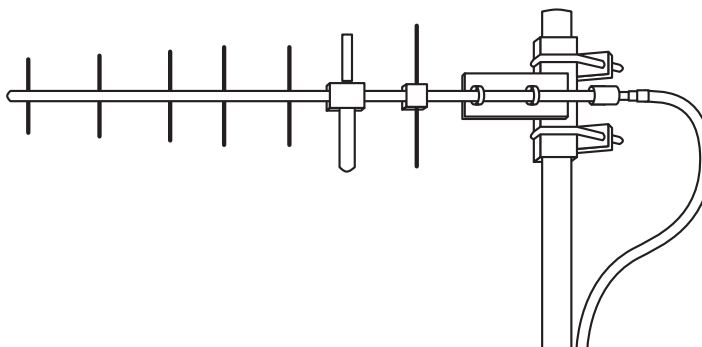


Figure 5-5. Typical Yagi Antenna (mounted to mast)

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 Heliac®.

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

900 MHz. The choice of cable will depend on the required length, cost considerations, and the amount of signal loss that can be tolerated.

Table 5-1. Length vs. Loss in Coaxial Cables at 900 MHz

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

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

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

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

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

*Refer to [Table 5-3](#) for allowable power settings of the transceiver for each antenna type.

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

The DataMover ESS-II Transceiver is factory set to +29 dBm

power output to maintain compliance with the FCC's Digital Transmission System (DTS) Part 15 rules. These rules limit power to a maximum of 8 dBm/3 kHz, thus the ESS-II Transceiver is factory set to +29 dBm. When calculating maximum transceiver power output for ESS-II installations, use +29 dBm if antenna gain is 6 dBi or less. See [How Much Output Power Can be Used? on Page 144](#) for power control of higher gain antennas.

5.1.5 How Much Output Power Can be Used?

The transceiver is normally supplied from the factory set for a nominal +30 dBm (+29 dBm for ESS-II) RF power output setting; this is the maximum transmitter output power allowed under FCC rules. The power must be *decreased* from this level if the antenna system gain exceeds 6 dBi. The allowable level is dependent on the antenna gain, feedline loss, and the transmitter output power setting.

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

5.1.6 Conducting a Site Survey

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

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

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

With the hand-held antenna positioned near the proposed mounting spot, a technician can check for synchronization with the Access Point station (shown by a lit LINK LED on the front panel) and measure the reported RSSI value. (See [“Antenna Aiming” on Page 134](#) 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-3 EMBEDDED MANAGEMENT SYSTEM section Page 27](#).

5.1.7 A Word About Radio Interference

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

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

- Systems installed in rural areas are least likely to encounter interference; those in suburban and urban environments are more likely to be affected by other devices operating in the license-free frequency band and by adjacent licensed services.
- Use a directional antenna at remote sites whenever possible. Although these antennas may be more costly than omnidirectional types, they confine the transmission and reception pattern to a comparatively narrow lobe, that minimizes interference to (and from) stations located outside the pattern.
- If interference is suspected from a nearby licensed system (such as a paging transmitter), it may be helpful to use horizontal polarization of all antennas in the network. Because most other services use vertical polarization in this band, an additional 20 dB of attenuation to interference can be achieved by using horizontal polarization. Another approach is to use a bandpass filter to attenuate all signals outside the 900 MHz band.
- Multiple Access Point units can co-exist in proximity to each other with only very minor interference. Each network name has a different hop pattern. (See [“Protected Network Operation using Multiple Access Points” on Page 13](#).) Additional isolation can be achieved by using separate directional antennas with as much vertical or horizontal separation as is practical.
- If constant interference is present in a particular frequency zone (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 Page 57 for more information on Skip Zones.
- 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.

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

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

Calculating System Gain

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

1. Determine the antenna system gain by subtracting the feedline loss (in dB) from the antenna gain (in dBi). For example, if the antenna gain is 9.5 dBi, and the feedline loss is 1.5 dB, the antenna system gain would be 8 dB. (If the antenna system gain is 6 dB or less, no power adjustment is required.)
2. Subtract the antenna system gain from 36 dBm (the maximum allowable EIRP). The result indicates the maximum transmitter power (in dBm) allowed under the rules. In the example above, this is 28 dBm.
3. If the maximum transmitter power allowed is less than 30 dBm, set the power to the desired level using the Management System.
(Main Menu>>Radio Configuration>>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 (28.7 dBm for ESS-II).

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

Antenna System Gain (Antenna Gain in dBi* minus Feedline Loss in dB†)	Maximum Power Setting (PWR command) ESS Radio	Maximum Power Setting (PWR command) ESS-II Radio	EIRP (in dBm)
Omni 6 (or less)	30	28	36
Omni 9	27	26	36
Yagi 12	24	23	36
Yagi 14	22	Not allowable	36
Yagi 16	20	Not allowable	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 143](#).

For assistance in the conversion of dBm to Watts, please see [dBm-WATTS-VOLTS CONVERSION CHART on Page 147](#).

5.2 dBm-WATTS-VOLTS CONVERSION CHART

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

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

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





6 TECHNICAL REFERENCE

Contents

6.1 DATA INTERFACE CONNECTORS	151
6.1.1 LAN Port	151
6.1.2 COM1 Port	152
6.1.3 COM2 Port	152
6.2 FUSE REPLACEMENT PROCEDURE	153
6.3 TECHNICAL SPECIFICATIONS.....	154
6.4 CHANNEL HOP TABLE.....	157
6.5 SNMP USAGE NOTES	159
6.5.1 Overview	159



6.1 DATA INTERFACE CONNECTORS

Three data interface connectors are provided on the face of the 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).



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

6.1.1 LAN Port

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

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

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

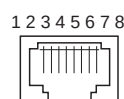


Figure 6-1. LAN Port (RJ-45) Pinout
(Viewed from the outside of the unit)

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

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

6.1.2 COM1 Port

To connect a PC to the transceiver's COM1 port use a DB-9M to DB-9F "straight-through" cable. These cables are available commercially, or may be constructed using the pinout information in [Figure 6-2](#) and [Table 6-2](#).

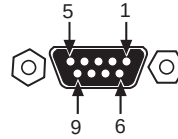


Figure 6-2. COM1 Port (DCE)
(Viewed from the outside of the unit.)

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

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

6.1.3 COM2 Port

To connect a PC to the transceiver's COM2 port use a DB-9F to DB-9M "straight-through" cable. These cables are available commercially, or may be constructed using the pinout information in [Figure 6-2](#) and [Table 6-2](#).

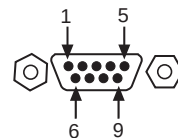


Figure 6-3. COM2 Port (DTE)
Viewed from the outside of the radio

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)	

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

Pin	Functions	DTE
6	Data Set Ready (DSR)	In]<—
7	Request-to-Send (RTS)	Out]—>
8	Clear-to-Send (CTS)	In]<—
9	Unused	

6.2 FUSE REPLACEMENT PROCEDURE

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

1. Disconnect the primary power source and all other connections to the unit.
2. Place the radio on its back and remove the four Phillips screws on the bottom cover.
3. Carefully separate the top and bottom covers. There is a flat ribbon cable between the top cover's LEDs and the unit motherboard. You do not need to disconnect the ribbon cable.
4. Locate the fuse and fuse holder between the COM1 port and the power connector. See [Figure 6-4](#) for details.
5. Loosen the fuse from the holder using a very small screwdriver. Use a small pair of needle-nose pliers to pull the fuse straight up and remove it.
6. Using an Ohmmeter, or other continuity tester, verify the fuse is blown.
7. Install a new fuse by reversing the process.

Littelfuse P/N: 0454002; 452 Series, 2 Amp SMF Slo-Blo
SIMREX P/N: ESS-FUSE-2A

8. Install the covers and check the transceiver for proper operation.

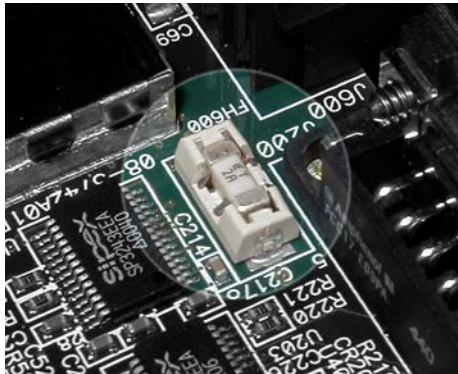


Figure 6-4.
Internal Fuse and Holder
Assembly Location

6.3 TECHNICAL SPECIFICATIONS

GENERAL

Temperature Range:	–30° C to +60° C (–22° F to 140° F)
Humidity:	95% at +40° C (104° F); non-condensing
Primary Power:	10–30 Vdc (13.8 Vdc Nominal)
External Power Supply Options:	110–120/210–220 Vac
Supply Current (typical):	(9 Watts Maximum @ 1 Watt RF Output)
Transmit:	7 watts (10.5–24 Vdc) 9 watts (24.5–30 Vdc)
Receive:	2.8 watts (10.5–24 Vdc) 3.5 watts (24.5–30 Vdc)
MTBF:	35 Years (Telcordia Method 1, Case 3)
Size (Excluding mtg. hardware):	1.25" x 6.75" x 4.5" (H x W x D) 3.15 x 17.15 x 11.43 cm
Mounting w/Optional Hardware:	• DIN Rail • Flat surface mounting brackets • 19" rack (1U high)
Weight:	908 g / 2 lb
Case:	Cast Aluminum
Boot Time:	≈ 30 sec
Time Required to Associate with Access Point:	≈ 20 sec

APPROVALS/HOMOLOGATION

-
- FCC Part 15.247
ESS FCC identifier: E5MDS-NH900
ESS-II FCC identifier: T72-DMESSII
 - Industry Canada RSS-210
ESS certification no.: 3738A 12098
ESS-II certification no.: 6492A-DMESSII

SIMREX Corporation

- UL/CSA Class 1, Div. 2; Groups A, B, C and D hazardous locations
- Contact factory for information on availability and governmental approvals in other countries

MANAGEMENT

- HTTP, HTTPS (Embedded Web server)
- Telnet, SSH, COM1 serial port (Text-based menu)
- SNMP v1/v2/v3
- SYSLOG
- SIMREX D-View MS™

DATA CHARACTERISTICS

PORTS:

Ethernet:

Interface Connectors:	RJ-45 Standard
Data Rate:	10BaseT (10 Mbps)

Serial (2 Ports):

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
Byte Formats:	7 or 8-bit; even, odd, or no-parity; 1 or 2 stop bits

OPERATING MODES:

- Configurable as Access Point or Remote Station

PROTOCOLS:

- Wireless: CSMA/CA (Collision Avoidance)
- Ethernet: IEEE 802.3, Ethernet II, Spanning Tree (Bridging), IGMP
- TCP/IP: DHCP, ICMP, UDP, TCP, ARP, Multicast, SNMP, TFTP
- Serial: PPP, Encapsulation over IP (tunneling) for serial async multidrop protocols including Modbus, DNP.3, DF1, BSAP
- Special: Allen-Bradley EtherNet/IP* - Modbus/TCP (optional)

CYBER SECURITY

- SIMREX Cyber Security Suite, Level 1 (ESS-II only):
 - AES-128 encryption (optional)
- SIMREX Cyber Security Suite, Level 2:
 - RC4-128 encryption (ESS only)
 - Automatic rotating key algorithm
 - Authentication: 802.1x, RADIUS, EAP/TLS, PKI, PAP, CHAP
 - Management: SSL, SSH, HTTPS
 - Approved AP/Remotes list (local authentication)
 - Failed login lockdown
 - 900 MHz operation and proprietary data framing

RADIO CHARACTERISTICS**GENERAL:**

Frequency Range:	902–928 MHz ISM Band
Frequency Hopping Range:	ESS: Ten user-configurable 2.5 MHz-wide zones, each containing 8 frequencies (ESS) ESS-II: From one and up to 75 overlapping channels
Hop Patterns:	8192, 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) $\pm$ 1.0 dB, set by user
Duty Cycle:	Continuous
Modulation Type:	Binary CPFSK
Output Impedance:	50 Ohms
Spurious:	–67 dBc
Occupied Bandwidth:	DataMover ESS: 316.5 kHz DataMover ESS-II: 600 kHz

RECEIVER:

Type:	Double conversion superheterodyne
Sensitivity:	DataMover ESS: –92 dBm @ 512 kbps < 1×10^{-6} BER DataMover ESS: –99 dBm @ 256 kbps < 1×10^{-6} BER DataMover ESS-II: –92 dBm @ 1 Mbps < 1×10^{-6} BER DataMover ESS-II: –97 dBm @ 512 kbps < 1×10^{-6} BER
Intermodulation:	59 dB Minimum (EIA)
Desensitization:	70 dB
Spurious:	60 dB

TRANSMIT/RECEIVE RANGE (Nominal)

	<u>DM ESS–256 kbps</u>	<u>DM ESS-II–512 kbps</u>
Fixed Range (typical):	15 miles (24 km)	12 miles (19 km)
Fixed Range (maximum):	60 miles (97 km)	30 miles (48 km)
Mobile Range (parked):	5 miles (8 km)	3 miles (5 km)
Mobile Range (moving):	3 miles (5 km)	1 mile (2 km)
	<u>DM ESS–512 kbps</u>	<u>DM ESS-II–1024 kbps</u>
Fixed Range (typical):	8 miles (13 km)	8 miles (13 km)
Fixed Range (maximum):	15 miles (24 km)	15 miles (24 km)

Note: Specifications subject to change without notice or obligation.

NOTE: Range calculations for fixed locations assume a 6 dBd gain Omnidirectional antenna on a 100 ft tower at the AP, a 10 dBd gain Yagi on a 25 ft mast at the remote with output power decreased to yield maximum allowable EIRP (36 dBm), a 10

dB fade margin, and a mix of agricultural and commercial terrain with line of sight.

Range calculations for mobile units assume a 6 dBd gain Omni on a 100 ft tower at the AP, a 5 dBd gain Omni with 1 watt output power at 6 ft height, a 10 dB fade margin, and 90% confidence with near line-of-sight in a mix of agricultural and commercial terrain.

Actual performance is dependent on many factors including antenna height, blocked paths, and terrain.

6.4CHANNEL HOP TABLE

The DataMover ESS transceiver's hop table consists of 80 channels, numbered 0 to 79 as listed in [Table 6-4](#). Center frequencies are calculated as follows (where Fn is the center frequency of channel n):

$$F_n = 902.5 \text{ MHz} + n * 316.5 \text{ kHz}$$

The DataMover ESS-II transceiver operates on the same channel assignments, but because the modulation bandwidth is 600 kHz instead of 316.5 kHz it is recommended that the installer restrict channel usage to every other channel for units operating in the same area.

NOTE: Channels 24, 26, and 55 are not used.

Table 6-4. Channel Hop Table

Zone	Channel	Frequency
1	0	902.5000 (ESS FHSS lowest channel)
1	1	902.8165 (ESS-II DTS lowest channel)
1	2	903.1330
1	3	903.4495
1	4	903.7660
1	5	904.0825
1	6	904.3990
1	7	904.7155
2	8	905.0320
2	9	905.3485
2	10	905.6650
2	11	905.9815
2	12	906.2980
2	13	906.6145
2	14	906.9310
2	15	907.2475

Table 6-4. Channel Hop Table (Continued)

Zone	Channel	Frequency
3	16	907.5640
3	17	907.8805
3	18	908.1970
3	19	908.5135
3	20	908.8300
3	21	909.1465
3	22	909.4630
3	23	909.7795
4	24	910.0960
4	25	910.4125
4	26	910.7290
4	27	911.0455
4	28	911.3620
4	29	911.6785
4	30	911.9950
4	31	912.3115
5	32	912.6280
5	33	912.9445
5	34	913.2610
5	35	913.5775
5	36	913.8940
5	37	914.2105
5	38	914.5270
5	39	914.8435
6	40	915.1600
6	41	915.4765
6	42	915.7930
6	43	916.1095
6	44	916.4260
6	45	916.7425
6	46	917.0590
6	47	917.3755
7	48	917.6920
7	49	918.0085
7	50	918.3250
7	51	918.6415
7	52	918.9580
7	53	919.2745
7	54	919.5910
7	55	919.9075
8	56	920.2240
8	57	920.5405

Table 6-4. Channel Hop Table (Continued)

Zone	Channel	Frequency
8	58	920.8570
8	59	921.1735
8	60	921.4900
8	61	921.8065
8	62	922.1230
8	63	922.4395
9	64	922.7560
9	65	923.0725
9	66	923.3890
9	67	923.7055
9	68	924.0220
9	69	924.3385
9	70	924.6550
9	71	924.9715
10	72	925.2880
10	73	925.6045
10	74	925.9210
10	75	926.2375
10	76	926.5540
10	77	926.8705
10	78	927.1870 (ESS-II DTS highest channel)
10	79	927.5035 (ESS FHSS highest channel)

6.5 SNMP USAGE NOTES

6.5.1 Overview

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

SNMPv3 Support

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

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

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

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

SNMPv3 Accounts

The following default accounts are available for the SNMP Agent:

enc_mdadmin—Read/write account using Authentication and Encryption

auth_mdadmin—Read/write account using Authentication

enc_mdviewer—Read only account using Authentication and Encryption

auth_mdviewer—Read only account using Authentication

def_mdviewer—Read only account with no Authentication or Encryption

Context Names

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

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

All accounts share the same default passwords:

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

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

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

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

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

Password-Mode Management Changes

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

Common Scenarios

- Passwords are currently being handled by the Manager. The assigned passwords are **Microwave** (Auth), and **Rochester** (Priv). Configuration is changed to manage the passwords locally. The passwords stored on the radio were **Fairport** (Auth), and **Churchville** (Priv) (If local passwords have *never* been used, then MDSAuthPwd and MDSPrivPwd will be used). These passwords will now be used by the Agent to re-generate keys. The Manager will need to know these passwords in order to talk to the Agent.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The same passwords will continue to be used, but now the Manager can change them.
- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Passwords are changed to **Brighton** (Auth) and **Perinton** (Priv). The Agent will immediately generate new keys based on these passwords and start using them. The Manager will have to be re-configured to use these new passwords.

- Passwords are currently being managed locally. The local passwords are **Fairport** (Auth) and **Churchville** (Priv). Configuration is changed to handle the passwords from the Manager. The Manager changes the passwords to **Brighton** (Auth) and **Perinton** (Priv). The radio is then rebooted. After a power-cycle, the radio will use the passwords stored in flash, which are **Fairport** (Auth) and **Churchville** (Priv). The Manager will have to be re-configured to use these new passwords.

Table 6-5. SNMP Traps (Sorted by Code)

SNMP Trap	Severity	Description
systemBoot(32)	INFORM	SNR Within threshold/Below threshold
systemReboot(33)	MAJOR	Telnet User Logged Out/Logged In
startScan(34)	INFORM	Reprogramming Started
rxBeaconErrored(35)	INFORM	Received Beacon - Netname Does Not Match
rxBeaconWrongNetworkName (36)	INFORM	Received Beacon - AP is Blacklisted
rxBeaconFromBlacklistAP(37)	MAJOR	Max Beacon Wait Time Exceeded
expectedSync(38)	INFORM	Expected Sync Lost/Established
hopSync(39)	INFORM	Hop Sync Lost/Established
snr(41)	INFORM	Scanning Started
ber(42)	INFORM	Bit Error Rate Below threshold/Above threshold
associated(43)	MAJOR	Association Lost/Established
apParmChange(44)	MINOR	Association Lost - AP Hop Parameter Changed
reprogStarted(45)	MAJOR	Reprogramming Failed
reprogComplete(46)	MAJOR	Rem Ethernet Link Connected/Disconnected
reprogFailed(47)	INFORM	Reprogramming Complete
telnetLogin(48)	MAJOR	Telnet Access Locked for 5 Min
httpLogin(49)	MAJOR	HTTP User Logged Out/Logged In
countrySkipZoneMismatch(50)	INFORM	Country/SkipZone Mismatch
desiredAPIPMismatch(51)	INFORM	Desired AP IP Addr Mismatch
eventLogCleared(52)	INFORM	Log Cleared
authDemoMode(53)	MAJOR	Auth Demo Mode Expired -- Rebooted Radio/Enabled
keyEntered(54)	MAJOR	Auth Key Entered - Key Valid/Key Invalid
apEthLinkDown(55)	MAJOR	Association Lost - AP's Ethernet Link Down
noBeacons(56)	MAJOR	MAC Param Changed
apNotApproved(57)	MAJOR	Current AP No Longer Approved
netnameChanged(58)	MAJOR	Association Lost - Local Network Name Changed
ipAddrChanged(59)	MAJOR	Association Lost - Local IP Address Changed
assocTryFail(60)	MAJOR	Association Attempt Success/Failed
remEthLinkLost(61)	INFORM	Received Beacon - Valid/Errored
consoleLogin(62)	MAJOR	Console User Logged Out/Logged In

Table 6-5. SNMP Traps (Sorted by Code) (Continued)

SNMP Trap	Severity	Description
consoleLockdown(63)	MAJOR	Console Access Locked for 5 Min
telnetLockdown(64)	INFORM	System Bootup (power on)
httpLockdown(65)	MAJOR	HTTP Access Locked for 5 Min
eventRemote(66)	INFORM	Remote added/removed from internal database
eventEndpoint(67)	INFORM	Endpoint added/removed from internal database
routeAdded(68)	INFORM	Radio attempted but failed to add a route to its internal routing table
routeDeleted(69)	INFORM	Radio attempted but failed to delete a route from its internal routing table
sinRemSwitch(70)	INFORM	Remote mode was switched (serial to ethernet, ethernet to serial)
ChanCnt(71)	INFORM	Number of channels defined does not match (Channel 130 only)
tftpConnection(73)	INFORM	TFTP Server on AP started or finished a transfer
apNetNameChanged(74)	MAJOR	Remote lost association due to a change in the AP's netname
ipConnectivityOK(75)	INFORM	Radio is associated AND 1) has an IP address statically defined, OR 2) received an IP address via DHCP
compressionChanged(76)	INFORM	Compression state has changed (enabled, disabled)
macDecryptError(77)	INFORM	MAC has received a packet that it could not decrypt
lanPortStatus(78)	INFORM	Ethernet port has changed (enabled, disabled)
tftpConnFailed(79)	INFORM	TFTP server on AP failed to transfer
sdbError(80)	INFORM	AP encountered an internal database error





7 GLOSSARY OF TERMS AND ABBREVIATIONS

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

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 42.)

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 and is ready to pass traffic.

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

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

Bits-per-second—See *BPS*.

BPDU—Bridge Protocol Data Units

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

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

CSMA/CA—Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD—Carrier Sense Multiple Access/Collision Detection

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

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

Data Circuit-terminating Equipment—See *DCE*.

Data Communications Equipment—See *DCE*.

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

Data Terminal Equipment—See *DTE*.

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

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

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

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

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

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

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

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

Digital Signal Processing—See *DSP*.

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

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

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

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

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

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

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

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

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

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

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

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

HTTP—Hypertext Transfer Protocol

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

ICMP—Internet Control Message Protocol

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

IEEE—Institute of Electrical and Electronic Engineers

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

LAN—Local Area Network

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

MAC—Media Access Controller

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

MIB—Management Information Base

Microcontroller Unit—See *MCU*.

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

continue to send data to the IP address that was assigned to the station. Mobile IP also uses DHCP when the station moves into a foreign network.

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

Mode—*See Device Mode.*

MTBF—Mean-Time Between Failures

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

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

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

NTP—Network Time Protocol

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

Passive Scanning—Scanning is a process used by stations to detect other access points on network to which it may connect if it needs to roam. Passive scanning is a slower process in which it listens for information offered by the access points on a regular basis. Active scanning is a faster process in which the station sends out probe message to which the access points respond. Passive scanning can be done while 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 station to connect to an access point from multiple locations without the need to reconfigure the network settings. For example, a remote transceiver that is connected to an access point may be turned off, moved to new site, turned back on, and, assuming the right information is entered, can immediately reconnect to the access point without user intervention.

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

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

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

Remote Terminal Unit—See *RTU*.

RFI—Radio Frequency Interference

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

RSSI—Received Signal Strength Indicator

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

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

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

SNMP—Simple Network Management Protocol

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

SNTP—Simple Network Time Protocol

SSL—Secure Socket Layer

SSH—Secure Shell

STP—Spanning Tree Protocol

Standing-Wave Ratio—See *SWR*.

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

TCP—Transmission Control Protocol

TFTP—Trivial File Transfer Protocol

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

UDP—User Datagram Protocol

UTP—Unshielded Twisted Pair

WINS—Windows Internet Naming Service. Part of Microsoft Windows NT and 2000 servers that manages the association of workstation names and locations with Internet Protocol addresses. It works without the user or an administrator having to be involved in each configuration change. Similar to DNS.

Zone—See *Frequency Zone*.



INDEX

Numerics

100BaseT 137
 10BaseT 137
 802.11b 9

A

Access Point (AP), defined 165
 accessories 16
 Active Scanning, defined 165, 169
 Actual Data Rate 84
 Add Associated Remotes 80
 AgeTime 93
 alarm conditions 126
 correcting 128
 Alarmed 124
 Antenna
 aiming 133
 directional 144
 Minimum Feedline Length versus Antenna Gain 142
 omnidirectional 141
 polarization 140
 selection 140
 SWR check 132
 system gain 165
 system gain vs. power output setting 146
 system gain, defined 165
 Yagi 141

AP

Auto Upgrade 92
 Reboot when Upgraded 92

application

IP-to-Serial 71
 Mixed-Modes 76
 Point-to-Multipoint Serial-to-Serial 73
 Point-to-Point Serial-to-Serial 72
 Serial Port 76

Approved

Access Points/Remotes List 79
 Remotes/Access Points List 80

Associated 124**Association**

Date 92
 defined 165
 Process 91
 Time 92

attenuation 22**Auth Traps Status 50**

Authorization Key 114, 117
 defined 165

Authorized Features 114**Auto Data Rate Menu**

RSSI Threshold/Delta 55
 SNR Threshold/Delta 55

Auto Key Rotation 79**Auto-Upgrade/Remote-Reboot 114****B**

Backhaul
 for Serial Radio Networks 7
 Network 8
 bandpass filter 144
 Beacon
 Period 52, 98, 99
 signal 91
 Begin Wizard 63
 Bit, defined 165
 Bits-per-second (bps), defined 165
 BPDU 96
 defined 165
 BPS, defined 165
 Bytes
 defined 165
 in on port 95
 in on socket 95
 out on port 95
 out on socket 95
 received 89, 90
 sent 89, 90

C**cable**

Ethernet crossover 22
 feedlines 141
 serial 22

Clear

Com# statistics 95
 Ethernet stats 90
 Log 87
 Wireless stats 90

Collocating Multiple Radio Networks 13**Commit Changes and Exit Wizard 65, 67, 68, 70, 71****compression 51, 99****Computer**

host, defined 168
 configuration 23, 65, 66, 68, 69, 70
 basic device parameters 40
 defaults 23
 DHCP server 46
 editing files 112
 Ethernet Port 45
 file 106, 121
 IP address 44
 network 42
 PPP Mode 70
 radio parameters 50
 scripts 105, 106
 security 77
 serial interfaces 60
 SNMP Agent 48
 TCP Mode 67
 UDP mode 64
 Connection Status 91
 connectors 151
 Contact 41

SIMREX Corporation

- cost of deployment 8
- Count 117
- CRC (Cyclic Redundancy Check), defined 165
- CSMA
 - CA, defined 165
 - CD, defined 165
- Current
 - Alarms 87
 - AP IP Address 92
 - AP Mac Address 92
- Custom Data Buffer Size 65, 67, 68, 70, 71

D

- data
 - baud 70
 - baud rate 65, 66, 68, 69
 - buffering 62, 68
 - compression 99
 - rate 51
- Database
 - Logging 44
 - Timeout 44
- Datagram, defined 166
- DataRate 93
- Date 41
 - Format 41
- dB, defined 166
- dBi, defined 166
- dBm
 - defined 166
 - watts-volts conversion 147
- DCE, defined 166
- default gateway 44
- defaults
 - reset to factory 117
- Delete
 - All Remotes 80
 - Remote 80
- Delimiter, defined 166
- deployment costs 8
- Description 41
- Device
 - IP Address 70
 - Mode 38, 42, 43
 - Mode, defined 166
 - Name 38, 41
 - Status 38, 124
- DHCP 44, 45
 - defined 166
 - Netmask 47
 - Server Configuration 43
- Diagnostic Tools 126
- dimensions 137
- DKEY command 132
- DNS Address 47
- DSP (Digital Signal Processing), defined 167
- DTE 10, 60
 - defined 167
- Dwell Time 52, 98
- Dynamic Mode 45

E

- EIA-232 10
- Embedded Management System 23
- Encapsulation, defined 167
- Encryption 79

- Phrase 80
- Ending Address 47
- Endpoint
 - defined 167
 - Listing 85
 - Listing Menu 93
- ENI, SIMREX DATAMOVER ESS 3
- Equalization, defined 167
- Ethernet
 - Address 44
 - Link (H/W) Watch 46
 - Link Poll Address 46
 - Packet Statistics 90
 - port enabled/disabled 46
 - Rate Limit 46
- Event Log 85, 86, 124, 126, 128, 129

F

- Fade Margin 167
- Feedline
 - selection 140, 141
- Filename 88, 101, 105
- firmware
 - installing 102
 - upgrade 101, 115
 - version 39, 41
- Flow Control 63, 65, 67, 68, 69, 70
 - hardware, defined 167
- Force Key Rotation 80
- Force Reboot 115
- Fragmentation
 - defined 167
 - Threshold 52, 98
- Frame, defined 167
- Frequency 116
 - hopping, defined 167
 - zone, defined 167
- fuse replacement 153

G

- gain
 - antenna, defined 165
 - system 145
- Glossary 165–171
- Go 117

H

- Hardware
 - flow control, defined 167
 - Version 39, 41
- Hop
 - Format 53
 - pattern 144
 - Pattern Seed 52
 - Pattern Seed, defined 168
 - Sync 124
- Hopping
 - channels 157
 - frequency, defined 167
 - pattern seed, defined 168
- Host computer, defined 168
- HTTP
 - defined 168
 - Security Mode 79

I

- IANA 61
- IAPP, defined 168
- ICMP, defined 168
- IEEE, defined 168
- IETF standard RFC1213 48
- IGMP, defined 168
- Image
 - Copy 101
 - file, defined 168
 - Verify 101
- ESS-II, differences of 3, 50, 51, 53, 55, 57, 94, 133, 139, 143
- Installation
 - antenna & feedline 140
 - feedline selection 141
 - general information 3
 - planning 137
 - requirements 137
 - site selection 139
 - site survey 143
- Interference 144
- Internet
 - Assigned Numbers Authority 61
 - Control Message Protocol, defined 168
- IP 46
 - Addr 117
 - Address 38, 42, 92, 93, 113
 - address 45
 - Address Configuration 43
 - Address Mode 45
 - Gateway 113
 - Mobile, defined 168
 - Protocol 64, 66, 67, 69, 70
 - tunneling 61

K

- Key
 - transmitter, for antenna SWR check 132
- KEY command 132

L

- LAN 45
 - defined 168
- Latency 99
- Latency, defined 168
- Latest AP Firmware Version 92
- LED
 - COM1 25
 - COM2 25
 - LAN 25, 122
 - LINK 25, 26, 122, 134, 144
 - PWR 25, 86, 88, 122, 126, 129
 - use during troubleshooting 121
- Link Established 71
- Local
 - Area Network, defined 168
 - IP Port 64, 66
 - Listening IP Port 69
- Location 41, 113
- Logged Events 129
- Lost Carrier Detected 90, 125

M

- MAC Address 92, 93, 96
- Management System 23

- user interfaces 29
- Maximum Remotes 43
- MD5, defined 168
- SIMREX DataMover ESS ENI 3
- SIMREX Security Suite 14
- measurements
 - radio 131
- Media Access Controller, defined 168
- MIB
 - defined 168
 - files 48
- Mobile 57
- Mobile Data
 - Beacon Period 59
 - Compression 59
 - configuration 57
 - Dwell Time 59
 - Fragmentation Threshold 59
 - RTS Threshold 60
- Mobile IP, defined 168
- Mobility
 - defined 169
- Mobility Capability 10
- MODBUS 68
- Mode
 - Device, defined 166
 - mixed 75
 - serial gateway interface 10
 - TCP 10
 - UDP 10
- Model Number 40
- MTBF, defined 169
- Multicast
 - IP Address 64
 - IP Port 64
- multiple
 - protocols 8
 - services 8

N

- NEMA 9
- net mask 44
- Network
 - Name 13, 21, 38, 42, 43, 113
 - Name, defined 169
 - Time Protocol (NTP), defined 169
 - wide diagnostics 169
- network
 - maintenance 99
 - operation principles 95
 - performance optimization 98
 - performance verification 84
- network design 11
 - antennas 12
 - collocating multiple radio networks 13
 - network name 12
 - repeaters 11
 - using multiple Access Points 13
 - Using the AP as a Store-and-Forward Packet Repeater 12
 - using two transceivers to form a repeater station 11
- NTP (Network Time Protocol), defined 169

O

- Outgoing Connection's Inactivity Timeout 68
- Owner 41

SIMREX Corporation

P

- Packet
 - defined 169
 - Redundancy Mode 65, 66
 - Size 117
 - Statistics 85, 89, 125
- Packets
 - Dropped 89, 90, 125
 - Received 89, 90
 - Received by Zone 90
 - Sent 89, 90
- Passive Scanning, defined 169
- Password Reset 117
- PC
 - connection to transceiver 22
- Performance Information Menu 98
- PING 21, 26, 143
 - defined 169
- Ping Utility 117
- PLC 9
 - defined 170
- Point-Multipoint System, defined 169
- Point-to-Point
 - LAN Extension 7
 - Link 7
- Poll, defined 169
- port
 - antenna 132
 - COM1 10, 22, 23, 24, 60, 71, 140, 152
 - COM2 10, 24, 60, 71, 152
 - Ethernet 21
 - IP 71
 - LAN 23, 24, 151
 - not Enabled 71
- Portability, defined 170
- ports
 - serial 8
- power
 - how much can be used 143
 - primary 22
 - transmitter power output 132
- PPP 62
- Primary Host Address 67
- Primary IP Port 68
- Programmable Logic Controller 9
- protocol
 - BPDU 96
 - ICMP, defined 168
 - IP 24, 46, 60
 - MODBUS 68
 - PPP 62
 - SNMP 29, 48, 159
 - defined 171
 - SNTP 43, 171
 - STP 96
 - STP, defined 171
 - TCP 60, 61, 67, 71, 75, 99
 - defined 171
 - TFTP 102
 - defined 171
 - UDP 60, 61, 71, 72, 75, 99
 - defined 171
- PuTTY usage 33
 - defined 170

R

- Radio
 - Frequency Interference 14, 144
 - Remote, defined 170
 - Test 115
- range, transmission 9
- Read Community String 49
- Reboot
 - Device 101
 - on Upgrade 115
- Receive errors 89, 90, 125
- Received Signal Strength Indicator 22, 139
 - defined 170
- Redundancy
 - Using multiple Access Points 13
- Remote
 - IP Address 66
 - IP Port 66
 - Listing 85
 - Listing Menu 92
 - Performance Listing 85, 94
 - radio, defined 170
 - Terminal Unit 9
 - Terminal Unit, defined 170
- Repeater 11
 - antennas 12
 - Network Name 12
 - Using the AP as a Store-and-Forward Packet Repeater 12
 - Using two transceivers to form a repeater station 11
- reprogramming 100
- Resetting the Password 117
- Restart DHCP Server 48
- Retries 90, 125
- Retrieve File 101, 106
- Retry errors 90, 125
- RetryEr 94
- RF Output Power 51, 84
- RFI 14
 - defined 170
- Roaming, defined 170
- RSSI 22, 84, 116, 125, 133, 139
 - by Zone 84, 85
 - defined 170
 - Threshold 53
- RTS Threshold 52, 98
- RTS/CTS handshaking 65
- RTU 9, 60, 71, 76
 - defined 170
- RxBMC 94
- RxPkts 94
- RxRate 94
- RxViaEP 94

S

- Save Changes 81
- SCADA 8, 9, 62
 - defined 171
- Scanning 124
 - Active, defined 169
 - Passive, defined 169
- Seamless Inter-Frame Delay 65, 67, 68, 70, 71
- Secondary
 - Host Address 68
 - IP Port 68
- security
 - Approved Access Points/Remotes List 79

- Auto Key Rotation 79
 - encryption 79
 - Encryption Phrase 80
 - Force Key Rotation 80
 - general information 3
 - HTTP Security Mode 79
 - risks 15
 - suite 14
 - Telnet Access 78
 - Two-Way Authentication 78
 - User Password 78
 - Send
 - File 106
 - Log 87
 - Sending LCP Requests 71
 - Serial
 - Configuration Wizard 62
 - Data Statistics 95
 - encapsulation 61
 - Mode 65, 67, 68, 69, 70
 - Number 39, 40
 - Port Statistics 125
 - radio networks, backhaul 7
 - Server Status 47
 - Signal strength 139
 - Signal-to-Noise Ratio 84
 - defined 171
 - Simple Network
 - Management Protocol, defined 171
 - Time Protocol, defined 171
 - Site selection 139
 - Skip Zone, defined 171
 - SNMP 29
 - Config Menu 43
 - defined 171
 - Mode 49, 78
 - traps 162
 - usage 159
 - V3 Passwords 50
 - SNR 53
 - defined 171
 - Threshold 53
 - SNTP 43
 - defined 171
 - Spanning Tree Protocol 96
 - Spanning Tree Protocol, defined 171
 - Specifications 154–157
 - SSH, defined 171
 - SSL, defined 171
 - Standing Wave Ratio 171
 - Starting
 - Address 47
 - Information Screen 40
 - State 93
 - Static IP
 - Address 45
 - Gateway 45
 - Netmask 45
 - Status 38, 64, 66, 67, 69, 70
 - STP, defined 171
 - subnet 45
 - SWR 132, 171
 - defined 171
 - performance optimization 132
 - Syslog Server 88
 - system gain, antenna 165
 - system gain, antenna (defined) 165
 - System Mode 113
- T**
- TCP 10, 61, 75, 99
 - Client 61
 - defined 171
 - Server 61
 - Telnet 71
 - Access 78
 - Test Mode 116
 - TFTP
 - defined 171
 - Host Address 87, 101, 105
 - Time-out 88
 - Timeout 101, 106
 - Time 41
 - Time to Live (TTL) 64
 - Transmission
 - Control Protocol, defined 171
 - range 9
 - transparent encapsulation 61
 - Trap
 - Community String 49
 - Manager 50
 - Manager, defined 171
 - Version 50
 - Troubleshooting 121–131
 - Using the Embedded Management System 122
 - Two-Way Authentication 78
 - TX Output Power 116
 - TxKey 116
 - TxPkt 94
 - TxPkts 94
 - TxViaEP 94
- U**
- UDP 10, 61, 72, 75, 99
 - defined 171
 - mode 64
 - Unit Name 113
 - Uptime 39, 41
 - User Datagram Protocol, defined 171
 - User Password 78
 - Using multiple Access Points 13
 - UTP, defined 171
- V**
- V3
 - Authentication Password 49
 - Privacy Password 49
 - via Remote 93
 - View
 - Approved Remotes 81
 - Current Alarms 88
 - Current Settings 63
 - Event Log 89
 - Log 87
 - volts-dBm-watts conversion 147
- W**
- watts-dBm-volts conversion 147
 - WINS
 - Address 47
 - defined 171

SIMREX Corporation

Wireless

Address 44

Network Status 85, 91

Packet Statistics 89

wizard

serial configuration 62

Write community String 49

Y

Yagi antenna 141

Z

Zone, defined 171

IN CASE OF DIFFICULTY...

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

TECHNICAL ASSISTANCE

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

NY Phone: 716 206-0174 E-Mail: techsupport@simrex.com

AZ Phone: 480 926-6069 Web: www.simrex.com

FACTORY SERVICE

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

If return of the equipment is necessary, you will be issued a Return Merchandise Authorization (RMA) number. The RMA number will help expedite the repair so that the equipment can be repaired and returned to you as quickly as possible. Please be sure to include the RMA number on the outside of the shipping box, and on any correspondence relating to the repair. No equipment will be accepted for repair without an RMA number.

A statement should accompany the radio describing, in detail, the trouble symptom(s), and a description of any associated equipment normally connected to the radio. It is also important to include the name and telephone number of a person in your organization who can be contacted if additional information is required.

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

SIMREX Corporation
(RMA No. XXXXXX)
5490 Broadway St.
Lancaster, NY 14086 USA

When repairs have been completed, the equipment will be returned to you by the same shipping method used to send it to the factory. Please specify if you wish to make different shipping arrangements. To inquire about an in-process repair, you may contact our Manufacturing/Service facility at 716-206-0174 (FAX: 716-204-0476), or via e-mail at techsupport@simrex.com.

SIMREX Corporation
5490 Broadway St.
Lancaster, NY 14086
General Business: +1 716 206-0174
FAX: +1 716 204-0476
Web: www.simrex.com