Operating Manual

SP 2.4E

2.4 GHz Spread Spectrum
Industrial Ethernet Bridge

Revision 1.00, January 10, 2003

SIMREX Corporation
2120 E. Nantuckett Dr.
Gilbert, AZ 85234
Phone: 480.926.6069
Fax: 305.675.7794
www.simrex.com

Warranty

Simrex Corporation warrants that each product will be free of defects in material and workmanship for a period of one (1) year for its products. The warranty commences on the date the product is shipped by Simrex Corporation. Simrex Corporation's sole liability and responsibility under this warranty is to repair or replace any product which is returned to it by the Buyer and which Simrex Corporation determines does not conform to the warranty. Product returned to Simrex Corporation for warranty service will be shipped to Simrex Corporation at Buyer's expense and will be returned to Buyer at Simrex Corporation's expense. In no event shall Simrex Corporation be responsible under this warranty for any defect which is caused by negligence, misuse or mistreatment of a product or for any unit which has been altered or modified in any way. The warranty of replacement shall terminate with the warranty of the product.

Warranty Disclaims

Simrex Corporation makes no warranties of any nature of kind, expressed or implied, with respect to the hardware, software, and/or products and hereby disclaims any and all such warranties, including but not limited to warranty of non-infringement, implied warranties of merchantability for a particular purpose, any interruption or loss of the hardware, software, and/or product, any delay in providing the hardware, software, and/or product or correcting any defect in the hardware, software, and/or product, or any other warranty. The Purchaser represents and warrants that Simrex Corporation has not made any such warranties to the Purchaser or its agents SIMREX CORPORATION EXPRESS WARRANTY TO BUYER CONSTITUTES SIMREX CORPORATION SOLE LIABILITY AND THE BUYER'S SOLE REMEDIES. EXCEPT AS THUS PROVIDED, SIMREX CORPORATION DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PROMISE.

Indemnification

The Purchaser shall indemnify Simrex Corporation and its respective directors, officers, employees, successors and assigns including any subsidiaries, related corporations, or affiliates, shall be released and discharged from any and all manner of action, causes of action, liability, losses, damages, suits, dues, sums of money, expenses (including legal fees), general damages, special damages, including without limitation, claims for personal injuries, death or property damage related to the products sold hereunder, costs and demands of every and any kind and nature whatsoever at law.

IN NO EVENT WILL SIMREX CORPORATION BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, BUSINESS INTERRUPTION, CATASTROPHIC, PUNITIVE OR OTHER DAMAGES WHICH MAY BE CLAIMED TO ARISE IN CONNECTION WITH THE HARDWARE, REGARDLESS OF THE LEGAL THEORY BEHIND SUCH CLAIMS, WHETHER IN TORT, CONTRACT OR UNDER ANY APPLICABLE STATUTORY OR REGULATORY LAWS, RULES, REGULATIONS, EXECUTIVE OR ADMINISTRATIVE ORDERS OR DECLARATIONS OR OTHERWISE, EVEN IF SIMREX CORPORATION HAS BEEN ADVISED OR OTHERWISE HAS KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND TAKES NO ACTION TO PREVENT OR MINIMIZE SUCH DAMAGES. IN THE EVENT THAT REGARDLESS OF THE WARRANTY DISCLAIMERS AND HOLD HARMLESS PROVISIONS INCLUDED ABOVE SIMREX CORPORATION IS SOMEHOW HELD LIABLE OR RESPONSIBLE FOR ANY DAMAGE OR INJURY, SIMREX CORPORATION'S LIABILITY FOR ANYDAMAGES SHALL NOT EXCEED THE PROFIT REALIZED BY SIMREX CORPORATION ON THE SALE OR PROVISION OF THE HARDWARE TO THE CUSTOMER.

Proprietary Rights

The Buyer hereby acknowledges that Simrex Corporation has a proprietary interest and intellectual property rights in the Hardware, Software and/or Products. The Purchaser shall not (i) remove any copyright, trade secret, trademark or other evidence of Simrex Corporation's ownership or proprietary interest or confidentiality other proprietary notices contained on, or in, the Hardware, Software or Products, (ii) reproduce or modify any Hardware, Software or Products or make any copies thereof, (iii) reverse assemble, reverse engineer or decompile any Software or copy thereof in whole or in part, (iv) sell, transfer or otherwise make available to others the Hardware, Software, or Products or documentation thereof or any copy thereof, except in accordance with this

Agreement.

SP 2.4E

2.4 GHz
Spread-Spectrum
Industrial Ethernet Bridge

WARNING

In order to comply with the FCC/IC adopted RF exposure requirements, this transmitter system will be installed by the manufacturer's reseller professional. Installation of all antennas must be performed in a manner that will provide at least 20 cm clearance from the front radiating aperture, to any user or member of the public.

This manual contains information of proprietary interest to Simrex Corporation. It has been supplied in confidence to purchasers and users of the SP 2.4E, and by accepting this material the recipient agrees that the contents will not be copied or reproduced, in whole or in part, without prior written consent of Simrex Corporation.

Simrex Corporation has made every effort to assure that this document is accurate and complete. However, the company reserves the right to make changes or enhancements to the manual and/or the product described herein at any time and without notice. Furthermore, Simrex Corporation assumes no liability resulting from any omissions in this document, or out of the application or use of the device described herein.

Simrex Corporation's products are appropriate are not authorized for utilization in applications where failure could result in damage to property or human injury or loss of life.

The electronic equipment described in this manual generates, uses, and radiates radio frequency energy. Operation of this equipment in a residential area may cause radio interference, in which case the user, at his own expense, will be required to take whatever measures necessary to correct the interference.

FCC Declaration of Conformity

This device 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 Complies with Industry Canada RSS210

SIMREX Corporation
2120 E. Nantuckett Dr.
Gilbert, AZ 85234
Phone: 480.926.6069
Fax: 305.675.7794
www.simrex.com

Manual Revision 1.00, January 13, 2003.

Contents

1. Introduction

1.0 Product Overview

The SP 2.4E is a high-performance wireless ethernet bridge, capable of providing reliable wireless data transfer between all types of equipment which have an ethernet interface. The SP 2.4E operates in the license-free 2400-2483.5 MHz ISM band, and is based on the same frequency-hopping technology found in Simrex Corporation's SP 2.4 product line. This technology has been utilized by Simrex Corporation's customers to provide robust communication in the harshest environments over distances up to 30 miles or more.

A typical application is to bridge remote ethernet PLC's to the LAN. Transparent MAC address filtering ensures that no local ethernet packets are transmitted over the RF channel, thus providing optimal data throughput and seamless integration of the PLC with the network. The ethernet interface is 10Base-T, and is compliant with the IEEE 802.3 standard.

An RS-232 port is used for configuring the operating parameters of the unit. Users have the ability to configure each SP 2.4E as a Master, Repeater or Slave. In addition, several other operating parameters can be modified through this port to optimize for point-to-point or point-to-multipoint communication, and to ensure secure and private data transmission. A diagnostics mode enables the Master to monitor the performance of all remote radios in the system.

1.1 Features

Key features of the SP 2.4E include:

- transmission within a public, license-exempt band of the radio spectrum[1] – this means that it can be used without access fees (such as those incurred by cellular airtime);
- a serial I/O data port allows the user to quickly configure the SP 2.4E's operating parameters.
- Standard IEEE 802.3 10BaseT UTP interface
- 64 sets of user-selectable pseudo-random hopping patterns, intelligently designed to offer the possibility of separately operating multiple networks while providing security, reliability and high tolerance to interference;
- encryption key with 65536 user-selectable values to maximize security and privacy of communications;
- built-in CRC-16 error detection and auto re-transmit to provide 100% accuracy of data;
- ease of installation and use – the SP 2.4E uses a subset of standard AT style commands.

[1] 2400-2483.5 MHz, which is license-free within North America; may need to be factory-configured differently for some countries including operation in Europe.

1.2 About this Manual

This manual has been provided as a guide and reference for installing and using the SP 2.4E. The manual contains instructions, suggestions, and information which will help you set up and achieve optimal performance from your equipment using the SP 2.4E.

It is assumed that users have either system integration or system design experience. Chapter 2 details the SP 2.4E's physical attributes. Chapter 3 explains the different modes of operation. Chapter 4 provides complete details of all configuration parameters; and, Chapter 5 is an installation/deployment guide. The Appendices, including the Glossary of Terms, are provided as informational references which you may find useful throughout the use of this manual as well as during operation.

Throughout the manual, you will encounter not only illustrations that further elaborate on the accompanying text, but also several symbols which you should be attentive to:

Caution or Warning: Usually advises against some action which could result in undesired or detrimental consequences.

Point to Remember: Highlights a key feature, point, or step which is worth noting, Keeping these in mind will make using the SP 2.4E more useful or easier to use.

Tip: An idea or suggestion is provided to improve efficiency or to make something more useful.

With that in mind, enjoy extending the boundaries of your communications with the SP 2.4E.

2. Electrical/Physical

2.1 Connectors and Indicators

The SP 2.4E connects to the users' equipment through a standard 8-pin RJ45 modular jack. Back panel connections are illustrated in Figure 1.

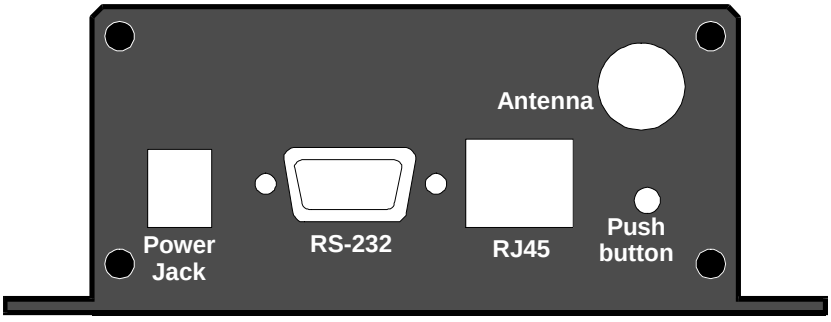


Figure 1 – Back Panel

The interface connectors and indicator lights are described below:

Power Jack - The SP 2.4E supports voltages ranging from 10 to 30VDC through this 2.1mm power jack. You may optionally provide power through pin 9 of the RS-232 port. This option must be specified when purchasing the unit. A built-in switching supply enables the SP 2.4E to maintain excellent power efficiency at all input voltage levels. The power source should be rated for at least 1A at 12V, or 500mA at 24V.

RS-232 Port – Standard female DB9 connector provides RxD, TxD and ground signals for connection to a DTE device. This port is only used for configuring the SP 2.4E. Use a regular straight-through serial cable when connecting this port to your computer or terminal. The Sp 2.4E operates at 2400 to 115,200 bps. The levels are active high RS-232 levels, and include (See Appendix B for a complete description):

Pin No.	Name	Description	I/O
2	RxD	Receive Data	O
3	TxD	Transmit Data	I
5	Gnd	Ground	

RJ45 –This port provides the connection to the ethernet via the 10BaseT medium. Use straight through wiring when connecting to the hub, and crossover wiring when connecting to the station. The pinout is given in Appendix B. Visit simrex.com for cable information and pricing.

Caution: Be sure to observe 10BaseT cabling conventions when connecting to the RJ45 modular jack: Use straight through wiring when connecting the SP 2.4E to the hub; Use crossover wiring when connecting the SP 2.4E to the station. See Appendix B for details.

Pushbutton – Press and release this button to enter configuration mode. You can also enter configuration mode by simply connecting to the RS-232 port and inputting characters. See Chapter 3 for more details.

Antenna - The SP 2.4E uses a reverse polarity TNC connector. Simrex Corporation can provide external cabling and antennas for applications in which the standard Rubber Duck antenna is not suitable.

Figure 2 illustrates the indicators found on the front panel.

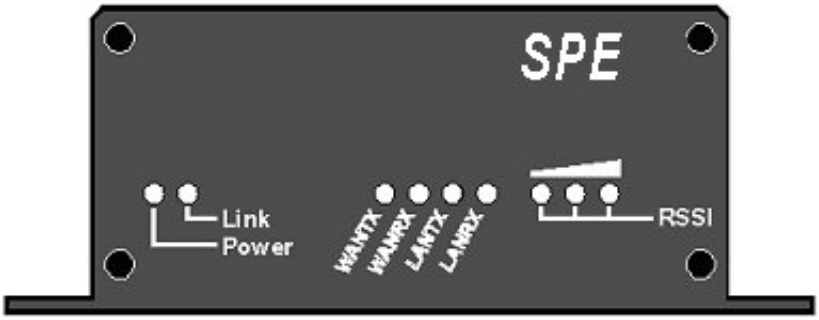


Figure 2 – Front Panel

Power LED - Indicates the unit is powered on.

Link LED - Indicates that there is a correctly wired signal path between the SP 2.4E and the station or hub. If the unit is configured as a slave or repeater, the Link LED won't turn on unless the unit is synchronized to the network AND there is a correctly wired signal path between the SP 2.4E and the station or hub.

WANTX LED - Indicates that data is being transmitted over the air.

WANRX LED - Indicates that data is being received over the air.

LANTX LED - Indicates that data is being sent to the LAN.

LANRX LED - Indicates that data is being received from the LAN.

Receive Signal Strength Indicator (RSSI) -. As the signal strength increases, the number of active RSSI LED's increases, starting with the furthest left.

MODE	RSSI1,2,3
Command Mode	off
Data Mode - Master	RSSI mode based on all received packets See Table 1 on next page
Data Mode - Repeater During Sync. Acquisition	alternating 300ms on
Data Mode - Repeater When Synchronized	RSSI mode based on packets received from Slaves* See Table 1 on next page
Data Mode - Slave During Sync. Acquisition	alternating 300ms on
Data Mode - Slave When Synchronized	RSSI mode based on packets received from the Repeater or Master with which it communicates See Table 1 on next page

*If Slaves have been silent for 2 seconds, repeater will base its RSSI on packets received from the Master.

2.2 Received Signal Strength Indicators (RSSI)

Signal strength, which is also reported in Register S123, is calculated based on the last four valid received packets with correct CRC, and represented by RSSI1, 2 and 3.

For slaves, packets are received on every single hop either from a repeater, or the master.

When calculating RSSI, the master takes into consideration all packets received from slaves and repeaters. Repeaters and slaves only transmit back to the master when they have information to send. Therefore, if no data is coming back to the master then RSSI will never get updated at the master, and the LED's will be off.

Table 1 - RSSI LED operation

Signal Strength (dBm)	RSSI1	RSSI2	RSSI3
-108	50% duty cycle	off	off
-101	on solid	off	off
-93	on solid	50% duty cycle	off
-86	on solid	on solid	off
-79	on solid	on solid	50% duty cycle
-71	on solid	on solid	on solid

2.3 DC Characteristics

Caution: Using any other power supply which does not provide the proper voltage or current could damage the SP 2.4E.

Sym	Characteristic	Min	Typ	Max	Units
V_{CC}	Supply Voltage	10	12	30	V
I_{CCR}	*Supply Current in Receive Mode	224	242	270	mA
I_{CCT0}	*Supply Current at 1mW Transmit	204	232	250	mA
I_{CCT1}	* Supply Current at 10mW Transmit	225	244	263	mA
I_{CCT2}	* Supply Current at 100mW Transmit	275	297	319	mA
I_{CCT3}	* Supply Current at 1W Transmit	448	492	536	mA
V_{IL}	Input Low Voltage (RS-232 pin 3)	-12		-6	V
V_{IH}	Input High Voltage (RS-232 pin 3)	6		12	V
V_{OL}	Output Low Voltage (RS-232 pin 2)	-12	-9	-6	V
V_{OH}	Output High Voltage (RS-232 pin 2)	6	9	12	V

*At 12VDC input

2.4 AC Characteristics

Sym	Characteristic	Min	Typ	Max	Units
T_{TOUT}	Reset Delay Time-Out Period		500		ms
T_{R2D}	Internal Reset to Data Mode		200		us

Figure 3 provides timing information for power-up reset. A fixed internal reset delay timer of roughly 500ms is triggered as the V_{POT} is reached.

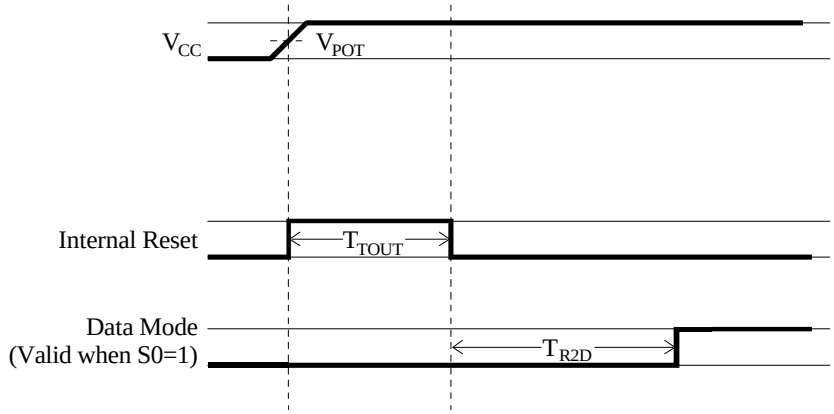


Figure 3. Reset Timing

3. Modes of Operation

The SP 2.4E can be easily configured to meet a wide range of needs and applications. The unit is designed such that all ethernet data is transferred through the RJ-45 port, and all configuration data is sent/received through the serial (RS-232) port.

The SP 2.4E will always be in one of three basic modes: **data mode**; **command mode**; and, **diagnostics mode**.

3.1 Data Mode

Data mode is the normal operating mode of the SP 2.4E. When in data mode, the SP 2.4E is communicating with other SP 2.4E's, and facilitating wireless ethernet communication amongst two or more ethernet-equipped computers. There are three basic elements to any SP 2.4E communications network:

? One unit configured as the **Master**

? Zero or more units configured as **Repeaters**

? One or more units configured as **Slaves**

The function of the Master is to provide synchronization for the entire network, and to control the flow of data. There is always one Master per network. When the units are not in peer to peer mode, the Master is the ultimate destination for all ethernet packets collected at the various repeaters and slaves in the network. With the network set up for Point-to-Multipoint communication, the Master broadcasts its ethernet packets to all repeaters and slaves in the system. The SP 2.4E is a frequency hopping transceiver, meaning that it "hops" to a new frequency after a predetermined time interval. This time interval is a fixed time of either 30 or 45 ms, depending on the absence or presence of repeaters in the system. The SP 2.4E hops according to a pseudorandom pattern of 76 different channels.

When configured as a Slave, the SP 2.4E searches for synchronization with a Master. Network topologies consisting of a single *Master* and virtually any combination of *Slaves* and *Repeaters* may be deployed. In additional, the system can be configure as a peer to peer network. The functionality of any particular SP 2.4E can be configured in the following network topologies:

- **Master Point-to-Point**: The unit is configured to communicate with a single *Slave*, either directly, or through one or more *Repeaters*.
- **Master Point-to-Multipoint**: The unit is configured to communicate with one or more *Slaves* and/or *Repeaters*.
- **Master Peer-to-Peer**: In this mode, the master sets the entire system into a peer-to-peer configuration including slaves and repeaters. In this mode data sent from one unit is received by all other units.
- **Slave**: The unit is configured to communicate with one *Master* either directly or through one or more *Repeaters.*
- **Repeater**: The unit is configured to pass information from either a *Master* or another *Repeater* onto subsequent *Repeaters* and/or *Slaves* and vice versa. The *Repeater* also acts as a *Slave* in the sense that, like a *Slave*, it is capable of sending/receiving ethernet packets through its RJ-45 port.

Examples of different network topologies are shown in Figure 4. Network 1 shows Point-to-Point communication between a Master and Slave. Network 2 makes use of a Repeater to communicate with the Slave. Network 3 illustrates a simple Point-to-Multipoint network with no Repeaters. Networks 4 and 5 give examples of Point-to-Multipoint networks consisting of both Repeaters and Slaves. There is effectively no restriction to the number of Repeaters and Slaves that can be added to a network. As seen in Network 4, a Master can communicate directly with both Slaves and Repeaters. Network 2 to Network 5 can all be configured in peer-to-peer mode by simply changing the master.

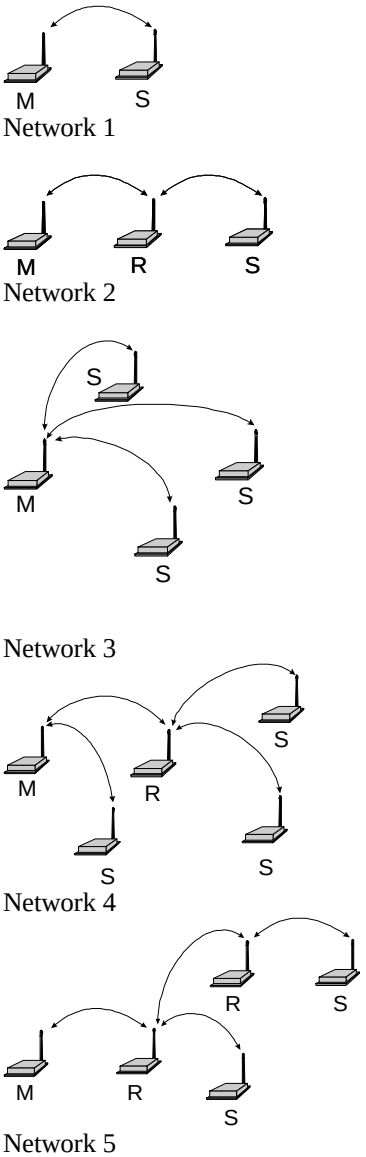


Figure 4 - Sample Network Topologies. Virtually any Combination of Slaves and Repeaters May be Used.

3.2 Command Mode

The SP 2.4E firmware has been designed to allow the user to customize operation through an AT Command Interface. This interface is ideal for direct interface with any terminal device or for higher level Windows-based software applications, but also contains user-friendly built-in register descriptions. These descriptions make it easy for the user to configure the unit by manually inputting AT Commands and modifying S-Register parameters, using any standard terminal program. To access the SP 2.4E's command mode:

1. Attach the supplied antenna.
2. Connect a straight through serial cable between the DB9 connector and the serial port on your PC
3. Run any terminal application program such as Hyperterminal
4. Set the terminal's serial port to any baud rate between 2400 and 115200 baud, 8N1, no flow control
5. Apply power to the SP 2.4E
6. Type 'at' <ENTER> two or three times until you see the response 'OK'. The first few characters that you type simply alert the unit that you wish to go into command mode. Type 'AT&V <ENTER>'

3.2.1 AT Command Interface

At this point you should see a menu similar to the following appear:

```
Operating Mode          S101=3
Repeaters Yes/No        S205=1          Network Address         S104=1
Unit Address            S105=1          Hop Pattern             S106=0
Encryption Key          S107=1          Output Power            S108=2
Packet Retransmissions  S113=0
Roaming                 S118=0
Remote Control          S122=0
Average RSSI value       S123=-0 dBm
Secondary Hop Pattern   S206=2          Packet Retry Limit      S213=2
OK
```

The SP 2.E is configured through an AT Command line interface using a command set which is very similar to a traditional Hayes telephone modem command set.

All line entries must be preceded by the characters 'AT'. The characters 'AT' are known as the attention characters and must be typed at the beginning of each command line. For example, to change the operating mode, type:

ATS101=2 <ENTER>

The unit should respond with 'OK.' The above command will set the operating mode to Master Point-to-Point.

Register settings are not immediately stored to non-volatile memory. Therefore if the unit is powered down at this point, the operating mode would revert to its previous value. To store any recently updated command registers, the following "write" command must be entered.

AT&W <ENTER>

3.3 Switching Between Command and Data Modes

Your SP 2.4E must be in **command mode** for it to execute a command. If you send characters when the unit is in **data mode**, the first few characters will be disregarded. To ensure you are in command mode, type 'at' <ENTER> two or three times until you get a response <OK>. It is important to note that any activity on the serial port will put the unit into command mode. Therefore, when the unit is running in normal data mode, it is recommended to have the serial port disconnected.

The terminal should be set between 2400 and 115200 baud 8N1, No Flow Control. In command mode, the SP 2.4E "autobauds," meaning that it will adapt to the baud rate of the DTE equipment to which it is connected.

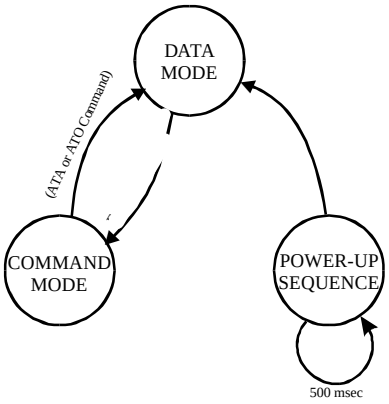


Figure 5. State Diagram

You can place the unit into data mode from command mode either by:

? Issuing the answer command (ATA <ENTER>); or,

? Issuing the online command (ATO <ENTER>).

These two commands are functionally identical. The SP 2.4E will now attempt to communicate with other SP 2.4E's.

To return to command mode, either:

? Press and release the pushbutton on the back of the unit, and then type 'at' <ENTER>. You should see the response 'OK'; or,

? Type several characters followed by 'at' <ENTER>. You should see the response 'OK'. The SP 2.4E looks for toggling of the RS-232 TxD line. Two or three characters is usually enough to trigger the unit into command mode.

Figure 5 provides a state diagram for power-up, command mode, and data mode.

3.4 Diagnostics Mode

The SP 2.4E has a useful tool for analyzing the performance of the network. From the master, you can remotely retrieve information from all repeaters and slaves in the system. You may also modify some of the operating parameters on remote slaves and repeaters. Diagnostic commands are described in greater detail in Section 4.4. Only the master may go into diagnostics mode.

To enter diagnostics mode:

1. Enter command mode in the usual manner;
2. Change the operating mode to diagnostics by typing: 'ATS101=5' <ENTER>
3. Type 'ATA' or 'ATO' <ENTER>

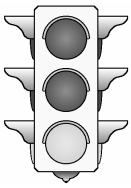
To exit diagnostics mode and go into data mode reset the modem or toggle the power.

See Section 4.4 for a description of the diagnostic commands.

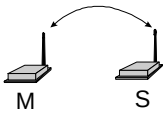
4. Configuration

This chapter provides a detailed description of the various operating parameters of the SP 2.4E. Section 4.1 provides a quick-start approach which outlines the minimum requirements for establishing communication between two SP 2.4E's. The settings will not necessarily provide optimal performance for your application, but will verify that the units are functioning correctly.

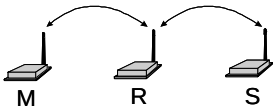
Section 4.2 describes the AT Command interface, and the various AT Commands. Section 4.3 covers all S-Register parameters which affect the operation of the unit, and Section 4.4 provides a description of all diagnostic features of the SP 2.4E.



Warning: After testing the units for correct operation using the quick-start approach, be sure to modify some of the security parameters such as Network Address and Encryption Key, to avoid unintentional communication with other users of SP 2.4E products.



Network 1



Network 2

Figure 6. Basic Networks

4.1 Quick Start Approach

There are several parameters that must be set in order to establish communication between a pair of SP 2.4E's.

The SP 2.4E is equipped with four standard factory default settings. Instead of manually configuring each individual operating parameter, a global command may be used to quickly configure the unit for a particular type of operation. For example, to quickly implement Network 1, apply Factory default 1 to the Master, and Factory default 2 to the Slave. To quickly set up Network 2, apply Factory 1 to the Master, Factory 3 to the Repeater, and Factory 4 to the Slave. *These defaults will get you started and only ensure that a link can be established, but do not necessarily provide the best performance.* Optimization of the communications link is discussed in later sections.

To implement the basic network illustrated in Figure 6, Network 1,

1. Attach the supplied antenna.
2. Connect a straight through serial cable between the DB9 connector and the serial port on your PC
3. Connect a 10BaseT cable between the SP 2.4E and the ethernet equipment. See Appendix B for cabling information.
4. Run any terminal application program such as Hyperterminal and set the terminal application's serial port settings between 2400 and 115200 baud, no flow control, 8N1.
5. Apply power
6. Type several characters followed by 'at' <ENTER>. The unit should respond with 'OK'.
7. Configure the unit to Factory Setting 1 by typing AT&F1 <ENTER>. This puts the unit into Master Point-to-multipoint mode.
8. Store these settings to memory by typing AT&W <ENTER>.
9. Put the unit into Data Mode by typing ATA (or ATO) <ENTER>
10. Perform above steps for the second unit, using Factory Setting 2 instead of Factory Setting 1. This will configure the second unit as a Slave.

The units should now be communicating. Be sure to modify the network address and/or the encryption key on both the master and slave units to ensure your SP 2.4E's don't inadvertently communicate with other SP 2.4E's that might happen to be in the same vicinity. A complete summary of the settings defined by all four factory settings can be found in Appendix C. Factory Default Settings.

For successful communication, all units in a network must have the same network address and encryption key

Settings are not immediately stored in non-volatile memory, therefore, the command &W is issued to store the current configuration into non-volatile memory. Settings are retained even after powering down. All user selectable parameters for the SP 2.4E are described in detail in Sections 4.2 and 4.3:

Checking the Link

To check if the units are communicating, observe the LED indicators. In general, if both the Master's and Slave's LINK LED's are ON, then the units should be able to communicate. If the link is good, up to three RSSI LEDs on the Slave should be active. The Slave's LINK LED will also be ON provided the SP 2.4E is correctly connected to the ethernet equipment., and if the link is absent (due to a fault at one end or another, such as misconfiguration), the RSSI LED's will be in either "scanning mode" or OFF. See Section 2.2 for complete LED operation.

The Master's RSSI LED's will not turn on until data is received over the air. The Master's LINK LED should turn on the instant the ethernet cable is plugged into the RJ-45 connector.

As ethernet packets are sent back and forth, you should see activity on the WANTX, WANRX, LANTX and LANRX LED's. Also, one or more of the Master's RSSI LED's will turn on as it receives data from the slave.

It is recommended that if the SP 2.4E will be deployed in the field where large distances separate the units, the units should be configured and tested in close proximity (*e.g.*, in the same room) first to ensure a good link can be established and settings are correct. This will facilitate troubleshooting, should problems arise.

4.2 AT Commands

Several AT Commands are supported by the SP 2.4E. These commands affect the operation of the unit in command mode and the transition between data and command modes. More commands and S-Register settings are discussed in Sections 4.3 and 4.4.

To make the command line more readable, you can insert as many spaces as desired. The command line holds up to 16 characters, not including the AT prefix. If you want to send more than one command line, wait for a response before entering the AT prefix at the start of the next command line.

To re-execute the previous command, enter A/. The unit will execute the previous command line. When in Command Mode, the SP 2.4E "autobauds", meaning that it will automatically adjust to the baud rate of the terminal. You may change the terminal baud rate while in Command Mode without losing communication with the unit.

The following is a description of all available commands. '*' denotes standard factory settings. All of the following commands must be preceded by "AT".

A Answer

Refer to Appendix A for a summary of the commands

The A command puts the unit into data mode, where it attempts to communicate with other compatibly configured SP 2.4E's (Type ATA <ENTER>).

Dxxxxx, DTxxxxx, DPxxxxx Dial

The D, DT or DP are identical commands which change the unit address to **xxxxx** and puts the unit into data mode (Type ATDxxxxx <return>).

I Identification

The 'I' command returns various information settings.

I0=	String up to 16 characters stored in non-volatile memory
I2	Issue ROM Check (OK or ERROR)
I3	Product Identification (Firmware Version)
I4	Firmware Date
I6	Firmware Time
I7	Serial Number

O On-line Mode

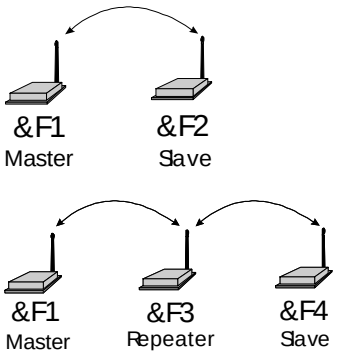
The O command puts the unit into data mode. This command is identical to the A command.

Z Reset and load stored configuration

The Z command resets the unit and loads the stored configuration.

&F Load Factory Default Configuration

The &F command resets the SP 2.4E and loads the default factory configuration.



&F1	Master Point-to-Multipoint. Designed to communicate with units configured as &F2 or &F3.
&F2	Slave. Designed to communicate with another unit configured as &F1.
&F3	Repeater. Designed to communicate with units configured as &F1 and &F4.
&F4	Slave working with factory default Repeater and factory default Master. Communicates directly with Repeater configured as &F3.

&V View Configuration

The &V command displays all S registers and their current values.

&W Write Configuration to Memory

Configuration options are not stored in non-volatile memory until the WRITE command (&W) is executed

The &W command stores the active configuration into the unit's non-volatile memory.

Sxxx? Read S register value

This command causes the SP 2.4E to display the current setting of S register xxx.

Sxxx=yyy Set S register value (see section 4.3 S-Registers)

This command sets the specified S register to a value specified by yyy.

Refer to Appendix A for a summary of the S-Registers.

4.3 S Registers

The S Registers described in this section affect the operating characteristics of the SP2.4E.

Only one Master can exist for each network.

S Register 101 - Operating Mode

The Operating Mode (register S101) partly defines the "personality" of the SP 2.4E. Allowable settings for this register are 1 through 6 as follows:.

? S101=1 Master Point to Multipoint
? S101=2 Master Point to Point
? S101=3 Slave
? S101=4 Repeater
? S101=5 Master - Diagnostics (see Section 4.4)
? S101=6 Master – Peer to Peer mode

The default for this register depends on which factory default is selected as shown below:

? Default for Factory Setting &F1 is 1 (Master Point-to-Multipoint)
? Default for Factory Setting &F2 is 3 (Slave)
? Default for Factory Setting &F3 is 4 (Repeater)
? Default for Factory Setting &F4 is 3 (Slave)

1)Master - Point to Multipoint. In any given network, there is always only one Master. All other units should be configured as either Slaves or Repeaters. When defined as a Point-to-Multipoint Master, the unit broadcasts all ethernet packets to all Slaves and Repeaters in the network, and is also the ultimate destination for data transmitted by all Slaves and Repeaters. Simrex Corporation uses a proprietary channel reservation scheme in Point to Multipoint that avoids collisions over the air. This improves the throughput and bandwidth efficiency of the overall system.

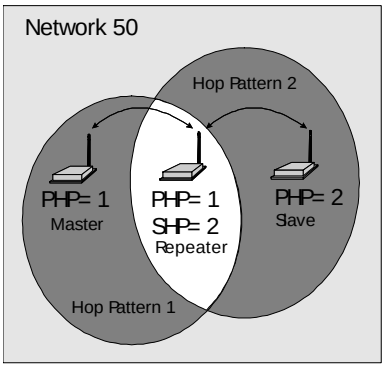


Figure 7 - Repeater Operation

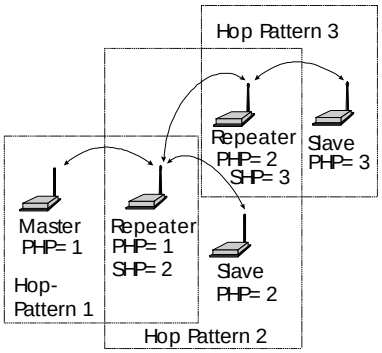


Figure 8 - A Network Utilizing Three Hopping Patterns

2)Master - Point to Point. This mode of operation provides for communication between the master and a single repeater or slave. The master will communicate only with the slave or repeater which shares a common unit address with the master. For example, if a Slave has been assigned Unit Address 100, and the Master wishes to communicate with that Slave, the Master's unit address must also be set to 100. If there are Repeaters in the network, they will pass the packet through to the Slave, and vice versa. Because Repeaters also have Slave functionality (i.e., a Repeater can be connected to a terminal), the Master can choose to communicate solely with a Repeater. This would be accomplished by assigning the same Unit Address to both the Master and the Repeater.

3)Master – Peer to Peer. This mode of operation provides for communication between the all the units in the system. Data will be sent from every slave, every repeater, and the master to every unit on the network. In other words, in Peer to Peer mode any slave can communicate with any other slave, repeater, or the master, and vise-versa. In this mode, of operation the unit address range limited from 1 to 200. This mode is also known as a Multipoint to Multipoint mode.

4)Slave. Up to 65535 Slaves may exist in a network, all of which communicate with the common Master (either directly or via Repeater(s)). Slaves cannot directly communicate with other slaves unless the master is in peer to peer mode.

5) Repeater. A more precise title would be Repeater/Slave, because a Repeater also has much of the same functionality as a Slave. A station can be connected at the Repeater location and communicate with the Master station. There is no restriction to the number of Repeaters in a network, allowing for communication over virtually limitless distances. The presence of one Repeater in a network automatically degrades system throughput by half. Additional Repeaters, regardless of the quantity, do not diminish system throughput any further. To understand Repeater operation, consider the SP 2.4E as belonging to two hopping patterns at the same time: The Primary Hopping Pattern and the Secondary Hopping Pattern. In Figure 7, the Master belongs to Hopping Pattern 1, and communicates with the Repeater on this hopping pattern. The Slave belongs to Hopping Pattern 2, and communicates with the Repeater on this hopping pattern. The whole system belongs to Network 50 (i.e., all units must be assigned the same Network Address (S104), which in this case was selected to be 50. Note that Slaves and Master only communicate on their respective Primary Hopping Pattern. Repeaters communicate on the Primary Hopping Pattern when communicating with the Master (or with another Repeater between itself and the Master). Repeaters communicate on their Secondary Hopping Pattern when communicating with Slaves (or with another Repeater between itself and the Slaves). Figure 8 shows another example.

S Register 104 - Network Address

The Network Address defines the network membership to which individual units can be a part of. By establishing a network under a common Network Address, the network can be isolated from any other concurrently operating network. As well, the Network Address provides a measure of privacy and security. Only those units which are members of the network will participate in the communications interchange. Valid values for the Network Address range from 0 to 65535, inclusive.

To enhance privacy and reliability of communications where multiple networks may operate concurrently in close proximity, it is suggested that an atypical value be chosen – perhaps something meaningful yet not easily selected by chance or coincidence.

Select a Network Address and assign it to all units which will be included in the network.

Default is 1.

Warning: Simrex Corproation strongly recommends changing the Network Address to a value different from the factory default before deploying the network.

S Register 105 - Unit Address

In point-to-point operation, the Unit Address on both the Master and Slave (or Repeater) units must be the same. In a multipoint system, the Unit Address uniquely identifies each Slave and Repeater from one another. Each unit in a multipoint system must have a unique Unit Address ranging from 1 to 65535. Do not use 0 as a Unit Address, and do not use a Unit Address more than once within the same Network. This is required because the Master must be able to acknowledge each unit individually, based on the Unit Address.

Use the same Unit Address on both units for point-to-point mode. In multipoint mode, set each Slave and Repeater to a different Unit Address.

Valid Unit Addresses are 1 to 65535.

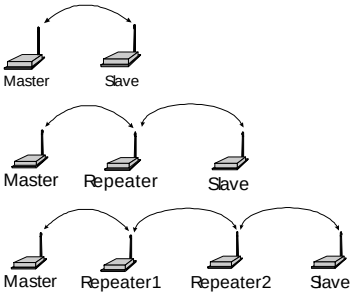
S Register 106 - Primary Hopping Pattern
S Register 206 - Secondary Hopping Pattern

Since the SP 2.4E is a frequency-hopping modem, the carrier frequency changes periodically according to one of 49 pseudo-random patterns, defined by the Primary and Secondary Hopping Patterns. Valid entries for each are 0 through 48.. Patterns 44 through 48 are user-editable patterns. See Appendix F for details.

The concept of Primary and Secondary Hopping Patterns was introduced in the discussion of S Register 101 (Operating Mode).

Using the designations M[a,] Rx[a,b] and Sx[a] where:
- *M* indicates Master;
- *R* indicates Repeater;
- *S* indicates Slave;
- *x* is the Unit Address;
- *a* is the primary hopping pattern; and,
- *b* is the secondary hopping pattern;

the following diagrams illustrate the methodology for deploying simple to complicated networks:



M[1] ? ? S1[1]

M[1] ? ? R1[1,2] ? ? S2[2]

M[1] ? ? R1[1,2] ? ? R2[2,3] ? ? S3[3]

M[1] ? ? R1[1,2] ? ? R2[2,3] ? ? R3[3,4] ? ? S4[4]

It is reasonable to consider a Repeater as being both a Slave and a Master, alternating between Primary and Secondary Hopping Patterns as the unit changes channel. Consider R1 in the illustration below. When communicating with the Master, R1 is acting like a Slave on Primary Hopping Pattern 1. When communicating with R2 and S4, R1 is acting like a Master on Secondary Hopping Pattern 2. If multiple Repeaters are used, they should have different Secondary Hopping Patterns:

Slaves and Masters do not use Secondary Hopping Patterns

M[1] ? ? R1[1,2] ? ? R2[2,5] ? ? S3[5]
? ? S4[2]
? ? R5[1,3] ? ? R6[3,6] ? ? S7[6]
? ? R8[1,4] ? ? S9[4]

Note that all units have a unique Unit Address.

Remember to assign a unique Unit Address (1 to 65535) to each unit in the system

Networks of any complexity can be created by linking multiple Repeaters and Slaves:

M[1] ? ? R1[1,2] ? ? S2[2]
? ? S3[2]
? ? R4[1,3] ? ? R5[3,6] ? ? S6[6]
? ? S7[6]
? ? R8[3,7] ? ? R9[7,8] ? ? S10[8]
? ? S11[1]
? ? S12[1]

With a limitation of 49 hopping patterns, one might suspect that there is a limitation to the number of repeaters in a system. However, if the units are far enough away from one another, hopping patterns may be reused in different sections of the network, without causing interference.

S Register 107 - Encryption Key

All units within a network must use the same encryption key.

The Encryption Key provides a measure of security and privacy of communications by rendering the transmitted data useless without the correct key on the receiver. Valid Encryption Keys range from 0 to 65535.

Keep in mind that all units within the network must use the same key for communications to succeed.

Warning: Simrex Corporation strongly recommends changing the Encryption Key to a value different than the factory default before deploying the network.

S Register 108 - Output Power Level

The Output Power Level determines at what power the SP 2.4E transmits. The SP 2.4E's sensitive receiver can operate with very low power levels, so it is recommended that the lowest power necessary is used; using excessive power contributes to unnecessary "RF pollution".

The allowable settings are:

0	10 mW	4	500 mW
1	50 mW	5	750 mW
***2**	**100 mW**	6	1 W
3	250 mW		

WARNING

In order to comply with the FCC/IC adopted RF exposure requirements, this transmitter system will be installed by the manufacturer's reseller professional. Installation of all antennas must be performed in a manner that will provide at least 20 cm clearance from the front radiating aperture, to any user or member of the public.

Modems with output power limited to 100mW can be purchase in compliance with different country radio regulations. SP 2.4E is standard 1W maximum output and SP 2.4E with CE approval is standard 100mW maximum output. Your maximum power setting will be shown on your unit's identification sticker.

Ideally, you should test the communications performance between units starting from a low power level and working upward until the RSSI is sufficiently high and a reliable link is established. Although the conditions will vary widely between applications, typical uses for some of the settings are described below:

Power	Use
10 mW	For in-building use, typically provides a link up to 300 feet on the same floor or up/down a level. Outdoors, distances of 10 km can be achieved if high-gain (directional) antennas are placed high above ground level and are in direct line-of-sight.
50 mW	200-500 ft indoors, 8-15 km* outdoors.
100 mW	400-800 ft indoors, 15-25 km* outdoors.
1000 mW (1 W)	Typically provides communications up to a distance of 1000 feet or more in-building on the same floor or up/down a few levels, depending on building construction (wood, concrete, steel, etc.). In ideal line-of-sight conditions, up to 30 km* or more can be achieved. Note that only an antenna with a gain of no more than 6 dBi may be used. Any higher is a violation of FCC rules. See IMPORTANT warning below.

* These outdoor distances assume antennas are mounted at least 100 ft above ground level.

IMPORTANT:

FCC Regulations allow up to 36 dBi effective radiated power (ERP). Therefore, the sum of the transmitted power (in dBm), the cabling loss and the antenna gain cannot exceed 36 dBi.

1 mW = 0 dBm

10 mW = 10 dBm

100 mW = 20 dBm

1000 mW = 30 dBm

For example, when transmitting 1 Watt (30 dBm), with cabling losses of 2 dB, the antenna gain cannot exceed 36 - 30 + 2 = 8 dBi. If an antenna with a gain higher than 8 dBi were to be used, the power setting must be adjusted appropriately. Violation of FCC regulations can result in severe fines.

S Register 113 - Packet Retransmissions

Packet Retransmissions refers to the radio packets, NOT to the ethernet packets. All ethernet packet retries and retransmissions are taken care of by the IEEE 802.3 ethernet protocol.

Simrex Corporation recommends setting the Packet Retransmissions to 0. In excessively noisy RF environments, you may need to change this parameter.

This register applies to both Master and Repeater operation. It does not apply to Slave operation. In point-to-multipoint mode, the Master will retransmit each radio data packet exactly the number of times defined by the Packet Retransmissions parameter. This parameter does not refer to the ethernet data packet. The SP 2.4E internally breaks down the ethernet packets into radio packets. In almost all situations, you should set S113=0 (no retransmissions). The IEEE 802.3 ethernet protocol will take care of any necessary retransmissions. Setting this parameter to a non-zero value will cause a significant reduction in throughput in most situations. In very noisy RF environments, you may want to increase this parameter slightly. In point-to-point mode, the Master will only retransmit the packet if it does not get an acknowledgement from the slave with which it is communicating. In point-to-point mode, you may safely set this parameter to a non-zero value.

Note that in this case, the Master will continue to retransmit until an acknowledgement is received, or the retransmission limit is reached. When the retransmission limit is reached, the Master discards the packet. The Master retransmits once at the beginning of each hopping interval. As discussed previously, the Repeater effectively behaves as both a Master and a Slave. When the Repeater is tuned to its Secondary Hopping Pattern (acting as a Master), the Packet Retransmissions Parameter comes into play. The Repeater will re-send packets of data on to Slaves or other Repeaters exactly the number of times defined by the Packet Retransmissions parameter.

Recipients of the packet will discard any duplicates. Valid settings for this parameter are 0 to 255 retransmissions. The default is 0.

Packet Retry Limit refers to the radio packets, NOT to the ethernet packets. All ethernet packet retries and retransmissions are taken care of by the IEEE 802.3 ethernet protocol.

S Register 213 - Packet Retry Limit

Packet Retry Limit is analogous to Packet Retransmissions, but specifically applies to Slaves and Repeaters. This parameter is not used by the Master. Because the Slave has the advantage of receiving acknowledgements from the Master, it is not necessary to blindly retransmit each packet. If the Slave does not get an acknowledgement on the next hop, it will retransmit its packet. This will continue until the Packet Retry Limit is reached or an acknowledgement is received. If the limit is reached, the unit will give up and discard the data. Valid settings are 0 to 255 retries. The default value is 2.

The Repeater makes use of this parameter when it is tuned to its Primary Hopping Pattern and is acting like a Slave.

S Register 118 - Roaming

This mode is activated on slaves and repeaters by setting register S118=1. In this mode, a slave/repeater looks for synchronization with a Master or repeater having the same network address and encryption key, but without regard for the hopping pattern S106. Once the slave/repeater finds such a master or repeater, it tunes to that master's/repeater's hopping pattern. If synchronization is lost, the slave/repeater will again begin searching for a new master/repeater. Using this algorithm, a mobile unit can 'roam' and automatically synchronize with a new master once it loses communication with the previous one. See Appendix F. The allowable settings for this register are:

***0 Disabled**
1 Enabled

S Register 122 - Remote Control

This register either disables or enables remote control at a repeater or slave unit. When disabled, a slave/repeater's settings may be remotely read by the master, but may not be remotely modified. When enabled, the slave/repeater allows the network master full remote control access. See Section 4.4.3 for details. The default is 0 - disabled.

S Register 123 - RSSI Reading

This register displays the average signal strength in dBm over the previous four hop intervals. The value in this register is also reflected in status lines RSSI1,2 and 3. See Section 2.2 for a description of RSSI, and how it is derived.

S Register 205 - Repeaters Yes/No

Set the Master's S205=1 for systems that include repeaters. Set the Master's S205=0 for systems that do not include repeaters.

4.4 Diagnostics, Statistics and Remote Control

The SP 2.4E provides several commands which are very useful for troubleshooting and analyzing the performance of the radio system.

4.4.1 Spectrum Analyzer Feature (ATG)

The command ATG <ENTER> causes the SP 2.4E to perform a sweep of the entire operating spectrum, giving a signal strength read-out in dBm for each channel as shown below:

```
Noise level, '*'- mean value, '.'- max value
ch 1  -138dBm   *
ch 2  -139dBm   *
ch 3  -139dBm   *
ch 4  -139dBm   *
ch 5  -139dBm   *
ch 6  -139dBm   *
ch 7  -130dBm   *
ch 8  -116dBm   *
ch 9  -135dBm   *
...
ch 201 -135dBm  *
ch 201 -135dBm  *
```

Channel 1 is at frequency 2401.6 MHz, with all subsequent channels in 400 kHz increments.

When deploying a network, the spectrum analyzer feature is useful for determining which parts of the ISM band may be noisy. This knowledge can be used to select an appropriate hopping pattern, or for creating a custom hopping pattern which avoids those frequencies.

4.4.2 Statistics (ATP)

The ATP <ENTER> command provides a list of several statistics as follows:

```
# of data packets sent = 0
# of data packets received = 0
# of Slave's retries = 0
# of Slave's packets dropped = 0
# of Slave's sync errors = 0
# of CRC errors = 0
OK
```

The SP 2.4E starts the statistics count at zero each time the unit is powered up, or after the ATP command has been issued. Entering the ATP command clears all statistics back to zero. The maximum limit for each statistic is 65535.

4.4.3 Remote Control and Diagnostics (S101=5)

This is a very powerful tool which allows users to remotely configure and interrogate all units in a multipoint system from the Master unit. Users can set the unit address of the master to match that of the slave/repeater of interest, set S101=5, go online, and interrogate/modify virtually all parameters of the remote repeater/slave unit. It should be noted that when the master goes online, all other units belonging to the network will synchronize with the master, but only the unit whose unit address matches the master's will respond to the master's diagnostic commands.

In addition, in diagnostics mode, the master can change its unit address 'on-the-fly,' avoiding the delays of going into command mode, modifying the unit address, going back online and re-synchronizing with the entire network, before interrogating a new slave/repeater. The master's unit address can be changed while still maintaining synchronization with the entire network, allowing for quick and efficient diagnostic sessions with all remote units. Ensure that register S122=1 on any slave/repeater that you wish to remotely modify.

Table 4 provides a diagnostics command summary. The first column is a list of commands that may be issued at the master. The second column is the corresponding remote register. In general, any command issued without any additional parameters is a read command. For example, if you type:

0 <ENTER>

The remote slave/repeater will send back the value if its S101 register. On the Master terminal screen, you would see:

0 (this is the 0 that you typed, echoed back locally)
3 (this indicates that the remote's S101=3)

If you type:

04 <return>

This command would change the remote's operating mode to S101=4 (repeater). The remote unit should return 'OK'. Remember, if the remote's S122=0 (remote control disabled), the remote will respond with 'ERROR'. In Table 4, Column 1, the meanings of the format is as follows:

COMMAND	A command without (x) indicates that you may not add any additional parameters. i.e., you may only read back the value of the remote's register. You may not modify that register. The only exception to this is the WRITE command '**e'**. Type '**e'** to force the write command (&W) at the remote unit.
COMMAND(x)	Indicates this command may be sent with or without a parameter. Issuing this command without a parameter reads the corresponding remote's register. Issuing this command with the additional parameter 'x' changes the corresponding remote's register to 'x'. Remember, any changes you wish to retain in the event of a powerdown or reset should be stored to non-volatile memory by issuing the write command 'e'.

Table 4 - Remote Control and Diagnostics

Command	Remote Register	Description
0(x)	S101	Operating Mode
2(x)	S108	Output Power
9(x)	S213	Retry Limit
a	test string	Read back 'OK' from remote
e	&W	Write
f	S123	RSSI
g(x)	S104	Network Address
h(x)	S106	Hopping Pattern
I(x)	S206	Secondary Hopping Pattern
j(x)	S113	Retransmissions
k1	statistics	Read # of data packets sent
k2	statistics	Read # of data packets received
k3	statistics	Read # of Slave's retries
k4	statistics	Read # of Slave's packets dropped
k5	statistics	Read # of Slave's sync errors
k6	statistics	Read # of CRC errors
k255	statistics	Clear statistics
m(x)	S118	Roaming

As mentioned previously in this section, there are some settings that can be changed to the master's own registers while in diagnostics mode. The most useful is the unit address. By changing the master's unit address to that of another slave in the network while in diagnostics mode, users can quickly interrogate/modify many different slave's settings without the delays associated with switching between command and data modes. The commands which apply to the master's own registers are shown in Table 5.

Table 5 - Master Diagnostics Commands

Command	Master Register	Description
r(x)	S105	Unit Address
s	S101	back to normal operating mode
u(x)	S104	Network Address
v(x)	S106	Hopping Pattern
w		Start Loopback test. In the loopback test, the master continuously sends data packets (one per hop) to the slave, which in turn, loops the packet back to the master. Correctly received packets at the master are denoted by a '.' Incorrectly received packets are denoted by a 'C'. The first channel of the hopping pattern is denoted with a '*'. In general, this test is useful for determining if there are any bad RF channels. Issue any valid command to terminate the loopback test.
y		Show loopback statistics, then clear them. This command should be issued before beginning the loopback test to ensure counters are set to zero.

5. Installation

The installation, removal or maintenance of all antenna components must be carried out by qualified and experienced professionals.

The installation, removal or maintenance of all antenna components must be carried out by qualified and experienced professionals.

The SP 2.4E complies with FCC part 15 for operation in the license-free 2400-2483.5 MHz ISM band. This chapter provides guidelines for installing and deploying equipment which incorporates the SP 2.4E.

5.1 Estimating the Gain Margin

Successful communication between SP 2.4E's is dependent on three main factors:

? System Gain

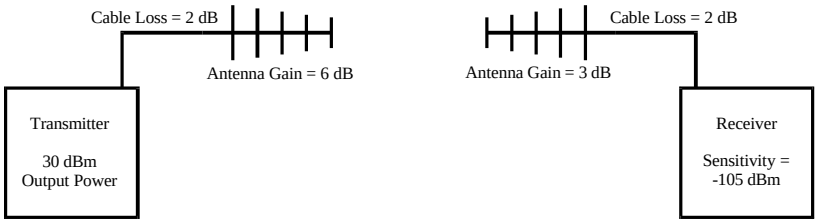
? Path Loss

? Interference

System gain is a calculation in dB describing the performance to be expected between a transmitter-receiver pair. The number can be calculated based on knowledge of the equipment being deployed. The following four factors make up a system gain calculation:

1. Transmitter power (user selectable)
2. Transmitter gain (transmitting antenna gain minus cabling loss between the transmitting antenna and the SP 2.4E)
3. Receiver gain (Receiving antenna gain minus cabling loss between the receiving antenna and the SP 2.4E)
4. Receiver sensitivity (Specified as -105 dBm on the SP 2.4E)

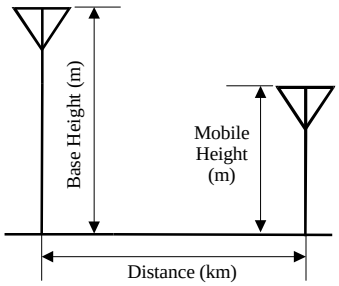
In the following illustration, the transmitting antenna has a gain of 6 dB, and the receiving antenna has a gain of 3 dB. The cable loss between the unit and the antenna is 2 dB on both the transmitting and receiving side.



The power level has been set to 30 dBm (1W) on the transmitter, and the receiver sensitivity for the SP 2.4E is -105 dBm.

System gain would be calculated to be:

30 - 2 + 6 + 3 - 2 + 105 = 140 dB.



When deploying your system, care must be taken to ensure the **path loss** (reduction of signal strength from transmitter to receiver in dB) between equipment does not exceed the system gain (140 dB in the above example). It is recommended to design for a **gain margin** of at least 10 dB to ensure reliable communication. Gain margin is the difference between system gain and path loss. Referring to the same example, suppose the path loss is 100 dB, the gain margin would be 40 dB, which is more than adequate for reliable communication.

Path loss is a very complicated calculation which mainly depends on the terrain profile, and the height of the antennas off the ground.

The following table provides path loss numbers for varying antenna heights and antenna separation: These numbers are real averages taken from rural environments. They do not apply to urban, non-line-of-sight environments.

Distance (km)	Base Height (m)	Mobile Height (m)	Path Loss (dB)
5	15	2.5	123.5
5	30	2.5	117.9
8	15	2.5	131.1
8	15	5	124.7
8	15	10	112
16	15	2.5	142.3
16	15	5	135.9
16	15	10	123.2
16	30	10	116.6
16	30	5	129.4
16	30	2.5	135.8

Once the equipment is deployed, you can verify the signal strength by entering into Command Mode and reading Register S123. This register provides the average signal strength in dBm. The minimum strength for communication is roughly -105 dBm. For consistent reliable communication, you should try to deploy the equipment such that signal strength exceeds -95 dBm.

5.2 Antennas and Cabling

This section describes the recommended procedure for installing cabling and antennas for use with the SP 2.4E.

The installation, removal or maintenance of all antenna components must be carried out by qualified and experienced professionals.

Never work on an antenna system when there is lightning in the area.

Direct human contact with the antenna is potentially unhealthy when the SP 2.4E is generating RF energy. Always ensure that the SP 2.4E equipment is powered down during installation.

5.2.1 Surge Arrestors

The most effective protection against lightning is to install two lightning (surge) arrestors: One at the antenna, and the other at the interface with the equipment. The surge arrestor grounding system should be fully interconnected with the transmission tower and power grounding systems to form a single, fully integrated ground circuit. Typically, both ports on surge arrestors are N-female.

5.2.2 Cabling

The following coax cables are recommended:

Cable	Loss (dB/100ft)
LMR 195	19
LMR 400	6.8
LMR 600	4.4

Factors to take into consideration when choosing a cable are:

? price;

? bend radius limitations (the lower performance cables generally can bend more sharply);

? performance requirements; and,

? distance between the equipment and the antenna.

When installing the cable, always begin fastening at the top near the antenna connector/surge arrestor. The cable must be supported at the top with a hose clamp or wrap lock, and at 5 ft intervals down the length of the tower. Over-tightening the fasteners will dent the cable and reduce performance. If properly grounded surge arrestors are not installed at both the top and the bottom of the cable, then the cable should be grounded to the tower at these locations using a cable grounding kit. If the tower is non-conductive, then a separate conductor, physically separate from the cable, should be run down the tower.

5.2.3 Antenna

The installation, removal or maintenance of all antenna components must be carried out by qualified and experienced professionals.

Never work on an antenna system when there is lightning in the area.

Always ensure that the SP 2.4E equipment is powered down during installation.

In order to comply with the FCC/IC adopted RF exposure requirements, this transmitter system will be installed by the manufacturer's reseller professional. Installation of all antennas must be performed in a manner that will provide at least 20 cm clearance from the front radiating aperture, to any user or member of the public.

To comply with FCC regulations, you must limit ERP to 36 dBm or less.

Before choosing an antenna, you should have some knowledge of the path loss and the topology of the equipment. If the equipment is in a fixed location and is to communicate with only one other unit also in a fixed location, then a Yagi antenna is suitable. Choose a Yagi with enough gain to ensure adequate gain margin. When deploying the Yagi, point the antenna towards the intended target, ensuring the antenna elements are perpendicular to the ground.

If the equipment must communicate with multiple or mobile transceivers, then select an Omni-directional antenna with appropriate gain.

The Effective Radiated Power (ERP) emitted from the antenna cannot exceed +36 dBm ERP.

With the SP 2.4E set to full power, ERP is calculated as follows:

ERP = 30 - (Cabling and Connector Losses) + (Antenna Gain) < 36

Use the guidelines in the previous section for calculating cable and connector losses. If cabling and connector losses are 2 dB, then the maximum allowable gain of the antenna will be 8 dB.

5.2.4 External Filter

Although the SP 2.4E is capable of filtering out RF noise in most environments, there are circumstances that require external filtering. Paging towers, and cellular base stations in close proximity to the SP 2.4E antenna can desensitize the receiver. Simrex Corporation's external cavity filter eliminates this problem. The filter has two N-female ports and should be connected in line at the interface to the RF equipment.

5.2.5 Weatherproofing

Type N and RTNC connectors are not weatherproof. All connectors should be taped with rubber splicing tape (weatherproofing tape), and then coated with a sealant.

A. Command Summary

The following provides a command summary for the SP 2.4E. Factory settings are denoted with a '*'.

AT Commands

A	On-line Mode
I	Identification
	I0 Custom
	I2 ROM Checksum test
	I3 Firmware Version
	I4 Firmware Date
	I6 Firmware Time
	I7 Serial Number
O	On-line Mode
Z	Reset and load stored configuration
&F	Load Factory Default
	&F1 Master
	&F2 Slave
	&F3 Repeater
	&F4 Slave through Repeater
&V	View Configuration
&W	Write configuration to memory
Sxx?	Read S register value
Sxx=yy	Set S register value

S Registers

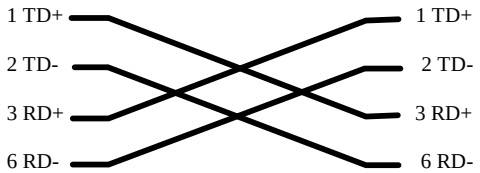
S101	Operating Mode
	1 - Master Point to Multipoint
	2 - Master Point to Point
	3 - Slave
	4 - Repeater
	5 - Master Diagnostics
	6- Peer to Peer
S104	Network Address [0...65535]
S105	Unit Address [1...65535]
S106	Primary Hopping Pattern [0...63]
S206	Secondary Hopping Pattern [0...63]
S107	Encryption Key [0...65535]
S108	Output Power Level
	0 = 10 mW, 1 = 50 mW, *2 = 100 mW,
	3 = 250mW, 4=500mW, 5=750mw, 6=1W
S113	Packet Retransmissions [0...255]
S213	Packet Retry Limit [0...255]
S118	Roaming
	*0 = Disabled, 1 = Enabled
S122	Remote Control
	*0 = Disabled, 1 = Enabled
S123	RSSI (dBm)
S205	Repeaters
	*0 = Disabled, 1 = Enabled

B. Ethernet and Serial Interfaces

The SP 2.4E uses a standard 8 pin RJ45 modular jack for the 10BaseT ethernet port. The pinout is as follows:

Pin Number	Signal	I/O
1	TD+	O
2	TD-	O
3	RD+	I
4	Unused	
5	Unused	
6	RD-	I
7	Unused	
8	Unused	

Use straight through 10BaseT cable when connecting to the hub. Use a 10BaseT crossover cable when connecting to a station (ethernet-equipped computer) as follows:



SP 2.4E **(DCE)**		Signal		User Terminal **(DTE)**
1				IN
2	? ? ?	RX	? ? ?	IN
3	? ? ?	TX	? ? ?	OUT
4				OUT
5		GND		IN
6				IN
7				OUT
8				IN

The signals in the RS-232 asynchronous serial interface are described below:

RX *Receive Data* - **Output from SP 2.4E** - Signals transferred from the SP 2.4E are received by the DTE via RX.

TX *Transmit Data* - **Input to SP 2.4E** - Signals are transmitted from the DTE via TX to the SP 2.4E.

GND *Signal Ground* - Provides a ground reference for all signals transmitted by both DTE and DCE.

C. Factory Default Settings

AT&F1 - Master Default Settings

Operating Mode	S101=1 (Master P-MP)
Network Address	S104=1
Unit Address	S105=1
Primary Hop Pattern	S106=0
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Packet Retransmissions	S113=0
Roaming	S118=0
Remote Control	S122=0
Secondary Hop Pattern	S206=2 (Don't Care)
Packet Retry Limit	S213=2 (Don't Care)
Repeaters Yes/No	S205=0

AT&F2 - Slave Default Settings

Operating Mode	S101=3 (Slave)
Network Address	S104=1
Unit Address	S105=2
Primary Hop Pattern	S106=0
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Packet Retransmissions	S113=1 (Don't Care)
Roaming	S118=0
Remote Control	S122=0
Secondary Hop Pattern	S206=2 (Don't Care)
Packet Retry Limit	S213=2
Repeaters Yes/No	S205=0

AT&F3 - Repeater Default Settings

Operating Mode	S101=4 (Repeater)
Network Address	S104=1
Unit Address	S105=3
Primary Hop Pattern	S106=0
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Packet Retransmissions	S113=0
Roaming	S118=0
Remote Control	S122=0
Secondary Hop Pattern	S206=2
Packet Retry Limit	S213=2
Repeaters Yes/No	S205=0

AT&F4 -Slave Through Repeater Default Settings

Operating Mode	S101=3 (Slave)
Network Address	S104=1
Unit Address	S105=4
Primary Hop Pattern	S106=2
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Packet Retransmissions	S113=1 (Don't Care)
Roaming	S118=0
Remote Control	S122=0
Secondary Hop Pattern	S206=2 (Don't Care)
Packet Retry Limit	S213=2
Repeaters Yes/No	S205=0

D. Hopping Patterns

This Appendix provides a guide for selecting appropriate hopping patterns (S106,S206). There are 49 hopping patterns: Patterns have been designed to notch out certain segments of the ISM band.

Pattern Number	Spectrum Used
0 - 7	2.4012 - 2.4824 GHz
8 - 10	2.4012 - 2.4312 GHz
11 - 13	2.4052 - 2.4352 GHz
14 - 16	2.4092 - 2.4392 GHz
17 - 19	2.4132 - 2.4432 GHz
20 - 22	2.4172 - 2.4472 GHz
23 - 25	2.4212 - 2.4512 GHz
26 - 28	2.4252 - 2.4552 GHz
29 - 31	2.4292 - 2.4592 GHz
32 - 34	2.4332 - 2.4632 GHz
35 - 37	2.4372 - 2.4672 GHz
38 - 40	2.4412 - 2.4712 GHz
41 - 43	2.4452 - 2.4752 GHz
44 - 46	2.4492 - 2.4792 GHz
47 - 48	2.4520 - 2.4820 GHz

Patterns 44 to 48 may be manually edited by entering AT&H at the Command Line. Each pattern must use a channel only once, and must consist of exactly 76 channels. There are 202 channels available ranging from Channel 1 at 2.4016 GHz up to Channel 202 at 2.4820 GHz

E. Technical Specifications

Electrical/Physical

Data Interface	10Base-T UTP (RJ45)
Configuration Interface	RS-232, 2400 baud to 115200 baud (DB9)
Indicators	Power, Link Integrity, WAN TX, WAN RX, LAN TX, LAN RX, RSSI
Throughput	Up to 115.2 kbps
Communications Range	Up to 30 km line of sight, elevated antennas
Memory	Non-volatile configuration memory
Buffer Capacity	256 frames
LAN Address Memory	Up to 10,000 addresses
Operating Modes	Point-to-point, Point-to-multipoint, Repeater, Peer to Peer, Diagnostics
Supply Voltage	10 – 30 VDC
Supply Current	250mA typical at 12VDC; 500mA max at 12VDC
Operating Frequency	2400 – 2483.5 MHz
System Gain	135 dB
Output Power	10mW, 50mW, 100mW, 250mW, 500mW, 750mW, 1W (user-configurable some models power limited to a maximum of 100mW for regulatory compliance)
Spreading Code	Frequency Hopping
Hopping Patterns	49 user-selectable
Error Detection	CRC-16 with auto retransmit
Enclosure Material	Extruded aluminum, raven black baked powder coat finish
Dimensions	3.72” x 4.25” x 1.72” (95 x 108 x 44 mm)
Antenna Connector	Reverse polarity TNC
Weight	Approx. 420 grams
Operating Environment	-40 to +75 C
Minimum Rejection	70 dB in band, 80 dB out of band
Approvals	FCC, Industry Canada, CE (power limited version 100mW)

F. Glossary

Terminology Used in the SP 2.4E Operating Manual

Asynchronous communications A method of telecommunications in which units of single bytes of data are sent separately and at an arbitrary time (not periodically or referenced to a clock). Bytes are "padded" with start and stop bits to distinguish each as a unit for the receiving end, which need not be synchronized with the sending terminal.

Attenuation The loss of signal power through equipment, lines/cables, or other transmission devices. Measured in decibels (dB).

Bandwidth The information-carrying capacity of a data transmission medium or device, usually expressed in bits/second (bps).

Baud Unit of signaling speed equivalent to the number of discrete conditions or events per second. If each signal event represents only one bit condition, then baud rate equals bits per second (bps) – this is generally true of the serial data port, so *baud* and *bps* have been used interchangeably in this manual when referring to the serial port; this is not always the case during the DCE-to-DCE communications, where a number of modulation techniques are used to increase the bps rate over the baud rate.

Bit The smallest unit of information in a binary system, represented by either a 1 or 0. Abbreviated "b".

Bits per second (b/s or bps) A measure of data transmission rate in serial communications. Also see *baud*.

Byte A group of bits, generally 8 bits in length. A byte typically represents a character of data. Abbreviated "B".

Characters per second (cps) A measure of data transmission rate for common exchanges of data. A character is usually represented by 10 bits: an 8-bit byte plus two additional bits for marking the start and stop. Thus, in most cases (but not always), *cps* is related to *bits per second (bps)* by a 1:10 ratio.

CRC (Cyclic Redundancy Check) An error-detection scheme for transmitted data. Performed by using a polynomial algorithm on data, and appending a checksum to the end of the packet. At the receiving end, a similar algorithm is performed and checked against the transmitted checksum.

Crossover cable (Also known as rollover, null-modem, or modem-eliminator cable) A cable which allows direct DTE-to-DTE connection without intermediate DCEs typically used to bridge the two communicating devices. Can also be used to make cabled DCE-to-DCE connections. The name is derived from "crossing" or "rolling" several lines, including the TX and RX lines so that transmitted data from one DTE is received on the RX pin of the other DTE and vice-versa.

Data Communications Equipment (DCE, also referred to as Data Circuit-Terminating Equipment, Data Set) A device which facilitates a communications connection between *Data Terminal Equipment* (DTEs). Often, two or more compatible DCE devices are used to "bridge" DTEs which need to exchange data. A DCE performs signal encoding, decoding, and conversion of data sent/received by the DTE, and transmits/receives data with another DCE. Common example is a modem.

Data Terminal Equipment (DTE) An end-device which sends/receives data to/from a DCE, often providing a user-interface for information exchange. Common examples are computers, terminals, and printers.

dBm Stands for "Decibels referenced to one milliwatt (1 mW)". A standard unit of power level commonly used in RF and communications work. *n* dBm is equal to $10^{(n/10)}$ milliwatt, so 0dBm = 1mW, -10dBm = 0.1mW, -20dBm = 0.01mW, etc.

DCE See *Data Communications Equipment*.

DTE See *Data Terminal Equipment*.

Flow Control A method of moderating the transmission of data so that all devices within the communications link (DTEs and DCEs) transmit and receive only as much data as they can handle at once. This prevents devices from sending data which cannot be received at the other end due to

conditions such as a full buffer or hardware not in a ready state. This is ideally handled by hardware using flow-control and handshaking signals, but can be controlled also by software using X-ON/X-OFF (transmitter on/off) commands.

Frequency-hopping A type of *spread spectrum* communication whereby the carrier frequency used between transmitter and receiver changes repeatedly in a synchronized fashion according to a specified algorithm or table. This minimizes unauthorized jamming (interference) and interception of telecommunications.

Full-duplex Where data can be transmitted, simultaneously and independently, bi-directionally.

Half duplex Exists when the communications medium supports bi-directional transmission, but data can only travel in one direction at the same time.

Handshaking A flow-control procedure for establishing data communications whereby devices indicate that data is to be sent and await appropriate signals that allow them to proceed.

Line-of-sight Condition in which a transmitted signal can reach its destination by travelling a straight path, without being absorbed and/or bounced by objects in its path.

Master The station which controls and/or polls one or more Slave stations in a point-to-point or point-to-multipoint network. Often functions as a server or hub for the network.

Non-volatile memory Memory which retains information which is written to it.

Null modem cable See *Crossover cable.*

Point-to-point A simple communications network in which only two DTEs are participants.

Point-to-multipoint A communications network in which a *Master* DTE communicates with two or more *Slave* DTEs.

Repeater A device which automatically amplifies or restores signals to compensate for distortion and/or attenuation prior to retransmission. A repeater is typically used to extend the distance for which data can be reliably transmitted using a particular medium or communications device.

RS-232 (Recommended Standard 232; more accurately, RS-232C or EIA/TIA-232E) Defined by the EIA, a widely known standard electrical and physical interface for linking DCEs and DTEs for serial data communications. Traditionally specifies a 25-pin D-sub connector, although many newer devices use a compact 9-pin connector with only the essential signaling lines used in asynchronous serial communications. Lines have two possible states: "high" (on, active, asserted, carrying +3 to +25 V) or "low" (off, inactive, disasserted, carrying -3 to -25 V).

RTU (Remote Terminal Unit) A common term describing a DTE device which is part of a wide-area network. Often a RTU performs data I/O and transmits the data to a centralized station.

Serial communications A common mode of data transmission whereby character bits are sent sequentially, one at a time, using the same signaling line. Contrast with parallel communications where all bits of a byte are transmitted at once, usually requiring a signal line for each bit.

Shielded cable Interface medium which is internally shrouded by a protective sheath to minimize external electromagnetic interference ("noise").

Slave A station which is controlled and/or polled by the Master station for communications. Typically represents one end of a point-to-point connection, or one of the terminal nodes in a point-to-multipoint network. Often a RTU is linked by a Slave DCE.

Spread spectrum A method of transmitting a signal over a wider bandwidth (using several frequencies) than the minimum necessary for the originally narrowband signal. A number of techniques are used to achieve spread spectrum telecommunications, including *frequency hopping*. Spread spectrum provides the possibility of sharing the same band amongst many users while increasing the tolerance to interference and noise, and enhancing privacy of communications.

Throughput A measure of the rate of data transmission passing through a data communication system, often expressed as bits or characters per second (bps or cps).