

# Operating Manual

---

## SP 2.4

2.4 GHz Spread Spectrum Modem

Revision 1.40, September 24, 2001

---

### ***SIMREX CORPORATION***

Offices in NY and Arizona

Phone: (480) 926-6069

Fax: (305) 675-7794

[www.simrex.com](http://www.simrex.com)

# SP 2.4

## 2.4 GHz Spread-Spectrum Wireless Modem

### 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.**

### **SIMREX CORPORATION**

Offices in NY and Arizona  
Phone: (480) 926-6069  
Fax: (305) 675-7794  
www.simrex.com

This manual contains information of proprietary interest to SIMREX CORPORATION. It has been supplied in confidence to purchasers and users of the SP 2.4, 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' products are appropriate for home, office, or industrial use, but 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 caused undesired operation.**

SIMREX CORPORATION's products are warranted against all failures which occur as a result of defective material or workmanship within 12 months of purchase by the user. This warranty does not extend to products that, in the opinion of SIMREX CORPORATION, have been subject to misuse, accidents, lightning strikes, improper installation or application, nor shall it extend to units which have, in SIMREX CORPORATION's opinion, been opened, tampered with or repaired by an unauthorized facility.

Manual SIMREX CORPORATION

HyperTerminal is copyrighted by Hilgraeve Inc, and developed for Microsoft. Microsoft and Windows are registered trademarks of Microsoft Corporation. pcANYWHERE and Symantec are registered trademarks of Symantec Corp. All other products mentioned in this document are trademarks or registered trademarks of their respective holders.  
Manual Revision 1.40, September 24, 2001.

# Contents

---

1.	Introduction	
1.0	Product Overview	1
1.1	Features	1
1.2	About this Manual	2
2.	Electrical/Physical	
2.0	Functional Block Diagram	3
2.1	Pinout	4
2.2	LED Operation	6
2.3	DC Characteristics	8
2.4	AC Characteristics	9
3.	Modes of Operation	11
3.1	Data Mode	11
3.2	Command Mode	12
3.2.1	AT Command Interface	13
3.3	Switching Between Command and Data Modes	13
4.	Configuration	
4.1	Quick Start Approach	15
4.2	AT Commands	16
	A - Answer	17
	E - Command Echo	17
	I - Identification	17
	O - Online Mode	17
	Q - Quiet Mode	17
	V - Result Codes Display	17
	W - Connection Result	18
	Z - Reset Modem and load stored configuration	18
	&C - DCD (Data Carrier Detect)	18
	&D - DTR (Data Terminal Ready)	18
	&F - Load Factory default configuration	18
	&K - Handshaking	18
	&S - DSR (Data Set Ready)	19
	&V - View Configuration	19
	&E - Framing Error Check	19
	&W - Write Configuration to memory	19
	Sxxx? - Read S register value	19
	Sxxx=yyy - Set S register value	19
	Command Result Codes	20
4.3	S Registers	21
	S Register 2 - Escape Code	21
	S Register 3 - CR Control Code	21
	S Register 4 - Linefeed Control Code	21
	S Register 5 - Backspace Control Code	21
	S Register 101 - Operating Mode	22
	S Register 102 - Serial Baud Rate	25
	S Register 103 - Wireless Link Rate	25
	S Register 104 - Network Address	26
	S Register 105 - Unit Address	26
	S Register 106 - Primary Hopping Pattern	26
	S Register 206 - Secondary Hopping Pattern	26
	S Register 107 - Encryption Key	28
	S Register 108 - Output Power Level	28
	S Register 109 - Hopping Interval	29
	S Register 110 - Data Format	30
	S Register 111 - Packet Minimum Size	30
	S Register 112 - Packet Maximum Size	30
	S Register 114 - Packet Size Control	30
	S Register 116 - Packet Character Timeout	30
	S Register 113 - Packet Retransmissions	31
	S Register 213 - Packet Retry Limit	32
	S Register 115 - Packet Repeat Interval	33
	S Register 117 - Modbus Mode	33
	S Register 118 - Roaming	34
	S Register 119 - Quick Enter to Command	34
	S Register 120 - RTS/DCD Framing	34
	S Register 121 - DCD Timeout	34

	S Register 122 - Remote Control .....	35
	S Register 123 - RSSI Reading .....	35
	S Register 124 – TDMA Duty Cycle .....	35
	S Register 125 – TDMA Max Address .....	35
	S Register 126 – Data Protocol .....	36
	S Register 127 – Address Filtering .....	37
	S Register 128 – Multicast Group .....	37
	S Register 129 – Secondary Master .....	37
4.4	Diagnostics, Statistics and Remote Control .....	38
4.4.1	Spectrum Analyzer Feature .....	38
4.4.2	Statistics .....	38
4.4.3	Remote Control and Diagnostics .....	39
5.	Installation .....	43
5.1	Estimating the Gain Margin .....	43
5.2	Antennas and Cabling .....	44
A.	Modem Command Summary .....	49
B.	Serial Interface .....	51
C.	Factory Default Settings .....	53
D.	Performance Tables .....	55
E.	Hopping Tables .....	57
F.	Technical Specifications .....	59
G.	Glossary .....	61

# 1. Introduction

---

## 1.0 Product Overview

The SP 2.4 is a high-performance wireless modem. Operating in the 2.400 to 2.4835 GHz ISM band, this frequency-hopping spread-spectrum module is capable of providing reliable wireless data transfer between almost any type of equipment which uses an asynchronous serial interface. The small-size and superior RF performance of this module make it ideal for many applications. Typical uses for this modem include:

- SCADA
- Traffic Control
- Remote Monitoring
- Fleet Management;
- Telemetry;
- Remote Camera/Robot Control;
- Security Systems; and,
- Display Signs.

While a pair of SP 2.4's can link two terminal devices ("point-to-point" operation), multiple modules can be used together to create a network of various topologies, including "point-to-multipoint" and "repeater" operation. Multiple independent networks can operate concurrently, so it is possible for unrelated communications to take place in the same or a nearby area without sacrificing privacy or reliability.

## 1.1 Features

Key features of the SP 2.4 include:

- transmission within a public, license-exempt band of the radio spectrum<sup>1</sup> – this means that it can be used without access fees (such as those incurred by cellular airtime);
- a serial I/O data port with handshaking and hardware flow control, allowing the SP 2.4 to interface directly to any equipment with an asynchronous serial interface.

---

<sup>1</sup>2.400 – 2.4835 GHz, which is license-free within the United States; may need to be factory-configured differently for some countries.

- 49 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 and reliability of data;
- ease of installation and use – the SP 2.4 uses a subset of standard AT style commands, very similar to those used by traditional telephone line modems.

While the typical application for the SP 2.4 is to provide a short- to mid-range wireless communications link between DTEs, it can be adapted to almost any situation where an asynchronous serial interface is used and data intercommunication is required.

## 1.2 About this Manual

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

It is assumed that users of the SP 2.4 have either system integration or system design experience. Chapter 2 details the physical attributes of the modem. 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 the operation of the wireless modem.

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 2.4 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 2.4.

# 2. Electrical/Physical

## 2.1 Connectors and Indicators

The SP 2.4 connects to the host equipment through a standard DB9 serial port. Other connectors and indicators are illustrated in Figure 1.

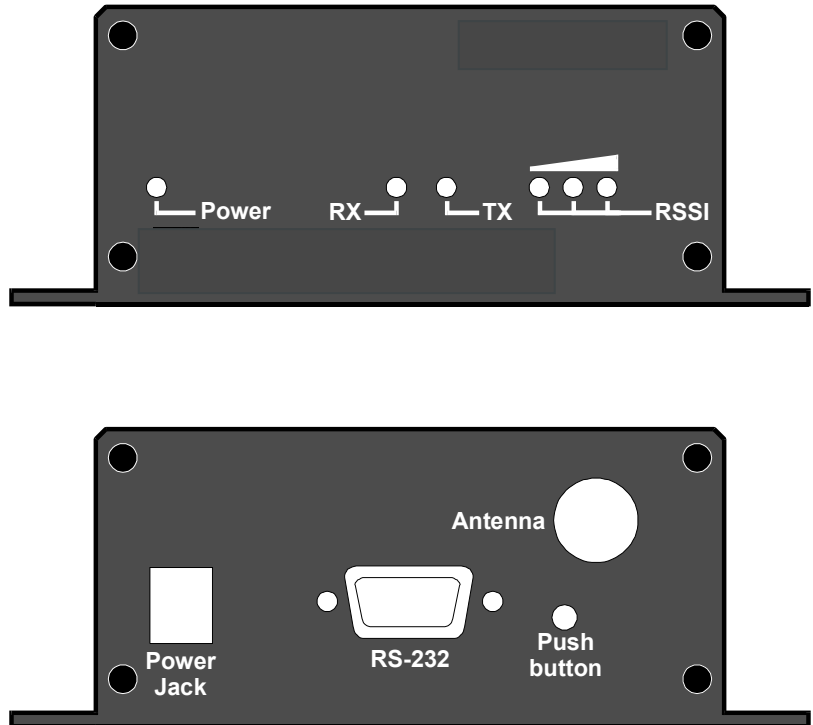


Figure 1 - Connectors and Indicators

The interface connectors and indicator lights are described below:

**Power LED** - Indicates the unit is powered on.

**RX/Sync LED** - Indicates the modem is synchronized and/or is receiving valid packets of data. See Section 2.2 for complete LED details

**TX LED** - Indicates the modem is transmitting data over the air. See Section 2.2 for complete LED details

**Receive Signal Strength Indicator (RSSI)** - As the signal strength increases, the number of active RSSI LED's increases, starting with the furthest left. See Section 2.2 for complete LED details

**Power Jack** - The modem supports voltage ranging from 10 to 30VDC through this 2.1mm power jack. The modem may optionally be powered through pin 9 of the RS-232 port. This option must be specified when purchasing the unit. A built-in switching supply enables the modem 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 (DCE)** - This port is used to interface the SP 2.4 to a DTE device and 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
1	DCD	Data Carrier Detect	O
2	RxD	Receive Data	O
3	TxD	Transmit Data	I
4	DTR	Data Terminal Ready	I
5	Gnd	Ground	
6	DSR	Data Set Ready	O
7	RTS	Request to Send	I
8	CTS	Clear to Send	O

**Push Button** - This button is non-operational on the SP 2.4 product.

**Antenna Connector** - The SP 2.4 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.

## 2.2 LED Operation

LED functionality is dependent on the mode of operation. Table 2 explains LED operation for the various modes.

**Table 2. LED Operation**

MODE	LED		
	RX	TX	RSSI1,2,3
Power Up (S0=1, S119=1)	off	off	blink 500ms on/500ms off
Power Up (S0=1, S119=0)	off	off	off
Power Up (S0=0)	off	off	off
Command Mode	off	off	off
Data Mode - Master	on while receiving valid data packets from slaves and repeaters in the network	on for the first portion of each hop interval.	RSSI mode based on all received packets See Table 3
Data Mode - Repeater During Sync. Acquisition	off	off	alternating 300ms on
Data Mode - Repeater When Synchronized	on for first portion of hop interval	on for second portion of hop interval	RSSI mode based on packets received from Slaves* See Table 3
Data Mode - Slave During Sync. Acquisition	off	off	alternating 300ms on
Data Mode - Slave When Synchronized	on	on when transmitting a packet.	RSSI mode based on packets received from the Repeater or Master with which it communicates See Table 3

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

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 3 - RSSI mode operation**

<b>Signal Strength (dBm)</b>	<b>RSSI1</b>	<b>RSSI2</b>	<b>RSSI3</b>
-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



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

## 2.3 DC Characteristics

Sym	Characteristic	Min	Typ	Max	Units
V <sub>CC</sub>	Supply Voltage	10	12	30	V
I <sub>CCR</sub>	*Modem Supply Current in Receive Mode	174	192	220	mA
I <sub>CCT0</sub>	*Modem Supply Current at 1mW Transmit	164	182	200	mA
I <sub>CCT1</sub>	*Modem Supply Current at 10mW Transmit	175	194	213	mA
I <sub>CCT2</sub>	*Modem Supply Current at 100mW Transmit	225	247	269	mA
I <sub>CCT3</sub>	*Modem Supply Current at 1W Transmit	398	442	486	mA
V <sub>IL</sub>	Input Low Voltage (Pins 3,4,7)	-12		-6	V
V <sub>IH</sub>	Input High Voltage (Pins 3,4,7)	6		12	V
V <sub>OL</sub>	Output Low Voltage (Pins 1,2,6,8)	-12	-9	-6	V
V <sub>OH</sub>	Output High Voltage (Pins 1,2,6,8)	6	9	12	V

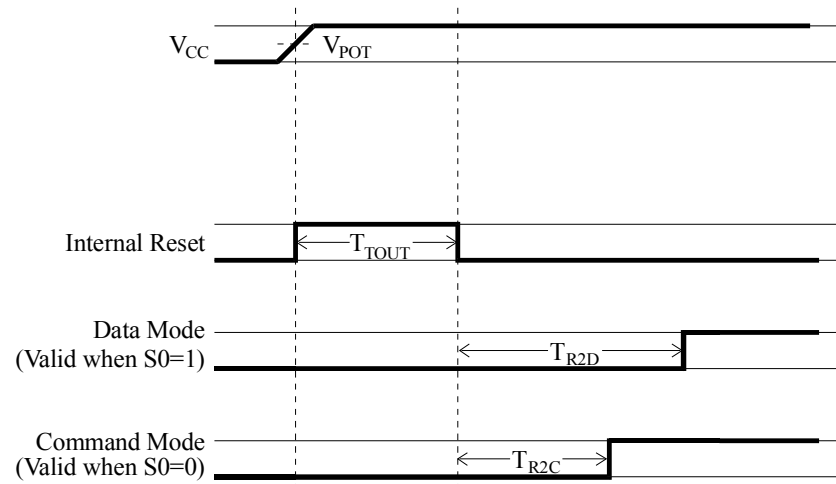
\*At 12VDC input

## 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*	0		5	s
$T_{R2C}$	Internal Reset to Command Mode		0		ms

\*Unit will enter into Command Mode upon power up if register S0=0. Unit will enter into Data Mode upon power-up if register S0=1. When powering up into Data Mode, an additional delay of 5 seconds is added if Register S119=1. See page 14 for details.

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 2.4 modem can be easily configured to meet a wide range of needs and applications. The modem is designed such that all communication is through one serial port. This port has two functions:

1. It provides the asynchronous interface with the host equipment for data that is sent/received on the RF channel. When operating in this fashion, the modem is said to be in **data mode**.
2. It is also used for configuring and programming the modem. When operating in this fashion, the modem is said to be in **command mode**.

In addition to **data mode** and **command mode**, there is a third mode of operation called **diagnostics mode**. The SP 2.4 will always be in one of these three modes.

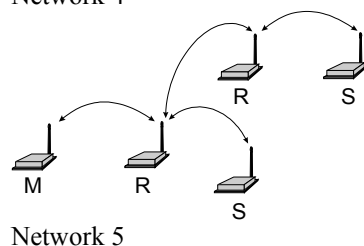
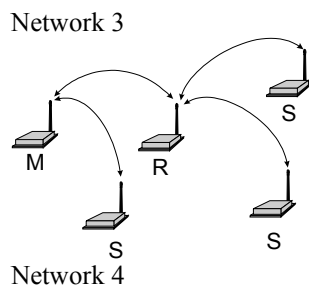
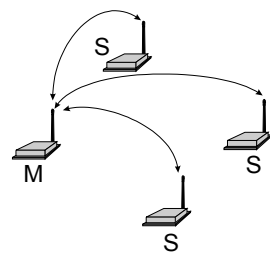
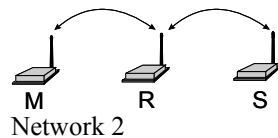
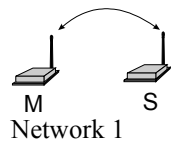
## 3.1 Data Mode

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

- One modem configured as the **Master**
- Zero or more modems configured as **Repeaters**
- One or more modems 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. The Master is the ultimate destination for all data collected at the various Repeater's and Slave's serial ports. With the network set up for Point-to-Multipoint communication, all data received at the Master's serial port is transmitted to every Repeater and Slave in the network. The SP 2.4 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 set by the user, and can range from 8ms to 120ms. The SP 2.4 hops according to a pseudorandom pattern of 76 different channels.

When configured as a Slave, the SP 2.4 searches for synchronization with a Master. Network topologies consisting of a single *Master* and virtually any combination of *Slaves* and *Repeaters* may be deployed. The functionality of any particular SP 2.4 can be configured as follows:



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

- **Master Point-to-Point:** The modem is configured to communicate with a single *Slave*, either directly, or through one or more *Repeaters*.
- **Master Point-to-Multipoint:** The modem is configured to communicate with one or more *Slaves* and/or *Repeaters*.
- **Slave:** The modem is configured to communicate with one *Master* either directly or through one or more *Repeaters*.
- **Repeater:** The modem 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 passes information to/from its serial 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 gives 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.

### 3.2 Command Mode

The SP 2.4 firmware has been designed to allow the user to customize the operation of the modem 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 2.4'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 9600 baud, 8N1
5. Apply power to the SP 2.4
6. While the three RSSI LED's are blinking, type 'mhz' (you have about 5 seconds to do this). The modem should respond with 'OK'.
7. Type 'AT&V <ENTER>'

### 3.2.1 AT Command Interface

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

```
BAUD = 9600
E1 Q0 V1 W0
DCD &C1   DTR &D0   Framing &E0   Handshaking &K3   DSR &S1
S0=1 S2=43 S3=13 S4=10 S5=8
Operating Mode           S101=1           Serial Baud Rate       S102=7
Wireless Link Rate       S103=2           Network Address        S104=1
Unit Address             S105=1           Hop Pattern            S106=0
Encryption Key           S107=1           Output Power           S108=2
Hop Interval             S109=4           Data Format             S110=1
Packet Min Size          S111=1           Packet Max Size        S112=43
Packet Retransmissions   S113=1           Quick enter to command S119=1
Packet Repeat Interval   S115=1           Character Timeout, ms  S116=8
RTS/DCD Framing, ms     S120=0           DCD Timeout, ms       S121=0
Secondary Hop Pattern    S206=2           Packet Retry Limit     S213=2
Average RSSI value       S123= -0 dBm    Modbus Mode            S117=0
Roaming                  S118=0           Packet Size Control    S114=0
Remote Control           S122=0
OK
```

The SP 2.4 is controlled 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 modem should respond with 'OK.' The above command will set the operating mode to Master Point-to-Point.

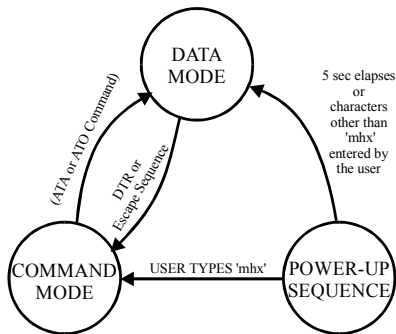
Register settings are not immediately stored to non-volatile memory, therefore if the modem is powered down at this point, the Operating Mode would revert to its previous value. To store any recently updated command registers, the following "write" command must be entered.

```
AT&W <ENTER>
```

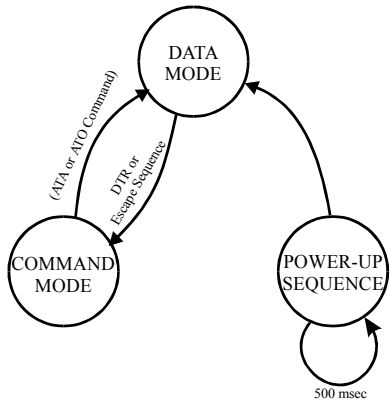
### 3.3 Switching Between Command and Data Modes

Your modem must be in **command mode** for it to execute a command. If you send characters when the modem is in **data mode**, the modem transmits the characters over the air.

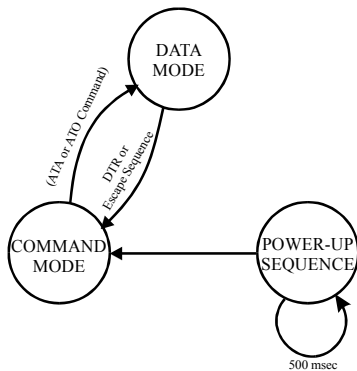
Depending on its settings, the modem will either power up in command mode or data mode. Normally, when first received from the factory, the unit will power up into data mode. During the first five seconds after power-up, the user is given the opportunity to avoid entering into data mode but instead enter into command mode by typing 'mhx'.



**Figure 5A. S0=1, S119=1 (factory default)**



**Figure 5B. S0=1, S119=0**



**Figure 5C. S0=0**



The escape sequence will not be accepted unless both the SP 2.4 and the terminal are set to the same baud rate

The terminal must be set for 9600 baud 8N1 in order for the modem to accept these characters. If 'mhz' is typed incorrectly, the modem will immediately enter into data mode. If the five seconds elapses without any response from the user, the modem will go into data mode.

In command mode, the modem “autobauds,” meaning that it will adapt to the baud rate of the DTE equipment to which it is connected. Therefore, when in command mode, you may change the baud rate of your equipment, and the SP 2.4 will automatically adjust to this baud rate once an AT string is issued. The new baud rate is stored in register S102. Several baud rates ranging from 2400 to 115200 may be selected.

You can place the modem into Data Mode from Command Mode either by:

- Issuing the answer command (ATA <ENTER>); or,
- Issuing the online command (ATO <ENTER>).

The modem will now attempt to communicate with other SP 2.4 modems. While in Data Mode, the modem will communicate through the serial port at the same baud rate as was last used in Command Mode<sup>2</sup>.

To return to Command Mode, you can either:

- Send the escape sequence. (The escape sequence consists of 1 second of inactivity, followed by the characters '+++’ followed by another second of inactivity.); or,
- Toggle the DTR line (depending on the &D parameter see pg 11).

The escape sequence must be issued at the baud rate that the modem has been set to. If the modem is set to 19200 baud, and the escape sequence is issued at 9600 baud, for example, the modem will not recognize it, and will not go into Command Mode.

Figure 5 provides a state diagram for power-up, command mode, and data mode. Note that there are three different variants of the state diagram which depend on the values of registers S0 and S119. See the appropriate sections for more details about these registers. The factory defaults are S0=1 and S119=1.

<sup>2</sup> It is possible to enter into Data Mode at a different baud rate from what is currently being used in Command Mode by issuing the command AT S102=x, where x is one of the valid baud rates. Care must be taken when setting the baud rate in this manner. If you issue another AT string after attempting to set the baud rate using AT S102 <ENTER>, the modem will again autobaud and automatically revert to the baud rate of the host equipment. For example, if your equipment is running at 9600 baud and you wish to set up the modem to run at 19200 baud, the following command line entry would be suitable:

AT S102=5&WA <ENTER>

The first part (S102=5) sets the baud rate to 19200. The next characters (&W) write this baud rate to memory. The last character (A) puts the modem into Data Mode. Once in Data Mode, the modem is unable to autobaud, and is fixed at 19200 baud. By combining several commands into one command line entry, and then immediately putting the modem online, the modem is not given a chance to autobaud back to 9600.

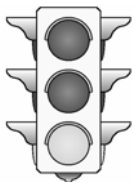
# 4. Configuration

This chapter provides a detailed description of the various operating parameters of the SP 2.4. Section 4.1 provides a quick-start approach which outlines the minimum requirements for establishing communication between two SP 2.4's. The settings will not necessarily provide optimal performance for your application, but will verify that the modems 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 modem, and Section 4.4 provides a description of all diagnostic features of the modem.

## 4.1 Quick Start Approach

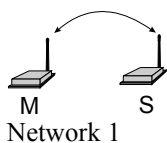
There are several parameters that must be set in order to establish communication between a pair of SP 2.4's.



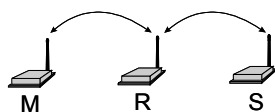
**Warning:** After testing the units for correct operation using the quick-start approach, be sure to modify some of the security parameters such as Network Address and Encryption Key, to avoid unintentional communication with other users of SP 2.4 products..

The SP 2.4 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 modem for a particular type of operation. For example, to quickly implement Network 1, Factory default 1 would be applied to the Master, and Factory default 2 would be applied 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,



Network 1



Network 2

**Figure 6. Basic Networks**

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 and set the terminal application's serial port settings to 9600 baud, 8N1
4. Apply power to the development SP 2.4
5. While the three RSSI LED's are blinking, type 'mhx' (you have about 5 seconds to do this). The modem should respond with 'OK'.
6. Configure the unit to Factory Setting 1 by typing AT&F1 <return>. This puts the unit into Master Point-to-point mode.
7. Store these settings to memory by typing AT&W <return>.
8. Put the modem into Data Mode by typing ATA (or ATO) <return>
9. 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. Remember, the parameters defined by Factory Settings 1 and 2 will likely not be the most ideal for your application, but will quickly allow you to test the units. A complete summary of the settings defined by all four factory settings can be found in Appendix C. Factory Default Settings.

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 2.4 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 on the development board which houses the Slave unit. If the link is good, up to three RSSI LEDs on the Slave modem should be active along with the RX/Sync LED, and if the link is absent (due to a fault at one end or another, such as misconfiguration), the LED's will be in either "scanning mode" or inactive. See Section 2.2 for complete LED operation.

Characters typed at the Master terminal should appear at the Slave's terminal, and vice versa. Also, verify that the RX LED blinks as packets of data are received at the Master modem. As data is sent from Slave to Master, the RX indicator should blink on as correct packets of data are received. At this point, the Master's RSSI LED's should become active. It is recommended that if the SP 2.4 will be deployed in the field where large distances separate the units, the modems 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 2.4. These commands affect the operation of the modem 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 modem will execute the previous command line. When in Command Mode, the modem "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 modem.

For the AT command protocol, an escape sequence consists of three consecutive escape codes preceded and followed by at least 1 second of inactivity. Typically, the '+' character is used as the escape code.

+++ preceded and followed by 1 second of inactivity



The escape sequence will not be accepted unless both the SP 2.4 and the terminal are set to the same baud rate

Note that the terminal must be configured to the same baud rate as the modem in order for the modem to recognize the escape sequence. The modem is unable to “autobaud” while in Data Mode.

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**

The A command puts the modem into data mode, where the modem attempts to communicate with other compatibly configured modems (Type ATA <return>).

#### **Dxxxxx, DTxxxxx, DPxxxxx Dial**

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

#### **E Command Echo**

Your modem is preset to return (or echo) commands to the host microprocessor when in Command Mode.

**E0** No Command Echo  
**\*E1** Command Echo

#### **I Identification**

The I command returns various modem information settings.

**I0=** String up to 16 characters stored in non-volatile memory  
**I1** Product Code (SP 2.4)  
**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 modem into data mode. This command is identical to the A command.

#### **Q Quiet Mode**

Your modem is preset to send responses when it executes commands, and there after to keep the host informed of its status.

**\*Q0** Enable modem responses  
**Q1** Disable modem responses

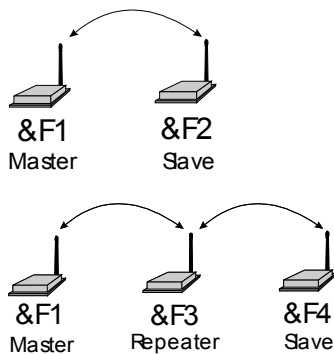
#### **V Result Codes display**

Your modem can either display result codes as words or numbers.

**V0** Display Result Codes as numbers  
**\*V1** Display Result Codes as words



Refer to Appendix A (page 49) for a summary of the modem commands



## W Connection Result

This parameter determines the modem response at the transition to Data Mode from Command Mode. Result codes can be found on page 20.

- \*W0** Reports computer (DTE) baud rate as CONNECT xxxx
- W1** Reports wireless rate between modems as CARRIER xxxx.

## Z Reset and load stored configuration

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

### &C DCD (Data Carrier Detect)

The &C command controls the modem's DCD output signal to the host microprocessor. This command determines when the DCD is active.

- &C0** DCD is always ON
- \*&C1** DCD on when modems are synchronized. DCD is always on when unit is configured as Master.
- &C2** DCD used for output data framing and Modbus mode. See page 33 for details.
- &C3** On modems configured as a Slave, DCD pulses for 2ms each time a valid synchronization packet is received from the master. The master sends a synchronization packet once per hop.

### &D DTR (Data Terminal Ready)

The &D command controls what action the modem performs when the DTR input line is toggled. The DTR input is controlled by the host microprocessor.

- \*&D0** DTR line is ignored, with the exception of multimaster mode. See S129
- &D1** Not Supported
- &D2** De-assert DTR to force the modem into command mode from data mode. DTR must be asserted before putting the modem back into data mode (The modem is put back into data mode in the normal manner using ATA or ATO)
- &D3** De-asserting DTR disconnects and resets modem. Modem will remain in this state until DTR again goes active.

### &F Load Factory Default Configuration

The &F command resets the modem and loads the default factory configuration.

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

## **&K Handshaking**

The &K command controls the handshaking between the modem and host microprocessor.

- &K0** Disable handshaking
- &K2** RTS/CTS input data framing. See page 33 for details.
- \*&K3** Enable hardware handshaking (RTS/CTS)

## **&S DSR (Data Set Ready)**

The &S command controls the DSR line for the modem, and determines when it is active

- &S0** DSR is always ON
- \*&S1** DSR is ON in Data Mode, OFF in Command Mode
- &S2** DTR/DSR signaling. With &S2, Slaves and repeaters output the state of the master's DTR on their local DSR line. Master outputs the state of a slave's DTR on its local DSR line only in point-to-point mode (i.e., DTR is a two-way signal transfer in point-to-point mode, and a one-way signal transfer in point-to-multipoint mode).
- &S3** In Multimaster Mode, set the primary master as &S3. See S129 for more details.

## **&V View Configuration**

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

## **&E Framing Error Check**

This command enables or disables Framing Error Check. When enabled, the modem looks for the stop bit. If the stop bit is absent, the byte is thrown out. When enabled, the modem also does a parity check. Note that the data format (number of data bits, parity type, and number of stop bits) is defined by S register 110.

- \*&E0** Disable Framing Error Check
- &E1** Enable Framing Error Check

## **&W Write Configuration to Memory**

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

## **Sxxx? Read S register value**

This command causes the modem 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.



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

### AT Command Result Codes

The SP 2.4 can display the results of a command as either text strings or numerical data. The following chart shows resulting text string and corresponding numeric result.

0	OK
3	NO CARRIER
4	ERROR
22	CONNECT 2400
21	CONNECT 3600
20	CONNECT 4800
19	CONNECT 7200
18	CONNECT 9600
17	CONNECT 14400
16	CONNECT 19200
15	CONNECT 28800
14	CONNECT 38400
13	CONNECT 57600
12	CONNECT 115200
6	CARRIER 84000
8	CARRIER 43000



Refer to Appendix A (page 49) for a summary of the S-Registers.



S Registers 2 through 5 cannot be stored to non-volatile memory.

## 4.3 S Registers

The S Registers described in this section affect the operating characteristics of the modem.

### S Register 0 - Auto Answer

If this register is set to zero, the modem will power up in command mode. If this register is set to one, the modem will power up in data mode.

### S Register 2 - Escape Code

This register contains the ASCII value of the escape character.

The default value (decimal 43) is equivalent to the ASCII character '+'. Values greater than 127 disable the escape feature and prevent you from returning to the Command Mode. This register cannot be stored to non-volatile memory. If the modem is reset, or powered down, the default value is restored.

**Default is '+' (decimal 43).**

### S Register 3 - CR Control Code

This register contains the ASCII value of the carriage return character.

This is the character that is used to end the command line and is also the character that appears after the modem sends a response. This register cannot be stored to non-volatile memory. If the modem is reset, or powered down, the default value is restored.

**Default is 'CR' (decimal 13).**

### S Register 4 - Linefeed Control Code

Register S4 sets the ASCII value of the linefeed character.

The modem sends the linefeed character after sending a carriage return character when sending text responses. This register cannot be stored to non-volatile memory. If the modem is reset, or powered down, the default value is restored.

**Default is 'LF' (decimal 10).**

### S Register 5 - Backspace Control Code

Register S5 sets the ASCII value of the backspace character.

This character is both the character created by entering BACKSPACE and the character echoed to move the cursor to the left. This register cannot be stored to non-volatile memory. If the modem is reset, or powered down, the default value is restored.

**Default is 'BS' (decimal 8).**



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 2.4. 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 - One Way Polling

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

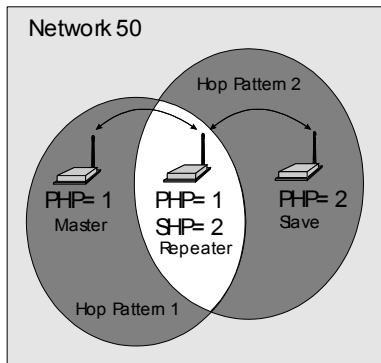
- Default for Factory Setting &F1 is 1 (Master Point-to-Multipoint)
- Default for Factory Setting &F2 is 3 (Slave)
- Default for Factory Setting &F3 is 4 (Repeater)
- Default for Factory Setting &F4 is 3 (Slave)

**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 modem broadcasts data to all Slaves and Repeaters in the network, and is also the ultimate destination for data transmitted by all Slaves and Repeaters. In addition, the Master defines the following network parameters to be utilized by all other modems in the network (See the appropriate sections for a complete description of these parameters):

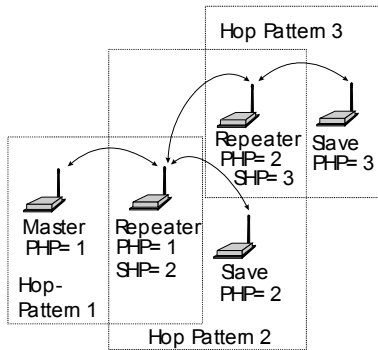
- Maximum Packet Size (S112)
- Minimum Packet Size (S111)
- Wireless Link Rate (S103)
- Hop Interval (S109)

**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) 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 only provide acknowledgement for packets of data sent by the Master when the Master is in Point-to-Point mode. In multipoint mode, multiple slaves would conflict with one another if they were all trying to acknowledge the Master at the same time. The Master does, however, send acknowledgements to all messages it receives from Slaves. The Master initiates communications by sending a broadcast message to all Slaves. All Slaves are free to respond in a “Slotted ALOHA” fashion, meaning that each Slave can choose one of several windows in which to transmit. If there happens to be two Slaves attempting to talk at the same time, the Master may not receive the data, and the Slaves therefore would not get an acknowledgement. At this point, the Slaves would attempt to get the information through at random time intervals, thus attempting to avoid any more conflicts. Special parameters which control the Slave’s response characteristics can be modified with S Registers S115 and S213.



**Figure 7 - Repeater Operation**



**Figure 8 - A Network Utilizing Three Hopping Patterns**



If there is no DTE connected to the Repeater, turn off handshaking (&K0) and set the baud rate to 115K.

**4) Repeater.** A more precise title would be Repeater/Slave, because a Repeater also has much of the same functionality as a Slave. A terminal can be connected at the Repeater location and communicate with the Master terminal. 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 2.4 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.

If the Repeater is not also being used as a Slave (there is no DTE connected to the serial port), it is recommended that the Repeater’s baud rate be set to 115K, and that handshaking be disabled (&K0). This will help ensure a smooth flow of data through the network.

**6) Master - One Way Polling.** This mode of operation represents a combination of diagnostics mode (See Section 4.4.3) and point-to-point mode. Similar to point-to-point operation, the master allows only one slave or repeater to send data at any given time. Only the slave or repeater whose unit address matches the master's unit address can send data. The difference however, is in the Master's functionality. The master is incapable of sending any data to the remote slave or repeater. Incoming data on the master's serial port is used for changing the operating parameters of the master 'on the fly', as opposed to normal point-to-point operation in which this data would be sent over the air to the remote modem. As in diagnostics mode (See Section 4.4.3) all slaves and repeaters with matching network addresses and encryption keys are synchronized to the master's network. The user can issue a special command to the master modem to change its unit address, thereby allowing the master to immediately begin receiving data from a different slave or repeater in the network. This method of communication is ideal for multipoint networks in which all data flow is from slave to master. The terminal equipment connected to the master modem has the freedom to choose how frequently, and the order in which each slave will be polled, and there is virtually no delay between polling one slave and the next. The following commands may be issued to the master. The x represents a valid parameter for the register.

Command	Master Register	Description
r(x)	S105	Unit Address
s	S101	back to normal operating mode
t(x)	S109	Hopping Interval
u(x)	S104	Network Address
v(x)	S106	Hopping Pattern

For example, to change the unit address of the master to 242, issue the following command:

```
r242 <ENTER>
```

The master will immediately begin receiving data from the slave or repeater in the network whose unit address is 242.

Note that all slaves and repeaters in the network whose unit address doesn't match the master's may still accumulate data in their buffers from the connected RTU or terminal equipment. The slave will begin to transmit all accumulated data the instant the master's poll packet contains a unit address matching its own.

## S Register 102 - Serial Baud Rate

The Serial Baud Rate is the current speed that the modem is using to communicate with the DTE. In command mode, the modem “autobauds,” meaning that it will adapt to the baud rate of the DTE equipment to which it is connected. Therefore, when in command mode, you may change the baud rate of your equipment, and the SP 2.4 will automatically adjust to this baud rate once an AT string is issued. The new baud rate is stored in register S102. If you issue a command to change the value of S102, the instant you issue another command, the baud rate will revert back to that of the DTE equipment. Therefore, it is advisable to operate in Command Mode at the desired baud rate for Data Mode.

See page 14 for additional information.

The possible values are:

1	115200
2	57600
3	38400
4	28800
5	19200
6	14400
*7	9600
8	7200
9	4800
10	3600
11	2400

It is generally advisable to choose the highest rate that your terminal equipment will handle to maximize performance, unless a limitation on the available bandwidth is desired. If the DTE is a personal computer, the port can usually be used reliably at 115200. Issuing the &Fx command (factory default) does not affect the current setting of S102.

## S Register 103 - Wireless Link Rate

The Wireless Link Rate is the speed and optimization method for which modems will communicate over the RF link. It is only necessary to set this parameter on the Master unit. Units configured as Repeaters and Slaves will ignore this setting, and adjust automatically to the rate of the Master.

The allowable settings are:

*2	<b>Fast without Forward Error Correction</b>
4	Fast with Forward Error Correction

Depending on the application requirements, each mode will provide different throughput and performance. Appendix E. Performance Tables give some indication of the performance to be expected in each mode.

In general, Forward Error Correction (FEC) reduces throughput, but in some environments will actually increase throughput. FEC can reduce the number of bad data packets, and hence reduce the need to retransmit.



The Master determines the Wireless Link Rate. This setting on all other modems is ignored..



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



**Warning:** SIMREX CORPORATION strongly recommends changing the Network Address to a value different from the factory default before deploying the network.



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 104 - Network Address

The Network Address defines the 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.

**Default is 1.**

## 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. This register also serves as the starting unit address of a range of unit addresses that a point-to-point master communicates with in TDMA mode. See the description of registers S124 and S125 for a complete explanation of TDMA mode.

## S Register 106 - Primary Hopping Pattern

## S Register 206 - Secondary Hopping Pattern

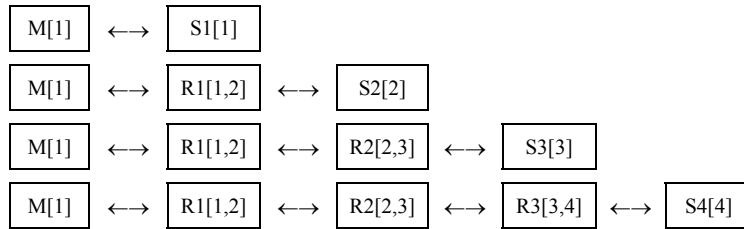
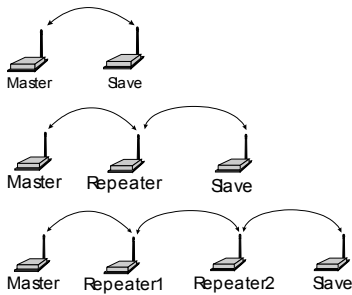
Since the SP 2.4 is a frequency-hopping modem, the carrier frequency changes periodically according to one of 49 pseudo-random patterns, defined by the Primary and Secondary Hopping Patterns. Valid entries for each are 0 through 48. Patterns 44 through 48 are user-editable patterns. See Appendix F for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

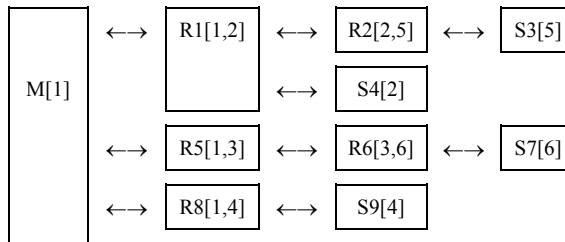
- $M$  indicates Master;
- $R$  indicates Repeater;
- $S$  indicates Slave;
- $x$  is the Unit Address;
- $a$  is the primary hopping pattern; and,
- $b$  is the secondary hopping pattern;

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




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:

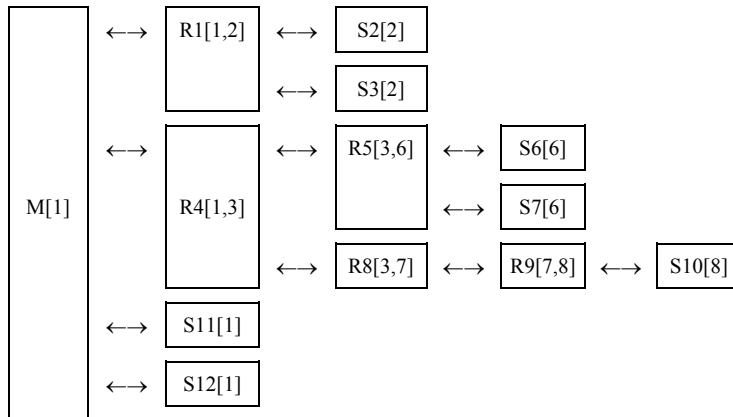
 Slaves and Masters do not use Secondary Hopping Patterns



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:



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.



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



**Warning:** SIMREX CORPORATION strongly recommends changing the Encryption Key to a value different than the factory default before deploying the network.

## S Register 107 - 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.

## S Register 108 - Output Power Level

The Output Power Level determines at what power the SP 2.4 transmits. The SP 2.4'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	<b>100 mW</b>	6	1 W
3	250 mW		

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
1 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.
10 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.

---



The hopping interval is controlled by the master. The slave and repeater units will use the hopping interval setting from the master.

## S Register 109 - Hopping Interval

This option determines the frequency at which the modems change channel. Note that the Master controls this parameter for the entire network. This setting is ignored in units configured as Slaves or Repeaters.

The allowable settings are:

1	8 msec
2	12 msec
3	16 msec
*4	20 msec
5	30 msec
6	45 msec
7	80 msec
8	120 msec
9	100 msec



**Warning:** Communication will fail if the hopping interval is not set according to the guidelines of Appendix E.

Some of the shorter hop intervals are incompatible in combination with:

- repeaters in the system;
- the value set for link rate (S103); and,
- larger maximum packet sizes (S112).

See Appendix E for optimal Hopping Interval settings in relation to packet size and link rate.

## S Register 110 - Data Format

This register determines the format of the data on the serial port. Allowable settings are:

*1	8 bits, No Parity, 1 Stop
2	8 bits, No Parity, 2 Stop
3	8 bits, Even Parity, 1 Stop
4	8 bits, Odd Parity, 1 Stop
5	7 bits, No Parity, 1 Stop
6	7 bits, No Parity, 2 Stop
7	7 bits, Even Parity, 1 Stop
8	7 bits, Odd Parity, 1 Stop
9	7 bits, Even Parity, 2 Stop
10	7 bits, Odd Parity, 2 Stop
11	9 bits, No Parity, 1 Stop

## S Register 111 - Packet Minimum Size

## S Register 112 - Packet Maximum Size

## S Register 114 - Packet Size Control

## S Register 116 - Packet Character Timeout

These settings determine the conditions under which the modem will transmit accumulated data over the air.

### S Register 111 - Minimum Size

Valid entries for this register are 1 to 255 bytes, which defines the minimum number of bytes to receive from the DTE before encapsulating them in a packet and transmitting over the air.

Note that if register S114=0 at any particular Repeater or Slave, that Repeater or Slave will ignore its own S111 register and abide by the Master's S111 setting. If S114=1 at any particular Repeater or Slave, that Repeater or Slave will use its own local S111 setting. The default for S111 is 1 byte.

### S Register 112 - Maximum Size

This setting has a range of 2 to 255, and defines the maximum number of bytes from the DTE which should be encapsulated in a packet. This value should be greater than the minimum packet size, but not smaller than is necessary for reliable communications. If the wireless link is consistently good and solid, a maximum size of 255 will yield the best throughput (depending on the higher level protocols of the connected equipment). However, if the link is poor (e.g., experiencing excessive interference) and data is frequently retransmitted, the maximum packet size should be reduced. This decreases the probability of errors within packets, and reduces the amount of traffic in the event that retransmissions are required.

Note that if register S114=0 at any particular Repeater or Slave, that Repeater or Slave will ignore its own S112 register and abide by the Master's S112 setting. If S114=1 at any particular Repeater or Slave, that Repeater or Slave will use its own local S112 setting. The default for S112 is 255 bytes.



When S114=0, the Minimum and Maximum Packet Size is controlled by the Master, therefore, the Slave and Repeater units will use the Minimum and Maximum Packet Size setting from the Master.

When S114=1, Slave and Repeater units will use their local S111 and S112 settings for packet size control in point-to-point mode

### **S Register 114 - Packet Size Control**

This register, when set to 1, allows for Repeater and Slaves' local S111 and S112 to override those of the Master when the system is operating in point-to-point mode. This may be useful for controlled asymmetrical data flow. The master always transmits in the first portion of the hop interval, with slaves and repeaters responding back to the master on the second portion of the hop interval. Setting the master's max packet size smaller than that of the slave would ensure that the master uses less of the available time within the hop interval for transmitting data, thereby allocating more time for the slave.

### **S Register 116 - Packet Character Timeout**

This register has valid entries of 0 to 254 milliseconds. The Packet Character Timeout timer looks for gaps in the data being received from the DTE. The timer is only activated after the Minimum Packet Size has been accumulated in the modem. After which, if the timer detects a gap in the data exceeding the Packet Character Timeout value, the modem will transmit the data.

The SP 2.4 will accumulate data in its buffers from the DTE until one of the following requirements is met (whichever occurs first):

- The Maximum Packet Size (in bytes) has been accumulated;
- The Minimum Packet Size has been accumulated AND the Packet Character Timeout interval has elapsed.

The default for the Packet Character Timeout is 8 ms. If set to 0 ms, the unit will buffer exactly the minimum packet size before transmitting.

### **S Register 113 - Packet Retransmissions**

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 data packet exactly the number of times defined by the Packet Retransmissions parameter. 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 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 until the limit is reached. This parameter is not necessary in Slave units since all Slaves receive acknowledgement from the Master, and needn't blindly retransmit if it has knowledge that the Master has received the packet. 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. The valid settings for this parameter are 0 to 255 retransmissions. The default is 1.

### **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 modem 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 115 - Packet Repeat Interval**

A parameter that is specific to Slaves and Repeaters is the Packet Repeat Interval.

The allowable settings are 1 through 255. The default is 1.

This parameter defines a range of random numbers that the Slave will use as the next slot in which it will attempt to send the packet. For example, if this register is set to 7, the Slave will choose a number between one and seven as the next slot in which to transmit. Suppose the random number generator picks 5, then the Slave will transmit in the fifth time slot. A Slave will transmit a maximum of once per hopping interval, however, depending on the duration of the hopping interval and the maximum packet size, more than one slot per hop is potentially available. The Slave will transmit more frequently when a Repeat Interval with a smaller range is selected. Choose 1 to have the Slave transmit in the first available slot. Choose higher intervals for less frequent transmission, or to avoid collisions between many Slaves in the system.

This register is always disregarded and taken as S115=1 in Point-to-Point mode.

## S Register 117 - Modbus Mode

Modbus Mode allows for the SP 2.4 to be fully Modbus compatible. For Modbus operation, the general requirement is to get the packet of data to the receiving serial port with no gaps in the data. The SP 2.4 incorporates a “Modbus Mode” which implements a delay at the receiving modem to ensure that no gaps are introduced. For most applications, the following settings are suitable for Modbus operation:

1. Set Modbus Mode parameter S117 = 1
2. Set the minimum packet size (S111) to 1 byte
3. Set the character timeout S116 (rounded to the nearest ms) to roughly 2.5 byte lengths. For example, at 9600 baud,  
$$S116 = 1/9600 \times 10 \times 2.5 \times 1000 = 2.6\text{ms}$$
  
Rounded up, S116 = 3ms
4. Set parameter S121 = 3 byte lengths. For example, at 19200 baud  
$$S121 = 1/19200 \times 10 \times 3 \times 1000 = 1.56\text{ms}$$
  
Rounded up, S121 = 2ms
5. Set S120 as follows:  
Slave Side  
$$S120 = (\text{Hop Interval in ms}) \times (1 + \# \text{ of Master retransmissions}) \times (1 + \# \text{ of Repeaters over 1})$$
  
eg. Hop Interval S109=4 (20 ms),  
Master Retransmissions S113=1  
Number of Repeaters in system = 2; then,  
$$S120 = 20 \times (1 + 1) \times (1 + 1) = 80 \text{ ms}$$
  
Master Side  
$$S120 = (\text{Hop Interval in ms}) \times (1 + \# \text{ of Repeaters over 1})$$
6. Try to set the hop interval as short as possible while still ensuring adequate throughput. It is recommended to set the Hop Interval and Maximum Packet Size as specified in Appendix E. Performance Tables. For example, for Master to Slave communication with no FEC, If a throughput of 60kbps is required, set the Hop Interval S109=3, and set the Maximum Packet Size S112=110.

The allowable settings for this register are:

<b>*0</b>	<b>Disabled</b>
1	Enabled

## 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 having the same network address and encryption key, but without regard for the hopping pattern S106. Once the slave/repeater finds such a master, it tunes to that master's hopping pattern. If synchronization is lost, the slave/repeater will again begin searching for a new master. Using this algorithm, a mobile unit can 'roam' and automatically synchronize with a new master once it loses communication with the previous one. It is essential that all Masters with which a roaming slave/repeater will be communicating with use a hopping pattern from within the same group. See Appendix F. The allowable settings for this register are:

\*0 Disabled  
1 Enabled

## S Register 119 - Quick Enter to Command

By setting this register to 1, a delay of 5 seconds is introduced at power-up before the modem goes into data mode. If, during these 5 seconds, the user enters 'mhx' the modem will instead go into Command Mode, and reply with 'OK'. The terminal baud rate must be set to 9600 baud. If an incorrect character is entered, the modem will immediately go into Data Mode. The default setting is 1 - Enabled.

## S Register 120 - RTS/DCD Framing

### S Register 121 - DCD Timeout

The SP 2.4 supports two special types of data framing:

- Input (or RTS/CTS) Data Framing; and,
- Output (or DCD) Data Framing

Input Data Framing is enabled by configuring the Handshaking Parameter as &K2. This type of framing makes use of the S120 parameter as illustrated in Figure 9. Parameter S120 can be set to any value between 0 and 254 ms.

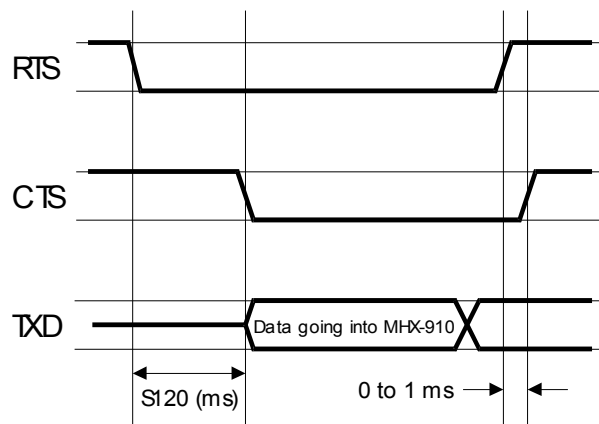


Figure 9 - Input Data Framing

To enable output (DCD) data framing, set the Data Carrier Detect parameter as &C2. This type of framing uses both S120 and S121 registers as shown in Figure 10. Valid ranges for each parameter are 0 to 254 ms



**Figure 10 - Output Data Framing**

### **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 124 - TDMA Duty Cycle**

### **S Register 125 - TDMA Max Address**

These two registers are valid when the SP 2.4 is configured as a point-to-point master (S101=2). Along with register S105, registers S124 and S125 define the range and duration for TDMA communication. In TDMA communication, the master allows data transfer with only one slave at a time. The master will first communicate with the slave or repeater whose unit address matches its own (i.e., register S105). The master will enable communication with this slave or repeater for the number of hop intervals defined by S124. The master will then increment the unit address of the slave with which it will communicate by one, and again communicate with the next slave for  $x$  number of hops, where  $x$  is set by register S124. This pattern continues until the TDMA Max Address is reached. For example, if the point-to-point master's S105=3, S124=3, and S125=30, the master will allow communication with the slave whose unit address is 3 for 3 hop intervals, followed by 3 hop intervals of communication with the slave whose unit address is 4, and so on up to the slave whose unit address is 30. At this point, the master begins the cycle back at the slave whose unit address is 3.

Some tips and important points to remember about TDMA are as follows:

- The number of TDMA slaves cannot exceed 200, i.e., the difference between the TDMA master's S125 and S105 registers cannot exceed 199.
- To disable TDMA, set S124=0, or set S125 less than S105. By factory default, TDMA is disabled.
- TDMA may be used in conjunction with Address Filtering and Multicast Association (see the description of S127 and S128). For example, it may be desirable to broadcast the Master's data to all Slaves, but receive in a TDMA fashion. To do this, set the Master's S105=0, and set all Slave's S127=1 and S128=1.
- It is possible to use repeaters in a TDMA system; however, there is no guarantee that the Master will receive packets sequentially from the Slaves in the system.
- It may be advisable to use output framing at the Master to keep track of which slave the packet is coming from (See S126 for details).
- Set Packet Retry Limit (S213) equal to one less than the Master's TDMA Duty Cycle on all units.
- All repeaters and slaves in the system must have a unique unit address which falls within the TDMA address range.
- TDMA networks which include repeaters can be difficult to set up. Contact Technical Support for assistance.

### **S Register 126 - Data Protocol**

This register controls the way in which the modem treats data to and from the user. Both the input and output may be framed or transparent as follows:

<b>S126</b>	<b>Input</b>	<b>Output</b>
<b>0</b>	Transparent	Transparent
<b>1</b>	Framed	Transparent
<b>2</b>	Transparent	Framed
<b>3</b>	Framed	Framed

In the transparent mode, the modem treats data from the user as a continuous stream. This is normal operation for the SP 2.4. When input framing is implemented, the data is sent to the modem from the user in frames which are separated by a time interval. The user can select the minimum time interval separation by defining an interval in milliseconds in register S116. When the modem detects a gap in the user's stream exceeding this value, the next byte of data is considered to be the start of a new frame. Input frames are structured as follows: The 1<sup>st</sup> byte is the upper byte of the recipient's unit address; the 2<sup>nd</sup> byte is the lower byte of the recipient's unit address; the bytes which follow make up the remainder of the data frame. There is no limit to the number of bytes in a frame. When input framing is implemented, it overrides the Unit Address defined by S105.

When output framing is implemented, three additional bytes of data are output to the user at the beginning of every received packet of data. The first byte is the upper byte of the original sender's unit address, the second byte is the lower byte, and the third byte is the packet length. No extra measures are taken to define the beginning of a frame.

### **S Register 127 - Address Filtering**

### **S Register 128 - Multicast Association**

Address Filtering and Multicast Association are registers which are valid for slaves. Each can be either disabled (0) or enabled (1). Address filtering allows more flexibility in defining which packets of data the slave will accept from the master. Multicast Association is a subset of Address Filtering and allows the slave to be a part of a special "multicast" group, separate from the rest of the network.

There are two unit address values – 0 and 65535 – which, when assigned to the master, have special meaning. When the master's Unit Address is 0, slaves associated with the multicast group will receive the master's data. When the master's Unit Address is 65535, all slaves with Address Filtering enabled will receive the master's data. The following table describes the operation of the slave for the different scenarios:

	<b>Network Master is a Point-to-Point Master</b>	<b>Network Master is a Point-to-Multipoint Master</b>
<b>Slave's S127=0 and S128=don't care (traditional SP 2.4 operation)</b>	Slave will receive and transmit data only if its Unit Address matches that of the Master	Slave will receive and transmit data with the Master without restriction
<b>Slave's S127=1 and S128=0</b>	Slave will receive data when the Master's Unit Address is 65535, or when it matches that of the Slave. Slave will transmit only when its Unit Address matches the Master's.	Slave will receive data when the Master's Unit Address is 65535, or when it matches that of the Slave. Slave may transmit regardless of the Master's Unit Address.
<b>Slave's S127=1 and S128=1</b>	In addition to the above, the Slave will also receive data from the Master if the Master's Unit Address is 0.	In addition to the above, the Slave will also receive data from the Master if the Master's Unit Address is 0.

### **S Register 129 - Secondary Master**

In systems which have more than one master in close proximity, it is desirable to have all masters transmitting at the same time. Set the primary master as &S3 and S129=0. This will provide a synchronizing pulse on the DSR line, which should be tied to the DTR line of all secondary masters. Secondary masters must be set as &D0 and S129=1. The hopping interval on all masters must match

## 4.4 Diagnostics, Statistics and Remote Control

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

### 4.4.1 Spectrum Analyzer Feature (ATG)

Issuing the command ATG <return>, causes the SP 2.4 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 202 -135dBm  *
```

Channel 1 is at frequency 2.4016 GHz, 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 <return> 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 2.4 starts the statistics count at zero each time the unit is powered up, or after the ATP command has been issued. By entering the ATP command, all statistics are cleared 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 user to remotely configure and interrogate all units in a multipoint system from the Master unit. Simply by having knowledge of the unit address of each slave/repeater in the system, 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 <return>
```

The remote slave/repeater will send back the value of 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 modem.
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
1(x)	S102	Baud Rate
2(x)	S108	Output Power
3(x)	S110	Data Format
4(x)	S115	Repeat Interval
5(x)	S116	Character Timeout
6(x)	S120	RTS/DCD Framing
7(x)	S121	DCD Timeout
8(x)	S117	Modbus Mode
9(x)	S213	Retry Limit
a	test string	Read back 'OK' from remote
b(x)	&E	Framing
c(x)	&C	DCD
d(x)	&K	Handshaking
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
l(x)	S119	Quick Enter to Command Mode
m(x)	S118	Roaming
n(x)	S114	Packet Size Control
o(x)	S111	Min Packet Size
p(x)	S112	Max Packet Size
q(x)	S128	Multicast Group
.(x)	S126	Data Protocol
/(x)	S127	Address Filtering

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
t(x)	S109	Hopping Interval
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 2.4 complies with FCC part 15 for operation in the license-free 2.4000 to 2.4835 GHz ISM band. This chapter provides guidelines for installing and deploying equipment which incorporates the SP 2.4 module.

## 5.1 Estimating the Gain Margin

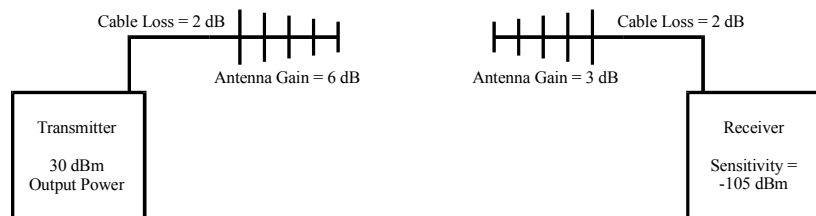
Successful communication between SP 2.4's is dependent on three main factors:

- 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 0, 10, 20 or 30 dBm)
2. Transmitter gain (transmitting antenna gain minus cabling loss between the transmitting antenna and the SP 2.4)
3. Receiver gain (Receiving antenna gain minus cabling loss between the receiving antenna and the modem)
4. Receiver sensitivity (Specified as -105 dBm on the SP 2.4)

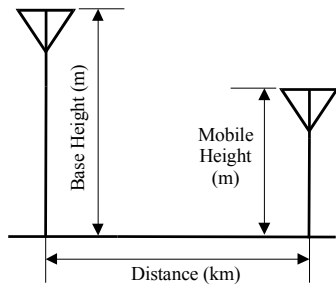
In the following illustration, the transmitting antenna has a gain of 6 dB, and the receiving antenna has a gain of 3 dB. The cable loss between the modem and the antenna is 2 dB on both the transmitting and receiving side.



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

System gain would be calculated to be:

$$30 - 2 + 6 + 3 - 2 + 105 = 140 \text{ dB.}$$



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 2.4

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 2.4 is generating RF energy. Always ensure that the SP 2.4 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.



*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 2.4 is generating RF energy. Always ensure that the SP 2.4 equipment is powered down during installation.*



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

### 5.2.3 Antenna

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 2.4 set to full power, ERP is calculated as follows:

$$\text{ERP} = 30 - (\text{Cabling and Connector Losses}) + (\text{Antenna Gain}) < 36$$

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 2.4 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 2.4 antenna can desensitize the receiver. SIMREX CORPORATION' 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. Modem Command Summary

The following provides a command summary for the SP 2.4. Factory settings are denoted with a ‘\*’.

## AT Commands

A	Answer
E	Command Echo E0 No Echo * E1 Command Echo
I	Identification I0 Custom I1 Product Code I2 ROM Checksum test I3 Firmware Version I4 Firmware Date I6 Firmware Time I7 Serial Number
O	On-line Mode
Q	Quiet Mode * Q0 Enables Result Codes Q1 Disables Result Codes Result Codes Display
V	V0 Display as Numbers * V1 Display as Words
W	Connection Result * W0 Reports DTE as CONNECT xxxx W1 DTE) rate as CARRIER xxxx. W2 Reports DCE as CONNECT xxxx
Z	Reset and load stored configuration
&C	DCD (Data Carrier Detect) *&C0 DCD is always on &C1 DCD is on when modems are synchronized &C2 DCD used for output data framing &C3 DCD sync pulse
&D	DTR (Data Terminal Ready) *&D0 DTR ignored &D2 DTR disconnects and switches to command &D3 DTR disconnects and resets modem
&F	Load Factory Default &F1 Master &F2 Slave &F3 Repeater &F4 Slave through Repeater
&K	Handshaking &K0 Disable Handshaking &K2 RTS/CTS Input Framing * &K3 Enable Handshaking
&S	DSR (Data Set Ready) &S0 DSR is always on * &S1 DSR on in data, off in command mode &S2 DSR/DTR signaling
&V	View Configuration
&W	Write configuration to memory
Sxx?	Read S register value
Sxx=yy	Set S register value
<b>Result Codes</b>	
0	OK 18 CONNECT 9600
3	NO CARRIER 17 CONNECT 14400
4	ERROR 16 CONNECT 19200
22	CONNECT 2400 15 CONNECT 28800
21	CONNECT 3600 14 CONNECT 38400
20	CONNECT 4800 13 CONNECT 57600
19	CONNECT 7200 12 CONNECT 115200
8	CARRIER 43000 6 CARRIER 84000

## S Registers

S0	Auto Answer 0 = power up in Command Mode, *1 = power up in Data Mode
S2	Escape code [0...255] default '+' (43)
S3	CR character [0...255] default <cr> (13)
S4	Line Feed [0...255] default <lf> (10)
S5	Backspace [0...255] default <bs> (8)
S101	Operating Mode 1 - Master Point to Multipoint 2 - Master Point to Point 3 - Slave 4 - Repeater 5 - Master Diagnostics
S102	Serial Baud Rate 1 = 115200, 2 = 57600, 3 = 38400 4 = 28800, 5 = 19200, 6 = 14400 *7 = 9600, 8 = 7200, 9 = 4800, 10 = 3600, 11 = 2400
S103	Wireless Link Rate *2 = Fast w/o FEC 4 = Fast with FEC
S104	Network Address [0...65535]
S105	Unit Address [1...65535]
S106	Primary Hopping Pattern [0...48]
S206	Secondary Hopping Pattern [0...48]
S107	Encryption Key [0...65535]
S108	Output Power Level 0 = 10 mW, 1 = 50 mW, *2 = 100 mW, 3 = 250 mW 4=500mW, 5=750mw, 6=1W
S109	Hopping Interval 1 = 8 msec, 2 = 12 msec, 3 = 16 msec, *4 = 20 msec, 5 = 30 msec, 6 = 45 msec, 7 = 80 msec, 8 = 120 msec, 9 = 100 msec
S110	Data Format * 1 = 8N1, 2 = 8N2, 3 = 8E1, 4 = 8O1 5 = 7N1, 6 = 7N2, 7 = 7E1, 8 = 7O1 9 = 7E2, 10 = 7O2, 11 = 9N1
S111	Packet Minimum Size [1...Maximum Size]
S112	Packet Maximum Size [2...255]
S113	Packet Retransmissions [0...255]
S213	Packet Retry Limit [0...255]
S114	Packet Size Control *0=Disabled, 1=Enabled
S115	Packet Repeat Interval [1...255] Default = 1
S116	Packet Character Timeout [0...254 ms]
S117	Modbus Mode *0 = Disabled, 1 = Enabled
S118	Roaming *0 = Disabled, 1 = Enabled
S119	Quick Enter to Command 0 = Disabled, *1 = Enabled
S120	RTS/DCD Framing Interval [0...254 ms]
S121	DCD Timeout [0...254 ms]
S122	Remote Control *0 = Disabled, 1 = Enabled
S123	RSSI (dBm)
S124	TDMA Duty Cycle
S125	TDMA Max Address
S126	Data Protocol
S127	Address Filtering
S128	Multicast Group
S129	Secondary Master



# B. Serial Interface

The SP 2.4 uses 8 pins on the DB9 connector for asynchronous serial I/O.

The signals in the asynchronous serial interface are described below:

**DCD** *Data Carrier Detect - Output from Modem* - When asserted (TTL low), DCD informs the DTE that a communications link has been established with another SP 2.4.

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

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

**DTR** *Data Terminal Ready - Input to Modem* - Asserted (TTL low) by the DTE to inform the modem that it is alive and ready for communications.

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

**DSR** *Data Set Ready - Output from Modem* - Asserted (TTL low) by the DCE to inform the DTE that it is alive and ready for communications. DSR is the modem's equivalent of the DTR signal.

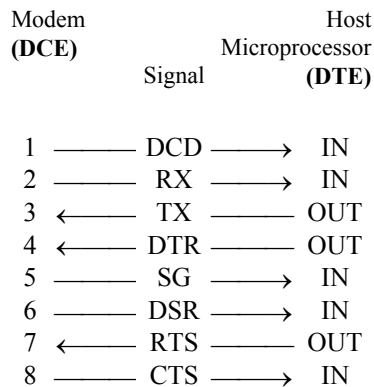
**RTS** *Request to Send - Input to Modem* - A "handshaking" signal which is asserted by the DTE (TTL low) when it is ready. When hardware handshaking is used, the RTS signal indicates to the DCE that the host can receive data.

**CTS** *Clear to Send - Output from Modem* - A "handshaking" signal which is asserted by the DCE (TTL low) when it has enabled communications and transmission from the DTE can commence. When hardware handshaking is used, the CTS signal indicates to the host that the DCE can receive data.

*Notes:* It is typical to refer to RX and TX from the perspective of the DTE. This should be kept in mind when looking at signals relative to the modem (DCE); the modem *transmits* data on the RX line, and *receives* on TX.

"DCE" and "modem" are often synonymous since a modem is typically a DCE device.

"DTE" is, in most applications, a device such as a host microprocessor.



Arrows denote the direction that signals are asserted (e.g., DCD originates at the DCE and tells the DTE that a carrier is present).



# C. Factory Default Settings

## AT&F1 - Master Default Settings

E1, Q0, V1, W0, S0=1, S2=43, S3=13, S4=10, S5=8

DCD	&C1 (On)
DTR	&D0 (DTR is ignored)
Framing	&E0 (Disabled)
Handshaking	&K3 (Enabled)
DSR	&S1 (On in Data, Off in Command)
Operating Mode	S101=1 (Master P-MP)
Serial Baud Rate	S102=7 (9600 baud)
Wireless Link Rate	S103=2 (Fast, No FEC)
Network Address	S104=1
Unit Address	S105=1
Primary Hop Pattern	S106=0
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Hop Interval	S109=4
Data Format	S110=1 (8N1)
Packet Minimum Size	S111=1
Packet Maximum Size	S112=43
Packet Retransmissions	S113=1
Packet Size Control	S114=0
Packet Repeat Interval	S115=1 (Don't Care)
Character Timeout (ms)	S116=8
Modbus Mode	S117=0
Roaming	S118=0
Quick Enter to Command	S119=1
RTS/DCD Framing (ms)	S120=0
DCD Timeout (ms)	S121=0
Remote Control	S122=0
TDMA Duty Cycle	S124=0
TDMA Max Address	S125=200
Data Protocol	S126=0
Address Filtering	S127=0 (Don't Care)
Multicast Group	S128=0 (Don't Care)
Secondary Master	S129=0
Secondary Hop Pattern	S206=2 (Don't Care)
Packet Retry Limit	S213=2 (Don't Care)

## AT&F2 - Slave Default Settings

E1, Q0, V1, W0, S0=1, S2=43, S3=13, S4=10, S5=8

DCD	&C1 (On)
DTR	&D0 (DTR is ignored)
Framing	&E0 (Disabled)
Handshaking	&K3 (Enabled)
DSR	&S1 (On in Data, Off in Command)
Operating Mode	S101=3 (Slave)
Serial Baud Rate	S102=7 (9600 baud)
Wireless Link Rate	S103=2 (Fast, No FEC) (Set by Master)
Network Address	S104=1
Unit Address	S105=2
Primary Hop Pattern	S106=0
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Hop Interval	S109=4 (Set by Master)
Data Format	S110=1 (8N1)
Packet Minimum Size	S111=1
Packet Maximum Size	S112=43
Packet Retransmissions	S113=1 (Don't Care)
Packet Size Control	S114=0
Packet Repeat Interval	S115=1
Character Timeout (ms)	S116=8
Modbus Mode	S117=0
Roaming	S118=0
Quick Enter to Command	S119=1
RTS/DCD Framing (ms)	S120=0
DCD Timeout (ms)	S121=0
Remote Control	S122=0
TDMA Duty Cycle	S124=0 (Don't Care)
TDMA Max Address	S125=200 (Don't Care)
Data Protocol	S126=0
Address Filtering	S127=0
Multicast Group	S128=0
Secondary Master	S129=0 (Don't Care)
Secondary Hop Pattern	S206=2 (Don't Care)
Packet Retry Limit	S213=2

## AT&F3 - Repeater Default Settings

E1, Q0, V1, W0, S0=1, S2=43, S3=13, S4=10, S5=8

DCD	&C1 (On)
DTR	&D0 (DTR is ignored)
Framing	&E0 (Disabled)
Handshaking	&K3 (Enabled)
DSR	&S1 (On in Data, Off in Command)
Operating Mode	S101=4 (Repeater)
Serial Baud Rate	S102=7 (9600 baud)
Wireless Link Rate	S103=2 (Fast, No FEC) (Set by Master)
Network Address	S104=1
Unit Address	S105=3
Primary Hop Pattern	S106=0
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Hop Interval	S109=4 (Set by Master)
Data Format	S110=1 (8N1)
Packet Minimum Size	S111=1
Packet Maximum Size	S112=43
Packet Retransmissions	S113=1
Packet Size Control	S114=0
Packet Repeat Interval	S115=1
Character Timeout (ms)	S116=8
Modbus Mode	S117=0
Roaming	S118=0
Quick Enter to Command	S119=1
RTS/DCD Framing (ms)	S120=0
DCD Timeout (ms)	S121=0
Remote Control	S122=0
TDMA Duty Cycle	S124=0 (Don't Care)
TDMA Max Address	S125=200 (Don't Care)
Data Protocol	S126=0
Address Filtering	S127=0
Multicast Group	S128=0
Secondary Master	S129=0 (Don't Care)
Secondary Hop Pattern	S206=2
Packet Retry Limit	S213=2

## AT&F4 -Slave Through Repeater Default Settings

E1, Q0, V1, W0, S0=1, S2=43, S3=13, S4=10, S5=8

DCD	&C1 (On)
DTR	&D0 (DTR is ignored)
Framing	&E0 (Disabled)
Handshaking	&K3 (Enabled)
DSR	&S1 (On in Data, Off in Command)
Operating Mode	S101=3 (Slave)
Serial Baud Rate	S102=7 (9600 baud)
Wireless Link Rate	S103=2 (Fast, No FEC) (Set by Master)
Network Address	S104=1
Unit Address	S105=4
Primary Hop Pattern	S106=2
Encryption Key	S107=1
Output Power	S108=2 (100mW)
Hop Interval	S109=4 (Set by Master)
Data Format	S110=1 (8N1)
Packet Minimum Size	S111=1
Packet Maximum Size	S112=43
Packet Retransmissions	S113=1 (Don't Care)
Packet Size Control	S114=0
Packet Repeat Interval	S115=1
Character Timeout (ms)	S116=8
Modbus Mode	S117=0
Roaming	S118=0
Quick Enter to Command	S119=1
RTS/DCD Framing (ms)	S120=0
DCD Timeout (ms)	S121=0
Remote Control	S122=0
TDMA Duty Cycle	S124=0 (Don't Care)
TDMA Max Address	S125=200 (Don't Care)
Data Protocol	S126=0
Address Filtering	S127=0
Multicast Group	S128=0
Secondary Master	S129=0 (Don't Care)
Secondary Hop Pattern	S206=2 (Don't Care)
Packet Retry Limit	S213=2



# D. Performance Tables

The scope of this appendix is to find the best possible performance and maximum packet size at different modes of operation. The setup assumes a baud rate of 115k, no retries and no retransmissions.

**WARNING: Communication will fail if the maximum packet size (S112) exceeds the recommended optimal packet size. .**

	Hop Interval	Optimal Packet Size (bytes)	Throughput (kbps)*
Slave <--> Master Communication. (No Repeater)  Link Rate S103=2	1 (8 ms)	14	20
	2 (12 ms)	66	52
	3 (16 ms)	110	66
	4 (20 ms)	154	74
	5 (30 ms)	255	83
	6 (45 ms)	255	56
	7 (80 ms)	255	31
	8 (120 ms)	255	21
Slave <--> Master Communication. (No Repeater)  Link Rate S103=4	1 (8 ms)	5	4
	2 (12 ms)	34	22
	3 (16 ms)	54	28
	4 (20 ms)	76	32
	5 (30 ms)	130	38
	6 (45 ms)	210	43
	7 (80 ms)	255	30
	8 (120 ms)	255	20
Repeater <--> Master Direct Communication.  Link Rate S103=2	1 (8 ms)	N/A	N/A
	2 (12 ms)	3	1
	3 (16 ms)	22	13
	4 (20 ms)	44	21
	5 (30 ms)	101	32
	6 (45 ms)	178	39
	7 (80 ms)	255	31
	8 (120 ms)	255	21
Repeater <--> Master Direct Communication.  Link Rate S103=4	1 (8 ms)	N/A	N/A
	2 (12 ms)	N/A	N/A
	3 (16 ms)	5	2
	4 (20 ms)	16	6
	5 (30 ms)	43	12
	6 (45 ms)	80	16
	7 (80 ms)	174	20
	8 (120 ms)	255	20
Slave <--> Master Through One or More Repeaters.  Link Rate S103=2	1 (8 ms)	N/A	N/A
	2 (12 ms)	3	1
	3 (16 ms)	22	13
	4 (20 ms)	43	21
	5 (30 ms)	93	31
	6 (45 ms)	174	38
	7 (80 ms)	255	31
	8 (120 ms)	255	21
Slave <--> Master Through One or More Repeaters.  Link Rate S103=4	1 (8 ms)	N/A	N/A
	2 (12 ms)	N/A	N/A
	3 (16 ms)	N/A	N/A
	4 (20 ms)	14	6
	5 (30 ms)	40	12
	6 (45 ms)	80	16
	7 (80 ms)	174	19
	8 (120 ms)	255	20



# E. 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



# F. Technical Specifications

## Electrical/Physical

Data Interface	Asynchronous RS-232
Signals	Sig. Gnd, TX, RX, DCD, DSR, DTR, RTS, CTS
Bandwidth / Data Rate	2,400 - 115,200 bps, uncompressed half-duplex, Approx. 85 kbps sustained in intelligent asymmetrical full-duplex transmission mode
Communications Range <sup>1</sup>	30 kilometres (19 miles)
Voltage Requirements	12 - 30 VDC,
Power Consumption	450 mA max, 250 mA typical at 1W transmit; 200 mA receive at 12V
Operating Frequency	2.4000 to 2.4835 GHz
System Gain	135 dB
Sensitivity	-105 dBm
Output Power	10 to 1000mW (user-selectable)
Spreading Code	Frequency Hopping
Hopping Patterns	49 pseudo-random, user-selectable
Error Detection	CRC-16 with auto re-transmit
Error Correction	User-selectable Forward Error Correction (FEC)
Adjacent Channel Rejection	> 60 dB
In-band Rejection	> 70 dB
Out-of-band Rejection	> 80 dB
Dimensions (LxWxH)	Encl: 3.5" x 4.25" x 1.7"
Weight	400 grams
Operating Environment	Temperature: -40 to +70°C Humidity: 5 to 95%, non-condensing
Storage Temperature	-40 to 90°C
Approvals	FCC, IC

1. Clear line-of-sight, elevated high-gain antennas.



# G. Glossary

## Terminology Used in the SP 2.4 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).