EEPROM Map

Location	Parameter
000	A5 (165 decimal) indicating that this EEPROM has been initialized. This value is always set to 0xA5 if the EEPROM has been initialized. When the microcontroller firmware is erased, the internal EEPROM also gets erased. When the firmware runs, it detects whether this byte contains an 0xA5 to know whether to load the rest of the values or to pick some reasonable defaults until the EEPROM gets downloaded. The defaults consist of intelligent mode, 19200 bps, no flow control, no crc checks.
001	Interface State flags
002-005	HORNET local address
006-009	broadcast address 1
010-013	broadcast address 2
014	Max Packet Tries
015	RF Packet Length
016	Number of Ring Packets
017-020	Channel Tuning 'A' values (channels 1-4, respectively)
021-024	Channel Tuning 'B' values (channels 1-4, respectively)
025	Link Activity Threshold
026	Link Threshold1
027	Link Threshold2
028	Link Threshold3
029	Link Threshold4
030	Peak Offset
031-032	Sleep Time (Value to give to ASIC for how long it should sleep between polls)
	***** End of Values loaded into ASIC at powerup *****
033	Channel Mask
024	Link Timeout (How long to wait for a remote reply to a packet)
035	RNR Timeout (How long to wait for RTS after receiving a frame before issuing RNR)
036	0 if disabling RF receive capability (ie. scanner device)
037	Radio Flags (bit 0: Ignore Flow Control if set)
038	Transparent Buffer Delay
039	HoldLinkMode: 0=no wait, 1=until RTS, 2=until flush
040	DataRate as programmed into chip: 23=9600, 11=19200, 5=38400, 3=57600, 1=115200
041	Sleep Enabled flag: 00=disabled, anything else = enabled
042	Max Frame Tries
043-048	Firmware Version String
049-052	Default Destination
053	CSMA/CA setting
054-215	Unused
216-255	Transparent Receive List (10 entries * 4 bytes each)
256-511	ID Table
256	Field ID of first entry
257	Length of first entry
258	First byte of first entry (or second Field ID if first was 0 length) and so on until Field ID entry is 0 indicating no more ID Entries

Chapter 3
Interface

Mechanical Interfaces

Size

The Hornet utilizes a single Printed Wiring Board which will be 1.0'' x 1.5" x 0.3. The full mechanical specifications can be found in Appendix A.

Connector

The Connector on the HORNET is a 14 pin, 0.50 mm pitch FPC/FFC connector, JST part number 14FLZ-RSM1-TB or equivalent. Alternate part is 14FL-RSM1-TB. Orientation of pin 1 is shown in **Error! Reference source not found.**.

Physical Layout

The approximated physical layout is shown in the mechanical detail contain in Appendix A. The bottom side of the board contains both the digital circuitry and the Host/HORNET connector. The RF circuitry (top) is shielded with a metal can.

Antenna

The preliminary placement of a printed antenna is shown. For optimum performance, all metal (sidewalls, guides, etc.) should be kept a minimum of 0.TBD" away from these edges. It may be necessary to offset the HORNET to one side of the cavity.

Electrical Interface

Table 1 describes the electrical interface pin out, name, description, and characteristics of the signals between the Host and HORNET:

Pin or Terminal No.	Signal Name	Direction	Functional Description	Signal Characteristics (1)	Impedance
1	TX	Input to HORNET	Transmit Data - 0 to +3.3 Volt data or commands per the Hornet Interface Specification. Host to check for CTS being asserted (logic 0) on byte by byte basis before sending information to HORNET. "1"= idle state, data bit or stop bit "0"= data bit, or start bit Power Down - Logic 0 (0V), All logic circuits powered off .	0 to +3.3 VDC "1"= 2.31 Vmin "0"= .56 Vmax (1)	47K min. 30 pF max. 3.3K min.
2	RX	Output from HORNET	Receive Data- 0 to +3.3 Volt data or status per the Hornet Interface Specification. HORNET to check for RTS being asserted (logic 0) on byte by byte basis before sending information to Host. "1"= idle state, data bit or stop bit "0"= data bit, or start bit Power Down - Logic 0 (0V), All logic circuits powered off .	0 to +3.3 VDC "1"= 2.9 Vmin @ IOL = 100uA. "0"= 0.4 Vmax @ IOH= -100 uA	3.6K max. 3.3K min.
3	CTS	Output from HORNET	Clear to Send - TX Flow Control for HORNET to hold off Host data, indicating HORNET is busy receiving an incoming message, sending an outgoing message, or data buffer is full. HORNET will accept and buffer a minimum of 2 additional bytes after a low to high transition of CTS. CTS will be valid 20 milli-seconds after initial power up (high to low transition of DTR). "1" = HORNET not ready to receive data from host. "0" = HORNET ready to receive data from host Power Down - Logic 0 (0V), All logic circuits powered off.	0 to +3.3 VDC "1"= 2.9 Vmin @ IOL = 100uA. "0"= 0.4 Vmax @ IOH= -100 uA	3.6K max. 3.3K min.
4	RTS	Input to HORNET	Request to Send - RX Flow Control for Host to hold off HORNET data. "1" = Host not ready to receive data from HORNET. "0" = Host ready to receive data from HORNET	0 to +3.3 VDC "1"= 2.31 Vmin "0"= .56 Vmax (1)	47K min 30 pF max.

			Power Down- Logic 0 (0V), All logic circuits powered off.		3.3K min.
5		Reserved	HORNET programming		
6	DTR	Input to HORNET	Data Terminal Ready- Control Signal used to power down HORNET. A high disconnects power (via a FET Switch) to all other HORNET circuitry minimizing power consumption (<20 uA) "1" = Hornet Off. Power to I/O circuitry disconnected "0" = Hornet ON. (RF = Sleep, Scan, RX, or TX) Power Down- Logic 1 (3.3V), Controlled by host.	0 to +3.3 VDC "1"= 2.31 Vmin "0"= .56 Vmax (1)	1 M min 30 pF
7		Reserved	Hornet programming		
8	RI	Output from Hornet	Ring Indicate- RI indicates when an Hornet is ready to send RX data to host. RI is asserted immediately following an address match of an incoming message. Hornet will then check for RTS = "0" before delivering message. RI will be de-asserted after: a) message is delivered and RF link terminated. b) RTS is still high after pre-programmed time-out period is exceeded, a Receiver Not Ready (RNR) will then be sent back to Hornet sending original message, and RF link will then be terminated. "1" - No message for host "0" - Hornet has or receiving message for host. Power Down - Logic 0 (0V), All logic circuits powered off.	0 to +3.3 VDC "1"= 2.9 Vmin @ IOL = 100uA. "0"= 0.4 Vmax @ IOH= -100 uA	3.6K max. 3.3K min.
9		Reserved	Hornet programming		
10		Reserved	Hornet programming		
11	+3.3 VDC	Input to Hornet	Primary Power to Hornet (VDD)	+3.3 VDC +/- 5%	
12		NC	NOT USED		open
13		NC	NOT USED		open
14	SG	I/O	Ground return for all control and signal lines	0 VDC	TBD

(1) Based on VDD = 3.3 VDC

Chapter 4
Protocol

Overview

This chapter describes the two methods in which a host computer communicates via the Hornet: a Transparent Mode and a Message Mode. In general, a host computer is connected to the Hornet via a serial interface and can wirelessly communicate to other host computers that are each connected to their own radios. Although the Hornet interface logic is CMOS level, a CMOS to RS-232 adapter is available to enable connection to a host computer through its standard RS-232 COM port.

Transparent Mode is protocol independent and is designed to replace a cable or wire. In this mode, data into the serial port results in the exact data out of the receiving Hornet's serial port. Within the Transparent Mode, there are two configurations: Command and Data. In the Data configuration, all data that is sent by the host to the Hornet is sent over the air to a predefined target radio that relays this data to its host. Thus the Hornet simulates a wired connection to another host. In the Command configuration, the host computer is able to send commands to its radio in order to change the configuration settings, such as the destination address. A radio operating in Transparent Mode can switch between Command and Data settings by toggling the Request To Send (RTS) signal.

In Message Mode, all communication is performed using a structured message format. Addressing and other operating parameters are controlled via the message format as described in this specification.

The operating mode for each radio upon power up is determined by its non-volatile EEPROM settings. These settings also pre-define many other operating parameters which are described below. In addition, it is possible to switch between Transparent and Message Modes in real time by using the built-in commands.

EEPROM Variables

The Hornet is configured using its on-board EEPROM that contains all of the settings used to control the radio. These settings include: the operating mode (Transparent or Message mode), the data rate, various link timeouts, the address of the radio and many other non-volatile features. These values are programmed with defaults at the factory and can be read or changed via the 'XE' command in Message Mode.

A PC utility program exists for managing these settings and for reading and writing the settings. This utility and the variables are described in Chapter 2: *Getting Started.*

Bypass EEPROM Settings

In special circumstances where the EEPROM settings in a device are unknown thereby making it difficult to communicate with the device, the user can bypass the EEPROM settings. Since new settings cannot be downloaded without knowing the device data rate configuration, a special port pin is set aside on the microcontroller to allow the device to detect the special bypass setting. If this setting is detected on power-up, the device will set its baud rate to 19,200 bps regardless of the EEPROM settings. This bypass setting can be entered by shorting Port B pin 0 to ground as the device is powered up. This is pin 40 on the Atmel microcontroller. The jumper should be removed after power up and the device should now communicate at 19,200 bps.

Addressing

The Hornet contains a sophisticated addressing scheme that can be configured to meet the needs of a particular application. There are four addresses that the radio is aware of at any given time, which are called SRC1, SRC2, SRC3 and DEST. All of these are configured and maintained in the non-volatile EEPROM memory.

SRC1 is the address of the radio. Any data sent from the host or over the air with this address will be accepted by the radio as its own. Additionally, when in Message Mode, any message coming from the host (over the UART) with an address of all 0's is also treated as if it is addressed directly to the radio.

SRC2 is the broadcast address. All radios can be configured with an address in SRC2 so that any messages sent using this address as the destination address would be accepted by all radios as a broadcast message. The radios treat these messages special at the physical layer by not replying with an ACK. Also the sender will not wait for an ACK when sending with this address. If a broadcast address is not desired for a particular application, this address should match SRC1 to avoid accidentally interpreting data as a broadcast. Normally, an address of "FFFFFFFF" is used as the broadcast address.

SRC3 is the transparent address. SRC3 is treated like an alternate to the broadcast address (SRC2) in all ways for both sending and receiving. It can be used as a broadcast address for a subset of radios in a network. It is often configured so that SRC3 matches DEST so that some units running in Transparent Mode can talk to certain targets without needing to broadcast and without needing to send a command to set an address.

DEST is the Default Destination address setup in non-volatile EEPROM. If no destination address is specified in Transparent Mode, data is sent out using this address as the destination address. This allows Transparent Mode devices to talk directly to other devices without needing to address them via the command configuration. Once a Command Mode "&D" Destination Address command is sent, this new address is used until the next power cycle where DEST is again loaded with the non-volatile value.

SRC1 and DEST can be changed for the current session when in transparent command configuration. DEST is always specified in the message frame when in Message Mode.

Serial Interface

The serial interface between the Host and the Hornet consists of six interface signals. Except where noted below, these follow standard RS-232 conventions. The data rate is programmed into the EEPROM and can range from 1200bps to 19,200 bps for the standard configuration. The radio can be factory configured to enable a serial interface up to 115,200 bps, however with this configuration the Request To Send (RTS) signal from the host must be asserted prior to transmission in order to wake the radio from sleep.

Signal	Direction	Usage
TXD	Host → Hornet	Transmit Data (8N1)
RXD	Hornet → Host	Receive Data (8N1)
RTS	Host → Hornet	Request To Send. Message Mode: If asserted, the host is ready to receive data from the radio. If de-asserted, the host is not ready and the radio will assert Ring Indicate to try to wake up the host for a specified time if data is pending. Transparent Mode: If asserted, host is in data configuration. If de-asserted, host is in command configuration.
CTS	Hornet → Host	Clear To Send. If asserted, the radio is ready to receive data from the host. If de-asserted, the radio is busy (probably processing packets over the air) and cannot accept data from the host.
DTR	Host → Hornet	Data Terminal Ready. If asserted the radio is powered up.
RI	Hornet → Host	Ring Indicate. In message mode, this signal is asserted by the radio if RTS is de-asserted and the radio has data pending to send to the host. This signal is also toggled on and off repeatedly if the radio fails its power-on self-test.

Figure 4 Serial Interface

Transparent Mode

As mentioned above, the Hornet when in Transparent Mode simply forwards all received data across the air to a radio at a destination previously set up either by default or by using the Destination command in the Command Configuration. There is no attempt to interpret the data being sent or to look for special sequences or commands. This mode allows the serial interface to look like a wire to the communicating devices since the data does not need to be framed before sending it over the link.

Transparent Mode is selected via an EEPROM variable selection using the EEPROM.EXE utility (see the EEPROM Utility document). By deselecting "Message Mode" on the screen of this utility and downloading the settings to a target radio, this target radio will enter Transparent Mode as soon as it is power cycled.

As previously discussed, there is a Command Mode that can be entered when the Hornet is running in Transparent Mode. This Command Mode is used to change various operating parameters, such as the default target address. However, as soon as a Hornet is reset, these operating parameters will revert to the default values as stored in its EEPROM. (To change the settings permanently, the radio must be downloaded with the new EEPROM settings using commands provided in Message Mode. This download process is automated using the EEPROM Utility).

The Command Configuration is entered by de-asserting the RTS line from the Host to the Hornet. Normal Data Configuration is re-entered by re-asserting this RTS line. The Hornet continuously monitors this RTS line except when it is busy sending data over the air, which can be determined by the Host by watching the CTS line. When CTS is de-asserted, the Host knows that the Hornet is busy and is not listening to any serial port activity.

Command Configuration

Once a Hornet determines that it is in Command Configuration (RTS is de-asserted), it looks for a few special sequences that it interprets as commands. These are the accepted commands:

&Sxxxxxxxx Set Source Address.

Where xxxxxxxx is any 8-digit hex value (4 bytes) which is the new working address of this radio. If an address shorter than 8 digits is supplied then the missing digits are assumed to be leading 0's. This is a volatile change and the radio will revert to its EEPROM default source address on the next power cycle or reset.

&Dxxxxxxxx Set Destination Address.

Where xxxxxxxx is any 8-digit hex value (4 bytes) which is the address of the destination. If an address shorter than 8 digits is supplied then the missing digits are assumed to be leading 0's. Any data sent in Transparent mode in this session will be targeted at the destination address specified here. This is a volatile change and the radio will revert to its EEPROM default address on the next power cycle or reset.

&M Enter Message Mode

Ends Transparent Mode and causes the radio to enter into the Message Mode of operation. The radio will return to the Transparent Mode when the power is cycled or a command is issued in Message Mode to return the radio to Transparent Mode. The primary use of this command is to be able to take a device that is programmed for Transparent Mode and have it accept commands such as to download new operating parameters. There is a message string in Message Mode that will cause the radio to return to Transparent Mode if this is desired. (See 'XE' commands).

Each command must be ended with a Carriage Return and Line Feed (CRLF) sequence and the Hornet will respond to each command with either a '1' or a '0' followed by a CRLF sequence depending on the outcome of the command, where '1' means success and '0' means failure. If a Host sends a CRLF sequence with no command preceding it, the radio responds with a '1' to let the host know that the radio is listening and in command configuration.

Message Mode

In Message Mode, the Hornet will communicate with the host using frames of data. Multi-byte fields in a frame are formatted according to little-endian (PC-compatible) format where the lower order byte occurs first. The format of these frames is shown in Figure 5

Field Name	Description	Size / Format
Start of Text (STX)	Special Character designating the beginning of a frame.	1 byte = 0x02
Command String	2 character ASCII value identifying the kind of frame being sent.	2 bytes
Sequence Number	16 bit counter which can be used to guarantee that multiple frames are in the correct sequence.	2 bytes
Source Address	Hex address of the originator of this message. For frames sent from the host to the Hornet, this field is always set to all 0's and is filled in by the Hornet with the radio's source address.	4 bytes
Destination Address	Hex address of the final destination of this frame. For messages from the host that are destined only for the local radio this field should always be set to all 0's. For broadcasts to all radios within range, set this field to all F's.	4 bytes
Data Length	16-bit integer identifying the number of bytes of data in the Message Data field (Range is 0-96).	2 bytes
Message Data	The format of this field depends on what type of frame is being sent. See various descriptions below.	0 to 96 bytes
CRC	This is the 16-bit CRC-CCITT value over the entire frame after the STX field and before this field. The polynomial is $X^{16} + X^{12} + X^5 + 1$. The preload value ix 0xFFFF.	2 bytes
End of Text (ETX)	Special Character designating the end of a frame.	1 byte = 0x03

Figure 5 Message Format

Data Transparency

To differentiate control characters such as STX and ETX from normal data inside a frame, a Data Link Escape character (DLE 0x10) is used. Anytime that an STX (0x02), ETX (0x03) or a DLE (0x10) occurs in a frame as normal data it is preceded by a DLE character and then exclusive-OR'ed with 0x40. Thus, STX, ETX, and DLE should never occur in a frame except when intended to be a reserved control character.

In the reverse direction, if a DLE is encountered in a frame, it is thrown away and the next character is exclusive-OR'ed with 0x40 to put it back to its intended value. Likewise, if an STX or ETX is encountered, it must be delimiting a frame and should be treated as such.

Supported Messages

Send Frame Request

This command is sent from a Host to its local Hornet requesting that some data be sent over the air to a remote target. The radio should respond to this command with an 'sf' reply frame which will contain the proper error codes. On the remote end, the radio should respond to its Host with an 'rf' frame indicating that some data has been received. The requests are in all capital letters (i.e. SF) and the responses will be in all lower case letters.

Field Name	Description	Size / Format
Start of Text (STX)	Special Character designating the beginning of a frame.	1 byte = 0x02
Command String	'SF'	2 bytes
Sequence Number	16 bit counter which can be used to guarantee that multiple frames are in the correct sequence.	2 bytes
Source Address	This field is always set to 0x00000000 and is filled in by the Hornet with the radio's source address.	4 bytes
Destination Address	Hex address of the final destination of this frame. For broadcasts to all radios within range, set this field to all F's.	4 bytes
Data Length	16-bit integer identifying the number of bytes of data in the Message Data field (Range is 0-96).	2 bytes
Message Data	This field contains the payload being sent to the remote unit.	0 to 96 bytes
CRC	This is the 16-bit CRC-CCITT value over the entire frame as described above.	2 bytes
End of Text (ETX)	Special Character designating the end of a frame.	1 byte = 0x03

Figure 6 Send Frame Request Message Format

Send Frame Reply

Sent from a Hornet to its Host identifying the disposition of a previously sent 'SF' frame. The Message Data field contains the error codes (see Error Codes section).

Field Name	Description	Size / Format
Start of Text (STX)	Special Character designating the beginning of a frame.	1 byte = 0x02
Command String	'sf' (lower case).	2 bytes
Sequence Number	16 bit counter which matches the Sequence Number of the original 'SF' frame.	2 bytes
Source Address	Contains the address of the local Hornet.	4 bytes
Destination Address	Contains the destination address contained in the original 'SF' frame.	4 bytes
Data Length	0x0002.	2 bytes
Error Code	Error Code for the disposition of the original 'SF' frame. See Error Codes below.	1 byte
Secondary Error Code	Contains the number of times the data had to be retransmitted.	1 byte
CRC	This is the 16-bit CRC-CCITT value over the entire frame as described above.	2 bytes
End of Text (ETX)	Special Character designating the end of a frame.	1 byte = 0x03

Figure 7 Send Frame Reply Message Format

Receive Frame

Sent from a Hornet to its host after receiving a 'SF' frame over the air. This message delivers the payload contained in the 'SF' frame to the Host.

Field Name	Description	Size / Format
Start of Text (STX)	Special Character designating the beginning of a frame.	1 byte = 0x02
Command String	'rf' (lower case)	2 bytes
Sequence Number	16 bit counter as contained in the original 'SF' frame.	2 bytes
Source Address	Contains the address of the remote Hornet that sent the original 'SF' frame.	4 bytes
Destination Address	Contains the destination address as contained in the original 'SF' frame.	4 bytes
Data Length	16-bit integer identifying the number of bytes of data in the Message Data field (Range is 0-96).	2 bytes
Message Data	This field contains the payload as sent from the originator of the 'SF' frame.	0 to 96 bytes
CRC	This is the 16-bit CRC-CCITT value over the entire frame as described above.	2 bytes
End of Text (ETX)	Special Character designating the end of a frame.	1 byte = 0x03

Figure 8 Receive Frame Message Format