XBee™/XBee-PRO™ OEM RF Modules

XBee/XBee-PRO OEM RF Modules

ZigBee™ Networks

RF Module Operation

RF Module Configuration

Appendices

Product Manual v8.x17 Beta - ZigBee Protocol

For OEM RF Module Part Numbers: XB24-...-002
                                                        XBP24-...-002

ZigBee OEM RF Modules by MaxStream, Inc.

Firmware Versions: 8.017 - Coordinator, Transparent Operation
                                        8.117 - Coordinator, API Operation
                                        8.217 - Router, Transparent Operation
                                        8.317 - Router, API Operation

Technical Support: Phone: (801) 765-9885

Live Chat: www.maxstream.net

E-mail: rf-xperts@maxstream.net

Contents

1. XBee/XBee-PRO OEM RF Modules

The XBee and XBee-PRO OEM RF Modules were engineered to operate within the ZigBee protocol and support the unique needs of low-cost, low-power wireless sensor networks. The modules require minimal power and provide reliable delivery of data between remote devices.

Both modules operate within the ISM 2.4 GHz frequency band and are pin-for-pin compatible with each other.

1.1. Key Features

High Performance, Low Cost

XBee

 • Indoor/Urban: up to 100′ (30 m)

 • Outdoor line-of-sight: up to 300′ (100 m)

 • Transmit Power: 1 mW (0 dBm)

 • Receiver Sensitivity: -92 dBm

XBee-PRO

 • Indoor/Urban: up to 300′ (100 m)

 • Outdoor line-of-sight: up to 1 mile (1500 m)

 • Transmit Power: 100 mW (20 dBm) EIRP

 • Receiver Sensitivity: -100 dBm

RF Data Rate: 250,000 bps

Advanced Networking & Security

Retries and Acknowledgements

DSSS (Direct Sequence Spread Spectrum)

Each direct sequence channel has over 65,000 unique network addresses available

Point-to-point, point-to-multipoint and peer-to-peer topologies supported

Self-routing, self-healing and fault-tolerant mesh networking

Low Power

XBee

 • TX Current: 45 mA (@3.3 V)

 • RX Current: 50 mA (@3.3 V)

 • Power-down Current: < 10 µA

XBee-PRO

 • TX Current: 215 mA (@3.3 V)

 • RX Current: 55 mA (@3.3 V)

 • Power-down Current: < 10 µA

Easy-to-Use

No configuration necessary for out-of box RF communications

AT and API Command Modes for configuring module parameters

Small form factor

Extensive command set

Free X-CTU Software
(Testing and configuration software)

Free & Unlimited Technical Support

1.1.1. Worldwide Acceptance

FCC Approval (USA) Refer to Appendix A [p34] for FCC Requirements.
Systems that contain XBee/XBee-PRO RF Modules inherit MaxStream Certifications.

ISM (Industrial, Scientific & Medical) **2.4 GHz frequency band**

Manufactured under **ISO 9001:2000** registered standards

XBee/XBee-PRO RF Modules are optimized for use in **US**, **Canada**, **Australia, Israel and Europe** (contact MaxStream for complete list of agency approvals).

1.2. Specifications

Table 1-01.   Specifications of the XBee/XBee-PRO OEM RF Module (PRELIMINARY)

Specification	XBee	XBee-PRO
Performance		
Indoor/Urban Range	up to 100 ft. (30 m)	Up to 300' (100 m)
Outdoor RF line-of-sight Range	up to 300 ft. (100 m)	Up to 1 mile (1500 m)
Transmit Power Output (software selectable)	1mW (0 dBm)	60 mW (18 dBm) conducted, 100 mW (20 dBm) EIRP*
RF Data Rate	250,000 bps	250,000 bps
Serial Interface Data Rate (software selectable)	1200 - 115200 bps (non-standard baud rates also supported)	1200 - 115200 bps (non-standard baud rates also supported)
Receiver Sensitivity	-92 dBm (1% packet error rate)	-100 dBm (1% packet error rate)
Power Requirements		
Supply Voltage	2.8 – 3.4 V	2.8 – 3.4 V
Operating Current (Transmit)	45mA (@ 3.3 V)	If PL=0 (10dBm): 137mA(@3.3V), 139mA(@3.0V) PL=1 (12dBm): 155mA (@3.3V), 153mA(@3.0V) PL=2 (14dBm): 170mA (@3.3V), 171mA(@3.0V) PL=3 (16dBm): 188mA (@3.3V), 195mA(@3.0V) PL=4 (18dBm): 215mA (@3.3V), 227mA(@3.0V)
Operating Current (Receive)	50mA (@ 3.3 V)	55mA (@ 3.3 V)
Power-down Current	not supported	not supported
General		
Operating Frequency Band	ISM 2.4 GHz	ISM 2.4 GHz
Dimensions	0.960" x 1.087" (2.438cm x 2.761cm)	0.960" x 1.297" (2.438cm x 3.294cm)
Operating Temperature	-40 to 85º C (industrial)	-40 to 85º C (industrial)
Antenna Options	Integrated Whip, Chip or U.FL Connector	Integrated Whip, Chip or U.FL Connector
Networking & Security		
Supported Network Topologies	Point-to-point, Point-to-multipoint, Peer-to-peer & Mesh	
Number of Channels (software selectable)	16 Direct Sequence Channels	12 Direct Sequence Channels
Addressing Options	PAN ID, Channel and Addresses	PAN ID, Channel and Addresses
Agency Approvals		
United States (FCC Part 15.247)	OUR-XBEE	OUR-XBEEPRO
Industry Canada (IC)	4214A XBEE	4214A XBEEPRO
Europe (CE)	ETSI	ETSI (Max. 10 dBm transmit power output)*

* When operating in Europe: XBee-PRO RF Modules must be configured to operate at a maximum transmit power output level of 10 dBm. The power output level is set using the PL command. The PL parameter must equal "0" (10 dBm).

Additionally, European regulations stipulate an EIRP power maximum of 12.86 dBm (19 mW) for the XBee-PRO and 12.11 dBm for the XBee when integrating high-gain antennas.

Antenna Options: The ranges specified are typical when using the integrated Whip (1.5 dBi) and Dipole (2.1 dBi) antennas. The Chip antenna option provides advantages in its form factor; however, it typically yields shorter range than the Whip and Dipole antenna options when transmitting outdoors. For more information, refer to the "XBee Antenna" application note located on MaxStream's web site (http://www.maxstream.net/support/knowledgebase/article.php?kb=153).

1.3. Mechanical Drawings

Figure 1-01. Mechanical drawings of the XBee/XBee-PRO OEM RF Modules (antenna options not shown)
The XBee and XBee-PRO RF Modules are pin-for-pin compatible.
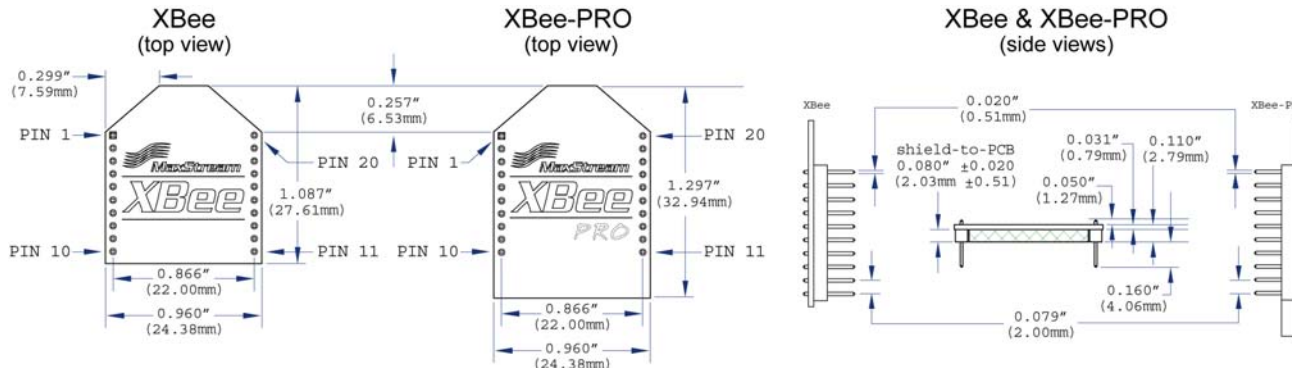
1.4. Mounting Considerations

The XBee/XBee-PRO RF Module was designed to mount into a receptacle (socket) and therefore does not require any soldering when mounting it to a board. The XBee Development Kits contain RS-232 and USB interface boards which use two 20-pin receptacles to receive modules.

Figure 1-02. XBee Module Mounting to an RS-232 Interface Board.
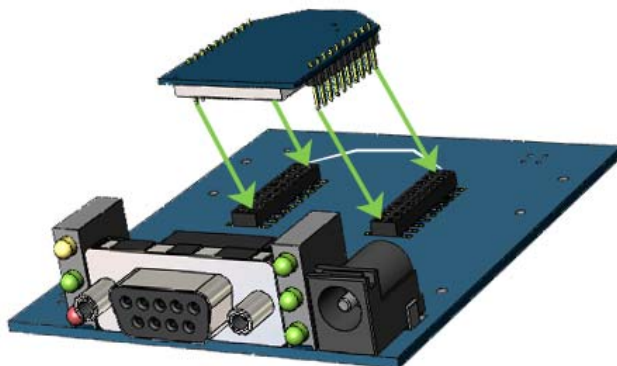
The receptacles used on MaxStream development boards are manufactured by Century Interconnect. Several other manufacturers provide comparable mounting solutions; however, MaxStream currently uses the following receptacles:

- Through-hole single-row receptacles -
Samtec P/N: MMS-110-01-L-SV (or equivalent)

- Surface-mount double-row receptacles -
Century Interconnect P/N: CPRMSL20-D-0-1 (or equivalent)

- Surface-mount single-row receptacles -
Samtec P/N: SMM-110-02-SM-S

MaxStream also recommends printing an outline of the module on the board to indicate the orientation the module should be mounted.

1.5. Pin Signals

Figure 1-03. XBee/XBee-PRO RF Module Pin Number

(top sides shown - shields on bottom)

Table 1-02.   Pin Assignments for the XBee and XBee-PRO Modules
(Low-asserted signals are distinguished with a horizontal line above signal name.)

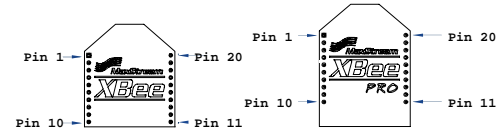| Pin #	Name	Direction	Description
1	VCC	-	Power supply
2	DOUT	Output	UART Data Out
3	DIN / $\overline{\text{CONFIG}}$	Input	UART Data In
4	DO8*	Output	Digital Output 8
5	$\overline{\text{RESET}}$	Input	Module Reset (reset pulse must be at least 200 ns)
6	PWM0 / RSSI	Output	PWM Output 0 / RX Signal Strength Indicator
7	[reserved]	-	Do not connect
8	[reserved]	-	Do not connect
9	$\overline{\text{DTR}}$ / SLEEP_RQ* / DI8	Input	Pin Sleep Control Line or Digital Input 8
10	GND	-	Ground
11	AD4* / DIO4*	Either	Analog Input 4 or Digital I/O 4
12	$\overline{\text{CTS}}$ / DIO7*	Either	Clear-to-Send Flow Control or Digital I/O 7
13	ON / $\overline{\text{SLEEP}}$	Output	Module Status Indicator
14	VREF*	Input	Voltage Reference for A/D Inputs
15	Associate / AD5* / DIO5*	Either	Associated Indicator, Analog Input 5 or Digital I/O 5
16	$\overline{\text{RTS}}$* / AD6* / DIO6*	Either	Request-to-Send Flow Control, Analog Input 6 or Digital I/O 6
17	AD3* / DIO3*	Either	Analog Input 3 or Digital I/O 3
18	AD2* / DIO2*	Either	Analog Input 2 or Digital I/O 2
19	AD1* / DIO1*	Either	Analog Input 1 or Digital I/O 1
20	AD0* / DIO0*	Either	Analog Input 0 or Digital I/O 0

* Functions not supported at the time of this release.

Design Notes:

- Minimum connections: VCC, GND, DOUT & DIN
- Minimum connections for updating firmware: VCC, GND, DIN, DOUT, RTS & DTR
- Signal Direction is specified with respect to the module
- Module includes a 50k Ω pull-up resistor attached to $\overline{\text{RESET}}$
- Several of the input pull-ups can be configured using the PE command
- Unused pins should be left disconnected

1.6. Electrical Characteristics

Table 1-03.   DC Characteristics of the XBee & XBee-PRO (VCC = 2.8 - 3.4 VDC)

Symbol	Parameter	Condition	Min	Typical		Max	Units
V_{IL}	Input Low Voltage	All Digital Inputs	-	-		0.35 * VCC	V
V_{IH}	Input High Voltage	All Digital Inputs	0.7 * VCC	-		-	V
V_{OL}	Output Low Voltage	I_{OL} = 2 mA, VCC >= 2.7 V	-	-		0.5	V
V_{OH}	Output High Voltage	I_{OH} = -2 mA, VCC >= 2.7 V	VCC - 0.5	-		-	V
II_{IN}	Input Leakage Current	V_{IN} = VCC or GND, all inputs, per pin	-	0.025		1	uA
II_{OZ}	High Impedance Leakage Current	V_{IN} = VCC or GND, all I/O High-Z, per pin	-	0.025		1	uA
TX	Transmit Current	VCC = 3.3 V	-	45 (XBee)	215 (PRO)	-	mA
RX	Receive Current	VCC = 3.3 V	-	50 (XBee)	55 (PRO)	-	mA
PWR-DWN	Power-down Current	SM parameter = 1	-	< 10		-	uA

1.7. Definitions

Table 1-04.   Terms and Definitions

ZigBee Node Types	

Coordinator	A node that has the unique function of forming a network. The Coordinator is responsible for establishing the operating channel and PAN ID for an entire network. Once established, the Coordinator can form a network by allowing Routers and End Devices to join to it. Once the network is formed, the Coordinator functions like a Router (it can participate in routing packets and be a source or destination for data packets).
	
	  -- One Coordinator per PAN
	  -- Establishes/Organizes PAN
	  -- Can route data packets to/from other nodes
	  -- Can be a data packet source and destination
	  -- Mains-powered
	
	Refer to the XBee/XBee-PRO Coordinator section [p17] for more information.

Router	A node that creates/maintains network information and uses this information to determine the best route for a data packet. A router must join a network before it can allow other Routers and End Devices to join to it.
	
	A Router can participate in routing packets and is intended to be a mains-powered node.
	
	  -- Several Routers can operate in one PAN
	  -- Can route data packets to/from other nodes
	  -- Can be a data packet source and destination
	  -- Mains-powered
	
	Refer to the XBee/XBee-PRO Router section [p17] for more information.

End Device	End Devices have no routing capacity. End Devices must always interact with their parent node (Router or Coordinator) in order to transmit or receive data.
	
	An End Device can be a source or destination for data packets but cannot route packets. End Devices can be battery-powered and offer low-power operation.
	
	  -- Several End Devices can operate in one PAN
	  -- Can be a data packet source and destination
	  -- All messages are relayed through a Coordinator or Router
	  -- Low power
	
	End Devices are not supported in this release.

ZigBee Protocol	
PAN	Personal Area Network - A data communication network that includes a Coordinator and one or more Routers/End Devices. Network formation is governed by Network Maximum Depth, Maximum Child Routers and Maximum Children End Devices.
Joining	The process of a node becoming part of a ZigBee PAN. A node becomes part of a network by joining to a Coordinator or a Router (that has previously joined to the network). During the process of joining, the node that allowed joining (the parent) assigns a 16-bit address to the joining node (the child).

Table 1-04.   Terms and Definitions

Network Maximum Depth	The level of descendents from a Coordinator. In a MaxStream PAN, the Network Maximum Depth is 5.
Maximum Child Routers	The maximum number of Routers than can join to one node. The maximum number of Child Routers in a MaxStream PAN is 6.
Maximum Child End Devices	The maximum number of End Devices than can join to one node. The maximum number of Child End Devices in a MaxStream PAN is 14.
Network Address	The 16-bit address assigned to a node after it has joined to another node.
Operating Channel	The frequency selected for data communications between nodes. The operating channel is selected by the Coordinator on power-up.
Energy Scan	A scan of RF channels that detects the amount of energy present on the selected channels. The Coordinator uses the energy scan to determine the operating channel.
Route Request	Broadcast transmission sent by a Coordinator or Router throughout the network in attempt to establish a route to a destination node.
Route Reply	Unicast transmission sent back to the originator of the route request. It is initiated by a node when it receives a route request packet and its address matches the Destination Address in the route request packet.
Route Discovery	The process of establishing a route to a destination node when one does not exist in the Routing Table. It is based on the AODV (Ad-hoc On-demand Distance Vector routing) protocol.
ZigBee Stack	ZigBee is a published specification set of high-level communication protocols for use with small, low-power modules. The ZigBee stack provides a layer of network functionality on top of the 802.15.4 specification. For example, the mesh and routing capabilities available to ZigBee solutions are absent in the 802.15.4 protocol.

2. ZigBee Networks
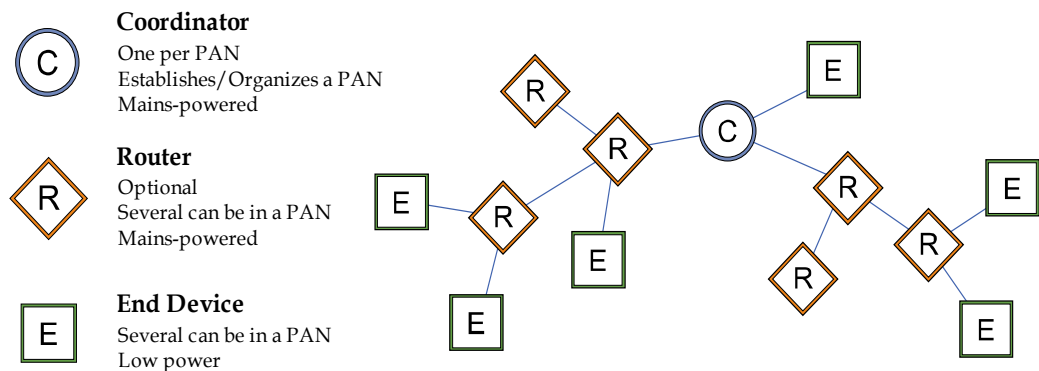
2.1. ZigBee Network Formation

A ZigBee PAN is formed by nodes joining to a Coordinator or to a previously joined Router. Once the Coordinator defines the operating channel and PAN ID, it can allow Routers and End Devices to join to it. When a node joins a network, it receives a 16-bit Network Address.

Once a Router has joined the network, it can also allow other nodes to join to it. Joining establishes a parent/child relationship between two nodes. The node that allowed the join is the parent and the node that joined is the child. The parent/child relationship is not necessary for routing; however, it is necessary for network formation and Network Address assignment. If a Coordinator does not exist, a network cannot be formed. A node cannot transmit or receive data until it has joined a PAN.

2.1.1. Node Types

A ZigBee PAN consists of one Coordinator and one or more Routers and/or End Devices. Refer to the Coordinator [p17] and Router [p17] sections of the "RF Module Operation" chapter for more information regarding each node type.

Figure 2-01. Node Types / Sample of a Basic ZigBee Network Topology

Coordinator
One per PAN
Establishes/Organizes a PAN
Mains-powered

Router
Optional
Several can be in a PAN
Mains-powered

End Device
Several can be in a PAN
Low power

End Devices are not supported at the time of this release.

2.1.2. Network Limitations

MaxStream ZigBee PANs are limited to the following boundaries:

• Maximum Children - The Coordinator and each joined Router can support up to 20 children, 6 of which can be Routers (Maximum Child Routers). Refer to Figure 2-02.
• Network Maximum Depth - The Maximum Network Depth is 5 - Maximum Network Depth refers to the level of descendents from the Coordinator. Refer to Figure 2-03.

Refer to the definitions table [p8] for more information.

Figure 2-02. Maximum Number of Child Devices per Parent
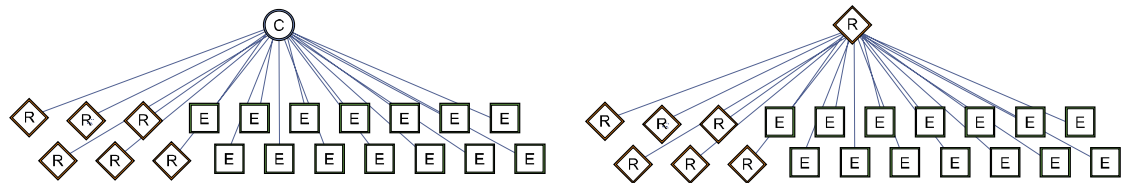
Coordinators (one per PAN) and Routers can have 6 Routers and 14 End Devices joined to them.

Figure 2-03. Maximum Network Depth

Network depth can span 5 levels deep.
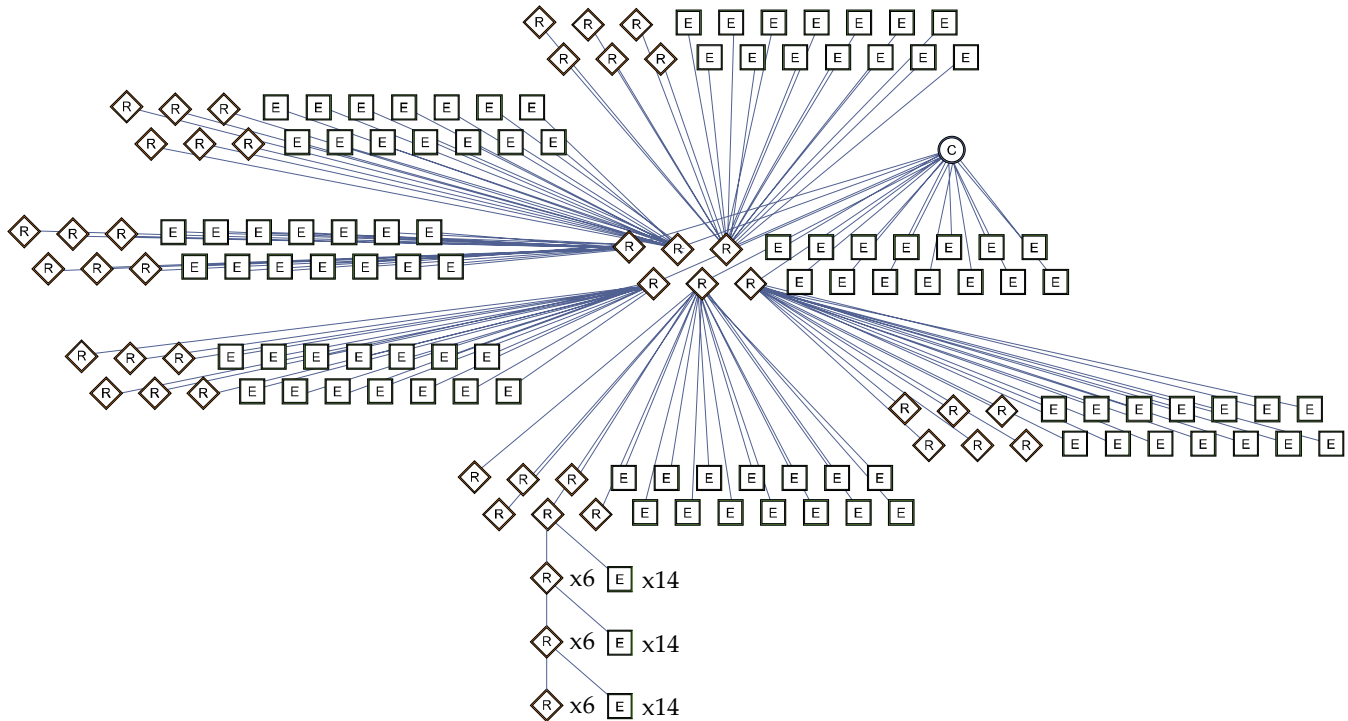
2.2. ZigBee Network Communications

2.2.1. ZigBee Addressing

The 802.15.4 protocol upon which the ZigBee protocol is built specifies two address types:

- 16-bit Network Addresses
- 64-bit Addresses

16-bit Network Addresses

A 16-bit Network Address is assigned to a node when the node joins a network. The Network Address is unique to each node in the network. However, Network Addresses are not static - it can change.

The following two conditions will cause a node to receive a new Network Address:

1. An End Device cannot communicate with its parent.
2. A Router or End Device, when it power cycles, sends an 802.15.4 Orphan Notification command to locate its parent. If the parent node does not respond, the Router or End Device considers itself not-joined and repeats the process of joining the network. Once the node joins the network, it and all of its descendents will receive a new Network Address.

Since all ZigBee communications use 16-bit addressing, a node's 16-bit address must be known before communications can take place.

64-bit Addresses

Each node contains a unique 64-bit address. The 64-bit address uniquely identifies a node and is permanent.

2.2.2. Mesh Routing

Mesh routing allows data packets to traverse multiple nodes (hops) in a network to route data from a source to a destination. The route a packet can take in a mesh network is independent of the parent/child relationships established during joining. Before transmitting a data packet from source to destination nodes, a route must be established. Route discovery is based on the AODV (Ad-hoc On-demand Distance Vector routing) protocol.

AODV (Ad-hoc On-demand Distance Vector) Routing Algorithm

Routing under the AODV protocol is accomplished using tables in each node that store in the next hop (intermediary node between source and destination nodes) for a destination node. If a next hop is not known, route discovery must take place in order to find a path. Since only a limited number of routes can be stored on a Router, route discovery will take place more often on a large network with communication between many different nodes.

When a source node must discover a route to a destination node, it sends a broadcast route request command. The route request command contains the source Network Address, the destination Network Address and a Path Cost field (a metric for measuring route quality). As the route request command is propagated through the network (refer to the Broadcast Transmission section [p13]), each node that re-broadcasts the message updates the Path Cost field and creates a temporary entry in its route discovery table.

When the destination node receives a route request, it compares the 'path cost' field against previously received route request commands. If the path cost stored in the route request is better than any previously received, the destination node will transmit a route reply packet to the node that originated the route request. Intermediate nodes receive and forward the route reply packet to the Source Node (the node that originated route request).

Refer to the ZigBee specification for more details.

2.2.3. Broadcast Transmissions

Broadcast transmissions within the ZigBee protocol are intended to be propagated throughout the entire network such that all nodes receive the transmission. This requires each broadcast transmission be retransmitted by all Router nodes to ensure all nodes receive the transmission.

Broadcast transmissions use a passive acknowledgment scheme. This means that when a node transmits a broadcast transmission, it listens to see if all of its neighbors retransmit the message. If one or more neighbor nodes do not retransmit the data, the node will retransmit the broadcast message and listen again for the neighbor nodes to forward the broadcast transmission.

Refer to the ZigBee specification for more details.

3. RF Module Operation

3.1. Serial Communications

The XBee/XBee-PRO OEM RF Modules interface to a host device through a logic-level asynchronous serial port. Through its serial port, the module can communicate with any logic and voltage compatible UART; or through a level translator to any serial device (For example: Through a MaxStream proprietary RS-232 or USB interface board).

3.1.1. UART Data Flow

Devices that have a UART interface can connect directly to the pins of the RF module as shown in the figure below.

Figure 3-01. System Data Flow Diagram in a UART-interfaced environment
(Low-asserted signals distinguished with horizontal line over signal name.)
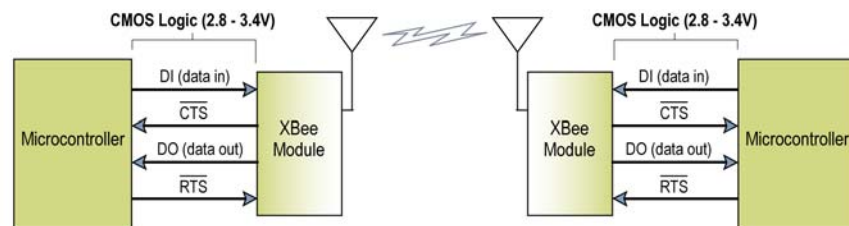
RTS flow control is not currently supported.

Serial Data

Data enters the module UART through the DI pin (pin 3) as an asynchronous serial signal. The signal should idle high when no data is being transmitted.

Each data byte consists of a start bit (low), 8 data bits (least significant bit first) and a stop bit (high). The following figure illustrates the serial bit pattern of data passing through the module.

Figure 3-02. UART data packet 0x1F (decimal number "31") as transmitted through the RF module
Example Data Format is 8-N-1 (bits - parity - # of stop bits)
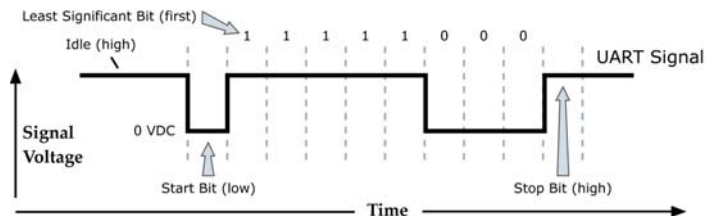
The module UART performs tasks, such as timing and parity checking, that are needed for data communications. Serial communications depend on the two UARTs to be configured with compatible settings (baud rate, parity, start bits, stop bits, data bits).

3.1.2. Transparent Operation

RF modules that contain the following firmware versions will support Transparent Mode: 8.0xx (Coordinator) and 8.2xx (Router).

When operating in Transparent Mode, modules are configured using AT Commands and API operation is not supported. The modules act as a serial line replacement - all UART data received through the DI pin is queued up for RF transmission. Data is sent to a module as defined by the DH (Destination Address High) and DL (Destination Address Low) parameters.

When RF data is received that is addressed to the module's 64-bit Address, the data is sent out the DO pin.

Serial-to-RF Packetization

Data is buffered in the DI buffer until one of the following causes the data to be packetized and transmitted:

1. No serial characters are received for the amount of time determined by the RO (Packetization Timeout) parameter. If RO = 0, packetization begins when a character is received.
2. Maximum number of characters that will fit (72) in an RF packet is received.
3. The Command Mode Sequence (GT + CC + GT) is received. Any character buffered in the DI buffer before the sequence is transmitted.

3.1.3. API Operation

API (Application Programming Interface) Operation is an alternative to the default Transparent Operation. The frame-based API extends the level to which a host application can interact with the networking capabilities of the module.

When in API mode, all data entering and leaving the module is contained in frames that define operations or events within the module.

Transmit Data Frames (received through the DI pin (pin 3)) include:

- RF Transmit Data Frame
- Command Frame (equivalent to AT commands)

Receive Data Frames (sent out the DO pin (pin 2)) include:

- RF-received data frame
- Command response
- Event notifications such as reset, associate, disassociate, etc.

The API provides alternative means of configuring modules and routing data at the host application layer. A host application can send data frames to the module that contain address and payload information instead of using command mode to modify addresses. The module will send data frames to the application containing status packets; as well as source, RSSI and payload information from received data packets.

The API operation option facilitates many operations such as the examples cited below:

-> Transmitting data to multiple destinations without entering Command Mode
-> Receive success/failure status of each transmitted RF packet
-> Identify the source address of each received packet

To implement API operations, refer to API sections [p29].

3.1.4. Flow Control

Figure 3-03. Internal Data Flow Diagram
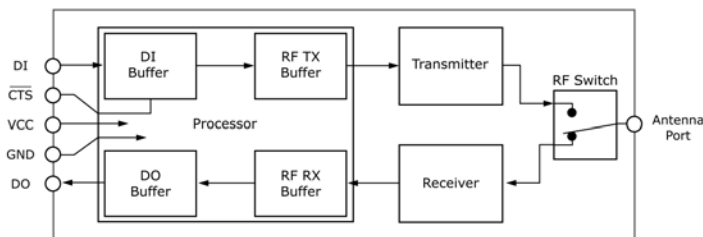
DI (Data In) Buffer

When serial data enters the RF module through the DI pin (pin 3), the data is stored in the DI Buffer until it can be processed.

Hardware Flow Control (CTS). When the DI buffer is 17 bytes away from being full; by default, the module de-asserts $\overline{CTS}$ (high) to signal to the host device to stop sending data [refer to D7 (DIO7 Configuration) parameter]. $\overline{CTS}$ is re-asserted after the DI Buffer has 34 bytes of memory available.

Cases in which the DI Buffer may become full and possibly overflow:

1. If the module is receiving a continuous stream of RF data, any serial data that arrives on the DI pin is placed in the DI Buffer. The data in the DI buffer will be transmitted over-the-air when the module is no longer receiving RF data in the network.

2. When data is ready to be transmitted, the module may need to discover a Network Address and/or a Route in order to reach the destination node. Discovery overhead may delay packet transmission.

    Refer to the ZigBee Networks --> Mesh Routing sections for more information.

Refer to the RO (Packetization Timeout) command description [p25] and the Mesh Routing section [p12] for more information.

DO (Data Out) Buffer

When RF data is received, the data enters the DO buffer and is sent out the serial port to a host device. Once the DO Buffer reaches capacity, any additional incoming RF data is lost.

Hardware Flow Control ($\overline{RTS}$). If $\overline{RTS}$ is enabled for flow control (D6 (DIO6 Configuration) Parameter = 1), data will not be sent out the DO Buffer as long as $\overline{RTS}$ (pin 16) is de-asserted.

Cases in which the DO Buffer may become full and possibly overflow:

1. If the RF data rate is set higher than the interface data rate of the module, the module will receive data from the transmitting module faster than it can send the data to the host.

2. If the host does not allow the module to transmit data out from the DO buffer because of being held off by hardware or software flow control.

$\overline{RTS}$ flow contol is not supported in this release.

3.2. XBee/XBee-PRO Networks

3.2.1. XBee/XBee-PRO Coordinator

Network Startup

In order to form a network, a Coordinator must select an unused operating channel and PAN ID on behalf of its network. To do this, the Coordinator first performs an energy scan on all channels as specified by its SC (Scan Channels) parameter. The scan time on each channel is determined by the SD (Scan Duration) parameter. Once the energy scan is completed, an Active Scan is issued. The Active Scan returns a list of discovered Coordinators and Routers (up to 5 results). The duration of the Active Scan on each channel is also determined by the SD parameter. An unoccupied operating channel is then chosen for PAN operations.

If the ID (PAN ID) parameter = 0xFFFF: The Coordinator will select a random PAN ID. Otherwise, the Coordinator will startup on its stored ID parameter.

After the Coordinator has started, it will allow nodes to join to it for a time based on its NJ (Node Join Time) parameter. If enabled, the Associate LED (D5 (DIO5 Configuration) command) will blink 1x per second after the Coordinator has started. At this point, the operating channel and PAN ID can be read using the CH (Operating Channel) and ID (PAN ID) commands. The 16-bit address of the Coordinator is always 0x0000.

If API is enable (AP parameter > 0):
The API Modem Status "Coordinator Started" is sent out the UART.

The AI (Association Indication) command can be used at any point during the Coordinator startup routine to determine the status of the startup operation.

3.2.2. XBee/XBee-PRO Router

Router Startup

A new Router must locate a Router that has already joined a PAN or a Coordinator to join to. To do this, it first issues an Active Scan on each of the SC channels. The scan duration on each of these channels is determined by the SD parameter. The Active Scan will return a list of discovered Coordinators and Routers (up to 5 results). The Router will then try to join to a parent (Router or Coordinator) that is allowing joining, based on the ID parameter. If ID = 0xFFFF, the Router will attempt to join a parent on any PAN ID. Otherwise, the Router will only attempt joining with a Router/Coordinator that operates on the PAN ID specified by the ID parameter. If a valid Router/Coordinator is found, the Router will attempt to join to that node. If the join succeeds, the Router has successfully started.

After the Router has started, it will allow nodes to join to it for a time based on the NJ (Node Join Time) parameter. If enabled, the Associate LED (D5 (DIO5 Configuration) command) will blink 2x per second after the Router has started. At this point, the operating channel and PAN ID can be read using the CH (Operating Channel) and ID (PAN ID) commands. The 16-bit Network Address of the Router can be read using the MY (16-bit Source Address) command.

If API is enable (AP parameter > 0):
The API Modem Status "Joined" is sent out the UART.

The AI (Association Indication) command can be used at any point during the Router startup routine to know the status of the startup operation.

Router Configuration

The SC (Scan Channel) and ID (PAN ID) parameter values affect Router startup by determining the channels the Router will scan [SC (Scan Channels) command] to find a parent to join and by determining the allowable PAN ID(s) the node will join (ID parameter).

Changing these parameters could be problematic if other nodes (children) have already joined the Router. These commands should not be changed once the Router has started and allowed nodes to join to it.

3.2.3. Network Reset

Resetting a Coordinator

Upon reset (Power-up, FR (Software Reset) or NR (Network Reset))**:**

1. If a Coordinator has formed a network, it will retain the PAN ID and operating channel information as well as a list of its child nodes. However, if either the SC (Scan Channels) or ID (PAN ID) parameters have changed and the Coordinator is reset, the Coordinator will startup using the new SC and/or ID values and will erase its list of child nodes.

2. If the Coordinator must change the operating channel of an established network, it can alert all nodes in the network to leave and reform the network by issuing the NR (Network Reset) command with a parameter of '1'. When this command is issued, the Coordinator sends a broadcast message across the entire network forcing all nodes to unjoin and rejoin to a new parent. The Coordinator will, after several seconds, restart and allow joining according to its saved NJ (Node Join Time) setting. Once the Coordinator has started, other nodes can join the PAN. The other nodes will attempt to rejoin by scanning all channels (as specified by the SC parameter) for a parent operating on the PAN ID (specified by its ID parameter). This will re-assign the 16-bit Network Addresses on all nodes. The NJ parameter value on the Coordinator must be non-zero if the NR command is issued to allow at least one Router to join to it.

Resetting a Router

Upon reset (Power-up, FR (Software Reset) or NR (Network Reset))**:**

1. If a Router has joined a network and a reset occurs (FR or power-up), the Router will send a broadcast transmission to find its parent in order to re-establish its operating channel, PAN ID and 16-bit Network Address. If the Router cannot find its parent, it will rejoin the network using its SC (Scan Channels) and ID (PAN ID) settings. This could change the Router's 16-bit Network Address.

2. Issuing an NR (Network Reset) command with a parameter of '0' will also cause a Router reset. The NR command will force the Router to rejoin the network and it may receive a different 16-bit Network Address. It will also erase the Router's list of child device addresses. This option should be used with caution.

3. Issuing an NR (Network Reset) command with a parameter of '1' will send a command to the Coordinator instructing it to reset the entire network. Resetting the entire network will reset all nodes and reform the PAN (Also refer to the "Resetting a Coordinator" section).

3.2.4. Network Mapping

The ND (Node Discover) command is useful for mapping out the network. When issued from the Coordinator or an End Device, the command sends a broadcast message across the network and returns a list of all nodes. Refer to the ND command for more information.

3.3. XBee/XBee-PRO Addressing

Each RF module has a unique 64-bit Address that is assigned at the factory that can be read using the SH (Serial Number High) and SL (Serial Number Low) commands. When a module starts or joins a network, it receives a 16-bit Network Address that is unique within the network; however, this address can change (refer to the 'ZigBee Addressing' section). In addition, each module can store a string-identifier using the NI (Node Identifier) command.

XBee/XBee-PRO RF modules can be addressed using their 64-bit Address, their NI-string or both the 64-bit Address and the 16-bit Network Address (API Mode). Under the ZigBee protocol, the 16-bit Network Address of a Coordinator is always "0". Nodes can address the Coordinator using its 16-bit Network Address.

3.3.1. 64-bit Addressing

To send a packet to an RF module using its 64-bit Address (Transparent Mode)

> Set the DH (Destination Address High) and DL (Destination Address Low) parameters of the source node to match the 64-bit Address (SH (Serial Number High) and SL (Serial Number Low) parameters) of the destination node.

To send a packet to an RF module using its 64-bit Address (API Mode)

> Use the ZigBee Transmit Request API frame to set the DH (Destination Address High) and DL (Destination Address Low) parameters of the source node to match the 64-bit Address (SH (Serial Number High) and SL (Serial Number Low) parameters) of the destination node.
>
> If the 64-bit Address of the destination node is not known, set 16-bit Destination Network Address to 0xFFFE (refer to the 'API Addressing section below).

Since the ZigBee protocol relies on the 16-bit Network Address for routing, the 64-bit Address must be converted into a 16-bit Network Address prior to transmitting data. If a module does not know the 16-bit Network Address for a given 64-bit Address, it will transmit a broadcast Network Address Discovery command. The module with a matching 64-bit Address will transmit its 16-bit Network Address back.

The modules maintain a table that can store up to seven 64-bit Addresses and their corresponding 16-bit Network Addresses.

3.3.2. API Addressing

API Mode provides the ability to store and maintain 16-bit Network Address tables on an external processor. The 16-bit Network Address information is provided to the application through the following:

- The ZigBee Transmit Status Frame
  (contains the current 16-bit Network Address of the remote)
- The ND and DN commands
  (return 64-bit and 16-bit Network Addresses of remote nodes)

With this information, a table can be built in an application that maps a 64-bit Address to the corresponding 16-bit Network Address.

The ZigBee Transmit Request API frame specifies the 64-bit Address and the Network Address (if known) that the packet should be sent to. By supplying both addresses, the module will forego Network Address Discovery and immediately attempt to route the data packet to the remote. If the Network Address of a particular remote changes, Network Address and route discovery will take place to establish a new route to the correct node. Upon successful packet delivery, the TX Status Frame will indicate the correct Network Address of the remote.

Table 3-01. Sample table mapping 64-bit Addresses to 16-bit Network Addresses

Index	64-bit Address	16-bit Network Address
0	0013 4000 4000 0001	1234
1	0013 4000 4000 0002	5678
2	0013 4000 4000 01A0	A479
3	0013 4000 4000 0220	1F70

3.3.3. NI-String Addressing

To send a packet to an RF module using its NI-string (Transparent Mode)

> Issue the DN (Destination Node) command using the NI (Node Identifier)-string of the destination node as the parameter.

To send a packet to an RF module using its NI-string (API Mode)

> Issue the DN command as stated above using the AT Command API frame.

When the DN command is issued, a broadcast transmission is sent across the network to discover the module that has a matching NI (Node Identifier) parameter. If a module is discovered with a matching NI-string, the DH and DL parameters will be configured to address the destination node and the command will return both the 64-bit Address and the 16-bit Network Address of the discovered node. Data can be transmitted after the DN (Destination Node) command finishes.

3.3.4. Coordinator Addressing

A Coordinator can be addressed using its 64-bit address or NI string as described in the "NI-String Addressing" section. Alternatively, since the ZigBee Coordinator has a Network Address of "0", it can be addressed by its 16-bit Network Address.

To send a transmission to a Coordinator using its 16-bit Network Address:

> Set the Destination Addresses of the transmitting module as shown below:
> DL (Destination Low Address) = 0
> DH (Destination High Address) = 0

3.3.5. Broadcast Addressing

Broadcast transmissions are sent using a 64-bit address of 0x0000FFFF. Any RF module in the PAN will accept a packet that contains a broadcast address. When configured to operate in Broadcast Mode, receiving modules do not send ACKs (Acknowledgements).

To send a broadcast packet to all modules

> Set the Destination Addresses of the transmitting module as shown below:
> DL (Destination Low Address) = 0x0000FFFF
> DH (Destination High Address) = 0x00000000

NOTE: When programming the module, parameters are entered in hexadecimal notation (without the "0x" prefix). Leading zeros may be omitted.

Refer to the "Broadcast Transmissions" section [p13] for more information.

3.4. Modes of Operation

3.4.1. Idle Mode

When not receiving or transmitting data, the RF module is in Idle Mode. During Idle Mode, the RF module is also checking for valid RF data. The module shifts into the other modes of operation under the following conditions:

- Transmit Mode (Serial data in the DI Buffer is ready to be packetized)
- Receive Mode (Valid RF data is received through the antenna)
- Sleep Mode (End Devices only - not supported in this release)
- Command Mode (Command Mode Sequence is issued)

3.4.2. Transmit Mode

When serial data is received and is ready for packetization, the RF module will exit Idle Mode and attempt to transmit the data. The destination address determines which node(s) will receive the data.

Prior to transmitting the data, the module ensures that a 16-bit Network Address and route to the destination node have been established.

If the 16-bit Network Address is not known, Network Address Discovery will take place. If a route is not known, route discovery will take place for the purpose of establishing a route to the destination node. If a module with a matching Network Address is not discovered, the packet is discarded. The data will be transmitted once a route is established. If route discovery fails to establish a route, the packet will be discarded.

Figure 3-04. Transmit Mode Sequence
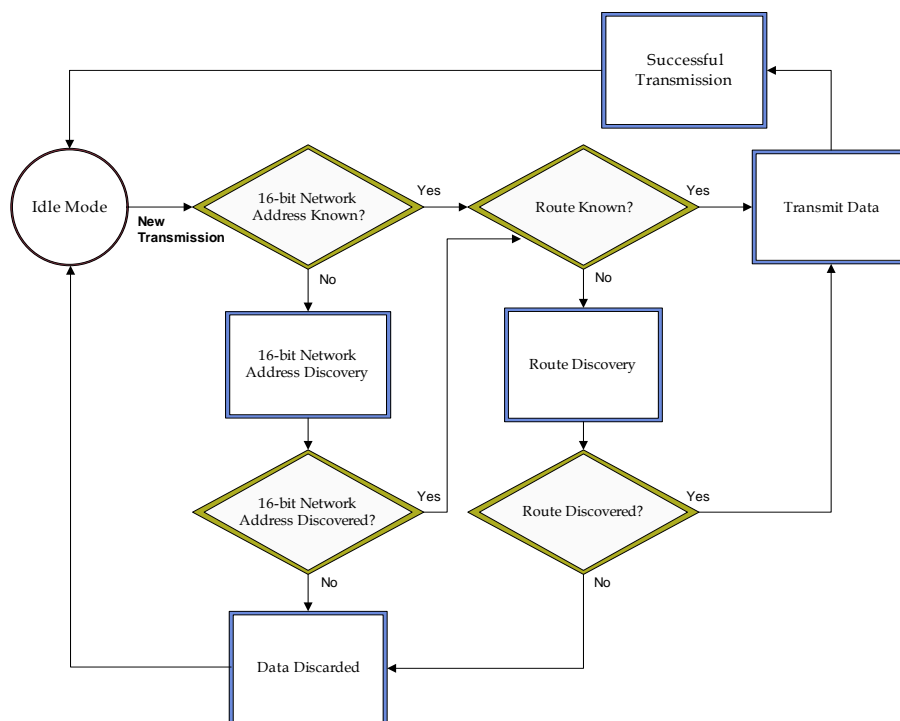
When data is transmitted from one node to another, a network-level acknowledgement is transmitted back across the established route to the source node. This acknowledgement packet indicates to the source node that the data packet was received by the destination node. If a network acknowledgement is not received, the source node will re-transmit the data.

3.4.3. Receive Mode

If a valid RF packet is received and its address matches the RF module's MY (16-bit Source Address) parameter, the data is transferred to the DO buffer.

3.4.4. Command Mode

To modify or read RF Module parameters, the module must first enter into Command Mode - a state in which incoming serial characters are interpreted as commands. Refer to the API Mode section [p29] for an alternate means of configuring modules.

AT Command Mode

To Enter AT Command Mode:

Send the 3-character command sequence "+++" and observe guard times before and after the command characters. [Refer to the "Default AT Command Mode Sequence" below.]

Default AT Command Mode Sequence (for transition to Command Mode):

 • No characters sent for one second [GT (Guard Times) parameter = 0x3E8]
 • Input three plus characters ("+++") within one second [CC (Command Sequence Character) parameter = 0x2B.]
 • No characters sent for one second [GT (Guard Times) parameter = 0x3E8]

All of the parameter values in the sequence can be modified to reflect user preferences.

NOTE: Failure to enter AT Command Mode is most commonly due to baud rate mismatch. Ensure the 'Baud' setting on the "PC Settings" tab matches the interface data rate of the RF module. By default, the BD parameter = 3 (9600 bps).

To Send AT Commands:

Send AT commands and parameters using the syntax shown below.

Figure 3-05. Syntax for sending AT Commands


```
"AT"        ASCII        Space        Parameter         Carriage
Prefix  +  Command  +  (Optional)  +  (Optional, HEX)  +  Return

Example:  ATDL 1F<CR>
```
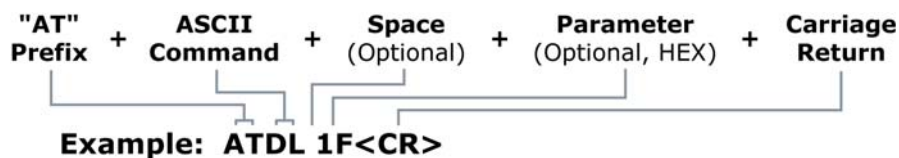
To read a parameter value stored in the RF module's register, omit the parameter field.

The preceding example would change the RF module Destination Address (Low) to "0x1F". To store the new value to non-volatile (long term) memory, subsequently send the WR (Write) command.

For modified parameter values to persist in the module's registry after a reset, changes must be saved to non-volatile memory using the WR (Write) Command. Otherwise, parameters are restored to previously saved values after the module is reset.

System Response. When a command is sent to the module, the module will parse and execute the command. Upon successful execution of a command, the module returns an "OK" message. If execution of a command results in an error, the module returns an "ERROR" message.

To Exit AT Command Mode:

1.   Send the ATCN (Exit Command Mode) command (followed by a carriage return).
     [OR]
2.   If no valid AT Commands are received within the time specified by CT (Command Mode Timeout) Command, the RF module automatically returns to Idle Mode.

For an example of programming the RF module using AT Commands and descriptions of each configurable parameter, refer to the "RF Module Configuration" chapter [p24].

3.5. Network Startup Examples

Start the Coordinator

1. Determine the operating channels list using the SC (Scan Channels) command and the PAN ID to operate using the ID (PAN ID) command. The default SD (Scan Duration) parameter value should suffice. If these values are changed from the defaults, they must be written to non-volatile memory using the WR (Write) command.

2. The Associate LED, if enabled using the D5 (DIO5 Configuration) parameter, will start blinking 1x per second once the Coordinator has started.

   If API is enabled (AP parameter > 0): The API Modem Status "Coordinator Started" is sent out the UART.

3. The AI (Association Indication) parameter will be 0 signifying a successful startup.

4. The MY (16-bit Source Address) attribute is 0
   (the 16-bit Network Address of a ZigBee Coordinator).

5. After startup, the Coordinator will allow joining based on its NJ (Node Join Time) value.

6. It is recommended that the Coordinator be configured with an NI-String identifier. This NI-String identifier should be written to non-volatile memory using the WR (Write) command to be preserved through power-loss.

Adding a Child (Router)

1. Determine the operating channel list (SC) and the desired PAN ID to join (ID) (0xFFFF - join any Pan). The default SD parameter should suffice. If these values are changed from the defaults, they must be written to non-volatile memory using the WR (Write) command.

2. The Router, on power-up, will attempt to locate a parent to join according to its SC and ID parameters.

3. Once the Router has joined a parent, the Associate LED, if enabled (D5), will start blinking 2x per second. The ID and CH parameters will reflect the operating PAN ID and Channel. The MY parameter will reflect the 16-bit Network Address of the Router. The MP command returns the 16-bit Network Address of the Router's parent (node it joined to).

   If API is enabled (AP parameter > 0): The API Modem Status "Joined" is sent out the UART.

4. If the Router is not joining as expected, the AI (Association Indication) parameter can be read to determine the cause of failure.

   Verify the PAN contains a Coordinator or nearby joined Router that has matching Channel (SC, CH) and PAN ID (ID) settings and is allowing nodes to join to it (NJ parameter).

5. Once the Router has joined a PAN, the Router will allow joining based on the NJ parameter.

6. It is recommended that the Router be configured with a unique NI-String identifier. This NI-String identifier should be written to non-volatile memory using the WR (Write) command to be preserved through power-loss.

Transmit Data

1. Start a Coordinator (refer to instructions above).

2. Add one or more Child Router(s) to the Coordinator (refer to instructions above).

3. Once the Coordinator has started, all Routers and End Devices should join to a parent and their Associate LED should blink 2x per second.

4. If any nodes have not joined, read the AI command to determine why.

5. Issue the ATND command on the Coordinator to get a list of all nodes on the network.

6. Use the 'Terminal' tab of the X-CTU Software to send serial data between nodes. The data should be transmitted from the source to the destination node as specified by the DH & DL parameters.

7. (Optional) Change the Desination Address on any node to one of the 64-bit Addresses discoverd using the ND command in step 5 (DH, DL Commands, or in the 'ZigBee Transmit Request' API Frame). Then repeat step 6 to transmit data.

4. RF Module Configuration

Two command mode protocols are supported by the XBee/XBee-PRO RF Modules: AT and API. The AT Command Mode protocol [p22] is printable and is intended for manual entry of commands and viewing parameter values. The API Command Mode protocol [p29] is a binary protocol and is intended for programmatic gets and sets of values.

Each command mode protocol requires its own firmware version. Refer to the VR (Firmware Version) command in the Diagnostics table to determine firmware versions.

4.1. AT Command Programming Examples

Refer to the 'X-CTU' section of the Development Guide [Appendix B] for more information regarding the X-CTU configuration software.

Setup

The programming examples in this section require the installation of MaxStream's X-CTU Software and a serial connection to a PC. (MaxStream stocks RS-232 and USB boards to facilitate interfacing with a PC.)

1. Install MaxStream's X-CTU Software to a PC by double-clicking the "setup_X-CTU.exe" file. (The file is located on the MaxStream CD and under the 'Software' section of the following web page: www.maxstream.net/support/downloads.php)

2. Mount the RF module to an interface board, then connect the module assembly to a PC.

3. Launch the X-CTU Software and select the 'PC Settings' tab. Verify the baud and parity settings of the Com Port match those of the RF module.

NOTE: Failure to enter AT Command Mode is most commonly due to baud rate mismatch. Ensure the 'Baud' setting on the 'PC Settings' tab matches the interface data rate of the RF module. By default, the BD parameter = 3 (which corresponds to 9600 bps).

Sample Configuration: Modify RF Module Destination Address

Example: Utilize the X-CTU "Terminal" tab to change the RF module's DL (Destination Address Low) parameter and save the new address to non-volatile memory.

After establishing a serial connection between the RF module and a PC [refer to the 'Setup' section above], select the "Terminal" tab of the X-CTU Software and enter the following command lines ('CR' stands for carriage return):

Method 1 (One line per command)

Send AT Command	**System Response**
+++	OK <CR> (Enter into Command Mode)
ATDL <Enter>	{current value} <CR> (Read Destination Address Low)
ATDL1A0D <Enter>	OK <CR> (Modify Destination Address Low)
ATWR <Enter>	OK <CR> (Write to non-volatile memory)
ATCN <Enter>	OK <CR> (Exit Command Mode)

Method 2 (Multiple commands on one line)

Send AT Command	**System Response**
+++	OK <CR> (Enter into Command Mode)
ATDL <Enter>	{current value} <CR> (Read Destination Address Low)
ATDL1A0D,WR,CN <Enter>	OK<CR> OK<CR> OK<CR>

Sample Configuration: Restore RF Module Defaults

Example: Utilize the X-CTU "Modem Configuration" tab to restore default parameter values.

After establishing a connection between the module and a PC [refer to the 'Setup' section above], select the "Modem Configuration" tab of the X-CTU Software.

1. Select the 'Read' button.

2. Select the 'Restore' button.

4.2. Command Reference Tables

XBee/XBee-PRO RF Modules expect numerical values in hexadecimal. Hexadecimal values are designated by a "0x" prefix. Decimal equivalents are designated by a "d" suffix. Table rows are sorted by command category, then by logic of most commonly used.

Special

Table 4-02.   Special Commands

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
WR	Special	**Write**. Write parameter values to non-volatile memory so that parameter modifications persist through a subsequent resets. Note: Once WR is issued, no additional characters should be sent to the module until after the "OK\r" response is received.	CRE	--	--
RE	Special	**Restore Defaults**. Restore module parameters to factory defaults. RE command does not reset the ID parameter.	CRE	--	--
FR	Special	**Software Reset**. Reset module. Responds immediately with an "OK" then performs a reset ~100ms later. Use of the FR command will cause a network layer restart on the node if SC or ID were modified since the last reset.	CRE	--	--
NR	Special	**Network Reset**. Reset network layer parameters on one or more modules within a PAN. Responds immediately with an "OK" then causes a network restart. All network configuration and routing information is consequently lost. *If NR = 0*: Resets network layer parameters on the node issuing the command. This option is only supported on Routers and End Devices and must be used with caution. Refer to the "Resetting Coordinator" section for more information. *If NR = 1*: Sends broadcast transmission to reset network layer parameters on all nodes in the PAN.	RE (when NR=0), CRE (when NR=1)	0 - 1	--

1. Node types that support the command: C = Coordinator, R = Router, E = End Device

Networking & Security

Table 4-03.   Networking Commands (Sub-categories designated within {brackets})

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
CH	Networking {Addressing}	**Operating Channel**. Read the channel number used for transmitting and receiving between RF modules. Uses 802.15.4 channel numbers.	CRE	0, 0x0B-0x1A *(XBee)* 0, 0x0C-0x17 *(XBee-PRO)* [read-only]	0
ID	Networking {Addressing}	**PAN ID**. Set/Get the PAN (Personal Area Network) ID. *Coordinator* - Set the preferred Pan ID. Set (ID = 0xFFFF) to auto-select. *Router / End Device* - Set the desired Pan ID. When the device searches for a Coordinator, it attempts to only join to a parent that has a matching Pan ID. Set (ID = 0xFFFF) to join a parent operating on any Pan ID. Changes to ID should be written to non-volatile memory using the WR command. ID changes are not used until the module is reset (FR, NR or power-up).	CRE	0 - 0x3FFF, 0xFFFF	0x0123 (291d)
DH[2]	Networking {Addressing}	**Destination Address High**. Set/Get the upper 32 bits of the 64-bit destination address. When combined with DL, it defines the destination address used for transmission. 0x000000000000FFFF is the broadcast address for the PAN. DH is not supported in API Mode. 0x0000000000000000 is the Coordinator's 16-bit Network Address.	CRE	0 - 0xFFFFFFFF	0
DL[2]	Networking {Addressing}	**Destination Address Low**. Set/Get the lower 32 bits of the 64-bit destination address. When combined with DH, DL defines the destination address used for transmission. 0x000000000000FFFF is the broadcast address for the PAN. DL is not supported in API Mode. 0x0000000000000000 is the Coordinator's 16-bit Network Address.	CRE	0 - 0xFFFFFFFF	0xFFFF (Coordinator) 0 (Router/ End Device)
MY	Networking {Addressing}	**16-bit Network Address**. Get the 16-bit Network Address of the module.	CRE	0 - 0xFFFE [read-only]	0xFFFE
MP	Networking {Addressing}	**16-bit Parent Network Address**. Get the 16-bit parent Network Address of the module.	RE	0 - 0xFFFE [read-only]	0xFFFE
SH	Networking {Addressing}	**Serial Number High**. Read high 32 bits of the RF module's unique IEEE 64-bit address. 64-bit source address is always enabled.	CRE	0 - 0xFFFFFFFF [read-only]	factory-set
SL	Networking {Addressing}	**Serial Number Low**. Read low 32 bits of the RF module's unique IEEE 64-bit address. 64-bit source address is always enabled.	CRE	0 - 0xFFFFFFFF [read-only]	factory-set
RN	Networking {Addressing}	**Random Delay Slots**. Set/Read the minimum value of the back-off exponent in the CSMA-CA algorithm (used for collision avoidance). If RN = 0, collision avoidance is disabled during the first iteration of the algorithm (802.15.4 - macMinBE).	CRE	0 - 3 [exponent]	3
NI	Networking {Identification}	**Node Identifier.** Stores a string identifier. The register only accepts printable ASCII data. In AT Command Mode, a string can not start with a space. A carriage return ends the command. Command will automatically end when maximum bytes for the string have been entered. This string is returned as part of the ND (Node Discover) command. This identifier is also used with the DN (Destination Node) command.	CRE	20-Byte printable ASCII string	--

Table 4-03.   Networking Commands (Sub-categories designated within {brackets})

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
BH	Networking {Identification}	**Broadcast Hops.** Set/Read the maximum number of hops for each broadcast data transmission. Setting this to 0 will use the maximum number of hops.	CRE	0 - 7	
NT	Networking {Identification}	**Node Discover Timeout.** Set/Read the amount of time a node will spend discovering other nodes when ND or DN is issued.	CRE	0 - 0xFC [x 100 msec]	0x3C (60d)
ND	Networking {Identification}	**Node Discover.** Discovers and reports all RF modules found. The following information is reported for each module discovered. 　　MY<CR> 　　SH<CR> 　　SL<CR> 　　NI<CR> (Variable length) 　　PARENT_NETWORK ADDRESS (2 Bytes)<CR> 　　DEVICE_TYPE<CR> (1 Byte: 0=Coord, 1=Router, 2=End Device) 　　STATUS<CR> (1 Byte: Reserved) 　　PROFILE_ID<CR> (2 Bytes) 　　MANUFACTURER_ID<CR> (2 Bytes) 　　<CR> After (NT * 100) milliseconds, the command ends by returning a <CR>. ND also accepts a Node Identifier (NI) as a parameter (optional). In this case, only a module that matches the supplied identifier will respond. If ND is sent through the API, each response is returned as a separate AT_CMD_Response packet. The data consists of the above listed bytes without the carriage return delimiters. The NI string will end in a "0x00" null character. Once the ND command has finished executing, the API will return one more AT_CMD_Response packet (with no data).	CE	optional 20-Byte NI or MY value	--
DN	Networking {Identification}	**Destination Node.** Resolves an NI (Node Identifier) string to a physical address (case-sensitive). The following events occur after the destination node is discovered: <AT Firmware> 　1. DL & DH are set to the extended (64-bit) address of the module with the matching NI (Node Identifier) string. 　2. OK (or ERROR)\r is returned. 　3. Command Mode is exited to allow immediate communication <API Firmware> 　1. The 16-bit network and 64-bit extended addresses are returned in an API Command Response frame. If there is no response from a module within (NT * 100) milliseconds or a parameter is not specified (left blank), the command is terminated and an "ERROR" message is returned. In the case of an ERROR, Command Mode is not exited.	CRE	up to 20-Byte printable ASCII string	--
SC	Networking {Joining}	**Scan Channels**. Set/Read the list of channels to scan. *Coordinator* - Bit field list of channels to choose from prior to starting network. *Router/End Device* - Bit field list of channels that will be scanned to find a Coordinator/Router to join. Changes to SC should be written using WR command. SC changes are not used until the module is reset (FR, NR or power-up). Bit (Channel):　0 (0x0B)　4 (0x0F)　8 (0x13)　12 (0x17) 　　　　　　　　1 (0x0C)　5 (0x10)　9 (0x14)　13 (0x18) 　　　　　　　　2 (0x0D)　6 (0x11)　10 (0x15)　14 (0x19) 　　　　　　　　3 (0x0E)　7 (0x12)　11 (0x16)　15 (0x1A)	CRE	1 - 0xFFFF[bitfield] (bits 0, 13, 14, 15 not allowed for XBee-PRO	0x1FFE (All XBee-PRO channels)
SD	Networking {Joining}	**Scan Duration**. Set/Read the scan duration exponent. Changes to SD should be written using WR command. *Coordinator* - Duration of the Active and Energy Scans (on each channel) that are used to determine an acceptable channel and Pan ID for the Coordinator to startup on. *Router / End Device* - Duration of Active Scan (on each channel) used to locate an available Coordinator / Router to join during Association. Scan Time is measured as:(# Channels to Scan) * (2 ^ SD) * 15.36ms - The number of channels to scan is determined by the SC parameter. The XBee can scan up to 16 channels (SC = 0xFFFF) and the XBee-PRO can scan up to 12 channels (0x1FFE). Sample Scan Duration times (13 channel scan): 　If SD = 0, time = 0.200 sec 　SD = 2, time = 0.799 sec 　SD = 4, time = 3.190 sec 　SD = 6, time = 12.780 sec	CRE	0 - 7 [exponent]	3
NJ	Networking {Joining}	**Node Join Time**. Set/Read the time that a Coordinator/Router allows nodes to join. This value can be changed at run time without requiring a Coordinator or Router to restart. The time starts once the Coordinator or Router has started. The timer is reset on power-cycle or when NJ changes.	CR	0 – 0x40, 0xFF [x 1 sec]	0xFF (always allows joining)

Table 4-03.   Networking Commands (Sub-categories designated within {brackets})

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
AI	Networking {Joining}	**Association Indication**. Read information regarding last node join request: 0x00 - Successful completion - Coordinator started or Router/End Device found and joined with a parent. 0x21 - Scan found no PANs 0x22 - Scan found no valid PANs based on current SC and ID settings 0x23 - Valid Coordinator or Routers found, but they are not allowing joining (NJ expired) 0x24 - Router Full - Allow Join set, but cannot allow any more Routers to join 0x25 - Router Full - Allow Join set, but cannot allow any more End Devices to join 0x26 - Cannot join to a node because it was a child or descendent of this device 0x27 - Node Joining attempt failed 0x28 - Device is orphaned and is looking for its parent using Orphan Scans 0x29 - Router Start attempt failed' 0x2A - Coordinator Start attempt failed' 0xFF - Scanning for a Parent	CRE	0 - 0xFF [read-only]	--

1. Node types that support the command: C=Coordinator, R=Router, E=End Device
2. Command supported by modules using AT Command firmware only

RF Interfacing

Table 4-04.   RF Interfacing Commands

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
PL	RF Interfacing	**Power Level**. Select/Read the power level at which the RF module transmits conducted power.	CRE	0 - 4 (XBee / XBee-PRO) 0 = -10 / 10 dBm 1 = -6 / 12 dBm 2 = -4 / 14 dBm 3 = -2 / 16 dBm 4 = 0 / 18 dBm	4
CA	RF Interfacing	**CCA Threshold**. Set/Read the CCA (Clear Channel Assessment) threshold. Prior to transmitting a packet, a CCA is performed to detect energy on the channel. If the detected energy is above the CCA Threshold, the module will not transmit the packet.	CRE	0x24 - 0x50 [-dBm]	0x40 (-64d dBm)

1. Node types that support the command: C = Coordinator, R = Router, E = End Device

Serial Interfacing (I/O)

Table 4-05.   Serial Interfacing Commands

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
AP[2]	Serial Interfacing	**API Enable**. Enable API Mode. The AP parameter is only applicable when using modules that contain the following firmware versions: 8.1xx (Coordinator), 8.3xx (Router), 8.5xx (End Device)	CRE	1 - 2 1 = API-enabled 2 = API-enabled (w/escaped control characters)	1
BD	Serial Interfacing	**Interface Data Rate**. Set/Read the serial interface data rate for communication between the module serial port and host. Any value above 0x07 will be interpreted as an actual baud rate. When a value above 0x07 is sent, the closest interface data rate represented by the number is stored in the BD register.	CRE	0 - 7 (standard baud rates) 0 = 1200 bps 1 = 2400 2 = 4800 3 = 9600 4 = 19200 5 = 38400 6 = 57600 7 = 115200 0x80 - 0x1C200 (non-standard rates)	3
RO	Serial Interfacing	**Packetization Timeout**. Set/Read number of character times of inter-character silence required before packetization. Set (RO=0) to transmit characters as they arrive instead of buffering them into one RF packet.	CRE	0 - 0xFF [x character times]	3
D7	Serial Interfacing	**DIO7 Configuration**. Select/Read options for the DIO7 line of the RF module.	CRE	0 - 1 0 = Disabled 1 = CTS Flow Control	1
D5	Serial Interfacing	**DIO5 Configuration**. Configure options for the DIO5 line of the RF module. Options include: Associated LED indicator (LED blinks 1x/sec when the module is powered and 2x/sec when module is associated to a Coordinator.).	CRE	0 - 1 0 = Disabled 1 = Associated indication LED	1

Table 4-05.   Serial Interfacing Commands

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
P0	Serial Interfacing	**PWM0 Configuration**. Select/Read function for PWM0.	CRE	0 - 1 0 = Disabled 1 = RSSI PWM	1
RP	Diagnostics	**RSSI PWM Timer.** Time RSSI signal will be output after last transmission. When RP = 0xFF, output will always be on.	CRE	0 - 0xFF [x 100 ms]	0x28 (40d)

1. Node types that support the command: C = Coordinator, R = Router, E = End Device
2. Command supported by modules using API firmware only

Diagnostics

Table 4-06.   Diagnostics Commands

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
VR	Diagnostics	**Firmware Version**. Read firmware version of the module.	CRE	0 - 0xFFFF [read-only]	Factory-set
HV	Diagnostics	**Hardware Version**. Read hardware version of the module.	CRE	0 - 0xFFFF [read-only]	Factory-set

1. Node types that support the command:C = Coordinator, R = Router, E = End Device

AT Command Options

Table 4-07.   AT Command Options Commands

AT Command	Command Category	Name and Description	Node Type[1]	Parameter Range	Default
CT[2]	AT Command Mode Options	**Command Mode Timeout**. Set/Read the period of inactivity (no valid commands received) after which the RF module automatically exits AT Command Mode and returns to Idle Mode.	CRE	2 - 0x028F [x 100 ms]	0x64 (100d)
CN[2]	AT Command Mode Options	**Exit Command Mode**. Explicitly exit the module from AT Command Mode.	CRE	--	--
GT[2]	AT Command Mode Options	**Guard Times**. Set required period of silence before and after the Command Sequence Characters of the AT Command Mode Sequence (GT + CC + GT). The period of silence is used to prevent inadvertent entrance into AT Command Mode.	CRE	1 - 0x0CE4 [x 1 ms] (max of 3.3 decimal sec)	0x3E8 (1000d)
CC[2]	AT Command Mode Options	**Command Sequence Character**. Set/Read the ASCII character value to be used between Guard Times of the AT Command Mode Sequence (GT + CC + GT). The AT Command Mode Sequence enters the RF module into AT Command Mode. CC command is only applicable when using modules that contain the following "AT Command" firmware versions: 8.0xx (Coordinator), 8.2xx (Router), 8.4xx (End Device)	CRE	0 - 0xFF	0x2B ('+' ASCII)

1. Node types that support the command: C = Coordinator, R = Router, E = End Device
2. Command supported by modules using AT Command firmware only

4.3. API Operation

Non-API XBee/XBee-PRO RF Modules act as a serial line replacement (Transparent Operation) - all UART data received through the DI pin is queued up for RF transmission. When the module receives an RF packet, the data is sent out the DO pin with no additional information.

Inherent to Transparent Operation are the following behaviors:

- If module parameter registers are to be set or queried, a special operation is required for transitioning the module into Command Mode [refer to p22].
- In point-to-multipoint systems, the application must send extra information so that the receiving module(s) can distinguish between data coming from different remotes.

As an alternative to the default Transparent Operation, API (Application Programming Interface) Operations are available. API operation requires that communication with the module be done through a structured interface (data is communicated in frames in a defined order). The API specifies how commands, command responses and module status messages are sent and received from the module using a UART Data Frame.

4.3.1. API Frame Specifications

Two API modes are supported and both can be enabled using the AP (API Enable) command. Use the following AP parameter values to configure the module to operate in a particular mode:

- AP = 1: API Operation
- AP = 2: API Operation (with escaped characters)

API Operation (AP parameter = 1)

When this API mode is enabled (AP = 1), the UART data frame structure is defined as follows:

Figure 4-06. UART Data Frame Structure:

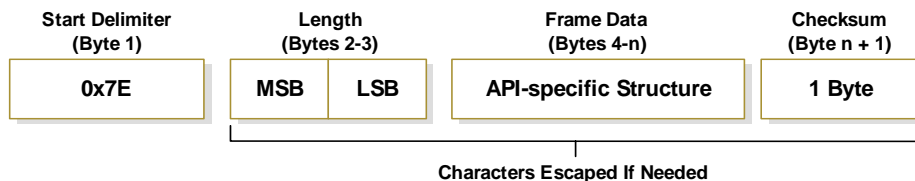| Start Delimiter (Byte 1)	Length (Bytes 2-3)		Frame Data (Bytes 4-n)	Checksum (Byte n + 1)
0x7E	MSB	LSB	API-specific Structure	1 Byte

MSB = Most Significant Byte, LSB = Least Significant Byte

Any data received prior to the start delimiter is silently discarded. If the frame is not received correctly or if the checksum fails, the module will reply with a module status frame indicating the nature of the failure.

API Operation - with Escape Characters (AP parameter = 2)

When this API mode is enabled (AP = 2), the UART data frame structure is defined as follows:

Figure 4-07. UART Data Frame Structure - with escape control characters:

Start Delimiter (Byte 1)	Length (Bytes 2-3)		Frame Data (Bytes 4-n)	Checksum (Byte n + 1)
0x7E	MSB	LSB	API-specific Structure	1 Byte

Characters Escaped If Needed

MSB = Most Significant Byte, LSB = Least Significant Byte

Escape characters. When sending or receiving a UART data frame, specific data values must be escaped (flagged) so they do not interfere with the data frame sequencing. To escape an interfering data byte, insert 0x7D and follow it with the byte to be escaped XOR'd with 0x20.

Data bytes that need to be escaped:

- 0x7E – Frame Delimiter
- 0x7D – Escape
- 0x11 – XON
- 0x13 – XOFF

Example - Raw UART Data Frame (before escaping interfering bytes):
        0x7E 0x00 0x02 0x23 0x11 0xCB

0x11 needs to be escaped which results in the following frame:
0x7E 0x00 0x02 0x23 0x7D 0x31 0xCB

Note: In the above example, the length of the raw data (excluding the checksum) is 0x0002 and the checksum of the non-escaped data (excluding frame delimiter and length) is calculated as:
0xFF - (0x23 + 0x11) = (0xFF - 0x34) = 0xCB.

Checksum

To test data integrity, a checksum is calculated and verified on non-escaped data.

To calculate: Not including frame delimiters and length, add all bytes keeping only the lowest 8 bits of the result and subtract the result from 0xFF.

To verify: Add all bytes (include checksum, but not the delimiter and length). If the checksum is correct, the sum will equal 0xFF.

4.3.2. API Types

Frame data of the UART data frame forms an API-specific structure as follows:

**Figure 4-08. UART Data Frame & API-specific Structure:**
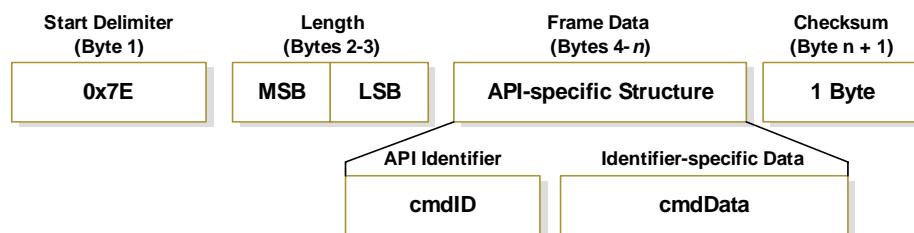
The cmdID frame (API-identifier) indicates which API messages will be contained in the cmdData frame (Identifier-specific data). Refer to the sections that follow for more information regarding the supported API types. Note that multi-byte values are sent big endian.

Modem Status

API Identifier: 0x8A
RF module status messages are sent from the module in response to specific conditions.

Figure 4-09. Modem Status Frames
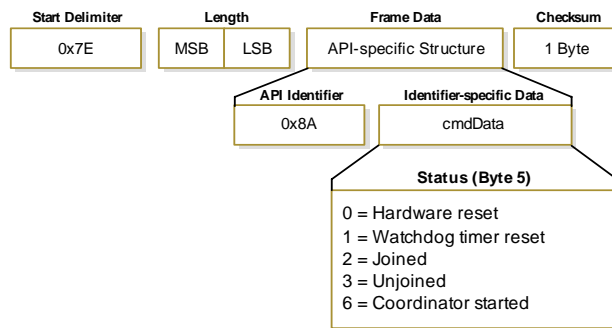
AT Command

API Identifier Value: 0x08

Allows for module parameter registers to be queried or set.
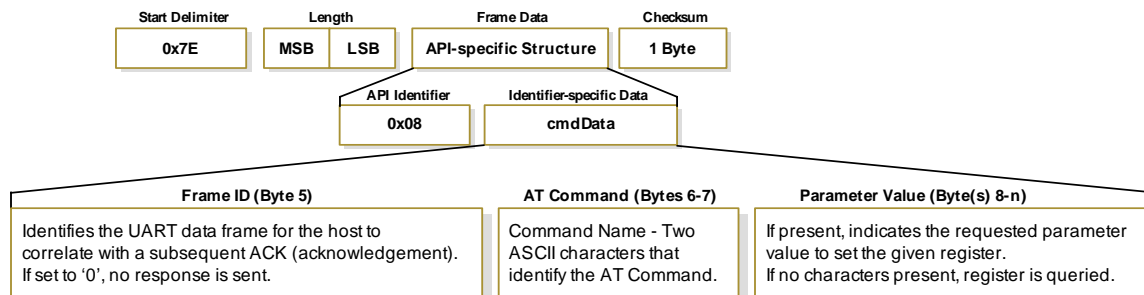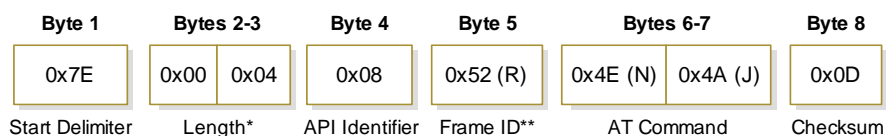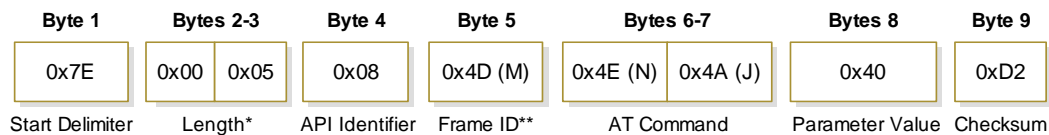
Figure 4-10. AT Command Frames

Start Delimiter	Length		Frame Data	Checksum
0x7E	MSB	LSB	API-specific Structure	1 Byte

API Identifier	Identifier-specific Data
0x08	cmdData

Frame ID (Byte 5)	AT Command (Bytes 6-7)	Parameter Value (Byte(s) 8-n)
Identifies the UART data frame for the host to correlate with a subsequent ACK (acknowledgement). If set to '0', no response is sent.	Command Name - Two ASCII characters that identify the AT Command.	If present, indicates the requested parameter value to set the given register. If no characters present, register is queried.

Figure 4-11. Example: API frames when reading the NJ parameter value of the module.

Byte 1	Bytes 2-3		Byte 4	Byte 5	Bytes 6-7		Byte 8
0x7E	0x00	0x04	0x08	0x52 (R)	0x4E (N)	0x4A (J)	0x0D
Start Delimiter	Length*		API Identifier	Frame ID**	AT Command		Checksum

* Length [Bytes] = API Identifier + Frame ID + AT Command

** "R" value was arbitrarily selected.

Figure 4-12. Example: API frames when modifying the NJ parameter value of the module.

Byte 1	Bytes 2-3		Byte 4	Byte 5	Bytes 6-7		Bytes 8	Byte 9
0x7E	0x00	0x05	0x08	0x4D (M)	0x4E (N)	0x4A (J)	0x40	0xD2
Start Delimiter	Length*		API Identifier	Frame ID**	AT Command		Parameter Value	Checksum

* Length [Bytes] = API Identifier + Frame ID + AT Command + Parameter Value

** "M" value was arbitrarily selected.

A string parameter used with the NI (Node Identifier), ND (Node Discover) and DH (Destination Address High) command is terminated with a 0x00 character.
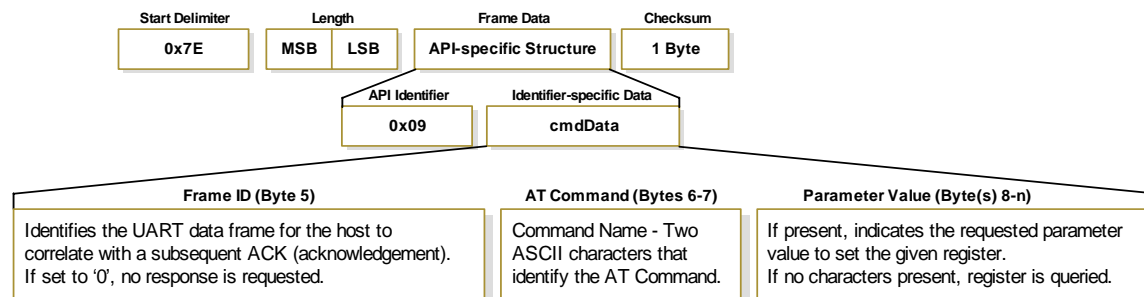
AT Command - Queue Parameter Value

API Identifier Value: 0x09

This API type allows module parameters to be queried or set. In contrast to the "AT Command" API type, new parameter values are queued and not applied until either the "AT Command" (0x08) API type or the AC (Apply Changes) command is issued. Register queries (reading parameter values) are returned immediately.

Figure 4-13. AT Command Frames
(Note that frames are identical to the "AT Command" API type except for the API identifier.)

Start Delimiter	Length		Frame Data	Checksum
0x7E	MSB	LSB	API-specific Structure	1 Byte

API Identifier	Identifier-specific Data
0x09	cmdData

| Frame ID (Byte 5)	AT Command (Bytes 6-7)	Parameter Value (Byte(s) 8-n)
Identifies the UART data frame for the host to correlate with a subsequent ACK (acknowledgement). If set to '0', no response is requested.	Command Name - Two ASCII characters that identify the AT Command.	If present, indicates the requested parameter value to set the given register. If no characters present, register is queried.

AT Command Response

API Identifier Value: 0x88
Response to previous command.

In response to an AT Command message, the module will send an AT Command Response message. Some commands will send back multiple frames (for example, the ND (Node Discover) command). These commands will end by sending a frame with a status of ATCMD_OK and no cmdData.

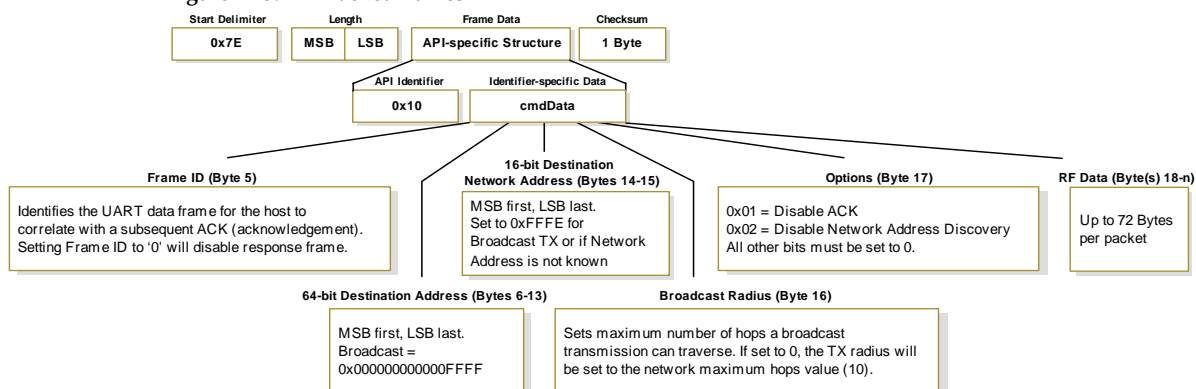**Figure 4-14. AT Command Response Frames.**
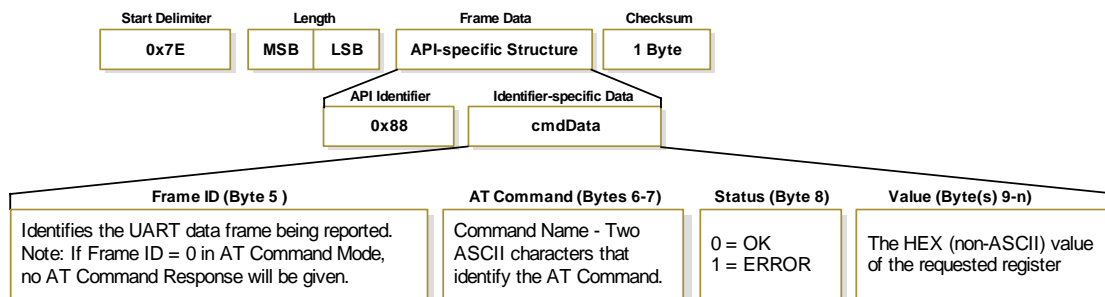
ZigBee Transmit Request

API Identifier Value: 0x10
A TX Request message will cause the module to send RF Data as an RF Packet.

Figure 4-15. TX Packet Frames

ZigBee Transmit Status

API Identifier Value: 0x8B
When a TX Request is completed, the module sends a TX Status message. This message will indicate if the packet was transmitted successfully or if there was a failure.
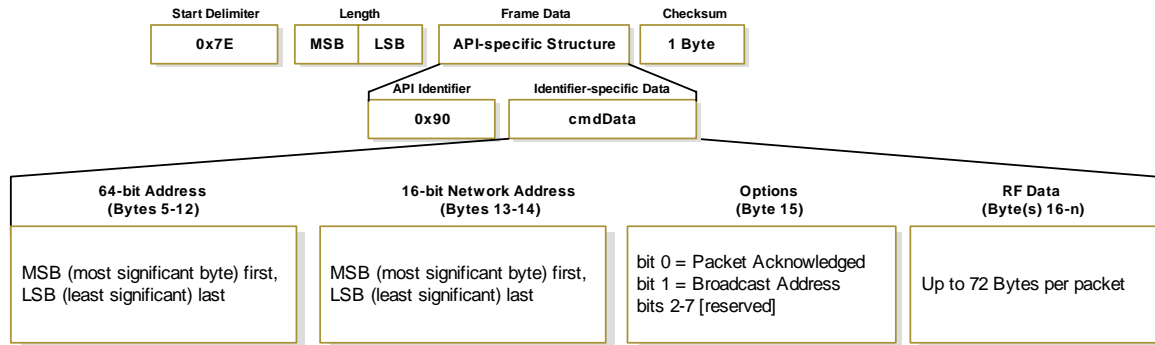
Figure 4-16. TX Status Frames
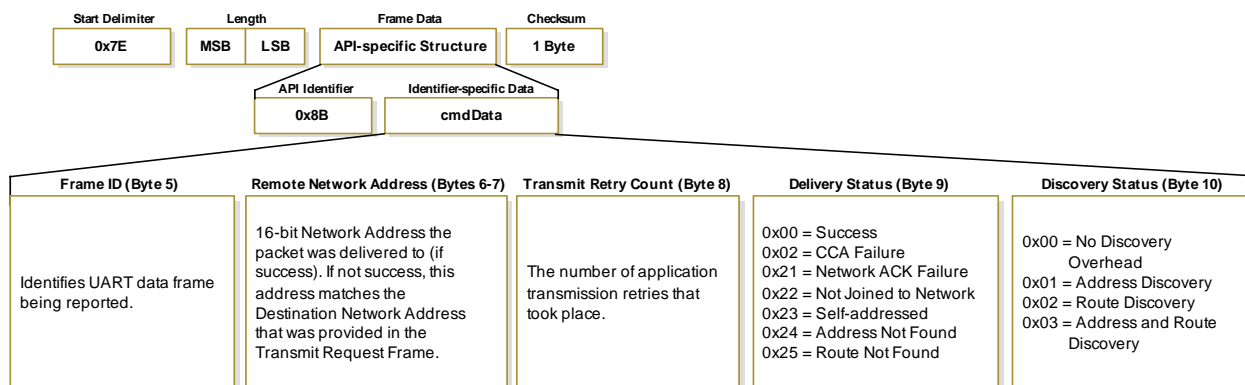
ZigBee Receive Packet

API Identifier Value: 0x90

When the module receives an RF packet, it is sent out the UART using this message type.

Figure 4-17. RX Packet Frames

Appendix A: Agency Certifications

FCC Certification

XBee/XBee-PRO RF Modules comply with Part 15 of the FCC rules and regulations. Compliance with the labeling requirements, FCC notices and antenna usage guidelines is required.

To fulfill FCC Certification requirements, the OEM must comply with the following regulations:

1. The system integrator must ensure that the text on the external label provided with this device is placed on the outside of the final product [Figure A-01].
2. XBee/XBee-PRO RF Modules may only be used with antennas that have been tested and approved for use with this module [refer to the antenna tables in this section].

OEM Labeling Requirements

WARNING: The Original Equipment Manufacturer (OEM) must ensure that FCC labeling requirements are met. This includes a clearly visible label on the outside of the final product enclosure that displays the contents shown in the figure below.

Figure A-01. Required FCC Label for OEM products containing the XBee/XBee-PRO RF Module

Contains FCC ID: OUR-XBEE/OUR-XBEEPRO*

The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (*i.*) this device may not cause harmful interference and (*ii.*) this device must accept any interference received, including interference that may cause undesired operation.

* The FCC ID for the XBee is "OUR-XBEE". The FCC ID for the XBee-PRO is "OUR-XBEEPRO".

FCC Notices

IMPORTANT: The XBee/XBee-PRO OEM RF Module has been certified by the FCC for use with other products without any further certification (as per FCC section 2.1091). Modifications not expressly approved by MaxStream could void the user's authority to operate the equipment.

IMPORTANT: OEMs must test final product to comply with unintentional radiators (FCC section 15.107 & 15.109) before declaring compliance of their final product to Part 15 of the FCC Rules.

IMPORTANT: The RF module has been certified for remote and base radio applications. If the module will be used for portable applications, the device must undergo SAR testing.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: Re-orient or relocate the receiving antenna, Increase the separation between the equipment and receiver, Connect equipment and receiver to outlets on different circuits, or Consult the dealer or an experienced radio/TV technician for help.

FCC-Approved Antennas (2.4 GHz)

XBee/XBee-PRO RF Modules can be installed using antennas and cables constructed with standard connectors (Type-N, SMA, TNC, etc.) if the installation is performed professionally and according to FCC guidelines. For installations not performed by a professional, non-standard connectors (RPSMA, RPTNC, etc) must be used.

The modules are FCC-approved for fixed base station and mobile applications on channels 0x0B - 0x1A (XBee) and 0x0C - 0x17 (XBee-PRO). If the antenna is mounted at least 20cm (8 in.) from nearby persons, the application is considered a mobile application. Antennas not listed in the table must be tested to comply with FCC Section 15.203 (Unique Antenna Connectors) and Section 15.247 (Emissions).

XBee OEM RF Modules (1 mW): XBee Modules have been tested and approved for use with all of the antennas listed in the tables below (Cable-loss IS NOT required).

XBee-PRO OEM RF Modules (60 mW): XBee-PRO Modules have been tested and approved for use with the antennas listed in the tables below (Cable-loss IS required when using antennas listed in Table A-02).

Table A-01. Antennas approved for use with the XBee/XBee-PRO RF Modules (Cable-loss is not required.)

Part Number	Type (Description)	Gain	Application*	Min. Separation
A24-HSM-450	Dipole (Half-wave articulated RPSMA - 4.5")	2.1 dBi	Fixed/Mobile	20 cm
A24-HABSM	Dipole (Articulated RPSMA)	2.1 dBi	Fixed	20 cm
A24-HABUF-P5I	Dipole (Half-wave articulated bulkhead mount U.FL. w/ 5" pigtail)	2.1 dBi	Fixed	20 cm
A24-QI	Monopole (Integrated whip)	1.5 dBi	Fixed	20 cm

Table A-02. Antennas approved for use with the XBee/XBee-PRO RF Modules (Cable-loss is required)

Part Number	Type (Description)	Gain	Application*	Min. Separation	Required Cable-loss
A24-C1	Surface Mount	-1.5 dBi	Fixed/Mobile	20 cm	-
A24-Y4NF	Yagi (4-element)	6.0 dBi	Fixed	2 m	8.1 dB
A24-Y6NF	Yagi (6-element)	8.8 dBi	Fixed	2 m	10.9 dB
A24-Y7NF	Yagi (7-element)	9.0 dBi	Fixed	2 m	11.1 dB
A24-Y9NF	Yagi (9-element)	10.0 dBi	Fixed	2 m	12.1 dB
A24-Y10NF	Yagi (10-element)	11.0 dBi	Fixed	2 m	13.1 dB
A24-Y12NF	Yagi (12-element)	12.0 dBi	Fixed	2 m	14.1 dB
A24-Y13NF	Yagi (13-element)	12.0 dBi	Fixed	2 m	14.1 dB
A24-Y15NF	Yagi (15-element)	12.5 dBi	Fixed	2 m	14.6 dB
A24-Y16NF	Yagi (16-element)	13.5 dBi	Fixed	2 m	15.6 dB
A24-Y16RM	Yagi (16-element, RPSMA connector)	13.5 dBi	Fixed	2 m	15.6 dB
A24-Y18NF	Yagi (18-element)	15.0 dBi	Fixed	2 m	17.1 dB
A24-F2NF	Omni-directional (Fiberglass base station)	2.1 dBi	Fixed/Mobile	20 cm	4.2 dB
A24-F3NF	Omni-directional (Fiberglass base station)	3.0 dBi	Fixed/Mobile	20 cm	5.1 dB
A24-F5NF	Omni-directional (Fiberglass base station)	5.0 dBi	Fixed/Mobile	20 cm	7.1 dB
A24-F8NF	Omni-directional (Fiberglass base station)	8.0 dBi	Fixed	2 m	10.1 dB
A24-F9NF	Omni-directional (Fiberglass base station)	9.5 dBi	Fixed	2 m	11.6 dB
A24-F10NF	Omni-directional (Fiberglass base station)	10.0 dBi	Fixed	2 m	12.1 dB
A24-F12NF	Omni-directional (Fiberglass base station)	12.0 dBi	Fixed	2 m	14.1 dB
A24-F15NF	Omni-directional (Fiberglass base station)	15.0 dBi	Fixed	2 m	17.1 dB
A24-W7NF	Omni-directional (Base station)	7.2 dBi	Fixed	2 m	9.3 dB
A24-M7NF	Omni-directional (Mag-mount base station)	7.2 dBi	Fixed	2 m	9.3 dB
A24-P8SF	Flat Panel	8.5 dBi	Fixed	2 m	8.6 dB
A24-P8NF	Flat Panel	8.5 dBi	Fixed	2 m	8.6 dB
A24-P13NF	Flat Panel	13.0 dBi	Fixed	2 m	13.1 dB
A24-P14NF	Flat Panel	14.0 dBi	Fixed	2 m	14.1 dB
A24-P15NF	Flat Panel	15.0 dBi	Fixed	2 m	15.1 dB
A24-P16NF	Flat Panel	16.0 dBi	Fixed	2 m	16.1 dB
A24-P19NF	Flat Panel	19.0 dBi	Fixed	2 m	19.1 dB

* If using the RF module in a portable application (For example - If the module is used in a handheld device and the antenna is less than 20cm from the human body when the device is operation): The integrator is responsible for passing additional SAR (Specific Absorption Rate) testing based on FCC rules 2.1091 and FCC Guidelines for Human Exposure to Radio Frequency Electromagnetic Fields, OET Bulletin and Supplement C. The testing results will be submitted to the FCC for approval prior to selling the integrated unit. The required SAR testing measures emissions from the module and how they affect the person.

RF Exposure

> ⚠ WARNING: To satisfy FCC RF exposure requirements for mobile transmitting devices, a separation distance of 20 cm or more should be maintained between the antenna of this device and persons during device operation. To ensure compliance, operations at closer than this distance is not recommended. The antenna used for this transmitter must not be co–located in conjunction with any other antenna or transmitter.

The preceding statement must be included as a CAUTION statement in OEM product manuals in order to alert users of FCC RF Exposure compliance.

European Certification

The XBee/XBee-PRO RF Module has been certified for use in several European countries. For a complete list, refer to www.maxstream.net.

If the XBee/XBee-PRO RF Modules are incorporated into a product, the manufacturer must ensure compliance of the final product to the European harmonized EMC and low-voltage/safety standards. A Declaration of Conformity must be issued for each of these standards and kept on file as described in Annex II of the R&TTE Directive.

Furthermore, the manufacturer must maintain a copy of the XBee/XBee-PRO user manual documentation and ensure the final product does not exceed the specified power ratings, antenna specifications, and/or installation requirements as specified in the user manual. If any of these specifications are exceeded in the final product, a submission must be made to a notified body for compliance testing to all required standards.

OEM Labeling Requirements

The 'CE' marking must be affixed to a visible location on the OEM product.

Figure A-02. CE Labeling Requirements

The CE mark shall consist of the initials "CE" taking the following form:

- If the CE marking is reduced or enlarged, the proportions given in the above graduated drawing must be respected.
- The CE marking must have a height of at least 5mm except where this is not possible on account of the nature of the apparatus.
- The CE marking must be affixed visibly, legibly, and indelibly.

Restrictions

Power Output: The power output of the XBee-PRO RF Modules must not exceed 10 dBm. The power level is set using the PL command and the PL parameter must equal "0" (10 dBm).

France: France imposes restrictions on the 2.4 GHz band. Go to www.art-telecom.Fr or contact MaxStream for more information.

Norway: Norway prohibits operation near Ny-Alesund in Svalbard. More information can be found at the Norway Posts and Telecommunications site (www.npt.no).

Declarations of Conformity

MaxStream has issued Declarations of Conformity for the XBee/XBee-PRO RF Modules concerning emissions, EMC and safety. Files are located in the 'documentation' folder of the MaxStream CD.

Important Note

MaxStream does not list the entire set of standards that must be met for each country. MaxStream customers assume full responsibility for learning and meeting the required guidelines for each country in their distribution market. For more information relating to European compliance of an OEM product incorporating the XBee/XBee-PRO RF Module, contact MaxStream, or refer to the following web sites:

CEPT ERC 70-03E - Technical Requirements, European restrictions and general requirements: Available at www.ero.dk/.

R&TTE Directive - Equipment requirements, placement on market: Available at www.ero.dk/.

Appendix B: Development Guide

Migrating from the 802.15.4 Protocol

This following are some of the differences in the ZigBee firmware assuming familiarity with the 802.15.4 application:

- ZigBee Command Set
- Address Assignment
- API / AT Firmware Versions

Also, refer to the "Getting Started" section [p23] for more information.

ZigBee Command Set

Modified Commands

- CH - Read Only command that displays the operating channel that was selected from SC.
- MY - Read Only command that displays the assigned 16-bit Network Address of the device.
- AI - ZigBee definitions added to this command. See documentation.
- A1, A2 and CE commands are not supported.

New Commands

- NJ (Node Join Time) - This value determines how long a Coordinator or Router will allow other devices to join to it. This command is supported on Coordinators & Routers only.
- MP (16-bit Parent Network Address). This value represents the 16-bit parent Network Address of the module.
- BH (Broadcast Hops). This value sets the maximum number of hops for each broadcast data transmission. Setting this to 0 will use the maximum number of hops.

API / AT Firmware Versions

The 802.15.4 firmware supports the AP command for setting the module into No API (AP=0), API without escaping (AP=1), or API with escaping (AP=2) modes. The first digit in the 802.15.4 firmware versions is a '1'.

The ZigBee firmware comes in different versions to support the API interface (AP 1, 2 modes) or the AT command set (AP 0 mode). The first digit in the ZigBee firmware versions is an '8'.

The following is a list of firmware versions:

- 8.0xx - Coordinator, AT Command support (Transparent Mode)
- 8.1xx - Coordinator, API support (AP 1, 2)
- 8.2xx - Router, AT Command support (Transparent Mode)
- 8.3xx - Router, API support (AP 1, 2)
- 8.4xx - End Device, AT Command support (Transparent Mode)
- 8.5xx - End Device, API support (AP 1, 2)

XBee/XBee-PRO Development Kits

The XBee Professional Development Kit includes the hardware and software needed to rapidly create long range wireless data links between nodes (XBee and XBee-PRO Starter Kits that contain fewer modules and accessories are also available).

Table B-01.   Items Included in the Development Kit

Item	Qty.	Description	Part #
XBee-PRO Module	2	(1) OEM RF Module w/ U.FL antenna connector (1) OEM RF Module w/ attached wire antenna	XBP24-AUI-002 XBP24-AWI-002
XBee Module	3	(1) OEM RF Module w/ U.FL antenna connector (1) OEM RF Module w/ attached whip antenna (1) OEM RF Module w/ chip antenna	XB24-AUI-002 XB24-AWI-002 XB24-ACI-002
RS-232 Development Board	4	Board for interfacing between modules and RS-232 nodes (Converts signal levels, displays diagnostic info, & more)	XBIB-R
USB Development Board	1	Board for interfacing between modules & USB nodes (Converts signal levels, displays diagnostic info, & more)	XBIB-U
RS-232 Cable (6′, straight-through)	1	Cable for connecting RS-232 interface board with DTE nodes (nodes that have a male serial DB-9 port - such as most PCs)	JD2D3-CDS-6F
USB Cable (6′)	1	Cable for connecting USB interface board to USB nodes	JU1U2-CSB-6F
Serial Loopback Adapter	1	[Red] Adapter for configuring the module assembly (module + RS-232 interface board) to function as a repeater for range testing	JD2D3-CDL-A
NULL Modem Adapter (male-to-male)	1	[Black] Adapter for connecting the module assembly (module + RS-232 interface board) to other DCE (female DB-9) nodes	JD2D2-CDN-A
NULL Modem Adapter (female-to-female)	1	[Gray] Adapter for connecting serial nodes. It allows users to bypass the radios to verify serial cabling is functioning properly.	JD3D3-CDN-A
Power Adapter (9VDC, 1 A)	1	Adapter for powering the RS-232 development board	JP5P2-9V11-6F
Battery Clip (9V)	1	Clip for remotely powering the RS-232 board w/ a 9V battery	JP2P3-C2C-4I
RPSMA Antenna	2	RPSMA half-wave dipole antenna (2.4 GHz, 2.1 dB)	A24-HASM-450
RF Cable Assembly	2	Adapter for connecting RPSMA antenna to U.FL connector	JF1R6-CR3-4I
CD	1	Documentation and Software	MD0030
Quick Start Guide	1	Step-by-step instruction on how to create wireless links & test range capabilities of the modules	MD0026

Interfacing Options

The development kit includes RS-232 and USB interface boards. The boards provide a connection to PC ports and therefore give access to the RF module registries. Parameters stored in the registry allow OEMs and integrators to customize the modules to suite the needs of their data radio systems.

The following sections illustrate how to use the interface boards for development purposes. The MaxStream Interface board provides means for connecting the module to any node that has an available RS-232 or USB connector. Since the module requires signals to enter at TTL voltages, one of the main functions of the interface board is to convert signals between TTL levels and RS-232 and USB levels.
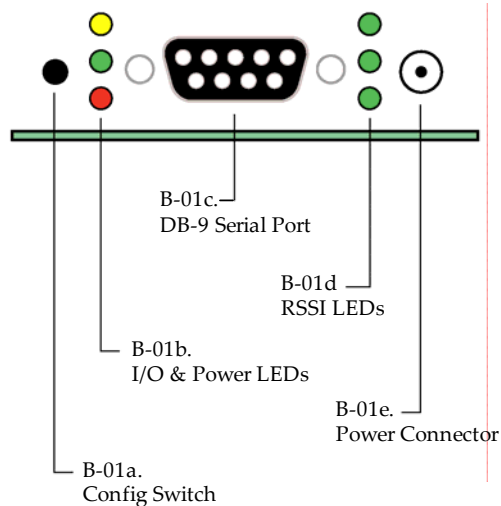
Note: In the following sections, an OEM RF Module mounted to an interface board will be referred to as a "Module Assembly".

RS-232 Development Board

External Interface

B-01a. Reset Switch

The Reset Switch is used to reset (re-boot) the RF module. This switch only applies when using the configuration tabs of MaxStream's X-CTU Software.

B-01b. I/O & Power LEDs

LEDs indicate RF module activity as follows:

Yellow (top LED) = Serial Data Out (to host)
Green (middle)　 = Serial Data In (from host)
Red (bottom)　　= Power/Association Indicator (Refer to the D5 (DIO5 Configuration) parameter)

Figure B-01. Front View

B-01c.
DB-9 Serial Port

B-01d
RSSI LEDs

B-01b.
I/O & Power LEDs

B-01e.
Power Connector

B-01a.
Config Switch

B-01c. Serial Port

Standard female DB-9 (RS-232) connector.

B-01d. RSSI LEDs

RSSI LEDs indicate the amount of fade margin present in an active wireless link. Fade margin is defined as the difference between the incoming signal strength and the module's receiver sensitivity.

3 LEDs ON　=　Very Strong Signal (> 30 dB fade margin)
2 LEDs ON　=　Strong Signal (> 20 dB fade margin)
1 LED ON　　=　Moderate Signal (> 10 dB fade margin)
0 LED ON　　=　Weak Signal (< 10 dB fade margin)

B-01e. Power Connector

5-14 VDC power connector

B-02a. DIP Switch
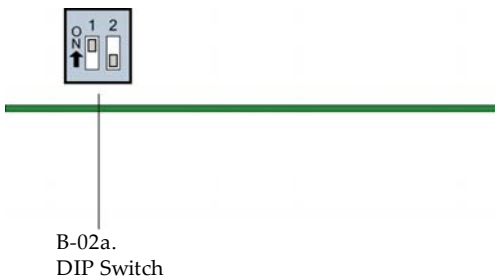
DIP Switch functions are not supported in this release. Future downloadable firmware versions will support DIP Switch configurations.

Figure B-02. Back View

B-02a.
DIP Switch

RS-232 Pin Signals

Figure B-03. Pins used on the female RS-232 (DB-9) Serial Connector
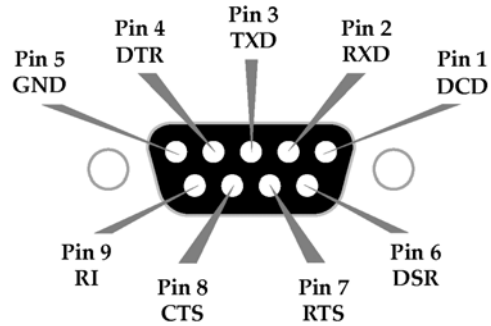
Table B-02.   Pin Assignments and Implementations

DB-9 Pin	RS-232 Name	Description	Implementation*
1	DCD	Data-Carrier-Detect	Connected to DSR (pin6)
2	RXD	Receive Data	Serial data exiting the module assembly (to host)
3	TXD	Transmit Data	Serial data entering into the module assembly (from host)
4	DTR	Data-Terminal-Ready	Can enable Power-Down on the module assembly
5	GND	Ground Signal	Ground
6	DSR	Data-Set-Ready	Connected to DCD (pin1)
7	$\overline{\text{RTS}}$ / CMD	Request-to-Send / Command Mode	Provides $\overline{\text{RTS}}$ flow control or enables Command Mode
8	$\overline{\text{CTS}}$	Clear-to-Send	Provides $\overline{\text{CTS}}$ flow control
9	RI	Ring Indicator	Optional power input that is connected internally to the positive lead of the front power connector

* Functions listed in the implementation column may not be available at the time of release.

Wiring Diagrams

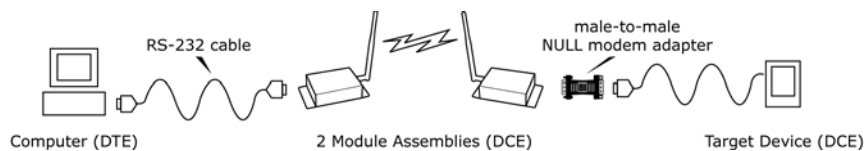**Figure B-04. DTE node (RS-232, male DB-9 connector) wired to a DCE Module Assembly (female DB-9)**
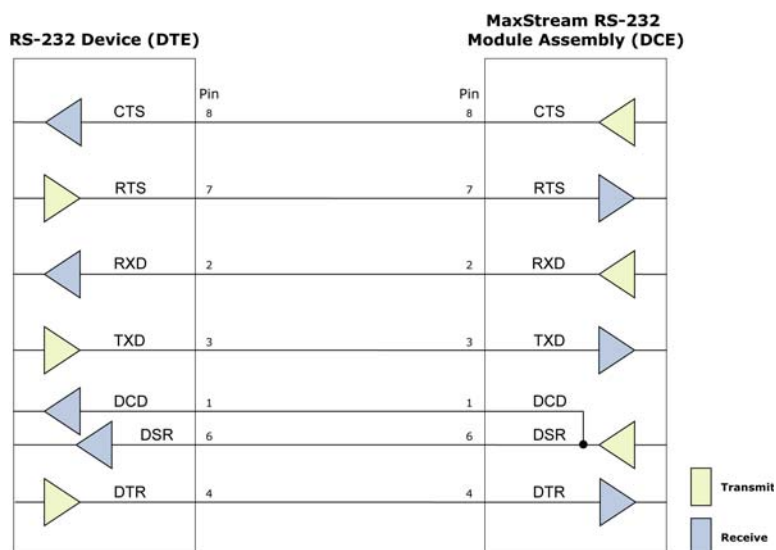
Figure B-05. DCE Module Assembly (female DB-9 connector) wired to a DCE node (RS-232, male DB-9)
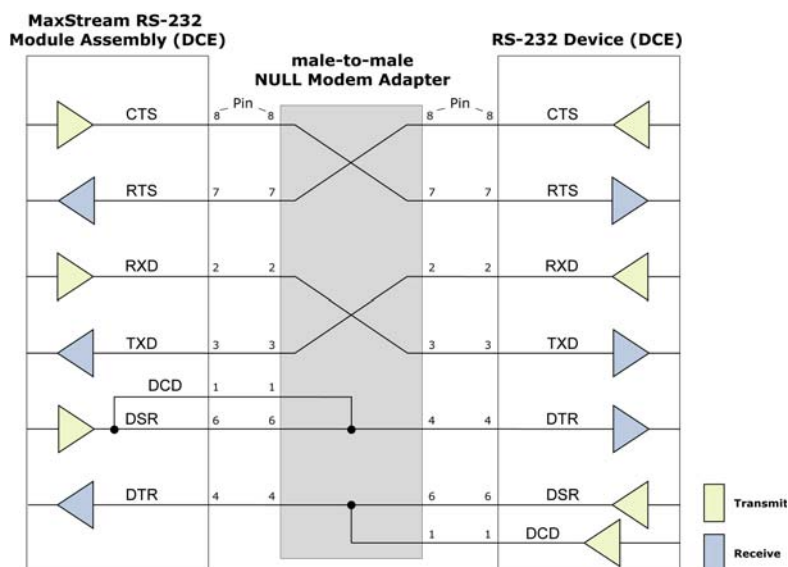
Sample Wireless Connection: DTE <--> DCE <--> DCE <--> DCE

Figure B-06. Typical wireless link between DTE and DCE nodes

Adapters

The development kit includes several adapters that support the following functions:

- Performing Range Tests
- Testing Cables
- Connecting to other RS-232 DCE and DTE nodes
- Connecting to terminal blocks or RJ-45 (for RS-485/422 nodes)

NULL Modem Adapter (male-to-male)

Part Number: JD2D2-CDN-A (Black, DB-9 M-M) The male-to-male NULL modem adapter is used to connect two DCE nodes. A DCE node connects with a straight-through cable to the male serial port of a computer (DTE).

Figure B-07. Male NULL modem adapter and pinouts
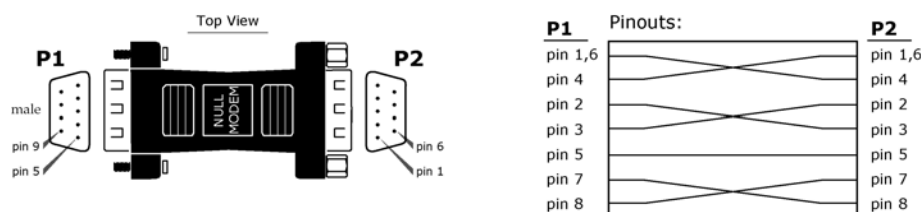
Figure B-08. Example of a MaxStream Radio Modem (DCE node) connecting to another DCE node)
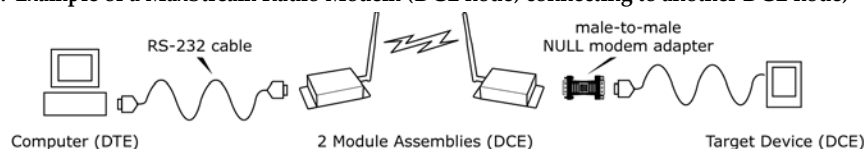
NULL Modem Adapter (female-to-female)

Part Number: JD3D3-CDN-A (Gray, DB-9 F-F) The female-to-female NULL modem adapter is used to verify serial cabling is functioning properly. To test cables, insert the female-to-female NULL modem adapter in place of a pair of module assemblies (RS-232 interface board + XTend Module) and test the connection without the modules in the connection.

Figure B-09. Female NULL modem adapter and pinouts
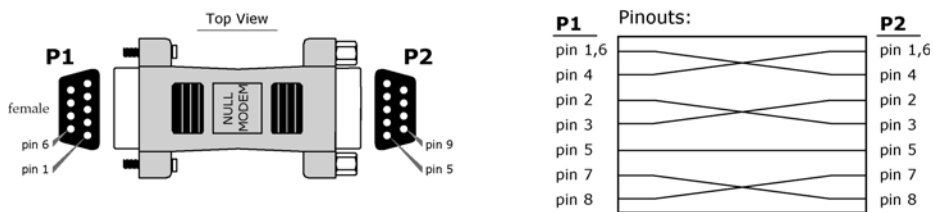
Serial Loopback Adapter

Part Number: JD2D3-CDL-A (Red, DB-9 M-F) The serial loopback adapter is used for range testing. During a range test, the serial loopback adapter configures the module to function as a repeater by looping serial data back into the radio for retransmission.

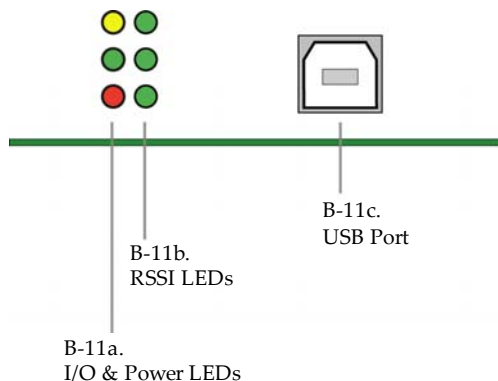**Figure B-10. Serial loopback adapter and pinouts**
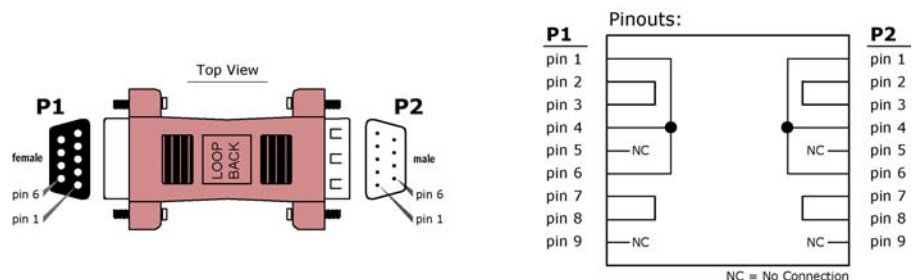
USB Development Board

External Interface

B-11a. I/O & Power LEDs

Figure B-11. Front View

B-11c.
USB Port

B-11b.
RSSI LEDs

B-11a.
I/O & Power LEDs

LEDs indicate RF module activity as follows:

Yellow (top LED) = Serial Data Out (to host)
Green (middle) = Serial Data In (from host)
Red (bottom)   = Power/Association Indicator (Refer to the D5 (DIO5 Configuration) parameter)

host   Module Assemblies   host

B-11b. RSSI LEDs

RSSI LEDs indicate the amount of fade margin present in an active wireless link. Fade margin is defined as the difference between the incoming signal strength and the module's receiver sensitivity.
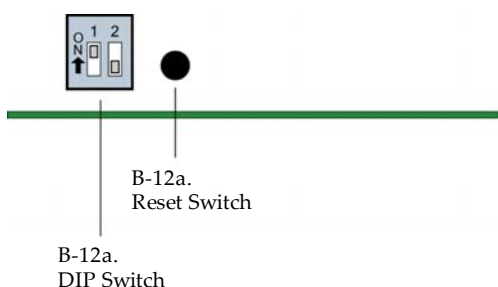
3 LEDs ON = Very Strong Signal (> 30 dB fade margin)
2 LEDs ON = Strong Signal (> 20 dB fade margin)
1 LED ON   = Moderate Signal (> 10 dB fade margin)
0 LED ON   = Weak Signal (< 10 dB fade margin)

B-11c. USB Port

Standard Type-B OEM connector is used to communicate with OEM host and power the RF module.

B-12a. DIP Switch

Figure B-12. Back View

B-12a.
Reset Switch

B-12a.
DIP Switch

DIP Switch functions are not supported in this release. Future down-loadable firmware versions will support the DIP Switch configurations.

B-12b. Reset Switch

The Reset Switch is used to reset (re-boot) the RF module.

USB Pin Signals

Table B-03.   USB signals and their implantations on the XBee/XBee-PRO RF Module

Pin	Name	Description	Implementation
1	VBUS	Power	Power the RF module
2	D-	Transmitted & Received Data	Transmit data to and from the RF module
3	D+	Transmitted & Received Data	Transmit data to and from the RF module
4	GND	Ground Signal	Ground

X-CTU Software

X-CTU is a MaxStream-provided software program used to interface with and configure Max-Stream RF Modules. The software application is organized into the following four tabs:

- PC Settings tab - Setup PC serial ports for interfacing with an RF module
- Range Test tab - Test the RF module's range and monitor packets sent and received
- Terminal tab - Set and read RF module parameters using AT Commands
- Modem Configuration tab - Set and read RF module parameters

Figure B-13. X-CTU User Interface (PC Settings, Range Test, Terminal and Modem Configuration tabs)
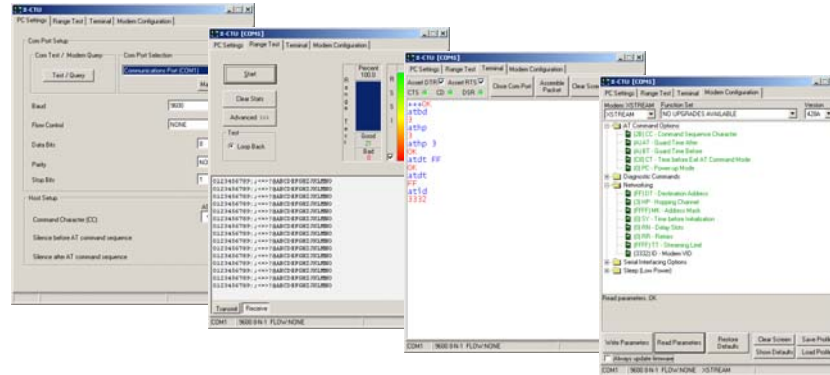
NOTE: PC Setting values are visible at the bottom of the Range Test, Terminal and Modem Configura–tion tabs. A shortcut for editing PC Setting values is available by clicking on any of the values.

Install

Double-click the "setup_X-CTU.exe" file and follow prompts of the installation screens. This file is located in the 'software' folder of the MaxStream CD and also under the 'Downloads' section of the following web page: www.maxstream.net/support/downloads.php

Setup

To use the X-CTU software, a module assembly (An RF module mounted to an interface Board) must be connected to a serial port of a PC. The interface data rate and parity settings of the serial port ("PC Settings" tab) must match those of the module (BD (Baud Rate) and NB (Parity) parameters).

Serial Communications Software

A terminal program is built into the X-CTU Software. Other terminal programs such as "HyperTer-minal" can also be used. When issuing AT Commands through a terminal program interface, use the following syntax:

Figure B-14. Syntax for sending AT Commands
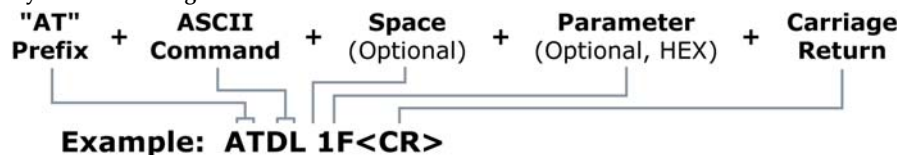
NOTE: To read a parameter value stored in a register, leave the parameter field blank.

The example above issues the DL (Destination Address Low) command to change destination address of the module to "0x1F". To save the new value to the module's non-volatile memory, issue WR (Write) command after modifying parameters.

Appendix C: Additional Information

1-Year Warranty

XBee/XBee-PRO RF Modules from MaxStream, Inc. (the "Product") are warranted against defects in materials and workmanship under normal use, for a period of 1-year from the date of purchase. In the event of a product failure due to materials or workmanship, MaxStream will repair or replace the defective product. For warranty service, return the defective product to MaxStream, shipping prepaid, for prompt repair or replacement.

The foregoing sets forth the full extent of MaxStream's warranties regarding the Product. Repair or replacement at MaxStream's option is the exclusive remedy. THIS WARRANTY IS GIVEN IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, AND MAXSTREAM SPECIFICALLY DISCLAIMS ALL WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL MAXSTREAM, ITS SUPPLIERS OR LICENSORS BE LIABLE FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCT, FOR ANY LOSS OF USE, LOSS OF TIME, INCONVENIENCE, COMMERCIAL LOSS, LOST PROFITS OR SAVINGS, OR OTHER INCIDENTAL, SPECIAL OR CONSE-QUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, TO THE FULL EXTENT SUCH MAY BE DISCLAIMED BY LAW. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES. THEREFORE, THE FOREGOING EXCLUSIONS MAY NOT APPLY IN ALL CASES. This warranty provides specific legal rights. Other rights which vary from state to state may also apply.

Ordering Information

Figure C-01. Divisions of the XBee/XBee-PRO RF Module Part Numbers
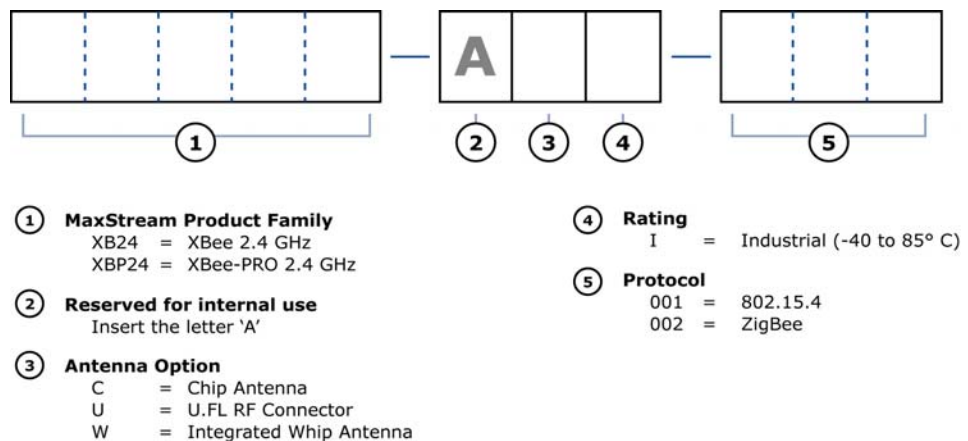
For example:

XBP24-AWI-002 = XBee-PRO OEM RF Module, 2.4 GHz, integrated whip antenna, Industrial temperature rating, ZigBee protocol

Contact MaxStream

Free and unlimited technical support is included with every MaxStream Radio Modem sold. For the best in wireless data solutions and support, please use the following resources:

Documentation: www.maxstream.net/support/downloads.php

Technical Support: Phone.   (866) 765-9885 toll-free U.S.A. & Canada
                                         (801) 765-9885 Worldwide

                         Live Chat.   www.maxstream.net

                         E-Mail.   rf-xperts@maxstream.net

MaxStream office hours are 8:00 am - 5:00 pm [U.S. Mountain Standard Time]