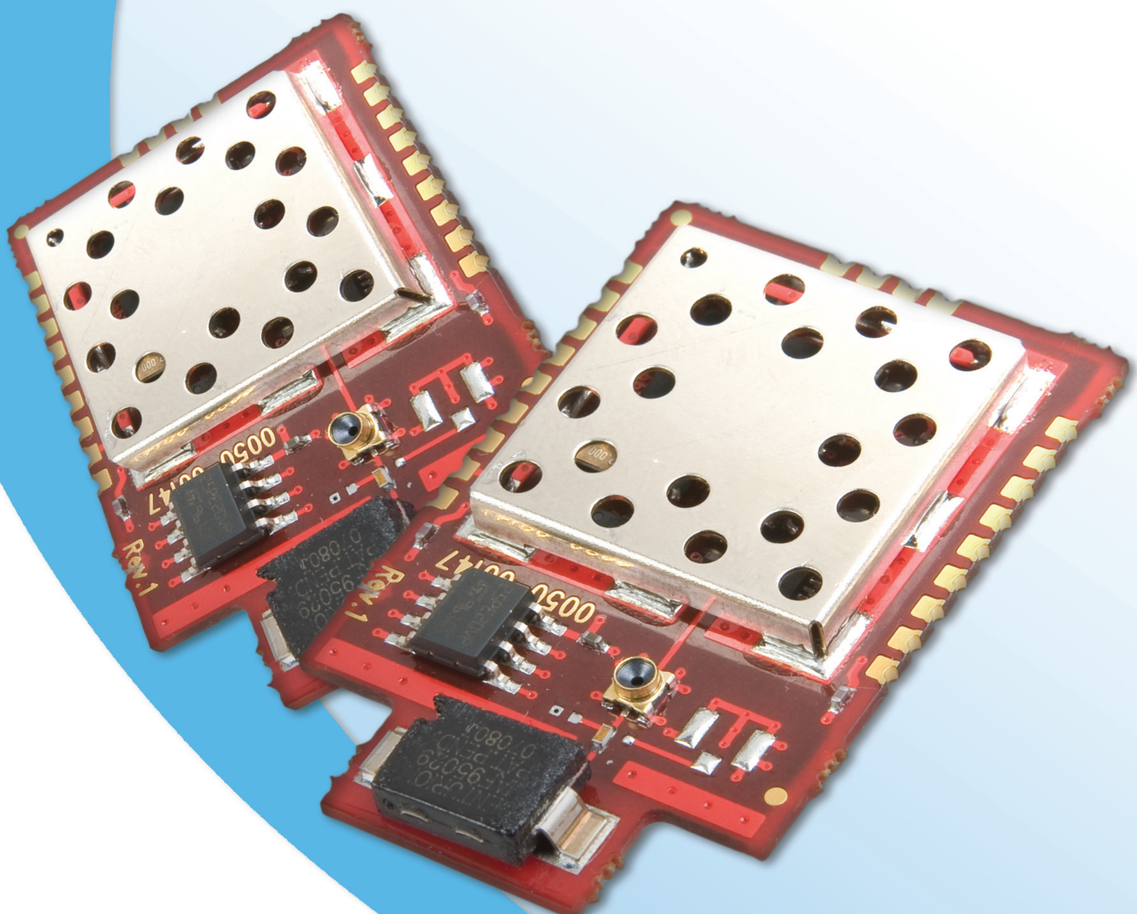
ZB2430 WIRELESS MODULE

USER MANUAL

Version 2.1



www.lairdtech.com

Innovative **Technology**
for a **Connected** World

Laird Technologies is the world leader in the design and manufacture of customized, performance-critical products for wireless and other advanced electronics applications.
Laird Technologies partners with its customers to find solutions for applications in various industries such as:

Network Equipment
Telecommunications
Data Communications
Automotive Electronics
Computers
Aerospace
Military
Medical Equipment
Consumer Electronics

Laird Technologies offers its customers unique product solutions, dedication to research and development, as well as a seamless network of manufacturing and customer support facilities across the globe.

This material is preliminary
Information furnished by Laird Technologies in this specification is believed to be accurate. Devices sold by Laird Technologies are covered by the warranty and patent indemnification provisions appearing in its Terms of Sale only. Laird Technologies makes no warranty, express, statutory, and implied or by description, regarding the information set forth herein. Laird Technologies reserves the right to change specifications at any time and without notice. Laird Technologies' products are intended for use in normal commercial and industrial applications. Applications requiring unusual environmental requirements such as military, medical life-support or life-sustaining equipment are specifically not recommended without additional testing for such application.

Limited Warranty, Disclaimer, Limitation of Liability
For a period of one (1) year from the date of purchase by the OEM customer, Laird Technologies warrants the OEM transceiver against defects in materials and workmanship. Laird Technologies will not honor this warranty (and this warranty will be automatically void) if there has been any (1) tampering, signs of tampering; 2) repair or attempt to repair by anyone other than an Laird Technologies authorized technician. This warranty does not cover and Laird Technologies will not be liable for, any damage or failure caused by misuse, abuse, acts of God, accidents, electrical irregularity, or other causes beyond Laird Technologies' control, or claim by other than the original purchaser. In no event shall Laird Technologies be responsible or liable for any damages arising: From the use of product; From the loss of use, revenue or profit of the product; or As a result of any event, circumstance, action, or abuse beyond the control of Laird Technologies, whether such damages be direct, indirect, consequential, special or otherwise and whether such damages are incurred by the person to whom this warranty extends or third party. If, after inspection, Laird Technologies' determines that there is a defect, Laird Technologies will repair or replace the OEM transceiver at their discretion. If the product is replaced, it may be a new or refurbished product.

REVISION HISTORY

REVISION HISTORY

Revision	Description
Version 1.0	03/17/09
Version 2.0	05/18/09
Version 2.1	05/29/09

TABLE OF CONTENTS

CONTENTS

OVERVIEW

PRODUCT DESCRIPTION

The Laird Technologies ZB2430 module is based on the IEEE 802.15.4 wireless communication standard and the robust ZigBee networking protocol. The ZB2430 provides OEMs with an industry leading 2.4 GHz module performance in a package that provides low power consumption, easy integration, long range, along with superior features and functionality. The ZB2430 requires no additional FCC licensing in the Americas. OEMs can easily make existing systems wireless with little or no RF expertise.

The ZB2430 is a member of the Laird Technologies FlexRF OEM transceiver family. The ZB2430 is a cost effective, high performance, Direct Sequence Spread Spectrum (DSSS) transceiver. It has been designed for integration into OEM systems operating under FCC part 15.247 regulations for the 2.4 GHz ISM band.

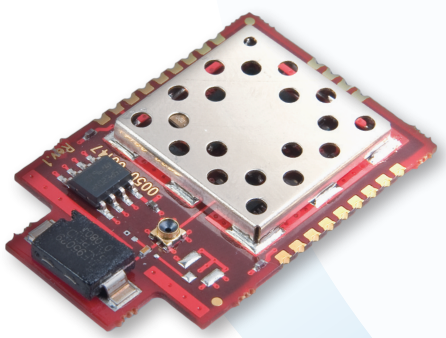
Fully transparent, these transceivers operate seamlessly in serial cable replacement applications. Communications include both system and configuration data via an asynchronous serial interface for OEM Host communications. All association and RF system data transmission/reception is performed by the transceiver.

This document contains information about the hardware and software interface between a Laird Technologies ZB2430 transceiver and an OEM Host. Information includes the theory of operation, specifications, interface definitions, configuration information and mechanical drawings.

NOTE: Unless mentioned specifically by name, the ZB2430 modules will be referred to as "radio" or "transceiver". Individual naming is used to differentiate product specific features. The host (PC/Microcontroller/Any device to which the ZB2430 module is connected) will be referred to as "OEM Host" or "Host."

KEY FEATURES

- Mesh architecture
- Retries and Acknowledgements
- Programmable Network Parameters
- Multiple generic I/O
- 250 kbps RF data stream
- Software selectable interface baud rates from 110 bps to 115.2 kbps
- Non-standard baud rates supported
- Low cost, low power and small size, ideal for high volume, portable and battery powered applications
- All modules are qualified for industrial temperatures (-40 °F to 176 °F {-40 °C to 80°C})
- Advanced configuration available using AT commands
- Easy to use Configuration and Test Utility software



OVERVIEW

IEEE 802.15.4 AND ZIGBEE OVERVIEW

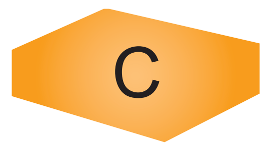
The ZB2430 uses the ZigBee protocol stack, a network layer protocol that uses small, low power digital transceivers based on the IEEE 802.15.4 hardware standard. The 802.15.4 standard is a specification for cost-effective, low data rate (<250 kbps) wireless technology designed for personal-area and device-to-device wireless networking operating in the unlicensed Industrial, Scientific and Medical (ISM) bands.

The IEEE 802.15.4 standard specifies the hardware requirements, including frequency bands, receiver sensitivity, modulation and spreading requirements. The ZigBee layer is the software layer that sits atop the 802.15.4 PHY/MAC layer and performs all packet routing and mesh networking.

There are three device types present in a ZigBee network: Coordinator (Full Function Device), Router (Full Function Device), and End Device (Reduced Function Device). Each network consists of a single coordinator, optional router(s), and optional end device(s).

COORDINATOR

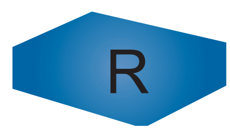
The coordinator is responsible for establishing the operating channel and PAN ID for the entire network. Once the coordinator has established a network, it allows routers and end devices to join the network; assigning each device a unique 16-bit network address. The coordinator is intended to be mains powered (always on).



- One Coordinator per network
- Establishes Channel and PAN ID
- Responsible for network formation and maintenance
- Full function device
- Packet routing capabilities
- Mains powered (always on)
- Power down modes are not supported
- Network address of 0x0000

ROUTER

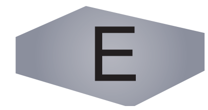
Routers are responsible for creating and maintaining network information and determining the optimal route for a data packet. Routers must first associate with the network before other devices can join through them. Routers are intended to be mains powered (always on).



- Multiple routers can be used
- Allows other routers/end devices to join the network
- Full function device
- Packet routing capabilities
- Mains powered (always on)
- Power down modes are not supported
- Unique network address dynamically assigned by parent

END DEVICE

End devices are incapable of routing data and must send data through their parent to communicate with other nodes. Ideally the end devices will be in sleep mode all the time. When they have data to send, they wake up, send the data and then go back to sleep. The parent (coordinator/router) of an end device should be mains powered to allow it to store data to be sent to the sleeping end device. End Device Sleep Timers control how often the end device wakes up and how long it is awake to receive messages. These timers are covered in greater detail later in this manual.



- Multiple end devices can be used
- No packet routing capabilities
- Can communicate with other devices in the network through its parent device
- Reduced function device
- Mains or battery powered
- Power down modes are supported
- Unique network address dynamically assigned by parent

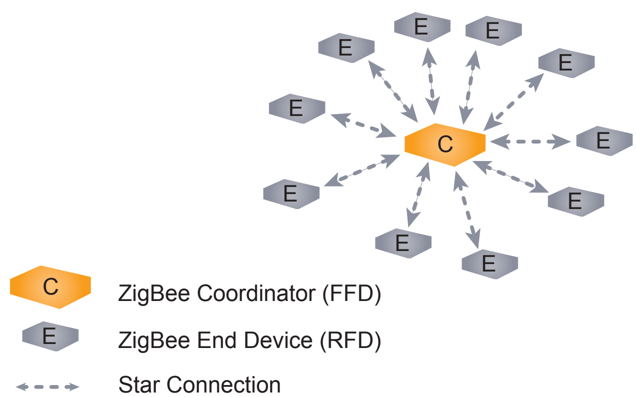
CREATING A NETWORK

The IEEE 802.15.4 MAC (Media Access Control software) provides support for two wireless network topologies: star and mesh. The management of these networks is performed by the ZigBee layer. All devices, regardless of topology, participate in the network using their unique 16-bit address that is assigned by the coordinator.

STAR TOPOLOGY

The star topology is the simplest topology offered. It allows any Full Function Device (FFD), which would be a coordinator, to communicate directly with any FFD or Reduced Function Device (RFD) within its range.

Star Topology

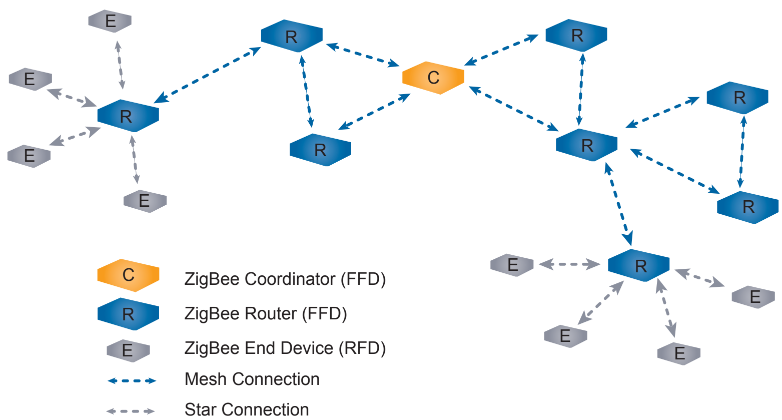


THEORY OF OPERATION

MESH TOPOLOGY

The mesh topology allows any FFD, which would be a coordinator or router, to communicate directly with any other device within its range and to have messages relayed to out of range devices via multi-hop routing. While FFD devices can communicate with a RFD, RFD's cannot directly route messages and must have their messages routed by their parent device (coordinator or router). ZigBee mesh enables the formation of more complex networks, including ad-hoc, self-organizing, and self-healing structures.

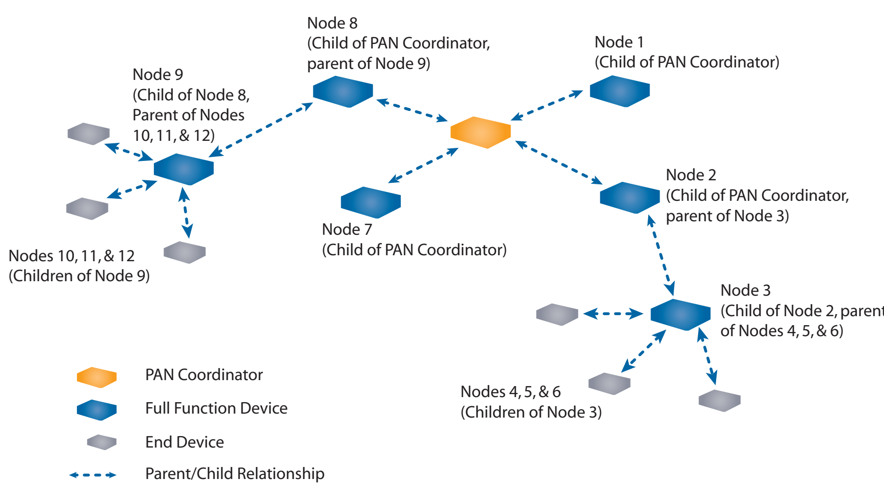
Mesh Topology



PARENT/CHILD RELATIONSHIP

ZigBee uses a parent/child relationship between network devices. The network begins with the coordinator as the first device on the network. When any new device (router or end device) associates with the coordinator, a relationship is established between them. The coordinator is the parent, and the device is the child. If a second device joins the network, a new parent/child relationship is created between the coordinator and the new device. If a device is not in range of the coordinator, it subsequently joins the network through a router, and becomes a child of that router. Network devices can have multiple children, but only one parent. By design, end devices cannot be parents and are always children of the coordinator or a router.

Parent/Child Relationship



THEORY OF OPERATION

NETWORK LIMITATIONS

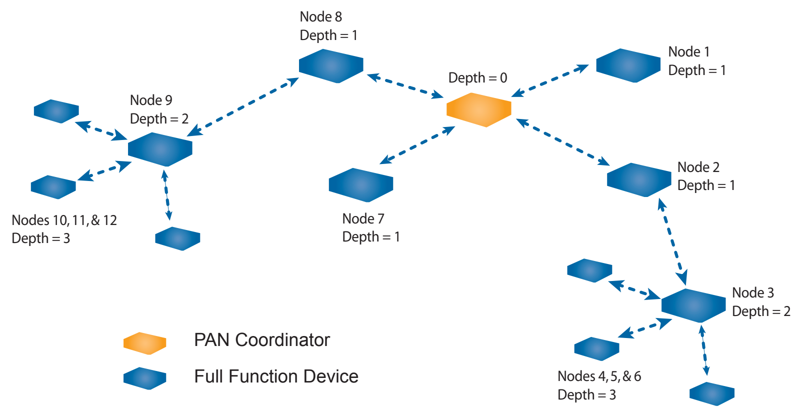
The ZigBee network structure and ultimate size are specified by Stack profiles. The Stack profiles define the maximum number of Layers, maximum number of children per parent, and the maximum number of routers that can be children. These parameters are set during code compilation and cannot be altered after compilation. The ZB2430 uses the restrictions specified by the Home Lighting and Controls profile.

The ZigBee coordinator determines the maximum number of children any device within its network is allowed. Of these children, a maximum number can be router-capable devices; while the remainder shall be reserved for end devices. Each device has an associated depth which indicates the minimum number of hops a transmitted packet must travel to reach the ZigBee coordinator.

MAXIMUM NETWORK DEPTH

The coordinator has a depth of zero and its children have a depth of 1. Maximum Network Depth specifies the maximum number of hops (Routers) that a node can be away from the coordinator. The Home Lighting and Controls profile limits the maximum network depth to 5.

Maximum Network Depth



MAXIMUM NUMBER OF CHILDREN PER PARENT

Maximum Number of Children specifies the total number of children that can be connected directly to a parent device on the current network. The Home Lighting and Control profile specifies the maximum number of children the coordinator and routers can have associated with them to be 20. Of those 20 children, a maximum of 6 routers can be router-capable devices while the remainder shall be end devices.

THEORY OF OPERATION

ZIGBEE ADDRESSING

The IEEE 802.15.4 standard from which the ZigBee protocol was derived specifies two types of addressing modes:

- 16-bit Network Address
- 64-bit MAC Address

16-BIT NETWORK ADDRESS

The 16-bit network (NWK) address is a unique address on the network. The coordinator always has a network address of 0x0000 and it will assign a network address to each radio within its range. Routers will then assign network addresses to radios within their range which have not previously been assigned an address. Because the 16-bit address is unique to each radio on the network, an addressed packet can be sent from any radio on the network to any other radio located anywhere on the network.

ENGINEER'S TIP: 16-bit Network Address

In a ZigBee network, nodes are assigned a 16-bit NWK address according to how the network formed. By design, the coordinator will always have a NWK address of 0x0000. The first router that associates with the coordinator is assigned a NWK address of 0x0001. The second router that associates with the coordinator is assigned an address of 0x143E. The 16-bit address is persistent through power loss and only resets when an NV Reset command is issued performed or NV Restore is disabled in EEPROM (EEPROM address 0x45, bit-3).

64-BIT NETWORK ADDRESS

The 64-bit MAC address consists of a 40-bit Organizationally Unique Identifier (OUI) and a 24-bit address programmed by the manufacturer. All ZB2430 transcievers have the same OUI of 0x00 0x00 0x00 0x50 0x67 and a unique 24-bit address. This address can be used to identify devices on a network, but cannot be used to route packets through the network

In order to send data to a specific device in the network, the OEM can compile a table, which lists the 64-bit MAC and the corresponding 16-bit Network address (refer to the following table). The ZB2430's built-in Discover IEEE Address and Discover Network Address commands allow the OEM to query the network and discover all available devices that respond within a fixed period.

Device Table Example

Index	MAC Address (64-bit)	NWK Address
0	0x00 0x00 0x00 0x50 0x67 0x12 0x34 0x56	0x0000
1	0x00 0x00 0x00 0x50 0x67 0x16 0x45 0x34	0x0001
2	0x00 0x00 0x00 0x50 0x67 0x34 0x21 0x78	0x143E

THEORY OF OPERATION

MESH ROUTING (AODV)

The ZigBee protocol uses the Ad-hoc On-Demand Distance Vector (AODV) routing algorithm. AODV allows nodes to pass messages through their neighbors to devices which they cannot communicate directly. This is done by discovering the routes along which messages can be passed using the shortest route possible.

The following Image shows a typical ZigBee network. The circles surrounding the 4 nodes represent the Personal Operating Space (POS) of each node. Because of the limited range, each node can only communicate with the neighboring node(s) next to it. When a node needs to send a message to a node which is not a neighbor, it broadcasts a Route Request (RREQ) message containing the source destination address, the network address of the destination radio and a path cost metric.

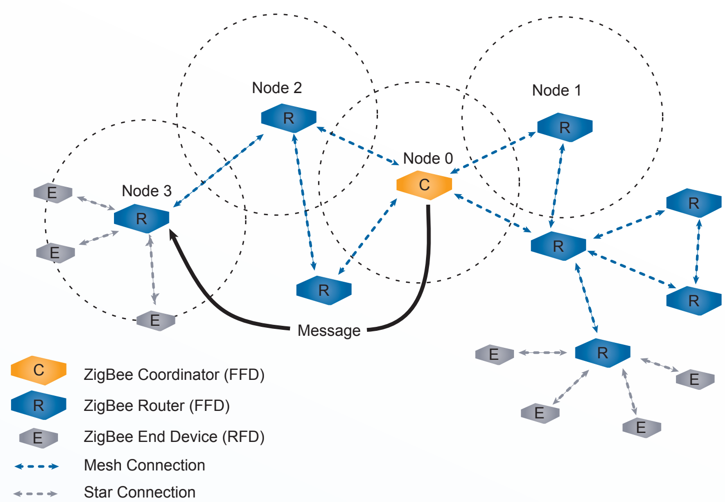
In the following example, Node 0 needs to send a message to Node 3; however, the two are not within communication range of each other. Node 0's neighbors are Node 1 and Node 2.

Since Node 0 cannot directly communicate with Node 3, it sends out a RREQ, which is heard by Nodes 1 and 2.

One of two things will happen when Nodes 1 and 2 receive the RREQ from Node 0:

- If a route is known or if they are the destination radio, they can send a Route Reply (RREP) back to Node 0.
- If they do not know the route and are also not the destination radio, they will rebroadcast the RREQ to their neighbors. The message keeps re-broadcasting until the lifespan (specified by the source radio) expires.

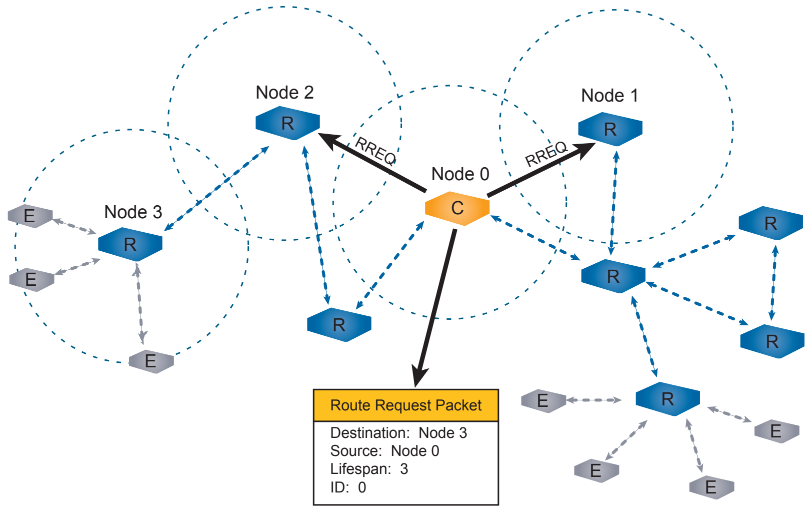
ZigBee AODV



THEORY OF OPERATION

Since Node 0 cannot directly communicate with Node 3, it sends out a RREQ, which is heard by Nodes 1 and 2.

ZigBee Route Request



One of two things will happen when Nodes 1 and 2 receive the RREQ from Node 0:

- If a route is known or if they are the destination radio, they can send a Route Reply (RREP) back to Node 0.
- If they do not know the route and are also not the destination radio, they will rebroadcast the RREQ to their neighbors. The message keeps re-broadcasting until the lifespan (specified by the source radio) expires.

If Node 0 does not receive a reply within a set amount of time, it will re-broadcast the message, this time with a longer lifespan and a new ID number.

In the following example, Node 1 does not have a route to Node 3 and therefore re-broadcasts the RREQ. Node 2, however, does have a route to Node 3. Therefore, Node 2 replies to the RREQ by sending out a RREP. Node 2 also sends a RREP to Node 3 so that it knows the route to Node 0.

COORDINATOR ADDRESSING

Since the Coordinator's NWK address is always 0x0000, it can be addressed using its 16-bit NWK address.

SERIAL INTERFACE

The ZB2430 transceiver module interfaces to the OEM Host via an asynchronous 3.3 V serial UART interface; allowing the module to be easily integrated into any 3.3 V system without requiring any level translation. The module can communicate with any logic and voltage compatible UART; or to any serial device with an additional level translator.

INTERFACE MODES

The ZB2430 has two different types of interface modes:

- Transparent Mode
- API Mode

TRANSPARENT MODE

When operating in Transparent Mode, the ZB2430 can act as a direct serial cable replacement in which received RF data is forwarded over the serial interface and vice versa. Additionally, many parameters can be configured using either AT commands or by toggling the Command/Data pin on the transceiver. In transparent mode, the radio needs to be programmed with the network address of the desired recipient. The destination address can be programmed permanently or on-the-fly.

When Transparent Mode is used, data is stored in the TX buffer until one of the following occurs:

- The RF packet size is reached (EEPROM address 0x5A)
- An Interface Timeout occurs (EEPROM address 0x58)

API MODE

API Mode is a powerful alternative to the default Transparent Mode of the ZB2430 and provides dynamic packet routing and packet accounting abilities to the OEM Host without requiring extensive programming by the OEM Host. API operation utilizes specific packet formats, specifying various vital parameters used to control radio settings and packet routing on a packet-by-packet basis. The API features can be used in any combination that suits the OEM's specific needs and can be different between radios operating on the same network.

API Mode provides an alternative method of configuring modules and message routing at the OEM Host level, without requiring the use of Command Mode. The ZB2430 has three API functions:

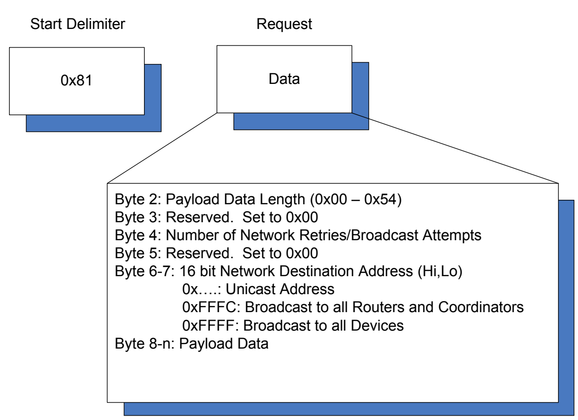
- Transmit API
- API Send Data Complete
- Receive API

API TRANSMIT PACKET

API Transmit Packet is a powerful command that allows the OEM Host to send data to a single or multiple (broadcast) transceivers on a packet-by-packet basis. This can be useful for many applications, including polling and/or mesh networks.

API Transmit Packet is enabled when bit-1 of the API Control byte is enabled. The OEM Host should use the format shown in the following graphic to transmit a packet over the RF.

Transmit API Packet Format



SERIAL INTERFACE

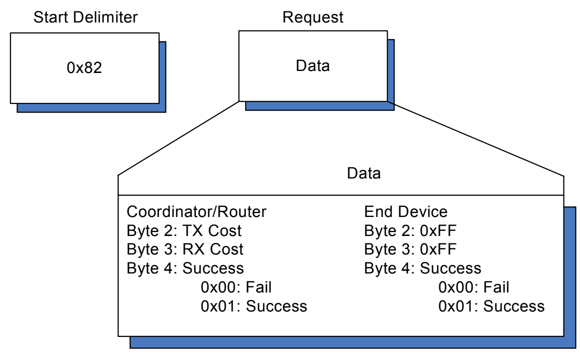
API SEND DATA COMPLETE

API Send Data complete can be used as a software acknowledgement indicator. When a radio sends an addressed packet, it will look for a received acknowledgement (transparent to the OEM Host). If an acknowledgement is not received, the packet will be retransmitted until one is received or all retries have been exhausted.

For applications where data loss is not an option, the OEM Host may wish to monitor the acknowledgement process using the API Send Data Complete. If an acknowledgement is not received (Failure), the OEM Host can send the packet to the transceiver once again. API Send Data Complete is enabled when bit-2 of the API Control byte is enabled. The transceiver sends the OEM Host the data shown in the following graphic upon receiving an RF acknowledge or exhausting all attempts.

NOTE: Send Data Complete may report a failure though the packet arrived due to timing issues. It will never report successful though unless the packet absolutely arrived

Send Data Complete Format

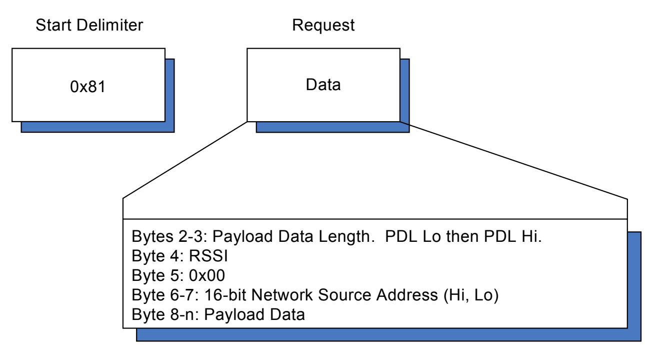


API RECEIVE PACKET

By default, the source MAC is not included in the received data string sent to the OEM Host. For applications where multiple radios are sending data, it may be necessary to determine the origin of a specific data packet. When API Receive Packet is enabled, all packets received by the transceiver will include the unique 24-bit address of the source radio as well as an RSSI indicator, which can be used to determine the link quality between the two.

API Receive Packet is enabled when bit-0 of the API Control byte is enabled. Upon receiving a RF packet, the radio sends its OEM Host the data as shown in the graphic below.

Receive API Packet Format



SERIAL INTERFACE

INTERFACE TIMEOUT

This parameter specifies a maximum byte gap between consecutive bytes. When that byte gap is exceeded, the bytes in the transmit buffer are processed as a complete packet. The Interface Timeout parameter (EEPROM address 0x58), in conjunction with the RF packet size, determines when a buffer of data will be sent out over the RF as a complete RF packet, based on whichever condition occurs first. When sending AT commands the entire command must be received without expiring the Interface Timeout. If the timeout expires the module will attempt to transmit or process the partial data. For this reason the OEM must use a microcontroller or the OEM Configuration Utility Software to configure the radio. Though the radios are accessible with normal terminal emulators, such as HyperTerminal, it is not possible to type AT commands and maintain the restrictions on Interface Timeout and RF Packet Size.

RF PACKET SIZE

RF Packet Size is used in conjunction with Interface Timeout to determine when to delineate incoming data as an entire packet based on whichever condition is met first. When the transceiver receives the number of bytes specified by RF Packet Size (EEPROM address 0x5A) without experiencing a byte gap equal to Interface Timeout, that block of data is processed as a complete packet. Every packet the transceiver sends over the RF contains extra header bytes not counted in the RF Packet Size. Therefore, it is much more efficient to send a few large packets than to send many short packets. In order to ensure AT command can still be issued it is not recommended to use an RF Packet Size of less than 7 bytes (0x07).

PACKET FRAME ENABLE

When Address 0x56, bit 7 is set (Packet Frame Enable), GIO_2 (Pin 4) will transition when data is present on the TX UART. In addition a delay can be added to toggle the pin prior to transmitting the data or to keep the line low after the transmission has ceased. The former can be used to wake a sleeping host when data has been relieved on the RF. The latter can be used similarly to a DE line for RS-485 systems.

- Address 0x46-47: PreTransmit delay. When Address 0x56, bit 7 is set (485 DE/RE), causes a delay to occur after toggling the 485 pin and prior to sending data out the serial port. This delay is 1ms per increment. Set to 0x0000 for no delay.
- Address 0x48-49: PostTransmit delay. Public. When Address 0x56, bit 7 is set (485 DE/RE), causes a delay to occur before toggling Pin 4 and after sending all but the last data byte out the serial port. This delay is 1ms per increment. Set to 0x0000 for no delay.
- Address 0x56, bit 6: 485 Invert. Public. If set, 485 pin will be Low when data is present. If clear, 485 pin will be High when data is present.

FLOW CONTROL

Although flow control is not required for transceiver operation, it is recommended to achieve optimum system performance and to avoid overrunning the serial buffers in the ZB2430. The ZB2430 uses separate buffers for incoming and outgoing data.

SERIAL INTERFACE

RXD DATA BUFFER AND CTS

As data is sent from the OEM Host to the radio over the serial interface, it is stored in the ZB2430's buffer until the radio is ready to transmit the data packet. As discussed previously in "Interface Modes", the radio waits to transmit the data until one of the following conditions occur (whichever occurs first):

- The RF packet size is reached (EEPROM address 0x5B)
- An Interface Timeout occurs (EEPROM address 0x58)

After sending the packet over the RF the data continues to be stored in the buffer until the radio receives an RF Acknowledgement (ACK) from the receiving radio (addressed mode), or all transmit retries/broadcast attempts have been utilized. Once an ACK has been received or all retries/attempts have been exhausted, the current data packet is removed from the buffer and the radio will begin processing the next data packet in the buffer.

To prevent the radio's RXD buffer from being overrun, it is strongly recommended that the OEM Host monitor the radio's CTS output. When the number of bytes in the RXD buffer reaches the value specified by CTS_ON (EEPROM address 0x5C), the radio de-asserts (High) CTS to signal to the OEM Host to stop sending data over the serial interface. CTS is re-asserted after the number of bytes in the RXD buffer is reduced to the value specified by CTS_OFF (EEPROM address 0x5D); signaling to the OEM Host that it may resume sending data to the transceiver.

NOTE: It is recommended that the OEM Host cease all data transmission to the radio while CTS is de-asserted (Low); otherwise potential data loss may occur.

TXD DATA BUFFER

As data to be forwarded to the OEM Host accumulates, it is stored in the ZB2430's outgoing buffer until the radio is ready to begin sending the data to the OEM Host. Once the data packet has been sent to the Host over the serial interface, it will be removed from the buffer and the radio will begin processing the next data packet in the buffer.

The transceiver will send any data to the OEM Host as soon as it has data to send. However, some OEM Hosts are not able to accept data from the transceiver all of the time.

ENGINEER'S TIP: Can a design be implemented using just TXD, RXD, and GND (three-wire interface)?

Yes. However, it is strongly recommended that the base hardware monitor the CTS pin of the radio. CTS is taken High by the radio when its interface buffer is getting full. The base hardware should stop sending at this point to avoid a buffer overrun (and subsequent loss of data).

A successful design can be implemented without monitoring CTS. However, the amount of latency the radio adds to the system, any additional latency caused by Transmit Retries, how often data is sent, non-delivery network timeouts and interface data rate and the size of the packets, must all be taken into account.

Laird Technologies can assist in determining whether CTS is required for a specific application.

ZB2430 ADDRESSING

BROADCAST TRANSMISSIONS

Since ZigBee is targeted for large-scale applications in which all radios may not be in range of a single radio, broadcast packets are retransmitted throughout the network. Broadcast transmissions in ZigBee utilize a passive acknowledgement mechanism. This means that the coordinator and all routers keep track of whether or not their neighbor(s) have relayed the broadcast packet. The packet will re-broadcast until all neighboring devices have received the packet. Any device can initiate a broadcast transmission by programming its destination address with a broadcast address. Subsequent broadcast attempts of the same packet are sent every 500 ms.

BROADCAST LIMITATIONS

Due to the rate-limit delay on broadcast packets where subsequent attempts are only sent at 500 ms intervals, it is possible that a broadcast transmission that is larger than the RF Packet Size could be received out of order. Care should be taken when broadcasting data larger than the RF Packet Size to ensure it is reassembled in the correct order.

Broadcast messages are further rate-limited on the entire network to prevent a broadcast storm from utilizing all available bandwidth. Broadcast messages are limited to 10 broadcast messages every 10 seconds.

Broadcast Addresses

Broadcast Address	Destination Group
0xFFFF	All devices in PAN
0xFFFE	Reserved
0xFFFC	All Routers and Coordinator
0xFFF8 - 0xFFFB	Reserved

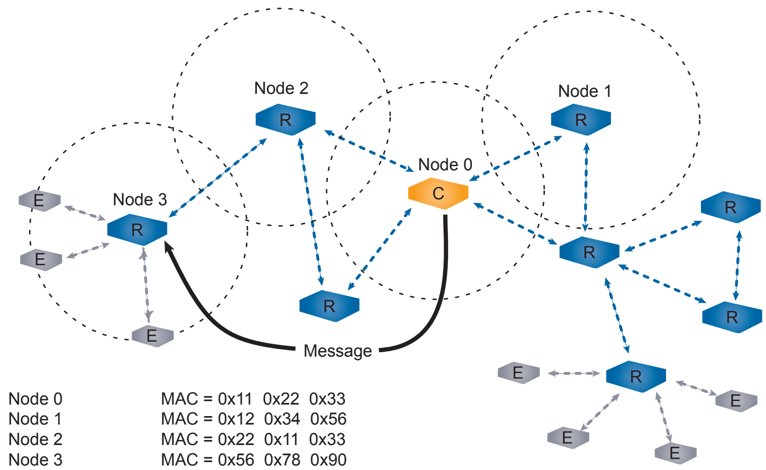
ENGINEER'S TIP: Sending a Broadcast Packet

While ZigBee does provide the means for broadcasting data packets throughout the network, because of the inherent delays associated with broadcast transmissions overall latency may increase, especially with larger networks. Because of the added latency and overall effect on the network, broadcast transmissions within a ZigBee network should be limited.

ZB2430 ADDRESSING

Every ZB2430 transceiver module has a unique static 64-bit MAC address that is programmed at the factory. Upon joining the network, the device is assigned a 16-bit NWK address. The NWK Address for Full Function Devices only changes on initial power-up and when a NV Reset command is issued to the radio. The NWK address for Reduced Function Devices will change if they can no longer communicate with their parent and they are successful finding a new parent. This means for mobile devices, the OEM must manage the radio tables to ensure the network is not overlapping.". The following graphic shows four nodes with the three Least Significant Bytes (LSBs) of each of their MAC addresses.

ZigBee Addressing by MAC - Node 0 to Node 3



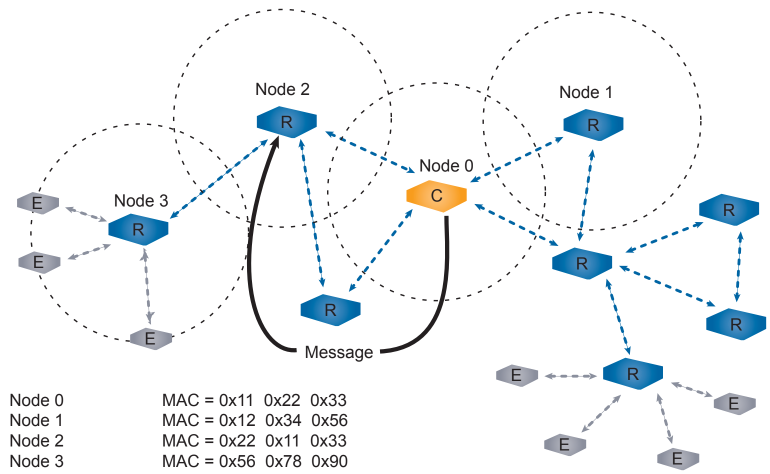
In previous sections (refer to "Mesh Routing (AODV)"), the Ad-Hoc On-Demand Vector routing protocol, Route Requests and Replies were discussed. Fortunately, the routing, RREQs and RREPs are not left up to the OEM Host and are all taken care of by the ZigBee protocol embedded in the ZB2430. A message can therefore be sent to a device anywhere on the network once its 16-bit NWK address is known.

Using the same example as before, assume that Node 0 needs to send a message to Node 3 which is out of Node 0's range. This can be done using the following procedure (note that the underlined values will vary from radio to radio):

1. Enter AT Command Mode →: 0x41 0x54 0x2B 0x2B 0x2B 0x0D
2. Wait for command response ←: 0xCC 0x43 0x4F 0x0D
3. Discover NWK Address →: 0xCC 0x8D 0x56 0x78 0x90
4. Wait for command response ←: 0xCC 0x00 0x01
5. Write 16-bit Destination NWK address →: 0xCC 0x10 0x00 0x00 0x01
6. Wait for command response ←: 0xCC 0x00 0x00 0x01
7. Exit AT Command Mode →: 0xCC 0x41 0x54 0x4F 0x0D
8. Wait for command response ←: 0xCC 0x44 0x41 0x54
9. Send data to device →

ZB2430 ADDRESSING

ZigBee Addressing by MAC - Node 0 to Node 2



Next, assume that Node 1 needs to send a message to Node 2, which is also out of its range. The procedure is the essentially the same as in graphic above. Note that the underlined values will vary from radio to radio.

10. Enter AT Command Mode ←:	0x41 0x54 0x2B 0x2B 0x2B 0x0D
11. Wait for command response →:	0xCC 0x43 0x4F 0x0D
12. Discover NWK Address ←:	0xCC 0x8D 0x22 0x11 0x33
13. Wait for command response →:	0xCC 0x14 0x3E
14. Write 16-bit Destination NWK address ←:	0xCC 0x10 0x00 0x14 0x3E
15. Wait for command response →:	0xCC 0x00 0x14 0x3E
16. Exit AT Command Mode ←:	0xCC 0x41 0x54 0x4F 0x0D
17. Wait for command response →:	0xCC 0x44 0x41 0x54
18. Send data to device ←	

ZB2430 ADDRESSING

SERIAL INTERFACE BAUD RATE

In order for the OEM Host and a transceiver to communicate over the serial interface they need to have the same serial data rate. This value determines the baud rate used for communicating over the serial interface to a transceiver.

For a baud rate to be valid, the calculated baud rate must be within ±3% of the OEM Host baud rate.

Serial Interface Baud Rate

Desired Baud Rate	Baud (0x42)	Minimum Interface Timeout[1] (0x58)	Stop Bit Delay (0x3F)
115200	0x08	0x02	0x02
57600	0x07	0x02	0x02
38400[2]	0x06	0x02	0x02
31250	0x05	0x02	0x02
19200	0x04	0x02	0x02
9600	0x03	0x03	0x03
4800	0x02	0x05	0x05
2400	0x01	0x09	0x09
1200	0x00	0x16	0x16
Non-standard	0xE3	Use equations below	Use equations below

Footnote:
1. Interface timeout = 1 ms per increment
2. Default baud rate

For baud rates other than those shown in the previous table the following equations can be used:

Baud Rate Equations

$$\text{Baud} = \frac{(256 + \text{Baud\_M}) \times (2^{\text{Baud\_E}}) \times \text{Frequency}}{2^{28}}$$

Where:

Frequency = 32 MHz
Baud_M = EEPROM Address 0x43
Baud_E = EEPROM Address 0x44

$$\text{Minimum Interface Timeout required} = \frac{20}{(\text{Baud Rate} \times 1\text{ ms})}$$

$$\text{Stop Bit Delay} = \frac{20}{(\text{Baud Rate} \times 1\text{ ms})}$$

NETWORKING

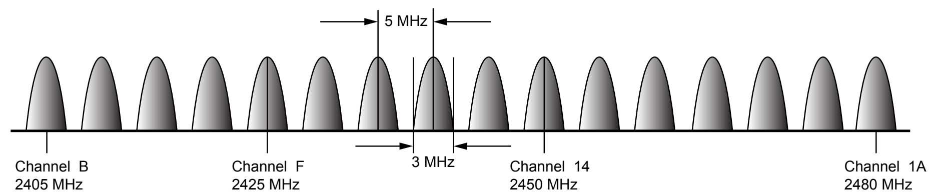
PAN ID

This (EEPROM address 0x79) 16-bit field is similar to a password or network number and helps differentiate collocated networks. A transceiver will not be associated with a network unless it's PAN ID and Channel Number match that of the coordinator. The range is 0x0000 to 0x3FFF.

RF CHANNEL NUMBER

(EEPROM Address 0x40) Channels 0x0B – 0x1A; 5 MHz spacing. The transceiver will operate only on the RF Channel Number specified in the EEPROM.

IEEE 802.14.4 RF Channels



NOTE: The ZB2430 is not approved for use on channel 0x1A and the channel number should therefore be selected accordingly.

RF Channel Number Settings

Radio Model	RF Channel Number Range (0x40)	Frequency Details & Regulatory Requirements	Countries
ZB2430	0x0B – 0x19	2400 – 2465 MHz	Global

CHANNEL SELECT

When enabled in EEPROM (EEPROM address 0x56, bit-3) the coordinator will select a channel permitted by the Channel Mask with the least amount of energy present. The coordinator will start on the first channel and if RF energy is detected or another network is detected, it will change to the next channel. This continues for all the channels and then the clearest channel is selected.

When a router is powered on, it will scan each channel, periodically sending beacons and searching for a parent. When the parent receives a beacon from the router, it sends an acknowledgement to the router, and the router is associated with that parent.

When disabled in EEPROM, the coordinator will use the RF Channel programmed at EEPROM address 0x40 to establish its network.

NETWORKING

CHANNEL MASK

This 32-bit field (EEPROM Address 0x30) specifies the range of allowable channels that the radio can select from when choosing an RF channel. In order for two devices to communicate, a common channel must be selected. At least one channel must be selected (set to 1).

To use the Channel Mask, enable Channel Select (EEPROM Address 0x56, bit 3). When Channel Select is enabled, the radio disregards the Channel specified at EEPROM address 0x40. When Channel Select is disabled, only the Channel specified at EEPROM Address 0x40 will be used.

CHANNEL MASK EXAMPLES:

The example shown in the graphic below enables all 2.4 GHz channels for possible use by selecting 0x07FFF800 as the Channel Mask. The Channel Mask enables you to allow all or to exclude specific channels from selection.

Channel Mask - Allow All Channels

Channel	Reserved	Reserved	Reserved	Reserved	Reserved	2480 MHz	2475 MHz	2470 MHz	2465 MHz	2460 MHz	2455 MHz	2450 MHz	2445 MHz	2440 MHz	2435 MHz	2430 MHz	2425 MHz	2420 MHz	2415 MHz	2410 MHz	2405 MHz	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
32-bit Mask	1F	1E	1D	1C	1B	1A	19	18	17	16	15	14	13	12	11	10	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
Binary	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0

Hex representation: 0 7 F F F 8 0 0

The example in the graphic below shows channels 0x14-0x1A as the only available channels to select from.

Channel Mask - Allow Channels 0x14-0x1A Only

Channel	Reserved	Reserved	Reserved	Reserved	Reserved	2480 MHz	2475 MHz	2470 MHz	2465 MHz	2460 MHz	2455 MHz	2450 MHz	2445 MHz	2440 MHz	2435 MHz	2430 MHz	2425 MHz	2420 MHz	2415 MHz	2410 MHz	2405 MHz	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
32-bit Mask	1F	1E	1D	1C	1B	1A	19	18	17	16	15	14	13	12	11	10	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
Binary	0	0	0	0	0	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Hex representation: 0 7 F 0 0 0 0 0

NETWORKING

Finally the following graphic shows channels 0x0B-0x10 as the only available channels to select from.

Channel Mask - Allow Channels 0x0B-0x10 Only

32-bit Mask	1F	1E	1D	1C	1B	1A	19	18	17	16	15	14	13	12	11	10
Channel	Reserved	Reserved	Reserved	Reserved	Reserved	2480 MHz	2475 MHz	2470 MHz	2465 MHz	2460 MHz	2455 MHz	2450 MHz	2445 MHz	2440 MHz	2435 MHz	2430 MHz
Binary	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Hex representation	0				0				0				1			

32-bit Mask	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0
Channel	2425 MHz	2420 MHz	2415 MHz	2410 MHz	2405 MHz	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved	Reserved
Binary	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0
Hex representation	F				8				0				0			

NOTE: When Channel Select is enabled in EEPROM, the initial network synchronization time will increase. Channel Select is disabled in EEPROM by default. All devices on the network should use the same setting for Channel Select.

POWER DOWN MODES (END DEVICES ONLY)

Power down modes, used only on end devices, allow the ZB2430 to operate at minimum current consumption while not in use. The ZB2430 provides two such modes (end devices only).

- Cyclic Sleep (Wake periodically based on software-controlled timer or pin interrupt)
- Deep Sleep (Wake on pin interrupt)

In order for a module to transition into Sleep Mode, the Sleep_Int pin (pin 12) must be logic High or floating. If this pin is pulled Low, the device will be forced out of Sleep Mode and will not be allowed to sleep until the pin returns to the High state. While in Sleep Mode, the module will not transmit/receive data until after waking up.

Sleep Mode Settings

Sleep Mode	Transition to Sleep	Transition to Wake	Current Draw (mA)
Cyclic Sleep	Automatic transition to Sleep mode after sending Data Request to Parent Device or Sleep_Int is asserted High. End Device wake time can also be configured in the EEPROM (EEPROM address 0x3B).	Automatic transition to Wake mode-occurs after an EEPROM selectable period or manual transition when Sleep_Int is pulled logic Low.	7.6 µA
Deep Sleep	Automatic transition to Sleep mode occurs after device has successfully associated with Network.	Manual transition to Wake mode occurs after Sleep_Int is pulled logic Low.	7.6 µA

NETWORKING

CYCLIC SLEEP

In Cyclic Sleep mode the end device will wake periodically to request data from its parent device. The rate at which the module wakes up to check for data is adjustable in EEPROM (EEPROM address 0x34, 16-bits) in 1 ms increments with a default setting of 1000 ms. The device will wakeup for the period specified by the End Device Wake time (EEPROM address 0x3B), send a data request to its parent, and then return to sleep until the next cycle.

NOTE: Setting the sleep rate to 0x0000 forces the module into Deep Sleep mode (see below).

DEEP SLEEP

Deep sleep mode is a power-down mode in which the ZB2430 automatically transitions to sleep mode after having associated with the Network. While in Deep Sleep Mode, the device will not wake up until interrupted by the Sleep_Int pin. To wake the device out of Deep Sleep Mode, Sleep_Int must be pulled logic Low. The device will return to Deep Sleep Mode after Sleep_Int is returned to the High state.

ENGINEER'S TIP: Transmitting and Receiving Data with a Sleeping End Device

- Data sent to the radio over the UART while it is sleeping will be lost. If the module wakes while receiving data over the UART, it will only see the data received since waking up.
- Incoming RF packets to the module will not keep it awake unless you enable Modify Wake upon RX in EEPROM (EEPROM address 0x45, bit-5).
- When sending data for the module to transmit, it is recommended that the module be forced awake using the Sleep_Int pin until the module is finished transmitting the data.
- The Sleep_Int pin also serves as the TEST or Force Recover pin for the module. If this pin is set low when the module resets the serial interface will be set to 9600-8-N-1 until the module is reset with the pin high.
- While the module is being kept awake using the Sleep_Int pin, it will send data requests to its parent device based on the Wake Poll rate specified in EEPROM (EEPROM address 0x3C) for as long as it is awake.
- A parent will only store data for a sleeping end device for a maximum amount of time specified by the Parent Hold Message EEPROM parameter (EEPROM address 0x39). A parent can hold up to three messages for sleeping End Devices.

SPECIFICATIONS

GENERAL SPECIFICATIONS

The following tables will provide specification information for the ZB2430 transceiver.

General Specifications

Feature	Implementation
Form Factor	Surface mount (SMT)
Antenna	Chip antenna (p/n Laird MAF95029) or U.FL connector
Serial UART Baud Rate	110 bps to 115200 bps. Non-standard baud rates are also supported.
Channels	15 Direct Sequence Channels
Security	Channelization, Network Identification

Footnote:
1. Feature not available at time of this release.

WIRELESS SPECIFICATIONS

The following tables will provide specification information for the ZB2430 transceiver.

Wireless Specifications

Feature	Implementation
Frequency Band	2400 – 2483.5 MHz
Channel Bandwidth	3 MHz
Channel Spacing	5 MHz
RF Data Rate (Raw)	250 kbps
Max Throughput	64 kbps
RF Technology	Direct Sequence Spread Spectrum
Modulation	0-QPSK
Sensitivity (1% PER)	-100 dBm typical
Range, Line of Site (based on 2 dBi gain antenna)	Up to 440 ft. at +2 dBm / Up to 3.5 miles at +20 dBm

DIMENSIONS

ZB2430 Physical Dimensions

Physical Component	Dimension
Length x Width x Height	1.0” x 1.55” x 0.22” (25.4 x 39.4 x 5.5 mm)

ENVIRONMENTAL SPECIFICATIONS

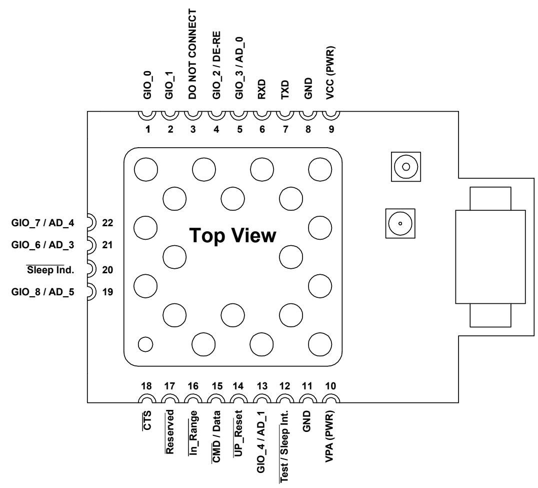
Temperature Restrictions For Operation and Storage

Parameter	Temperature Range
Acceptable Operating Temperature Range	-40°F to 185°F (-40°C to 85°C)
Acceptable Storage Temperature Range	-58°F to 185°F (-50°C to 85°C)

SPECIFICATIONS

PIN DETAILS

Terminal Layout on Module



IMPORTANT: Throughout this manual, some signal names will be shown with an overline. This is done to show that unlike other signals that are active when Low, that this signal is active when High. For example, the Clear To Send (CTS) signal is shown as CTS. This is done to show that when active that signal is High.

ENGINEER'S TIP: Design Notes

- All I/O is 3.3 V TTL.
- All inputs are weakly pulled High (20 k) and may be left floating during normal operation.
- Minimum Connections: VCC, VPA, GND, TXD, and RXD.
- Signal direction is with respect to the transceiver.
- Unused pins should be left disconnected.

SPECIFICATIONS

Pin Details

SMT Pin	Type	Signal Name	Function
1	O	GIO_0	Generic Output Pin
2	O	GIO_1	Generic Output Pin
3		Do not Connect	Has internal connection, for Laird Technologies use only.
4	I	GIO_2	Generic Input pin
5		Do not Connect	Has internal connection, for Laird Technologies use only.
6	I	RXD	Asynchronous serial data input to transceiver
7	O	TXD	Asynchronous serial data output from transceiver
8	GND	GND	Signal Ground
9	PWR	VCC	3.3 - 3.6 V ±50 mV ripple (must be connected)
10	PWR	VPA	3.3 - 3.6 V ±50 mV ripple (must be connected)
11	GND	GND	Signal Ground
12	I	Test / Sleep Int.	"Test Mode – When pulled logic Low and then applying power or resetting, the transceiver's serial interface is forced to a 9600, 8-N-1 rate. To exit Test mode, the transceiver must be reset or power-cycled with Test Mode pulled logic High or disconnected. Note: Because this mode disables some modes of operation, it should NOT be permanently pulled Low during normal operation. Sleep mode interrupt – When logic Low, forces End Device to wake up from sleep mode. When logic High, allows End Device to sleep and wake-up according to specified poll rate. Sleep mode interrupt function available on end devices only."
13		Do not Connect	Has internal connection, for Laird Technologies use only.
14	I	UP_Reset	RESET – Controlled by the ZB2430 for power-on reset if left unconnected. After a stable power-on reset, a logic Low pulse will reset the transceiver.
15	I	CMD/Data	When logic Low, the transceiver interprets OEM Host data as command data. When logic High or floating, the transceiver interprets OEM Host data as transmit data.
16	O	In_Range	When logic Low, the transceiver is associated with a parent and has been assigned a 16-bit network address. The coordinator will report In Range after selecting a clear channel to operate.
17		Do not Connect	Has internal connection, for Laird Technologies use only.
18	O	CTS	Clear to Send – Active Low when the transceiver is ready to accept data for transmission. High when input buffer is filling. Continuing to send data when CTS is high can cause buffer overflow and the loss of data.
19	I/O	GIO_8	Has Internal connection. Reserved for future GPIO.
20	O	Sleep_Ind	Sleep mode indicator. When logic Low, transceiver is in sleep mode. When logic High, transceiver is awake.
21		Do not Connect	Has internal connection, for Laird Technologies use only.
22	I	GIO_7	Has internal connection. Reserved for future GPIO.

Footnote:
1. Feature not implemented at time of this release.

SPECIFICATIONS

ELECTRICAL CHARACTERISTICS

The following tables detail the input and output voltage characteristics of the ZB2430 transceiver module.

Input Voltage Characteristics

Signal Name	Module Pin	High Min.	High Max.	Low Min.	Low Max.	Current Draw
GIO_2	4	Vdd - 0.25V	Vdd	0	0.9V	1 µA
RXD	6	Vdd - 0.25V	Vdd	0	0.9V	1 µA
Test / Sleep Int.	12	Vdd - 0.25V	Vdd	0	0.9V	1 µA
UP_Reset	14	Vdd - 0.25V	Vdd	0	0.9V	1 µA
CMD/Data	15	Vdd - 0.25V	Vdd	0	0.9V	1 µA
GIO_8*	19	Vdd - 0.25V	Vdd	0	0.9V	1 µA
GIO_7	22	Vdd - 0.25V	Vdd	0	0.9V	1 µA

*When configured as input

Output Voltage Characteristics

Signal Name	Module Pin	High Min.	High Max.	Low Min.	Low Max.	Maximum Current Source
GIO_0	1	Vdd - 0.25V	Vdd	0	0.25 V	20 mA
GIO_1	2	Vdd - 0.25V	Vdd	0	0.25 V	20 mA
TXD	7	Vdd - 0.25V	Vdd	0	0.25 V	4 mA
In Range	16	Vdd - 0.25V	Vdd	0	0.25 V	4 mA
CTS	18	Vdd - 0.25V	Vdd	0	0.25 V	4 mA
GIO_8*	19	Vdd - 0.25V	Vdd	0	0.25 V	4 mA
Sleep Ind.	20	Vdd - 0.25V	Vdd	0	0.25 V	4 mA

*When configured as input

PIN DEFINITIONS

Generic I/O

Both GI_n and GO_n pins serve as generic input/output pins. Reading and writing of these pins can be performed on-the-fly using CC Commands.

RXD and TXD

The ZB2430 accepts 3.3 VDC TTL level asynchronous serial data from the OEM Host via the RXD pin. Data is sent from the transceiver, at 3.3 V levels, to the OEM Host via the TXD pin.

Test/Sleep Int.

Test Mode – When pulled logic Low before applying power or resetting, the transceiver's serial interface is forced to 9600, 8-N-1 (8 data bits, No parity, 1 stop bit): regardless of actual EEPROM setting. The interface timeout is also set to 3 ms and the RF packet size is set to the default size of 0x54 (84 bytes). To exit, the transceiver must be reset or power-cycled with Test pin logic High or disconnected.

NOTE: Because this pin disables some modes of operation, it should NOT be permanently pulled Low during normal operation.

Sleep Mode Interrupt – When logic Low, forces end device to wake up from sleep mode. When logic High, allows end device to sleep and wake-up according to specified poll rate. Sleep Mode interrupt function available on end devices only.

SPECIFICATIONS

UP_Reset
UP_Reset provides a direct connection to the reset pin on the microprocessor and is used to force a soft reset. For a valid reset, reset must be asserted Low for an absolute minimum of 250 ns.

CMD/Data
When logic High, the transceiver interprets incoming serial data as transmit data to be sent to other transceivers. When logic Low, the transceiver interprets incoming serial data as command data. When logic Low, data packets from the radio will NOT be transmitted over the RF interface however incoming packets from other radios will still be received.

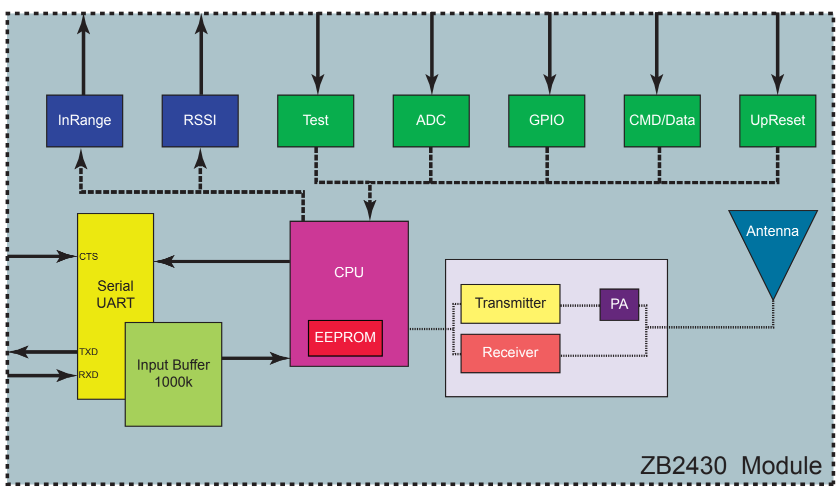
In_Range
The In Range pin will be driven low when the radio is associated with a network. In Range will always be driven low on a Coordinator.

CTS Handshaking
If the transceiver buffer fills up and more bytes are sent to it before the buffer can be emptied, data loss will occur. The transceiver prevents this loss by deasserting CTS High as the buffer fills up and asserting CTS Low as the buffer is emptied. CTS should be monitored by the Host device and when CTS is High, data flow to the radio should be stopped.

Sleep_Ind
Sleep Indicator output. Sleep Ind. can be used to determine whether or not the transceiver is sleeping. When logic Low, the transceiver is in sleep mode. When logic High, the transceiver is awake.

AD In
AD In can be used as a cost savings to replace analog-to-digital converter hardware with the onboard 12-bit ADC. Reading of this pin can be performed locally using the Read ADC command found in the On-the-Fly Control Command Reference, later in this document.

Operational Block Diagram



POWER REQUIREMENTS/CONSUMPTION INFORMATION

Wireless Specifications

Feature	Implementation			
Output Power EIRP (2dBi gain antenna)	'+2 dBm to +20 dBm			
Supply Voltage	3.3 - 3.6 V, ±50 mV ripple			
Current Draw (mA)	100% TX	100% RX	Cyclic Sleep	Deep Sleep
Z100	140 mA	40 mA	7.6 µA	7.6 µA
Z040	70 mA	40 mA	7.6 µA	7.6 µA
NOTE: Power down modes are not supported on Coordinator & Router devices.				

SPECIFICATIONS

EEPROM PARAMETERS

The OEM Host can program various parameters that are stored in EEPROM and become active after a power-on reset. The table below gives the locations and descriptions of the parameters that can be read/written by the OEM Host. Factory default values are also shown. Do not write to any EEPROM addresses other than those listed below. Do not copy one transceiver's EEPROM to another transceiver, as doing so may cause a malfunction in the transceiver.

EEPROM Parameters

Parameter	EEPROM Address	Length (Bytes)	Range	Default	Description
Baud Rate	0x42	1	0x00 - 0x08, 0xE3	0x06	0x00: 1200 0x01: 2400 0x02: 4800 0x03: 9600 0x04: 19200 0x05: 31250 0x06: 38400 0x07: 57600 0x08: 115200 0xE3: Enable Custom Baud rate NOTE: If any value other than 0x00-0x08 or 0xE3 is used, the radio will default to 9600 baud.
Baud_M	0x43	1	0x00 - 0xFF	0xFF	Used to calculate baud rate when Custom Baud Rate is enabled.
Baud_E	0x44	1	0x00-0xFF	0xFF	Used to calculate baud rate when Custom Baud Rate is enabled.
Control 0	0x45	1	0x01 - 0xFF	0x38	Settings are: bit-7: Reserved bit-6: Reserved bit-5: Modify Wake 0 = Disabled 1 = Enabled bit-4: Reload Sleep 0 = Disabled 1 = Enabled bit-3: NV Restore 0 = Disabled 1 = Enabled bit-2: End-to-End Acknowledgement 0 = Disabled 1 = Enabled bit-1: End Device Keep Awake 0 = Disabled 1 = Enabled bit-0: Use CheckSum 0 = Disabled 1 = Enabled NOTE: Added in FW version 2.4-9, CheckSum will increase the reliability of the link. This feature is enabled by default but does not exist in prior FW releases. Enabling this bit will not allow the radios to communicate with previous versions
PreTransmit Delay	0x46	2	0x0000 - 0xFFFF	0x0000	When Packet Frame Enable (0x56 bit 7) is enabled, setting the Pre Transmit Delay will cause the initial TX packet on the UART to be delayed by the value set here. Delay is in 1ms increments. This can be used to wake-up a host before sending data
Post Transmit Delay	0x48	2	0x0000 - 0xFFFF	0x0000	When Packet Frame Enable (0x56 bit 7) is enabled, setting the Post Transmit Delay will cause GIO_2 be stay in the transmit state for the delay set here, similar to DE for RS-485 systems. The delay is in 1ms increments

SPECIFICATIONS

EEPROM Parameters (Continued)

Parameter	EEPROM Address	Length (Bytes)	Range	Default	Description
MAC Retries	0x4B	1	0x00 - 0x07	0x03	Specifies the number of retries to use at the MAC level. A setting of 0x03 actually sends the packet up to 4 times. MAC retries can be set to 0x00, but since they occur faster than the transmit retries, the default setting is typically recommended.
Network Retries	0x4C	1	0x01 - 0x07	0x02	Specifies the maximum number of network retries. When MAC retries is not set to 0x00, the actual amount of transmit attempts is equal to MAC retries x Network Retries. Network Retries occur at a slower rate than MAC retries. Network retries are retries that occur between two connected nodes.
Broadcast Attempts	0x4D	1	0x00 - 0x05	0x04	Specified the maximum number of times to broadcast a packet. Attempts occur at 500ms intervals. There is a limit of 9 broadcast messages every 10 seconds.
End-to-End Retries	0x4E	1	0x00 - 0xFF	0x04	Specified the maximum number of times to retry an end to end packet. End to End Retries are only suitable for multi-hop packets. Attempts occur at 6s intervals.
Stale Limit	0x4F	1	0x01-0xFF	0x32	Specifies amount of time to keep a radio in the Radio Table without having received a packet from that particular radio. Prevents retries from being interpreted as new packets. Adjustable in 100 ms increments.
Control 1	0x56	1	0x01 - 0xFF	0x43	Settings are: bit-7: Packet Frame Enable 0 = Disabled 1 = Enabled bit-6: Packet Frame Invert 0 = Disabled 1 = Enabled bit-5: Reserved bit-4: Auto Destination 0 = Use Destination Address 1 = Use Auto Destination bit-3: Auto Channel 0 = Disabled 1 = Enabled bit-2: Reserved bit-1: Reserved bit-0: Reserved"
Interface Timeout	0x58	1	0x02 - 0xFF	0x04	Specifies a byte gap timeout, used in conjunction with RF packet size to determine when a packet coming over the interface is complete. NOTE: 1 ms per increment.
RF Packet Size	0x5A	2	0x0001 -0x0054	0x0054	Specifies the RF packet size. Note: RF packet size needs to be set to a minimum of six bytes in order to use the Enter AT command.
$\overline{\text{CTS}}$ On	0x5C	2	0x0001 - 0x01C0 Coordinator/ Router: 0x0001 - 0x0416 End Device: 0x0001 - 0x0096	Coordinator/ Router: 0x0190 End Device: 0x50	$\overline{\text{CTS}}$ will be deasserted (High) when the transmit buffer contains at least this many characters

SPECIFICATIONS

EEPROM Parameters (Continued)

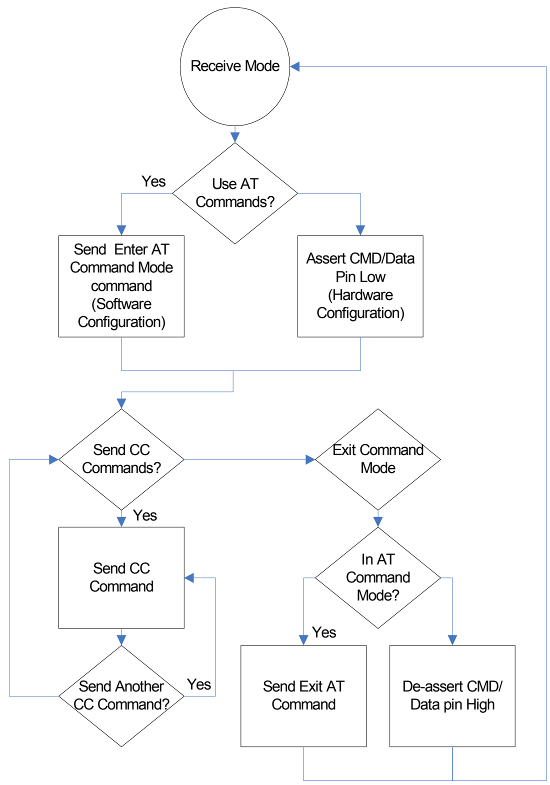
Parameter	EEPROM Address	Length (Bytes)	Range	Default	Description
CTS Off	0x5E	2	0x0001 - 0x01C0 Coordinator/ Router: 0x0001 - 0x0416 End Device: 0x0001 - 0x0096	Coordinator/Router: 0x0180 End Device: 0x50	Once CTS has been deasserted, CTS will be reasserted (Low) when the transmit buffer contains this many or less characters.
Power Control	0x63	1	0x00 - 0x03	0x00	Determines output power of transceiver. Z100S1: 0x00: 17 dBm; 0x01: 11 dBm; 0x02: 5 dBm; 0x03: -1 dBm Z040S1: 0x00: 10 dBm; 0x01: 7 dBm; 0x02: 4 dBm; 0x03: 1 dBm
Destination ID	0x76	2	0x0000 - 0xFFFF	R/E: 0x0000 C: 0x0001	Specifies destination for RF packets.
PAN ID	0x78	2	0x0000 - 0x3FFF	0x0001	Similar to network name. Radios must have the same PAN ID to associate with each other.
MAC ID	0x80	8	0x00 - 0xFF		Factory programmed 8 byte unique IEEE MAC address. NOTE: This address is write protected and cannot be modified.
Part Number	0x90	16	0x00 - 0xFF	—	Provides part number information. EEPROM byte 0x95 can be read to determine device type (C, R, or E).
API Control	0xC1	1	0x00 - 0xFF	0xF8	Settings are: bit-7: Reserved bit-6: Reserved bit-5: Reserved bit-4: Reserved bit-3: Reserved bit-2: API Send Data Complete 0 = Disabled 1 = Enable bit-1: Transmit API 0 = Disabled 1 = Enabled bit-0: Receive API 0 = Disabled 1 = Enabled
RSSI Threshold	0xC8	1	0x00 - 0xFF	—	The minimum RSSI required. Packets received with a weaker RSSI than this threshold will be discarded.
D.O.B.	0xE0	4	—	—	Provides factory calibration and test date.

CONFIGURATION

ENVIRONMENTAL SPECIFICATIONS

The ZB2430 can be configured using the CC Configuration Commands. These commands can be issued using either Hardware or Software Configuration. To use Hardware Configuration, the Command/Data pin of a transceiver must be asserted Low. Software Configuration can be used by entering AT Command Mode before issuing the CC commands.

ZB2430 Configuration Process



AT COMMANDS

The AT Command mode implemented in the ZB2430 creates a virtual version of the Command/Data pin. The "Enter AT Command Mode" command asserts this virtual pin Low (to signify Command Mode) and the "Exit AT Command Mode" command asserts this virtual pin High (to signify Data). Once this pin has been asserted Low, all On-the-Fly CC Commands documented in the manual are supported.

CONFIGURATION

ON-THE-FLY COMMANDS

The ZB2430 transceiver contains static memory that holds many of the parameters that control the transceiver operation. Using the "CC" command set allows many of these parameters to be changed during system operation.

Because the memory these commands affect is static, when the transceiver is reset, these parameters will revert back to the settings stored in the EEPROM.

While in Command mode, the incoming RF interface of the transceiver is active and packets sent from other transceivers will still be received; however no outgoing RF packets will be sent. The transceiver uses Interface Timeout/RF Packet Size to determine when a CC Command is complete. Therefore, there should be no delay between each character as it is sent from the OEM Host to the transceiver or the transceiver will not recognize the command.

When an invalid command is sent, the radio discards the data and no response is sent to the OEM Host. The following table shows a quick summary of the basic configuration and diagnostic commands available on the ZB2430. For detailed command information, please refer to the command descriptions immediately following the Command Quick Reference table.

Command Quick Reference

Command Name	Command (All bytes in Hex)	Return (All bytes in Hex)
Enter AT Command Mode	<0x41> <0x54> <0x2B> <0x2B> <0x2B> <0x0D>	<0xCC> <0x43> <0x4F> <0x4D>
Exit AT Command Mode	<0xCC> <0x41> <0x54> <0x4F> <0x0D>	<0xCC> <0x44> <0x41> <0x54>
Status Request	<0xCC> <0x00> <0x00>	<0xCC> <Firmware> <Status>
Read Channel	<0xCC> <0x02>	<0xCC> <Channel> <Channel Mask [3-0]>
Write Destination NWK Address	<0xCC> <0x10> <0x00> <NWK Hi> <NWK Lo>	<0xCC> <0x00> <NWK Hi> <NWK Lo>
Read Destination NWK Address	<0xCC> <0x11>	<0xCC> <0x00> <NWK Hi> <NWK Lo>
Auto Destination	<0xCC> <0x15> <Data>	<0xCC> <Data>
Read API Control	<0xCC> <0x16>	<0xCC> <API Control>
Write API Control	<0xCC> <0x17> <API Control>	<0xCC> <API Control>
Read Digital Input	<0xCC> <0x20>	<0xCC> <Data>
Read ADC	<0xCC> <0x21> <Data>	<0xCC> <ADC Hi> <ADC Lo>
Write Digital Outputs	<0xCC> <0x23> <Data>	<0xCC> <Data>
Set Max Power	<0xCC> <0x25> <Power>	<0xCC> <Power>
Read IEEE Clone	<0xCC> <0x80>	<0xCC> <0x80> <IEEE7-0>
Write IEEE Clone	<0xCC> <0x81> <IEEE7-0>	<0xCC> <0x81>
Add/Modify Radio Table	<0xCC> <0x85> <Action> <IEEE7-0> <NWK HI> <NWK Low> <NodeRelation>	<0xCC> <0x85>
Remove from Radio Table	<0xCC> <0x86> <Action> <IEEE7-0>	<0xCC> <0x86>
Read NWK Address	<0xCC> <0x8A> <0x00>	<0xCC> <0x8A> <NWK Hi> <NWK Lo>
Read Parent's NWK Address	<0xCC> <0x8A> <0x01>	<0xCC> <0x8A> <NWK Hi> <NWK Lo>
Discover NWK Address	<0xCC> <0x8D> <MAC [2-0]> <Data>	<0xCC> <NWK Hi> <NWK Lo> <Data [n-0]>
Discover IEEE Address	<0xCC> <0x8E> <NWK Hi> <NWK Lo> <Data>	<0xCC> <MAC [7-0]> <Data [n-0]>
Read Temperature	<0xCC> <0xA4>	<0xCC> <Temperature [1-0]>
EEPROM Byte Read	<0xCC> <0xC0> <Start> <Length>	<0xCC> <Start> <Length> <Data [n-0]>
EEPROM Byte Write	<0xCC> <0xC1> <Start> <Length> <Data>	<Start> <Length> <Last byte written>
Soft Reset	<0xCC> <0xFF>	None
Soft Reset with NV reset	<0xCC> <0xFF> <0xE3>	None

CONFIGURATION

COMMAND DESCRIPTIONS

Enter AT Command Mode

Prior to sending this command, the OEM Host must ensure that the transceiver's RF transmit buffer is empty. This can be accomplished by waiting up to one second between the last packet and the AT command. If the buffer is not empty, the radio will interpret the command as data and it will be sent over the RF. The ZB2430 accepts AT-like commands for command and control. The OEM can use the Enter AT Command Mode or the CMD/Data Pin to enter Command Mode. Before entering Command Mode the RX Buffer must be empty. Because a Parent can store messages for sleeping End Devices, it is possible, though unlikely that the RX buffer could take up to 512 times the Parent Hold Message (PHM) Timer to empty. For this reason the OEM should wait until the RX buffer is completely empty before sending AT commands.

Enter AT Command Mode

Command:	**<0x41> <0x54> <0x2B> <0x2B> <0x2B> <0x0D>**
# of bytes returned:	4
Response:	<0xCC> <0x43> <0x4F> <0x4D>

Exit AT Command Mode

The OEM Host should send this command to exit AT Command mode and resume normal operation.

Exit AT Command Mode

Command:	**<0xCC> <0x41> <0x54> <0x4F> <0x0D>**
# of bytes returned:	4
Response:	<0xCC> <0x44> <0x41> <0x54>

Status Version Request

The OEM Host issues this command to request the firmware and link status of the transceiver.

Status Version Request

Command:	**<0xCC> <0x00> <0x00>**
# of bytes returned:	3
Response:	<0xCC> <Firmware> <Type>
Parameter Range: <Firmware> = Radio Firmware version eg: 0x17 = v1.7 <Type> = 0x00: End Device 0x01: Router 0x02: Coordinator 0x03: Initialized - not started automatically 0x04: Initialized - not connected to anything 0x05: Discovering PAN's to join 0x06: Joining a PAN 0x07: Rejoining a PAN (only for End Devices) 0x08: Joined but not yet authenticated 0x09: Started a NWK as ZigBee Coordinator 0x0A: Device has lost info about its parent	

CONFIGURATION

Read Channel

The OEM Host issues this command to read the channel of the transceiver.

Read Channel

Command:	**<0xCC> <0x02>**
# of bytes returned:	6
Response:	<0xCC> <Channel> <ChMask>
Parameter Range: <Channel> = RF Channel currently in use <ChMask> = 32-bit Channel Mask being used	

Write Destination Address

The OEM Host issues this command to the transceiver to change the destination address

Write Destination Address

Command:	**<0xCC> <0x10> <0x00> <NWK Hi> <NWK Lo>**
# of bytes returned:	4
Response:	<0xCC> <0x00> <NWK Hi> <NWK Lo>
Parameter Range: <NWK Hi> = MSB of destination radio's NWK address <NWK Lo> = LSB of destination radio's NWK address	

Read Destination Address

The OEM Host issues this command to the transceiver to read the destination address.

Read Destination Address

Command:	<0xCC> <0x11>
# of bytes returned:	4
Response:	<0xCC> <0x00> <NWK Hi> <NWK Lo>
Parameter Range: <NWK Hi> = MSB of destination radio's NWK address <NWK Lo> = LSB of destination radio's NWK address	

CONFIGURATION

Auto Destination

The Host issues this command to change the Auto Destination setting. When issuing this command, the Auto Destination setting will only be changed if the corresponding enable bit is set. Otherwise, the command performs a read of Auto Destination.

Auto Destination

Command:	**<0xCC> <0x15> <Auto Dest>**
# of bytes returned:	2
Response:	<0xCC> <Auto Dest>

Parameter Range:
<Auto Dest> = bit 7: Ignored
bit 6: Ignored
bit 5: Ignored
bit 4: Read=0, Write =1
bit 3: Ignored
bit 2: Ignored
bit 1: Ignored
bit 0: Auto Destination

Read API Control

The OEM Host issues this command to read the API Control byte.

Read API Control

Command:	**<0xCC> <0x16>**
# of bytes returned:	2
Response:	<0xCC> <API Control>

Parameter Range:
<API Control> = bits 7-3: 0
bit-2: Send Data Complete
bit-1: Transmit API
bit-0: Receive API

CONFIGURATION

Write API Control

The OEM Host issues this command to write the API Control byte to enable or disable the API features.

Write API Control

Command:	**<0xCC> <0x17> <API Control>**
# of bytes returned:	2
Response:	<0xCC> <API Control>
Parameter Range: <API Control> = bits 7-3: Ignored bit-2: Send Data Complete bit-1: Transmit API bit-0: Receive API	

Read Digital Input

The OEM Host issues this command to read the state of GIO input pins. Pins configured as outputs will report their current state.

Read Digital Input

Command:	**<0xCC> <0x20>**
# of bytes returned:	2
Response:	<0xCC> <Digital In>
Parameter Range: <Digital In> = bit-0: GI0	

CONFIGURATION

Read ADC

The OEM Host issues this command to read the onboard 12-bit A/D converters. This command allows a very detailed amount of customization. The OEM Host can select which pin or sensor to monitor, the resolution of the measurement and the reference voltage to measure the input ADC against. Greater resolution will provide a more detailed response, but will introduce additional latency. The following equations can be used to determine the voltages associated with the ADC value returned:

Read ADC Equation

$$\text{ADIn} = \left(\frac{\text{ADC value}}{[\text{RES}]}\right) \times [\text{REFvoltage}]$$

Read ADC

Command:	**<0xCC> <0x21> <Channel> <Resolution> <Ref>**
# of bytes returned:	3
Response:	<0xCC> <Hi ADC> <Lo ADC>

Parameter Range:
<Channel> = 0x00: Cmd/Data
0x01: InRange
0x02: GI03
0x03: GI04
0x04: GI05
0x05: GI06
0x06: GI07
0x07: GI08
0x0D: Positive Voltage Reference = 1.25V
0x0E: Temperature Sensor
0x0F: Vdd
<Resolution> = 0x00: 8 bit resolution [RES=0x00FF]
0x01: 10 bit resoltution[RES=0x03FF]
0x02: 12 bit resolution [RES=0x0FFF]
0x03: 14 bit resolution [RES=0x3FFF]
<Reference> = 0x00: Internal 1.25V [REFvoltage= 1.25V]
0x01: External Reference on GI08
0x02: Vdd
0x03: Differential between pins GI07 and GI08
<Hi ADC> = MSB of requested 12-bit ADC value
<Lo ADC> = LSB of requested 12-bit ADC value

CONFIGURATION

Write Digital Outputs

The OEM Host issues this command to write both digital output lines to particular states. The OEM Host must write the value of all digital outputs at once. Each bit represents a GIO. The first 8 bits are reserved and not in use.

Write Digital Outputs

Command:	**<0xCC> <0x23> <Digital Out[1-0]>**
# of bytes returned:	2
Response:	0xCC <Digital Out [1-0]>
Parameter Range: <Digital Out> = bit-0: GO0 bit-1: GO1 bit-2: GO2 bit-3: GO3 bit-4: GO4 bit-5: GO5 bit-6: GO6 bit-7: GO7 bit-8-15 : Reserved	

Set Max Power

The OEM Host issues this command to adjust the maximum output power.

Set Max Power

Command:	**<0xCC> <0x25> <Max Pwr>**
# of bytes returned:	2
Response:	0xCC <Max Pwr>
Parameter Range: <Max Pwr> = Z100S1: 0x00: 17 dBm, 0x01: 11 dBm, 0x02: 5 dBm, 0x03: -1 dBm Z040S1: 0x00: 10 dBm, 0x01: 7 dBm, 0x02: 4 dBm, 0x03: 1 dBm	

CONFIGURATION

Read IEEE Clone

By default the radio will use the IEEE address in the EEPROM as a unique identifier. This EEPROM Address is burned in at the factory and cannot be changed. As an alternative the radio can use the IEEE Clone feature to use a different unique identifier.

Read IEEE Clone

Command:	**<0xCC> <0x80>**
# of bytes returned:	10
Response:	<0xCC> <0x80> <IEEE7-0>
Parameter Range: <IEEE7-0> = the 64-bit IEEE Address in the MAC Clone field	

Write IEEE Clone

By default the radio will use the IEEE address in the EEPROM as a unique identifier. This EEPROM Address is burned in at the factory and cannot be changed. As an alternative the radio can use the IEEE Clone feature to use a different unique identifier.

Write IEEE Clone

Command:	**<0xCC> <0x81> <IEEE7-0>**
# of bytes returned:	2
Response:	<0xCC> <0x81>
Parameter Range: <IEEE7-0> = the 64-bit IEEE Address in the MAC Clone field	

CONFIGURATION

Add/Modify Radio Table

The Radio table, which contains information about the parents and children of a device is dynamically created, but records are not expunged when elements are removed from the network. In order to maintain an accurate Radio Table, the OEM must occasionally maintain the table be modifying entries. This command is also used by the OEM when a device is being replaced and the IEEE address is being cloned.

Add/Modify Radio Table

Command:	**<0xCC> <0x80>**
# of bytes returned:	10
Response:	<0xCC> <0x80> <IEEE7-0>
Parameter Range: <Action>: 0x00 = RAM Only (will not persist through a reset) 0x01 = NVRAM (will persist through a reset) <IEEE7-0> = the 64-bit IEEE Address in the MAC Clone field <NWK Hi> = MSB of remote radio's NWK address <NWK Lo> = LSB of remote radio's NWK address <Node Relation> = PARENT = 0x00 CHILD_RFD = 0x01 CHILD_RFD_RX_IDLE = 0x02 CHILD_FFD = 0x03 CHILD_FFD_RX_IDLE = 0x04 NEIGHBOR = 0x05 OTHER = 0x06 NOTUSED = 0xFF	

Remove from Radio Table

The Radio table, which contains information about the parents and children of a device is dynamically created, but records are not expunged when elements are removed from the network. In order to maintain an accurate Radio Table, the OEM must occasionally maintain the table be modifying entries. This command is also used by the OEM when a device is being replaced and the IEEE address is being cloned.

Remove from Radio Table

Command:	**<0xCC> <0x86> <Action> <IEEE7-0>**
# of bytes returned:	2
Response:	<0xCC> <0x86>
Parameter Range: <Action>: 0x00 = RAM Only (will not persist through a reset) 0x01 = NVRAM (will persist through a reset) <IEEE7-0> = the 64-bit IEEE Address in the MAC Clone field	

CONFIGURATION

Read 16-bit NWK Address

The OEM Host issues this command to determine the 16-bit NWK address of the device it is connected to.

Read 16-bit NWK Address

Command:	**<0xCC> <0x8A> <0x00>**
# of bytes returned:	4
Response:	<0xCC> <0x8A> <NWK Hi> <NWK Lo>
Parameter Range: <NWK Hi> = MSB of radio's NWK address <NWK Lo> = LSB of radio's NWK address ***Note:*** *If the device has not yet been assigned, a NWK address of 0xFFFF will be returned.*	

Read 16-bit NWK Address of Parent Device

The OEM Host issues this command to determine the 16-bit NWK address of its parent device.

Read 16-bit NWK Address of Parent Device

Command:	**<0xCC> <0x8A> <0x01>**
# of bytes returned:	4
Response:	<0xCC> <0x8A> <NWK Hi> <NWK Lo>
Parameter Range: <NWK Hi> = MSB of Parent's NWK address <NWK Lo> = LSB of Parent's NWK address ***Note:*** *If the device has not yet been assigned, a NWK address of 0xFFFF will be returned.*	

CONFIGURATION

Discover 16-bit NWK Address of Remote Radio

The OEM Host issues this command to discover the 16-bit NWK address of a remote radio.

NOTE: This command is valid only for coordinators and/or router devices. This command will not issue a response if the requested address is unable to be located in the network. A timeout of several seconds should be assumed when using this command.

Discover 16-bit NWK Address of Remote Radio

Command:	**<0xCC> <0x8D> <IEEE [7-0]>**
# of bytes returned:	3
Response:	<0xCC> <NWK Hi> <NWK Lo>
Parameter Range: <IEEE> = 64-bit IEEE Address of remote radio <NWK Hi> = MSB of remote radio's NWK address <NWK Lo> = LSB of remote radio's NWK address	

Discover IEEE Address of Remote Radio

The OEM Host issues this command to discover the 64-bit IEEE address of a remote radio.

NOTE: This command is valid only for coordinators and/or router devices. This command will not issue a response if the requested address is unable to be located in the network. A timeout of several seconds should be assumed when using this command.

Discover IEEE Address of Remote Radio

Command:	**<0xCC> <0x8E> <0x00> <NWK Hi> <NWK Lo>**
# of bytes returned:	9
Response:	<0xCC> <IEEE [7-0]>
Parameter Range: <NWK Hi> = MSB of remote radio's NWK address <NWK Lo> = LSB of remote radio's NWK address <IEEE> = 64-bit IEEE Address of remote radio	

CONFIGURATION

Discover IEEE Address And Children of Remote Radio

The OEM Host issues this command to discover the 64-bit IEEE address of a remote radio as well as report a list of that device's children.

NOTE: This command is valid only for coordinators and/or router devices. This command will not issue a response if the requested address is unable to be located in the network. A timeout of several seconds should be assumed when using this command.

Discover IEEE Address And Children of Remote Radio

Command:	**<0xCC> <0x8E> <0x00> <NWK Hi> <NWK Lo> <0x01>**
# of bytes returned:	10+
Response:	<0xCC> <IEEE [7-0]> <Length> <List>
Parameter Range: <NWK Hi> = MSB of remote radio's NWK address <NWK Lo> = LSB of remote radio's NWK address <IEEE> = 64-bit IEEE Address of remote radio <Length> = Length of data to follow <List> = List of remote radio's associated devices [<Index n> <NWK Hi n> <NWK Lo n>]	

Read Temperature

The OEM Host issues this command to read the onboard temperature sensor.

NOTE: The temperature sensor is not calibrated and has a tolerance of ±3°C. For calibration instructions, contact Laird Technology's technical support.

Read Temperature

Command:	**<0xCC> <0xA4>**
# of bytes returned:	3
Response:	0xCC <+/-> <Temp.>
Parameter Range: <+/-> = 0x2B: + 0x2D: - <Temp.> = Temperature (Celsius) (0x08 - 0x50)	

CONFIGURATION

Read Voltage

The OEM Hosts issues this command to read the input voltage to the radio.

Read Voltage

Command:	**<0xCC> <0xC0> <0xA6>**
# of bytes returned:	2
Response:	<0xCC> <Voltage Integer> <Voltage Decimal>
Parameter Range: <Voltage Integer> = Integer portion of voltage reading <Voltage Decimal> = Decimal portion of voltage reading	
Example Output: 0xCC 0x03 0x37 <0x03> = Integer portion is 3 V <0x37> = decimal portion is .55 V Voltage level is 3.55 V	

EEPROM Byte Read

Upon receiving this command, a transceiver will respond with the desired data from the addresses requested by the OEM Host.

EEPROM Byte Read

Command:	**<0xCC> <0xC0> <Start> <Length>**
# of bytes returned:	4+
Response:	<0xCC> <Start> <Length> <Data>
Parameter Range: <Start> = EEPROM address to begin reading at <Length> = Length of data to be read <Data> = Requested data	

CONFIGURATION

EEPROM Byte Write

Upon receiving this command, a transceiver will write the data bytes to the specified address but will not respond to the OEM Host until the EEPROM write cycle is complete.

NOTE: The maximum length of data that can be written in a single write process is 0x50. If writing the entire 256-byte EEPROM, it is convenient to perform 64 byte (0x40) writes.

EEPROM Byte Write

Command:	**<0xCC> <0xC1> <Start> <Length> <Data>**
# of bytes returned:	3
Response:	<Start> <Length> <Last byte>
Parameter Range: <Start> = EEPROM address to begin writing at <Length> = Length of data to be written (Max = 0x50) <Data> = Data to be written <Last byte> = Value of last byte written	

Reset

Upon receiving this command, a transceiver will write the data bytes to the specified address but will not respond to the OEM Host until the EEPROM write cycle is complete.

Reset

Command:	**<0xCC> <0xFF>**
# of bytes returned:	0
Response:	None

CONFIGURATION

Soft Reset With NV Reset

The OEM Host issues this command to perform a soft reset of the transceiver and to erase the network settings stored in the radio's NV RAM. Any transceiver settings modified by CC commands will revert to the values stored in the EEPROM.

Soft Reset With NV Reset

Command:	**<0xCC> <0xFF> <0xE3>**
# of bytes returned:	0
Response:	None

ADVANCED NETWORK COMMANDS

Some applications may require a more extensive knowledge of the Network and its current configuration. For this reason, the ZB2430 includes several advanced commands which can be issued anytime the radio is in Command mode. Each of these commands include a 16-bit Return Mask which allows the OEM Host to select the information returned in the command response.

NOTE: All unused bits in the Return Mask should be set to "0".

Read Neighbor Table

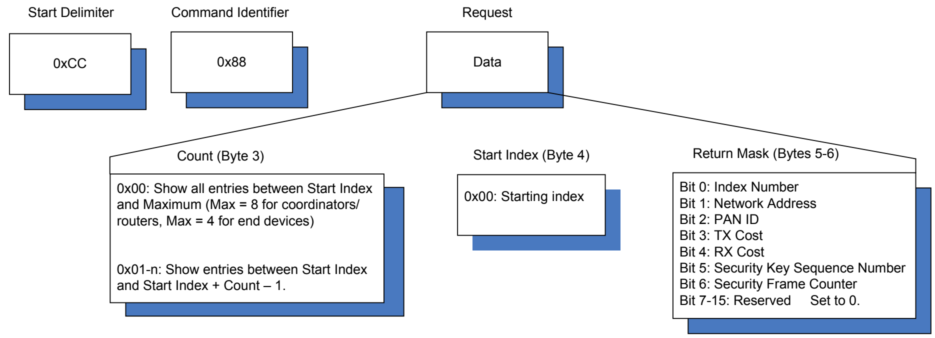
The Neighbor Table is stored in NV RAM. The table stores information about neighboring devices which are operating with the same Channel Mask, but not necessarily the same channel. The command format is shown in the following graphic.

COMMAND DEFINITIONS

- Start Index: Starting index within the Neighbor Table to begin reporting.
- Count: Number of entries to include in the Neighbor Table. Maximum number of indexes = 8 (Coordinator and Routers) and 4 (End Devices).
- Index Number: Index location of radio in Route Table.
- NWK Address: 16-bit NWK address of the neighboring device.
- PAN ID: The 16-bit PAN ID of the network to which the device belongs.
- TX Cost: Counter of transmission (success/failures)
- RX Cost: Average of received RSSI values for the specified device

CONFIGURATION

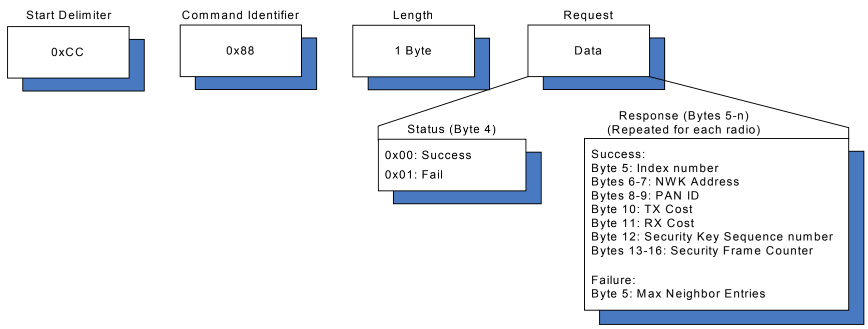
Read Neighbor Table



After issuing the Read Neighbor Table command, the radio will respond with the requested information as shown in the following graphic. The actual command response format may vary depending on the Return Mask setting used in the command.

NOTE: Command will only fail if more than the maximum number of neighbors is requested

Read Neighbor Table Response



CONFIGURATION

Read Route Table

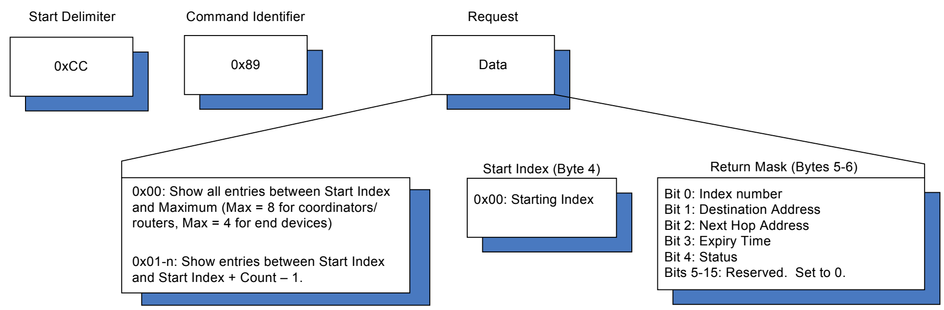
ZigBee coordinators and routers maintain a routing table in memory which is used to establish a route to a particular destination device.

NOTE: This command is not valid for end devices.

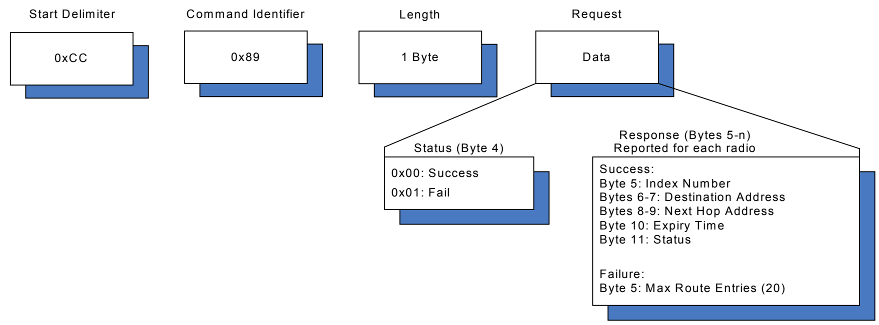
COMMAND DEFINITIONS

- Count: Number of entries to include in Route Table. Maximum number of indexes = 20
- Start Index: Starting index within the Route Table to begin reporting.
- Index Number: Index location of radio in Route Table.
- Destination Address: The 16-bit NWK address of the route.
- Next Hop Address: The 16-bit NWK address of the next radio on the way to the destination.
- Expiry Time: A countdown timer indicating the number of seconds until route expires. Expiry Time is set to 0x1E (30 s) when a new route is created.
- Status: The status of the route.
- Command will fail if the maximum requested entries is greater than 20

Read Route Table



Read Route Table Response



CONFIGURATION

Perform Scan

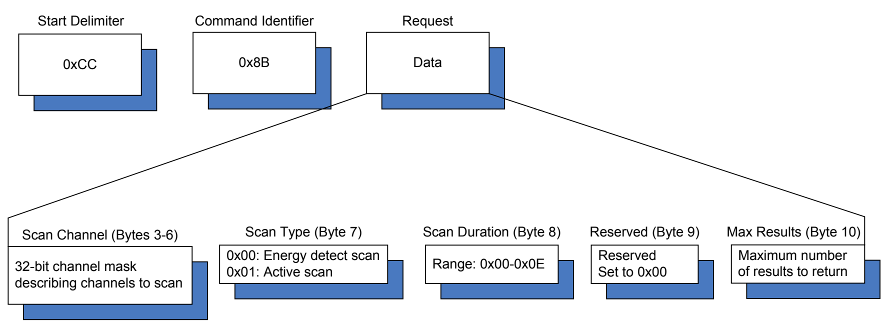
ZigBee coordinators and routers can manually scan selected channels for RF activity and other ZigBee devices/PAN IDs, etc.

NOTE: This command is not valid for end devices.

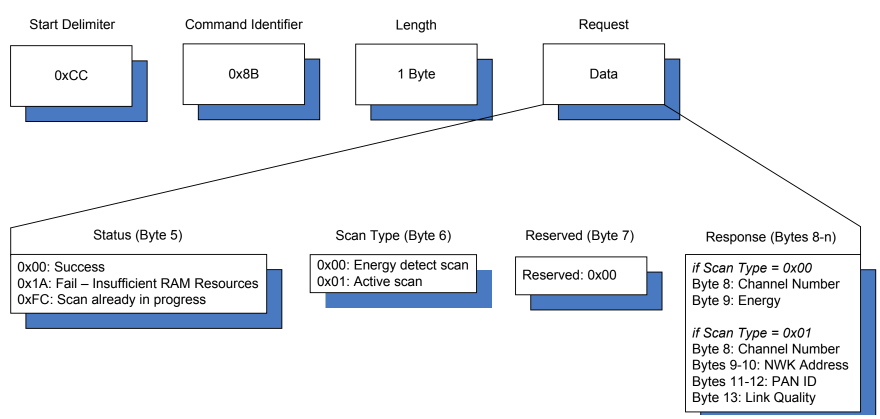
COMMAND DEFINITIONS

- Scan Channel: A 32-bit channel mask specifying the channel(s) to include in the scan.
- Scan Type: Specifies the type of scan to perform. Energy scan, the device will tune to each channel and perform an energy measurement. Active scan, the device tunes to each channel, sends a beacon request and listen for beacons from other ZigBee devices.
- Scan Duration: Duration of the Active and Energy scans on each channel selected. Time is measured as: (15.36 ms) x 2^(Scan Duration + 1)
- Max Results: The maximum number of results to report for Active scans. Ignored with Energy scan command.
- Status: Indicates the status of the current scan.
- Channel Number: 8-bit channel current measurement was taken from.
- Energy: The strength of the RF channel during the Energy scan.
- NWK Address: 16-bit NWK address of the neighboring device.
- PAN ID: The 16-bit PAN ID of the network to which the device belongs.
- Link Quality: The strength of the link between the current device and the device found during the Active scan

Perform Scan



Perform Scan Response



CONFIGURATION

Read Radio Table

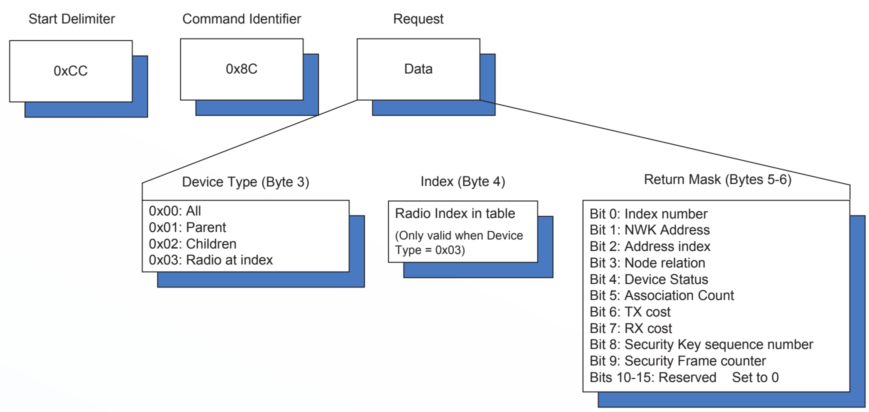
The Radio Table, stored in NV RAM, contains information about any parent or children it is associated with. The Radio Table stores relationship and link-state information which updates overtime the radio receives a packet from that device. To read a device's Radio Table, use the command format shown in the following graphic.

NOTE: This command is not valid for end devices.

COMMAND DEFINITIONS

- Index Number: Index location of radio in Radio Table (range = 0-20).
- NWK Address: 16-bit NWK address of the device.
- Node Relation: The type/relation of the device.
- Device Status: Status of the link between the two devices.
- TX Cost: Counter of transmission (success/failures). Failures are incremented on fail and decremented on success. Range is 0x00 - 0x07.
- RX Cost: Average of received RSSI values for the specified device

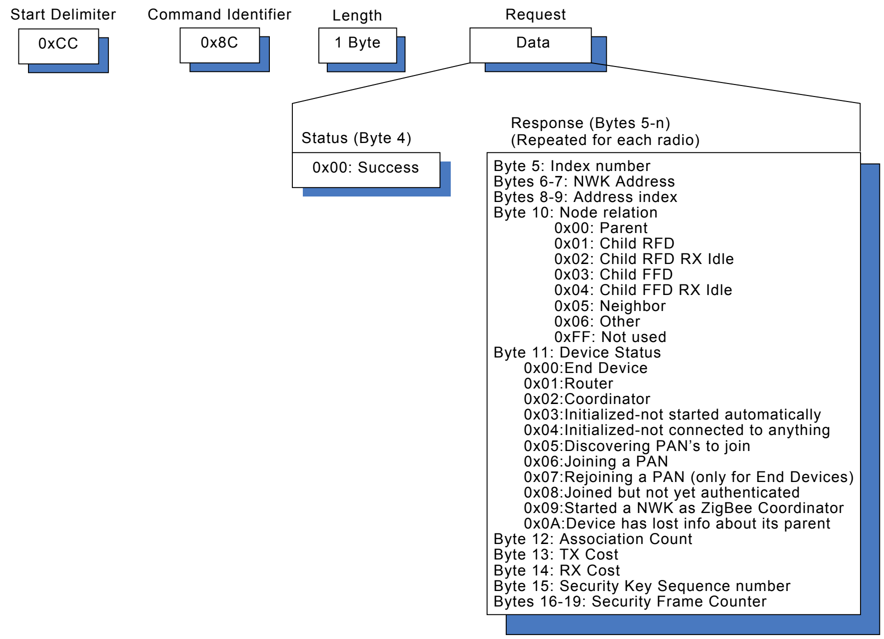
Read Radio Table



CONFIGURATION

After issuing the Read Radio Table command, the radio will respond with the requested information as shown in the following graphic. The actual command response format may vary depending on the Return Mask setting used in the command.

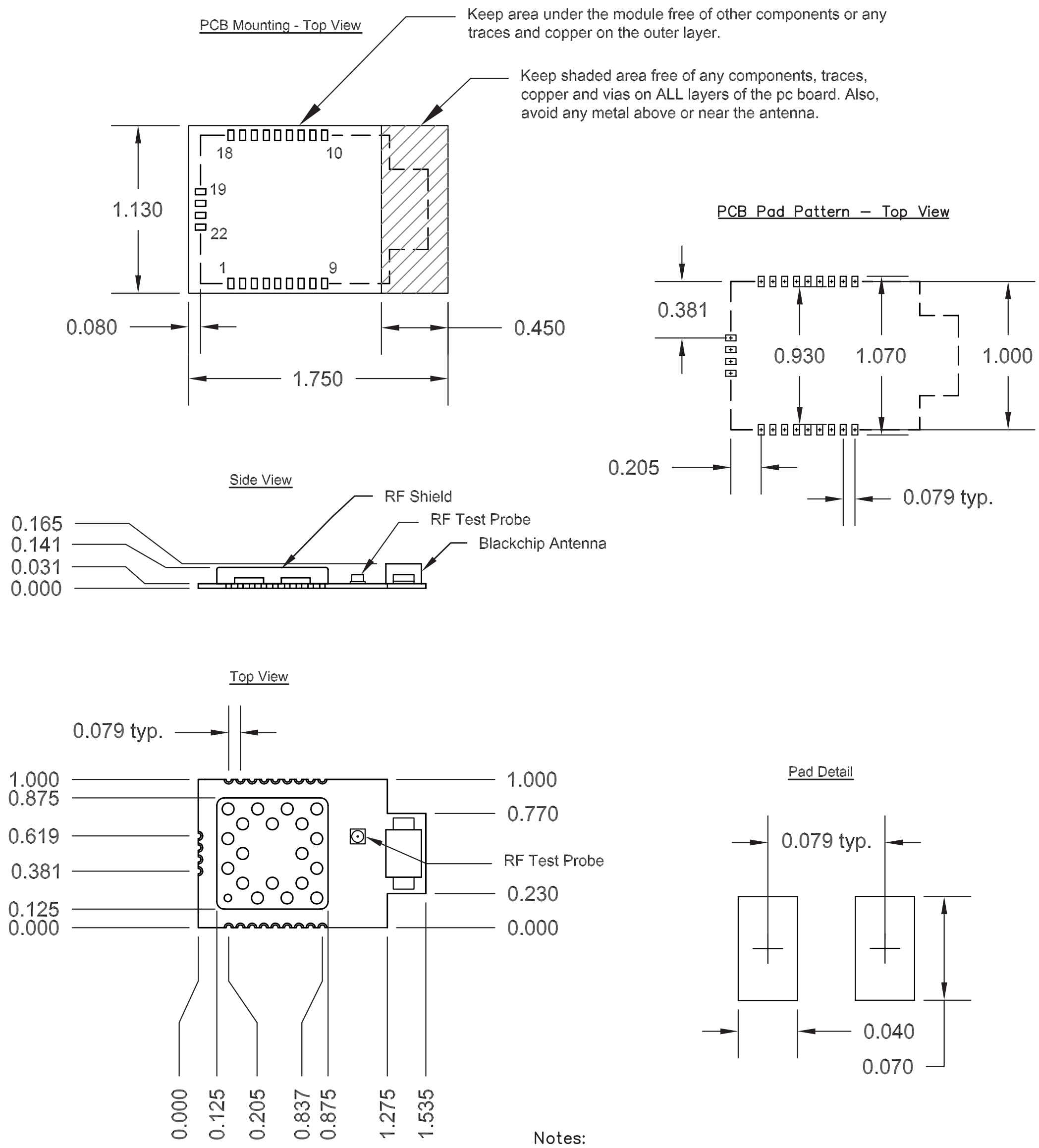
Read Radio Table Response



Beginning in version 2.1, the OEM now has the ability to edit the radio table of Coordinators and Routers. This will allow the OEM to manually remove units from the radio table which are no longer in the network and to recreate the radio table of a device for a field replacement.

DIMENSIONS

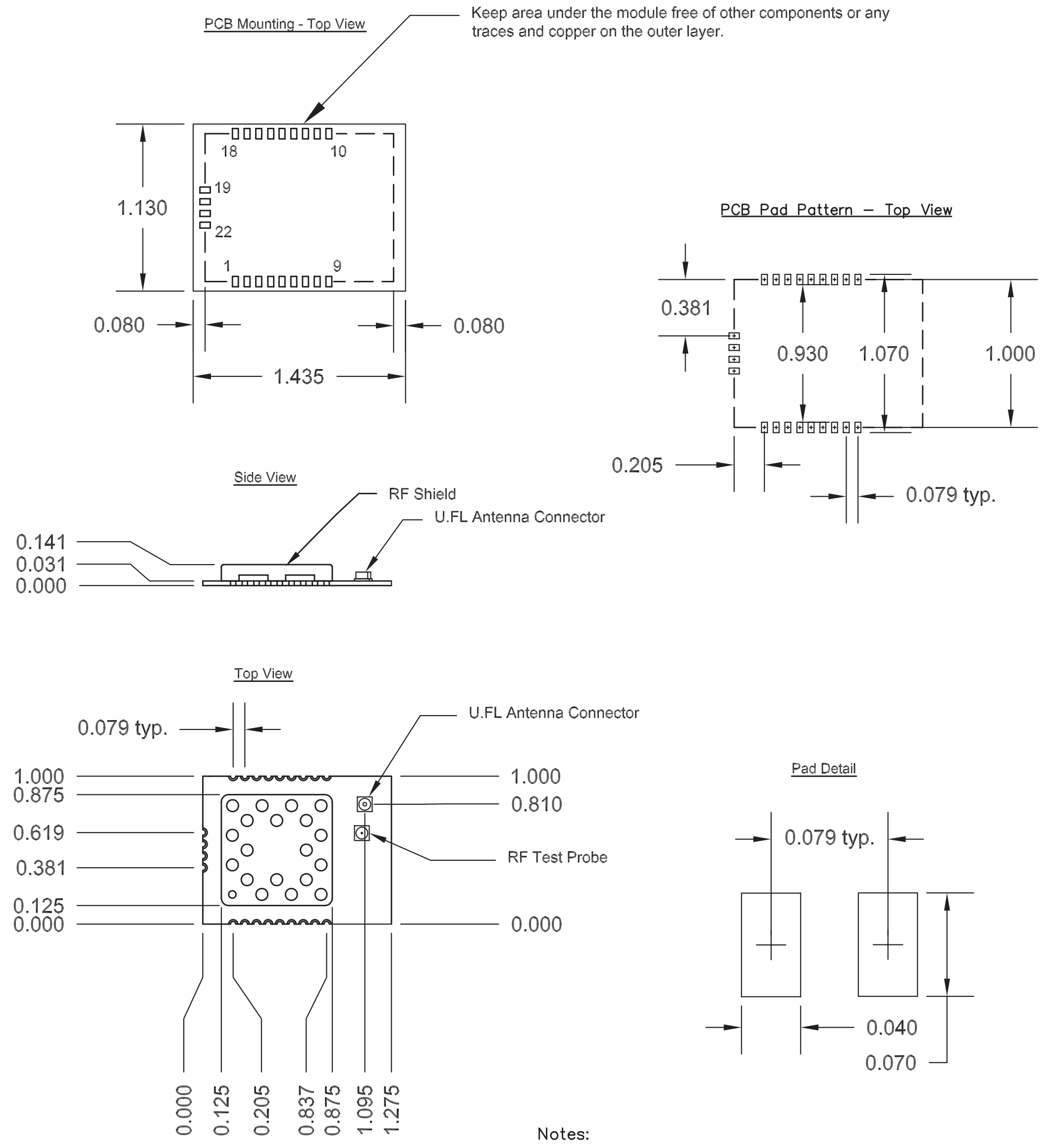
MECHANICAL DRAWING



Notes:
- All dimensions are +/– .005 inches
- PC Board Material is 0.031 thick FR4
- Board edge connections are 0.031 plated holes
- Not to exceed 260 degrees C during soldering

DIMENSIONS

MECHANICAL DRAWING



Notes:
- All dimensions are +/– .005 inches
- PC Board Material is 0.031 thick FR4
- Board edge connections are 0.031 plated holes
- Not to exceed 265 degrees C during soldering

COMPLIANCY INFORMATION

AGENCY IDENTIFICATION NUMBERS

Agency compliancy is a very important requirement for any product development. Laird Technologies has obtained modular approval for its ZB2430 product family so that the OEM only needs to meet a few requirements to use that approval. The corresponding agency identification numbers and approved antennas are listed in the following table:

Agency Identifcation Numbers

Part Number	US/FCC	CANADA/IC	ETSI
ZB2430-100	KQL-ZB2430-100	2268C-ZB2430	N/A
Z100S1 Family	KQL-Z100S1XFX	2286C-Z100S1XF	N/A
Z040S1 Family	KQL-Z100S1XFX	2286C-Z100S1XF	Approved

APPROVED ANTENNA LIST

This device has been designed to operate with the antennas listed below, and having a maximum gain of 5dB. Antennas not included in this list or having a gain of greater than 5dB are strictly prohibited for use with this device. The required antenna impedance is 50 Ohms.

Approved Antenna List

Laird Technologies Part Number	Manufacturer Part Number	Manufacturer*	Type	Gain (dBi)	ZB2430-100	Z100S1 Family	Z040S1 Family
–	FR05-S1-N-o-001	Fractus	Integral Chip	2	X	-	-
0600-00039	S151FC-L-(132)PX-2450S	Nearson	Omni	5	X	X	-
-	WIC2450-A	Laird/Centurion	Chip	2	-	X	X

*When configured as input

FCC/IC REQUIREMENTS FOR MODULAR APPROVAL

In general, there are two agency classifications of wireless applications; portable and mobile.

Portable
Portable is a classification of equipment where the user, in general, will be within 20 cm of the transmitting antenna. Portable equipment is further broken down into two classes; within 2.5 cm of human contact and beyond 2.5 cm

NOTE: Ankles, feet, wrists, and hands are permitted to be within 2.5 cm of the antenna even if the equipment is designated as being greater than 2.5 cm.

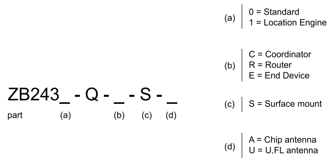
The ZB2430 is not agency approved for portable applications. The OEM is required to have additional testing performed to receive this classification. Contact Laird Technologies for more details.

Mobile
Mobile defines equipment where the user will be 20 cm or greater from the transmitting equipment. The antenna must be mounted in such a way that it cannot be moved closer to the user with respect to the equipment, although the equipment may be moved.

NOTE: Ankles, feet, wrists, and hands are permitted to be within 20 cm of mobile equipment.

COMPLIANCY INFORMATION

OEM EQUIPMENT LABELING REQUIREMENTS



WARNING! The OEM must ensure that FCC labeling requirements are met. This includes a clearly visible label on the outside of the OEM enclosure specifying the appropriate Laird Technologies FCC identifier for this product as well as the FCC notice below. The FCC identifiers are listed above.

An example of the label text:

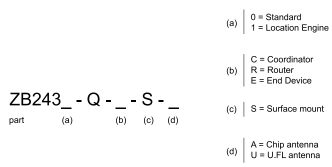
Contains FCC ID: KQL-ZB2430-100 / KQL-ZB2430D / KQL-Z100S1XFX

The enclosed device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

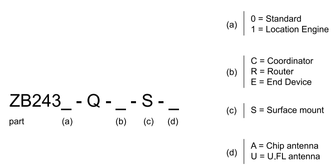
Label and text information should be in a size of type large enough to be readily legible, consistent with the dimensions of the equipment and the label. However, the type size for the text is not required to be larger than eight point.

ANTENNA REQUIREMENTS

To reduce potential radio interference to other users, the antenna type and its gain should be chosen so that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication.

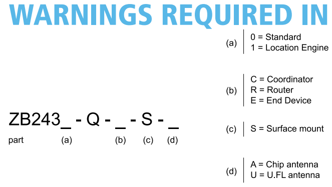


WARNING! This device has been tested with a U.FL connector with the above listed antennas. When integrated into the OEM's product, these fixed antennas require professional installation preventing end-users from replacing them with non-approved antennas. Any antenna not listed in the above table must be tested to comply with FCC Section 15.203 for unique antenna connectors and Section 15.247 for emissions. Contact Laird Technologies for assistance.



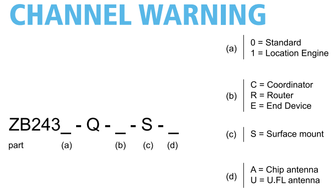
CAUTION! This device has been tested with a U.FL connector with the above listed antennas. When integrated into the OEM's product, these fixed antennas require professional installation preventing end-users from replacing them with non-approved antennas. Any antenna not listed in the above table must be tested to comply with FCC Section 15.203 for unique antenna connectors and Section 15.247 for emissions. Contact Laird Technologies for assistance.

WARNINGS REQUIRED IN OEM MANUALS



WARNING! This equipment has been approved for mobile applications where the equipment should be used at distances greater than 20 cm from the human body (with the exception of hands, feet, wrists, and ankles). Operation at distances of less than 20 cm is strictly prohibited and requires additional SAR testing.

CHANNEL WARNING



WARNING! This equipment has been approved for mobile applications where the equipment should be used at distances greater than 20 cm from the human body (with the exception of hands, feet, wrists, and ankles). Operation at distances of less than 20 cm is strictly prohibited and requires additional SAR testing.

ORDERING INFORMATION

To order one or more ZB2430 transceivers, contact Laird Technologies at 1.800.492.2320.

PRODUCT PART NUMBERS

Coordinator	Z100S1*FC
Router	Z100S1*FR
End Device	Z100S1*FE
Commissioner	Z100S1*FM
Coordinator	Z040S1*FC
Router	Z040S1*FR
End Device	Z040S1*FE
Commissioner	Z040S1*FM

* = A for integrated antenna; U for u.FL connector (external antenna)

SYSTEM DEVELOPMENT KIT (SDK)

To configure the ZB2430, the engineer will require the use of the Laird Technologies OEM ZB2430EZ family System Developer Kit (SDK). The EZ-SDK is designed to allow flexibility at the hardware interface level so that the EZ-SDK can easily be interfaced to the OEM product, to a PC for performance testing, or to any other device that will support RS232 or USB serial interfaces.

PRODUCT PART NUMBERS

Development Kit – External antenna SDK-Z100S1UF
Development Kit - Integrated antenna SDK-Z100S1AF
Development Kit – External antenna, CE SDK-Z040S1UF
Development Kit - Integrated antenna, CE SDK-Z040S1AF
Development Kit – External antenna OAD SDK-Z100S1UF-M
Development Kit - Integrated antenna OAD SDK-Z100S1AF-M
Development Kit – External antenna, CE, OAD SDK-Z040S1UF-M
Development Kit - Integrated antenna, CE, OAD SDK-Z040S1AF-M
Development Kits include one Coordinator module, two router modules and two end devices.

global solutions: **local** support ™

Americas: +1.800.492.2320
Europe: +44.1628.858.940
Asia: +852.2268.6567

wirelessinfo@lairdtech.com
www.lairdtech.com/wireless

GLOSSARY

Term	Definition
ADC	Analog-to-Digital Converter
Ad-hoc network	A wireless network composed of communicating devices without preexisting infrastructure. Typically created in a spontaneous manner and is self-organizing and self-maintaining.
API mode	An optional method of operating. This mode provides dynamic packet routing and packet account abilities to the OEM Host without requiring extensive programming by the OEM Host.
Association	The process of joining a ZigBee PAN. A device joins the Network by joining a Coordinator or Router which has previously associated with the Network. Upon joining, the Parent device issues a 16-bit Network Address to the device.
Broadcast	Broadcast packets are sent to multiple radios. The ZB2430 allows several different broadcast types including broadcast to all devices & broadcast to Coordinator & all Routers.
Broadcast jitter	The random delay which is automatically introduced by a device before relaying a broadcast packet to prevent packet collisions.
Channel	The frequency selected for data communications within the PAN. The channel is selected by the Network Coordinator on power-up.
Channel mask	The Channel Mask is a 32-bit field which specifies the range of allowable channels that the radio has to select from when choosing an RF channel. Valid only when Channel Select mode is enabled in EEPROM.
Clear channel assessment	An evaluation of the communication channel prior to a transmission to determine if the channel is currently occupied.
Coordinator	Responsible for establishing the operating channel and PAN ID for the entire Network. Once the Coordinator has established a Network, it allows Routers and End Devices to join the Network; assigning each device a unique 16-bit Network Address.
CTS	Clear To Send. The line drawn over the three letters is used to indicate that unlike most of the other signals, this signal is active when it is High.
DAC	Digital-to-Analog Converter
Destination address	This is the physical address of the device that a message is sent to.
EEPROM	Electronically Erasable Programmable Read-Only Memory
End device	A device that is located at the outer edges of the network. These devices are typically connected to some type of sensing or control device.
Energy scan	A sweep of the entire frequency band which reports noise readings on every channel & is also capable of detecting Coordinators and reporting their Channel location.
FFD	Full Function Device. The Network Coordinator & Routers are examples of FFD's.
Flow control	An optional feature that is used to achieve optimum system performance and to prevent overrunning the ZB2430's serial buffers.
GND	Ground
IEEE 802.15.4	IEEE standard for Low-Power Wireless Personal Area Networks (WPAN's). Specifies the physical interface between ZigBee devices.

GLOSSARY

Term	Definition
Latency	The amount of time delay between the moment an event is initiated and the moment that the effects of that event are detected.
Lifespan	The number of times that a message may be re-broadcast, if the broadcasting device does not know the route and is also not the destination.
MAC address	A unique 64-bit address assigned to each radio. This address cannot be modified and never changes. It is used by the network to identify the device when assigning 16-bit Network Addresses.
Maximum network depth	The maximum number or Routers (hops) that a device can be away from the Coordinator. The current profile limit is 5.
Maximum number of routers	The total number of children that can serve as Routers for a Network device. The current profile limit is 6.
Maximum number of children	The total number of children that can be associated with a single Network device. The current profile limit is 20; comprising of up to 6 Routers and 14 End Devices.
Mesh network	An interconnection of nodes where nodes are permitted to transmit data directly to any other node.
Multi-hop routing	Used to send information from one point to another point in a network, when the two points do not have a direct connection. i.e., if device A needs to send information to device G, it may require the message be transferred through devices C and E.
Neighbor table	A table used by the Coordinator and Router(s) to keep track of other devices operating in the same coverage area.
Network address	A unique 16-bit address assigned to a device upon joining a PAN. Used for routing messages between devices. Can be different each time a device is powered on. The address of the Coordinator is always 0x0000. Addresses are not assigned in numerical order.
Node	An electronic device that is attached to a network that is capable of sending, receiving and forwarding information over the network.
NV RAM	Non-volatile random access memory
NWK address	Network address
Operating channel	The specific frequency selected for data communications. The operating channel is determined by the Coordinator on power-up.
Orphan device	A device which has lost communication contact with or information about its Parent device.
Z040S1 Family	KQL-Z100S1XFX