Chipsmall
深圳市津利帝科技有限公司
Geelead Technology Limited
Chipsmall
采购部

ZB2430

TRANSCEIVER

AEROCOMM'S MOTTO OF "INSTANT WIRELESS" EXPRESSES OUR COMMITMENT TO FACILITATING FAST AND EASY RF INTEGRATION. OUR COMPREHENSIVE DEVELOPMENT TOOLS AND ENGINEERING SUPPORT HELP OEMS ACCELERATE TIME-TO-MARKET.

USER MANUAL

VERSION 2.0

AEROCOMM

Technical Support:	Phone: 800.492.2320
	E-mail: wireless.support@lairdtech.com
	Web: www.aerocomm.com/
Sales:	Phone: 800.492.2320
	E-mail: wireless.sales@lairdtech.com
	Web: www.aerocomm.com

Document Information

This material is preliminary

Information furnished by AeroComm in this specification is believed to be accurate. Devices sold by AeroComm are covered by the warranty and patent indemnification provisions appearing in its Terms of Sale only. AeroComm makes no warranty, express, statutory, and implied or by description, regarding the information set forth herein. AeroComm reserves the right to change specifications at any time and without notice.

AeroComm's 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, AeroComm warrants the OEM transceiver against defects in materials and workmanship. AeroComm 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 AeroComm authorized technician.

This warranty does not cover and AeroComm will not be liable for, any damage or failure caused by misuse, abuse, acts of God, accidents, electrical irregularity, or other causes beyond AeroComm's control, or claim by other than the original purchaser.

In no event shall AeroComm 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 AeroComm, 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, AeroComm determines that there is a defect, AeroComm 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	Description
Version 1.0	7/21/06 - Initial Release Version
Version 1.1	7/25/06 - Updated Pin definitions, corrected status request command to display 0x00 as firmware version, updated CC 08, CC 21 and EEPROM byte write commands. Corrected PAN ID EEPROM address to address 0x78. Updated Future Enhancements section.
Version 1.2	9/15/06 - Changed Reset to active Low. Changed pin 20 to Sleep pin and is active Low. Added second mechanical drawing.
Version 1.3	1/18/07 - Corrected Read Temperature command.
Version 1.4	7/6/07 - Internal Release.
Version 1.5	7/17/07 - Added pinout for pluggable module.
Version 1.6	8/24/07 - Added API command set. Added Neighbor, Route, & Radio Table commands. Added Energy scan command. Added NV with soft reset command. Added static network parameters information. Updated Broadcast section. Updated Serial Interface section. Updated Channel Mask section. Added power-down modes. Corrected status request response. Added MAC retries to EEPROM parameter list.
Version 1.7	Corrected Read Channel Command (was CC 02 00; changed to CC 02)
Version 1.8	12/17/07 - Updated Compliancy Information. Added approval for ZB2430-D. Updated Approved Antenna List.
Version 1.9	1/4/08 - Added new EEPROM parameters for firmware version 1.6 - End Device poll rate, Parent Hold Message, End Device Wake Time, End Device Wake Poll rate, Stop Bit Delay, Modify Wake upon RX, Reload Sleep, NV Restore enable/disable, & RS485 DE/RE.
Version 2.0	3/1/08- Updated ZB2430 Features, Updated Current Draw for High Power module, Updated RF Packet Size in RX Data Buffer and CTS, Updated Read Digital Input, Updated Read ADC, Updated Write Digital Output, Removed Discover 16-bit NWK Address command, Added Read Voltage cmd, Added Restore Default cmd, Added End-to-End Retries to EEPROM Parameters Table, Updated CTS On/Off Thresholds, Updated Read Neighbor Table Command

Contents

ZB2430 Transceiver Module

AeroComm's ZB2430 module is based on the IEEE 802.15.4 wireless communication standard and the robust ZigBee networking protocol and is one of the most powerful ZigBee compliant solutions on the market today. The ZB2430 provides OEMs with industry leading 2.4 GHz module performance in low power consumption, easy integration, long range, and superior features and functionality. Requiring no additional FCC licensing in the Americas, OEMs can easily make existing systems wireless with little or no RF expertise.

ZB2430 Features

- Mesh architecture
- Energy harvester compatible
- 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°C to 80°C)
- Advanced configuration available using AT commands
- Easy to use Configuration & Test Utility software

Overview

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

To boost data integrity and security, the ZB2430 uses DSSS technology featuring optional Advanced-Encryption Standards (AES)[1]. 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 an AeroComm 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.”

[1] Feature not available at the time of this release.

SPECIFICATIONS

Table 1: ZB2430 Specifications

<table>
<tr><th colspan="2">General</th></tr>
<tr><td>Interface Connector</td><td>SMT or Pluggable</td></tr>
<tr><td>Antenna</td><td>Chip antenna (p/n Laird MAF95029) or U.FL connector</td></tr>
<tr><td>Serial Interface Data Rate</td><td>Baud rates from 110 bps to 115,200 bps. Non-standard baud rates are also supported.</td></tr>
<tr><td>Channels</td><td>ZB2430-D: 15 Direct Sequence Channels
ZB2430-Q: 15 Direct Sequence Channels</td></tr>
<tr><td>Security</td><td>Channelization, Network Identification and optional 128-bit AES encryption[1]</td></tr>
<tr><th colspan="2">Transceiver</th></tr>
<tr><td>Frequency Band</td><td>2400 - 2483.5 MHz</td></tr>
<tr><td>Channel Bandwidth</td><td>3 MHz</td></tr>
<tr><td>Channel Spacing</td><td>5 MHz</td></tr>
<tr><td>RF Data Rate (Raw)</td><td>250 kbps</td></tr>
<tr><td>Max Throughput</td><td>64kbps</td></tr>
<tr><td>RF Technology</td><td>Direct Sequence Spread Spectrum</td></tr>
<tr><td>Modulation</td><td>0-QPSK</td></tr>
<tr><td>Output Power EIRP (2dBi gain antenna)</td><td>ZB2430-D: -12 dBm to +5 dBm
ZB2430-Q : +2 dBm to +20 dBm</td></tr>
<tr><td>Supply Voltage</td><td>3.0 - 3.5V, ±50mV ripple</td></tr>
<tr><td>Current Draw (mA)

Note: Power down modes are not supported on Coordinator & Router devices.</td><td>
<table>
<tr><th></th><th>100% TX</th><th>100% RX</th><th>Cyclic Sleep</th><th>Deep Sleep</th></tr>
<tr><td>ZB2430-D:</td><td>25 mA</td><td>27 mA</td><td>0.5 uA</td><td>0.5 uA</td></tr>
<tr><td>ZB2430-Q:</td><td>140 mA</td><td>44 mA</td><td>7.6 uA</td><td>7.6 uA</td></tr>
</table>
</td></tr>
<tr><td>Sensitivity (1% PER)</td><td>ZB2430-D:-90 dBm typical
ZB2430-Q:-100 dBm typical</td></tr>
<tr><td>Range, Line of Site (based on 2dBi gain antenna)</td><td>ZB2430-D: Up to 440 ft.
ZB2430-Q: Up to 440 ft. at +2 dBm / Up to 3.5 miles at +20 dBm</td></tr>
<tr><th colspan="2">Environmental</th></tr>
<tr><td>Temperature (Operating)</td><td>-40°C to 85°C</td></tr>
<tr><td>Temperature (Storage)</td><td>-50°C to +85°C</td></tr>
<tr><th colspan="2">Physical</th></tr>
<tr><td>Dimensions</td><td>1.0” x 1.35” x 0.22” (25.4 x 34.3 x 5.5 mm)</td></tr>
<tr><td></td><td></td></tr>
</table>

Table 1: ZB2430 Specifications

Certifications	
FCC Part 15.247	ZB2430-D: KQL-ZB2430D ZB2430-Q:KQL-ZB2430-100
Industry Canada (IC)	ZB2430-D: 2268C-ZB2430D ZB2430-Q:2268C-ZB2430
CE	ZB2430-D:Approved ZB2430-Q:Pending

[1] Feature not available at the time of this release.

PIN DEFINITIONS

The ZB2430 has a simple interface that allows OEM Host communications with the transceiver. Table 2 below shows the connector pin numbers and associated functions.

Table 2: Pin Definitions for the ZB2430 transceiver

SMT Pin	Pluggable Pin	Type	Signal Name	Function
1	4	O	GIO_0	Generic Output Pin
2	6	O	GIO_1	Generic Output Pin
3	8		Do not Connect	Has internal connection, for Aerocomm use only.
4	7	I	GI0_2/ DE-RE	Generic Input pin
5	19	I	GIO_3 / AD_0	Has Internal connection. Reserved for future GPIO.
6	3	I	RXD	Asynchronous serial data input to transceiver
7	2	O	TXD	Asynchronous serial data output from transceiver
8	10	GND	GND	Signal Ground
9	1	PWR	VCC	3.0 - 3.5 V ±50mV ripple (must be connected)
10	-	PWR	VPA	3.0 - 3.5 V ±50mV ripple (must be connected)[1]
11	-	GND	GND	Signal Ground
12	9	I	$\overline{\text{Test / Sleep Int.}}$	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	18	I/O	GIO_4 / AD_1	Has Internal connection. Reserved for future GPIO.
14	5	I	$\overline{\text{UP\_Reset}}$	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	11	I	$\overline{\text{CMD}}$/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	20	O	$\overline{\text{In Range}}$	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	16	I	$\overline{\text{RTS}}$	Request to Send – When enabled in EEPROM, the OEM Host can take this High when it is not ready to accept data from the transceiver. NOTE: Keeping $\overline{\text{RTS}}$ High for too long can cause data loss due to buffer overflow.[2]

Table 2: Pin Definitions for the ZB2430 transceiver

SMT Pin	Pluggable Pin	Type	Signal Name	Function
18	12	O	$\overline{\text{CTS}}$	Clear to Send - Active Low when the transceiver is ready to accept data for transmission. High when input buffer is filling. Contining to send data when CTS is high can cause buffer overflow and the loss of data.
19	14	I/O	GIO_8 / AD_5	Has Internal connection. Reserved for future GPIO.
20	13	O	$\overline{\text{Sleep Ind.}}$	Sleep mode indicator. When logic Low, transceiver is in sleep mode. When logic High, transceiver is awake.
21	17	I/O	GIO_6 / AD_3	Has Internal connection. Reserved for future GPIO.
22	15	I	GIO_7 / AD_4	Has Internal connection. Reserved for future GPIO.

1. May be left disconnected on ZB2430-D devices.
2. Feature not implemented at time of release.

ENGINEER'S TIP

Design Notes:

- All I/O is 3.3V TTL.
- All inputs are weakly pulled High (20k) and may be left floating during normal operation. When implemented, $\overline{\text{RTS}}$ will be weakly pulled Low.
- Minimum Connections: VCC, VPA, GND, TXD, & RXD.
- Signal direction is with respect to the transceiver.
- Unused pins should be left disconnected.

3

HARDWARE INTERFACE

PIN DEFINITIONS

Generic I/O

Both GIn and GOn 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 3.3V 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.**

UP_Reset

UP_Reset provides a direct connection to the reset pin on the ZB2430 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.

Command/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.

RTS Handshaking*

With RTS mode disabled, the transceiver will send any received data to the OEM Host as soon as it is received. However, some OEM Hosts are not able to accept data from the transceiver all of the time. With RTS enabled, the OEM Host can prevent the transceiver from sending it data by de-asserting RTS (High). Once RTS is re-asserted (Low), the transceiver will send packets to the OEM Host as they are received.

Note: Leaving $\overline{\text{RTS}}$ de-asserted for too long can cause data loss once the transceiver's receive buffer reaches capacity.

*Feature not implemented at time of release.

$\overline{\text{CTS}}$ 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 $\overline{\text{CTS}}$ High as the buffer fills up and asserting $\overline{\text{CTS}}$ Low as the buffer is emptied. $\overline{\text{CTS}}$ should be monitored by the Host device and data flow to the radio should be stopped when $\overline{\text{CTS}}$ is High.

$\overline{\text{Sleep Ind.}}$

Sleep Indicator output. $\overline{\text{Sleep Ind.}}$ 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.

TERMS & DEFINITIONS 4

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.

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.

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.

IEEE 802.15.4: IEEE standard for Low-Power Wireless Personal Area Networks (WPAN’s). Specifies the physical interface between ZigBee devices.

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.

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: The unique 16-bit address assigned to a device upon joining a PAN. This address is used for routing messages between devices and can be different each time a device is powered on. The Network Coordinator will always have a Network Address of 0x0000. Note that addresses are not assigned in numerical order.

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.

PAN: Personal Area Network. Includes a Network Coordinator and one or more Routers/End Devices. The Network formation is determined by the Maximum Network Depth, Maximum Number of Routers, and Maximum Number of Children.

PAN ID: Similar to a Network ID. Devices which are operating with different PAN ID's will not be associated to the same network.

Parent/Child: When a device joins the Network, it becomes a child of the device with which it is associated. Similarly, the device with which it associated becomes its parent device. Network devices can have multiple children, but only one parent. End Devices cannot be parents and are always children of the Coordinator or a Router. The Coordinator does not have a parent device.

POS: Personal Operating Space. The area within reception range of a specific device.

Profile: A collection of device descriptions, which together form a coorperative application. Devices utilizing different profiles will only support very basic inter-communications. The ZB2430 uses a private profile as specified by Aerocomm.

RFD: Reduced Function Device. The End Device is an example of an RFD.

Route Discovery: An operation using RREQ and RREP's in which a ZigBee Coordinator or Router discovers a route to a device outside its POS.

Route Reply (RREP): A ZigBee command used to reply to a Route Request command.

Route Request (RREQ): A ZigBee command used to discover paths through the network over which messages may be relayed.

Routing Table: A table in which the Coordinator or Router(s) store information required to participate in the routing of data packets throughout the network. The entire route is not stored, only the first step in the route.

Star Network: A network employing a single, central device through which all communication between devices must pass.

TX Cost: A counter of transmission successes/failures. TX Cost starts at 0x00, increments by one every time a packet fails to be delivered, and decrements by one every time a packet is successfully delivered. TX Cost has a range between 0x00 and 0x04.

Unicast: Unicast packets contain a destination address and are received by a single radio only. Unicast packets are point-to-point and do not include Broadcast packets.

ZigBee Stack: A Network specification based on the IEEE 802.15.4 Standard for Wireless Personal Area Networks (WPANs). The ZB2430 uses the Z-Stack (designed by TI) v.1.4.2 and complies to the ZigBee 2006 specification.

ZigBee Alliance: An association of companies working together to create a low-cost, low power consumption, two-way wireless communications standard (http://www.zigbee.org).

THEORY OF OPERATION 5

IEEE 802.15.4 & ZIGBEE OVERVIEW

The ZB2430 uses the ZigBee protocol stack, a network layer protocol which uses small, low power digital transceivers based on the IEEE 802.15.4 hardware standard. The 802.15.4 standard is a specification for a cost-effective, low data rate (<250 kbps), 2.4 GHz or 868/928 MHz wireless technology designed for personal-area and device-to-device wireless networking.

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 Reduced Function 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 netowork address dynamically assigned by parent

End Device

While Coordinators and Routers can communicate with any device type, End Devices can communicate only through their parent device. 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.

- 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 asssigned by parent

CREATING A NETWORK

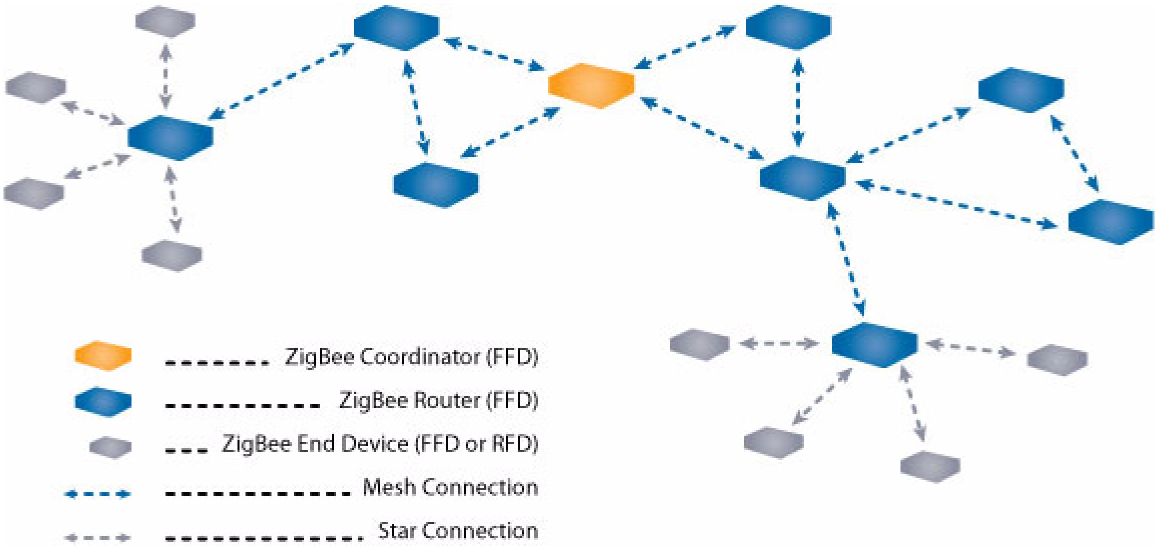
The IEEE 802.15.4 MAC provides support for two wireless network topologies: star and mesh. The management of these networks is performed by the ZigBee layer. All devices, regardless of topology, participate in the network using their unique 16-bit address assigned by the Coordinator.

Mesh

The mesh topology allows any Full Function Device (Coordinator or Router) to communicate directly with any other device within its range and to have messages relayed to devices which are out of range via multi-hop routing of messages. While a FFD device can communicate with a Reduced Function Device (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.

Figure 1 shows a typical ZigBee network architecture.

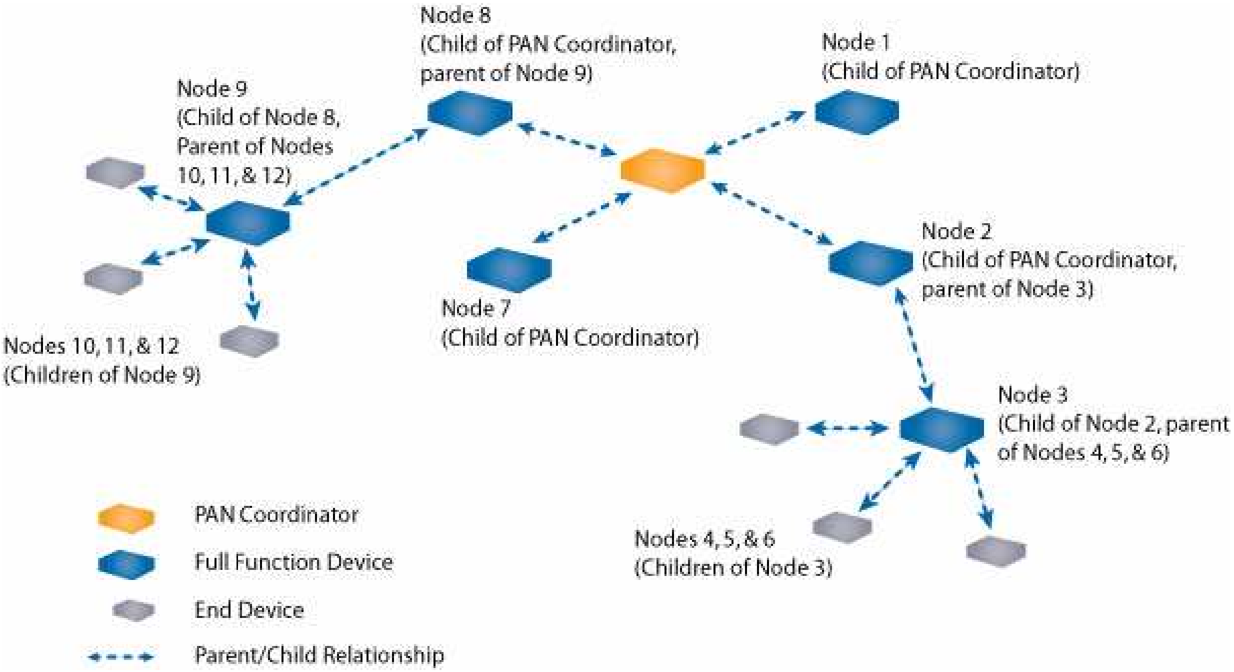
Figure 1: ZigBee Network Topologies



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 a new device (Router or End Device) associates with the Coordinator, it becomes a child of the Coordinator and similarly, the Coordinator becomes a parent of that device. If a second device joins the network, the Coordinator will once again become the parent and the device will become a child of the Coordinator. 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.

Figure 2: Parent/Child Relationship



NETWORK LIMITATIONS

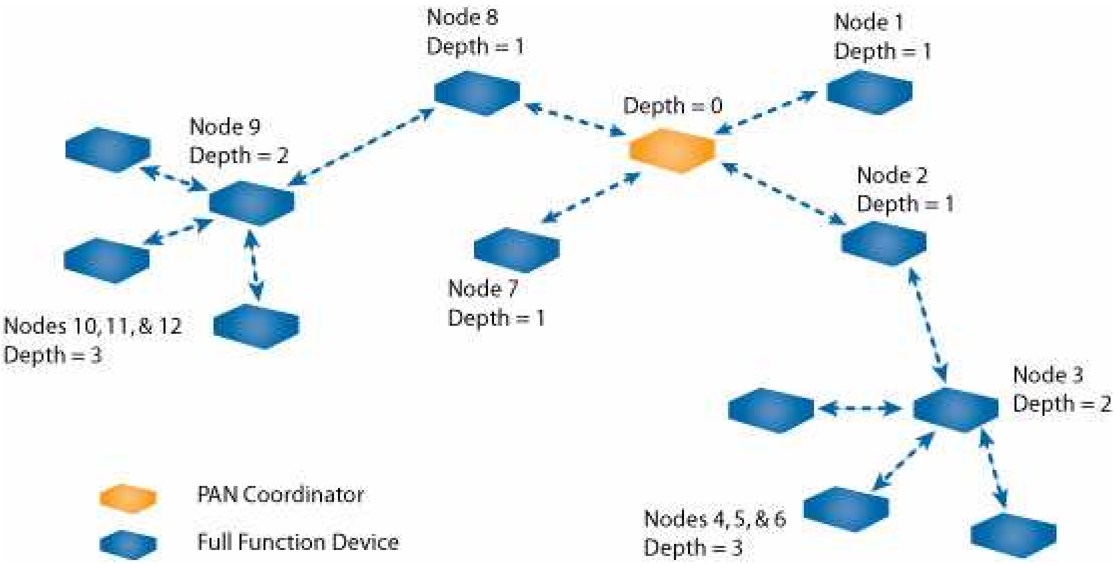
The ZigBee network structure and ultimate size are specified by Stack profiles. The Stack profiles define the maximum number of Layers, maximum number of Children per Parent, & maximum number of Routers that can be Children. These parameters are set during code compilation and cannot be altered after compilation. The ZB2430 uses the restricitions specified by the Home Lighting & 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 (see Figure 3: "Network Depth" on page 15).

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 & Controls profile limits the maximum network depth to 5.

Figure 3: Network Depth



Maximum Number of Children per Parent

The 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.

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 Network 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 Addresses.
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 to 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 MAC 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 transceivers have the same OUI of 0x00 0x00 0x00 0x50 0x67 which can be used to distinguish Aerocomm devices on a network but cannot be used to route packets throughout the network.

When a packet needs to be sent to a specific device through the network, the 16-bit network address **must** be used. 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 (see Table 3 below). 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.

Table 3: Device Table Example

Index	MAC Address (64-bit)	NWK Address (16-bit)
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

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.

Figure 4 below 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 example below, 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 (see Figure 5: "ZigBee Route Request" on page 17).

Figure 4: ZigBee AODV

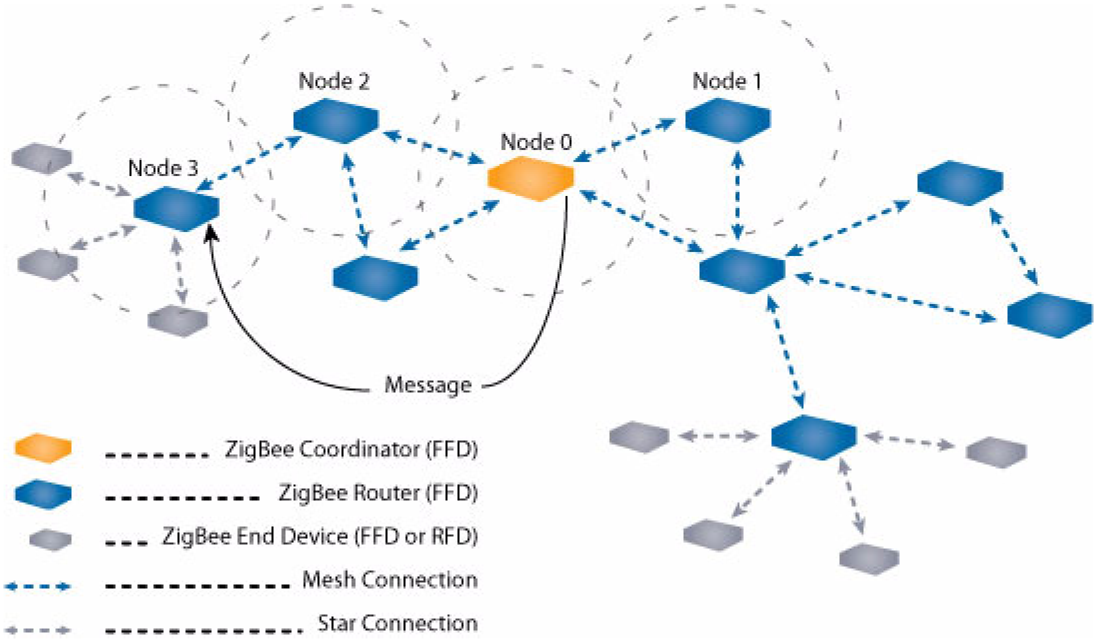
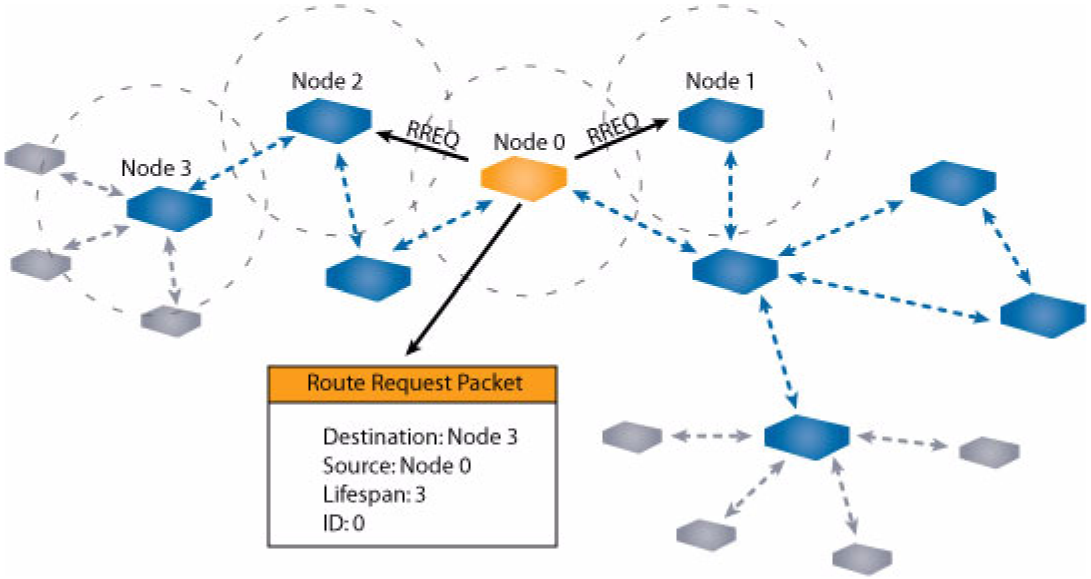


Figure 5: ZigBee Route Request



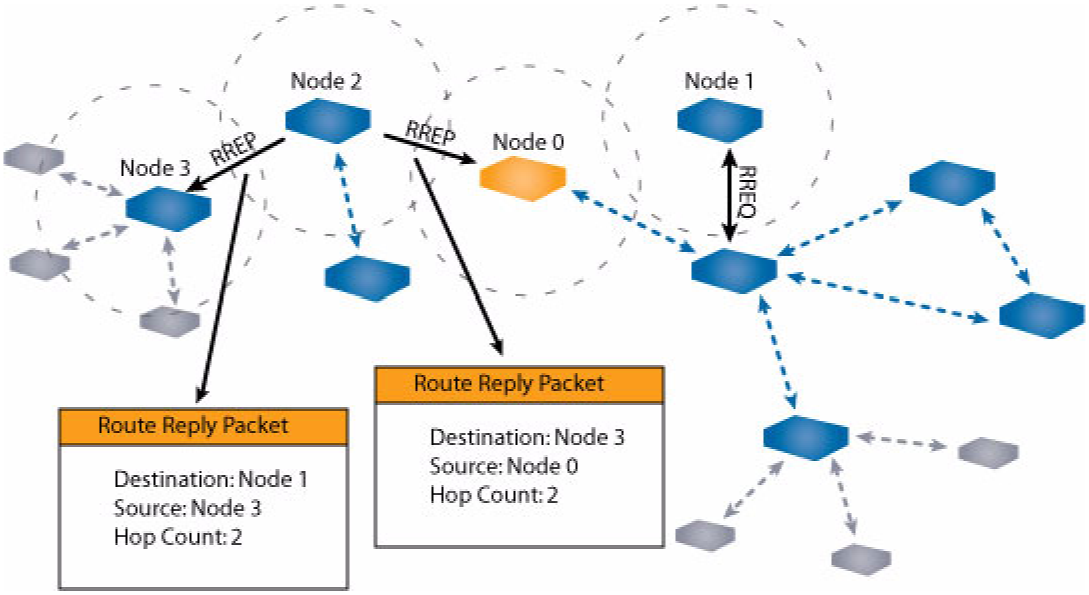
One of two things will happen when Nodes 1 and 2 receive the RREQ from Node 0:

- 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 rebroadcast the message, this time with a longer lifespan and a new ID number.

In the example, Node 1 does not have a route to Node 3 and therefore rebroadcasts the RREQ (see Figure 6: "ZigBee Route Reply" on page 18). Node 2 however, does have a route to Node 3 and therefore 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.

Figure 6: ZigBee Route Reply



Route Reply Packet

Destination: Node 1
Source: Node 3
Hop Count: 2

Route Reply Packet

Destination: Node 3
Source: Node 0
Hop Count: 2

Coordinator Addressing

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

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; meaning that the Coordinator and all Routers keep track of whether or not their neighbor(s) have relayed the broadcast packet and will re-broadcast the packet until all of their neighboring devices have received the packet. Any device can initiate a Broadcast transmission by programming its Destination Address with a Broadcast Address (see Table 4 on page 19). Subsequent broadcast transmissions occur every 500ms.

Table 4: Broadcast Addresses

Broadcast Address	Destination Group
0xFFFF	All devices in PAN
0xFFFE	Reserved
0xFFFD	All non-sleeping devices when *RXOn-WhenIdle* = True
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.

SERIAL INTERFACE

6

The ZB2430 transceiver module interfaces to the OEM Host via an asynchronous 3.3V serial UART interface; allowing the module to be easily integrated into any 3.3V 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 an alternative to the default Transparent operation 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 Mode utilizes specific frame-based 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 application specific needs.

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
- Receive API
- API Send Data Complete

For additional details and examples, please refer to the API section on page 41.