

ZigBee Technology Overview

Why ZigBee is needed

ZigBee is highly reliable

Acknowledgments at each hop

Mesh networking to find reliable route

Mesh networking essentially provides three enhanced capabilities to a wireless Network: extended range through multi-hop, ad-hoc formation of the network, and most importantly automatic route discovery and self healing.

End-to-end acknowledgments to verify data made it to the destination

ZigBee also provides automatic end-to-end acknowledgements. Your application can know whether a particular packet was received by the other node.

ZigBee enhances reliability through mesh networking, acknowledgments and use of the robust IEEE 802.15.4 standard.

ZigBee is Cost-Effective

The low cost of ZigBee is not just about low silicon cost. In addition to low MCU and radio costs, developing applications for ZigBee is cheap in other ways:

- It uses the 2.4GHz spectrum for worldwide distributions
- There are certification houses with expertise in 802.15.4 and ZigBee
- There are module vendors who provide ready-to-go ZigBee boards.
- Its core technology is free of patent infringements
- It requires only low cost development environments
- There are application profiles for ready-made vendor interoperability
- On other aspect that keeps the cost of ZigBee low is the ZigBee Alliance's careful choice of using patent-free technologies.

ZigBee is Low-Power

The real secret to low power consumption is ZigBee, in addition to radios and microcontrollers that can sleep, is low duty cycle. A node on a ZigBee network does not need to keep in constant contact with the network to remain on the network. In fact ZigBee networks are often quite silent.

ZigBee is Highly Secure

ZigBee uses the Advanced Encryption Standard (AES) for encryption and authentication. AES-128, is a block cipher that encrypts and decrypts packets in a manner that is very difficult to crack.

The reason it was adopted by ZigBee was for the following key reasons.

- Its an internationally recognized and trusted standard.
- It's free of patent infringements.

ZigBee is an Open Global Standard

ZigBee uses as its foundation the IEEE 802.15.4 specification for the lower MAC and PHY layers. IEEE defines a reliable radio standard in the 2.4GHz band that may be used worldwide.

ZigBee is Low data rate

In order to achieve low cost and low power, and considering the application space and markets ZigBee is aiming for, the ZigBee Alliance decided to keep the protocol designed for a low data rate environment particularly for wireless sensor networking and control.

ZigBee Introduction

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted towards automation and remote applications.

The ZigBee wireless networking standard fits into a market that is simply not filled by other wireless technologies. The market category ZigBee serves is called, "wireless sensor networking and control", or simply "wireless control". ZigBee is a standard networking protocol aimed at the wireless control market.

ZigBee Features

1. Low power consumption, simply implemented
2. Users expect batteries to last many months to years.
3. ZigBee/IEEE 802.15.4 has two modes they are active (transmit/receive) and sleep
4. Low cost (device, installation, maintenance)
5. Security
6. Reliability
7. Flexibility
8. Very small protocol stack
9. Interoperability and worldwide usability



10. High density of nodes per network (ZigBee's use of the IEEE 802.15.4 PHY and MAC allows networks to handle any number of devices. This attribute is critical for massive sensor arrays and control networks)
11. Simple protocol, global implementation (ZigBee's protocol code stack is estimated to be about 1/4th of Bluetooth's or 802.11's).

ZigBee Uses

ZigBee current focus is to define a general purpose, inexpensive, self organizing mesh network that can be used for industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, etc.

Smart Energy

Smart Energy offers utilities and energy service providers secure, easy-to-use wireless home area networks (HAN) for managing energy. Smart Energy gives these groups and their customers the power to directly communicate with thermostats and other smart appliances.

Home Entertainment and Control

Smart lighting, advanced temperature control, safety and security, movies and music

Home Awareness

Water sensors, power sensors, energy monitoring, smoke and fire detectors, smart appliances and access sensors

Mobile services

M-payment, m-monitoring, and control, m-security and access control, m-healthcare and tele-assist

Commercial Building

Energy monitoring, HVAC, lighting, access control

Industrial Plant

Process control, asset management, environmental management, energy management, industrial device control, machine-to-machine (M2M) communication

Personal Home and Health Care

ZigBee can monitor a patient's condition, including heart rate, blood pressure and other medical information and communicate this data securely to the hospital. This frees up the hospital bed early on, making medical care both less expensive and more comfortable for the patient.

ZigBee Device types

Every device in a ZigBee network is one of three types: a ZigBee Coordinator (ZC), a ZigBee Router (ZR), or a ZigBee End-Device (ZED)

ZigBee Coordinator

ZigBee coordinator forms the root of the network tree and might bridge to other networks. There is exactly one ZigBee coordinator in each network since it is the device that started the network originally. It is able to store information about the network, including acting as the Trust Centre & repository for security keys

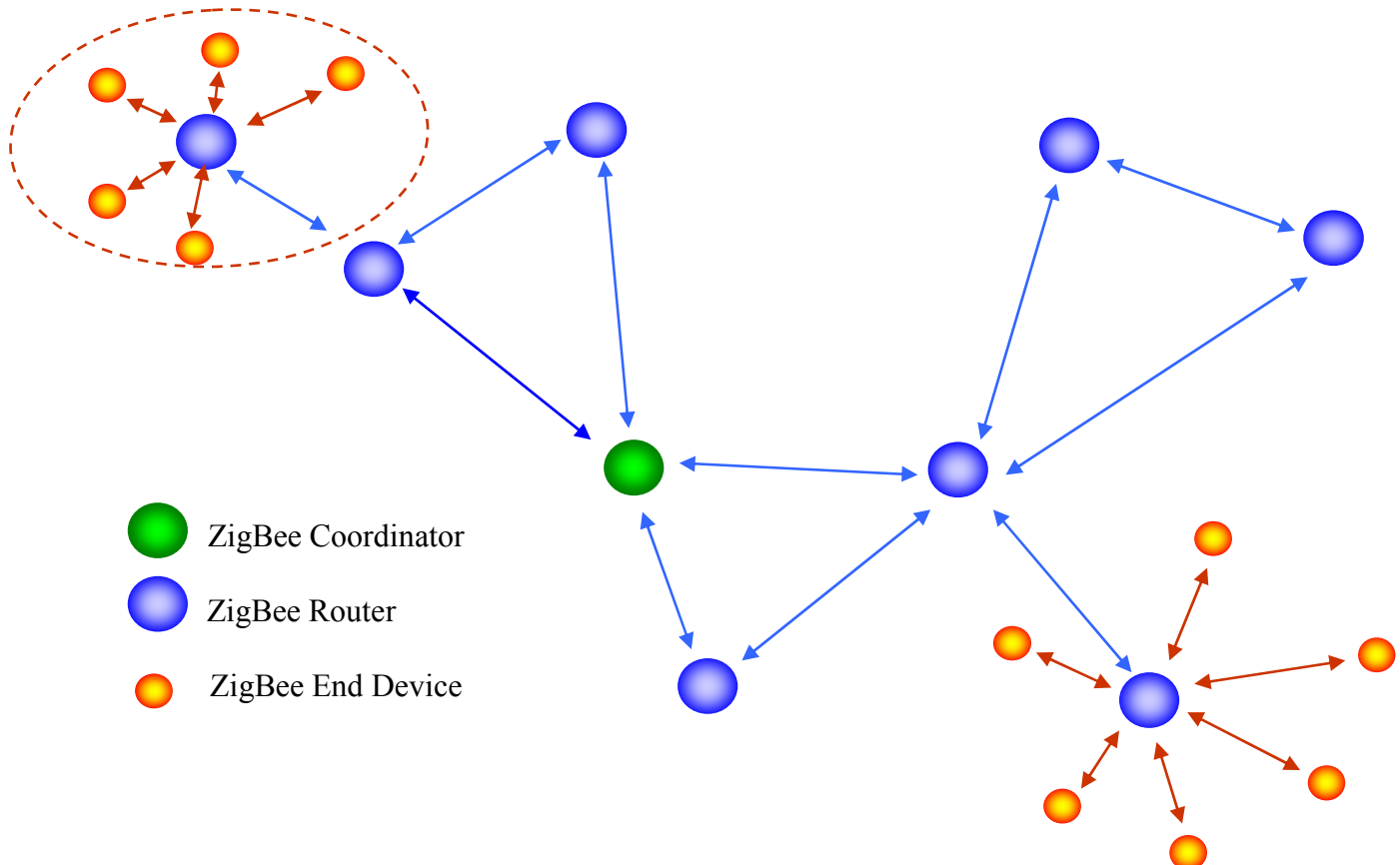
If a network is not secure, Coordinator acts as a router. In a ZigBee network there is one and only one coordinator per network.

ZigBee Router

Use a ZigBee Router to enhance the mesh in the network. ZigBee Routers can extend the range of the network and increase its reliability. ZRs like the ZigBee Coordinator route packets, and also allow other nodes to join the network.

ZigBee End-Device

ZigBee End-device contains just enough functionality to talk to the either the ZigBee Coordinator or Router. Use a ZigBee End-Device if the node must be battery-operated and sleep during network inactivity.



ZigBee Networking Concepts

ZigBee PANs

A single ZigBee network is called a Personnel Area network (PAN). ZigBee PANs are formed by the ZigBee Coordinators. Other ZigBee device types, ZigBee Router (ZR) and ZigBee End-Devices (ZED) join the ZigBee network, but do not form one themselves.

ZigBee Channels

ZigBee uses the same channel set as specified in 802.15.4. In the 2.4 GHz band, these channels are numbered 11 through 26. Channel numbers 0 through 10 are defined by the sub-1 GHz 802.15.4 radios, but ZigBee (at least to date), does not run on the sub-1 GHz radios.

The 802.15.4 radio forms the foundation for ZigBee. Two interesting points about this radio is that it is half-duplex and accesses one channel at a time. So, a device listening on channel 15 wont hear anything on channels 11 through 14 or 16 through 26

ZigBee as a protocol does not typically change channels. Bluetooth is a channel-hopping protocol and some believe that channel hopping is required for reliability.

PAN IDs

ZigBee Personnel Area Network identifiers (or PAN IDs) are used to logically separate a collection of ZigBee nodes from other ZigBee nodes in the same vicinity or on the same physical channel. This allows network A and network B to exist in close proximity without interfering with each other, other than consuming over the air bandwidth that they both share.

ZigBee PAN IDs are 16-bit numbers that range from 0x0000 to 0x3fff.

Extended PAN IDs

Extended PAN IDs are 64-bit numbers that uniquely identify a PAN. ZigBee communicate using the shorter 16-bit PAN ID for all communication except one. The beacon response issued as the result of a beacon request contains an Extended PAN ID to allow a node that wishes to join a network to pick exactly the right one.

Every time a ZigBee node wishes to join a network, it sends out a beacon request. It then pays attention to all of the beacon responses, and picks the "best" network out of these responses.

Network Address

The network address, also called NwkAddr, short address, or node address, is a called 16-bit number used to uniquely identify a particular node on a ZigBee network. The ZigBee Coordinator is always NwkAddr 0x0000.



Two ZigBee coordinators can exist on the same channel with NwkAddr 0x0000, because they are on different PAN IDs. The 16 bit Network address uniquely identifies a node in the network.

MAC Address

The MAC address, also called IEEE address, long address, or extended address, is a 64 bit number that uniquely identifies ZigBee device from all other ZigBee devices in the world. The top 24 bits of this address consist of the Organizational Unique Identifier (OUI). The lower 40 bits are managed by the OEM producing the boards.

The 64-bit MAC address has no direct relationship to the 16-bit Network address. If a node leaves one ZigBee network and joins another, its MAC address will remain the same, but Network address will likely change.

Groups

Groups are a way of collecting a set of nodes into a single addressable entity. A single data request can reach every node in a group. Groups are an optional feature in the ZigBee specification, but are mandatory in some profiles, such as in the Home Automation Profile.

Groups are interesting in that an entire set of devices can perform an action all at once.

Using Broadcasts

A broadcast is used to send a data request from one node to the entire ZigBee network, at least within a given radius. Broadcast come in three flavors

0xffff - Broadcast to all nodes

0xfffd - Broadcast to all non-sleeping nodes

0xfffc - Broadcast to routers only (including the ZigBee Coordinator)

Broadcasts are used by some underlying ZigBee management functions, such as route discovery or Network address request, and may also used by applications.

Endpoints

Within each node are endpoints. Endpoints, identified by a number between 1 and 240, define each application running in a ZigBee node (yes, a single ZigBee node can run multiple applications)

End points are virtual wires between applications. A node contain any number of end points (upto to 240), with any set of endpoint identifiers.

Endpoints serve three purposes in ZigBee

- Endpoints allow for different application profiles to exist within each node.

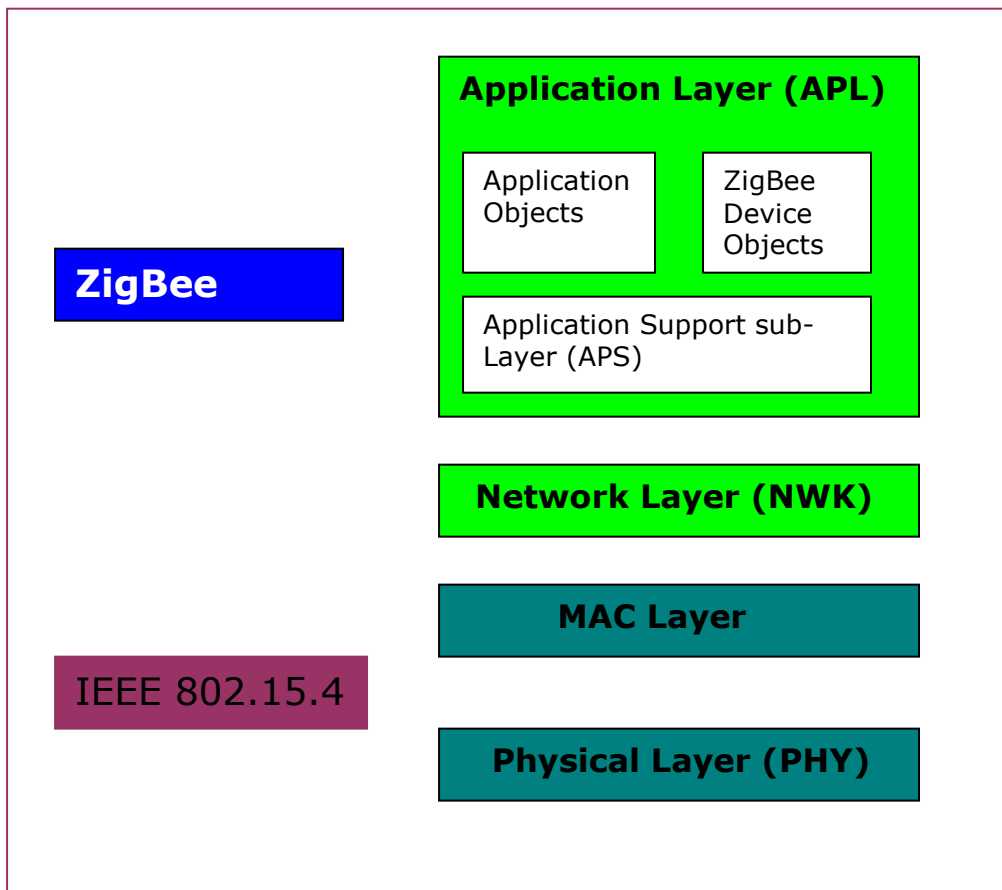
- Endpoints allow for separate control points to exist within each node.
- End points allow for separate devices to exist within each node

There is a special end point called a broadcast endpoint (0xff). Sending a data request to the broadcast end point will reach all end points within the node that matches the profile ID.

ZigBee AES 128-Bit Security

The ZigBee security suite is built on the Advanced Encryption (AES-128 bit) standard, a well-respected block cipher algorithm published by the National Institute of standards and Technology (NIST).

ZigBee Stack





IEEE 802.15.4 defines the specification for PHY and MAC layers of wireless networking, but it does not specify any requirements for higher networking layers.

The ZigBee standard defines only the networking, application, and security layers of the protocol and adopts IEEE 802.15.4 PHY and MAC layers as part of the ZigBee networking protocol.

Physical Layer

In ZigBee wireless networking, the lowest layer is the IEEE 802.15.4 physical layer or PHY. The PHY layer is responsible for activating the radio that transmits or receives packets. The PHY also selects the channel frequency and make sure the channel is currently used by any other device on another network.

MAC Layer

The Medium Access Layer (MAC) layer provides the interface between the PHY layer and NWK layer. The MAC layer provides the concept of network, including a PAN ID, and networking discovery through beacon requests and responses. It also provides per-hop acknowledgments and some of the commands for joining and forming a network. The MAC does not multi-hop or mesh

Network Layer

The Network layer is responsible for mesh networking, which includes broadcasting packets across the network, determining routes for unicasting packets, and generally making sure packets sent reliably from one node to another. The Network layer also has a set of commands for security purposes, including secure joining and rejoining. ZigBee networks are all secured at the Network layer, and the entire payload of the network frame is encrypted

Application Layer

The application layer is the highest protocol layer in the ZigBee wireless network and the hosts the application objects.

Application Support Sub-Layer

Application Support sub-Layer acts as a filter for the applications running above it on end points to simplify the logic in those applications. It understands what clusters and end points mean, and checks to see if the end point is a member of the Application Profile and (if present) group before sending the message on up.

The APS layer keeps a local binding table, a table which indicates the nodes or groups in the network that his node wishes to speak to

ZigBee device Object (ZDO) Layer

The ZDO layer includes ZigBee Device Profile is responsible for local and over –the air management of the network. It provides service services to discover other nodes and services in the network, is directly responsible for the current state of this node in the network.



ZigBee Stack comparison

Feature	ZigBee 2006	ZigBee 2007	ZigBee Pro
Size in ROM/RAM	Smallest	Small	Bigger
Stack Profile	0x01	0x01	0x02
Maximum hops	10	10	30
Maximum nodes in network	31,101	31,101	65,540
Mesh Networking	Yes	Yes	Yes
Broadcasting	Yes	Yes	Yes
Tree routing	Yes	Yes	No
Frequency Agility	No	Yes	Yes
Bandwidth used by Protocol	Least	More	Most
Fragmentation	No	Yes	Yes
Multicasting	No	No	Yes
Source routing	No	No	Yes
Symmetric Links	No	No	Yes
Standard Security (AES 128 bit)	Yes	Yes	Yes
High Security (SKKE)	No	No	Yes
Profiles support	Home Automation	Home Automation	Home Automation Smart Energy Commercial Building Industrial Plant Monitor

Compatible between ZigBee 2006, ZigBee 2007 and ZigBee Pro

- ZigBee 2007 is fully backward compatible with ZigBee 2006 devices: A ZigBee 2007 device may join and operate on a ZigBee 2006 network and vice versa.
- Due to differences in routing options, ZigBee Pro devices must become non-routing ZigBee End-Devices (ZEDs) on a ZigBee 2006 network, the same as for ZigBee 2006 devices on a ZigBee 2007 network must become ZEDs on a ZigBee Pro network. The applications running on those devices work the same, regardless of the stack profile beneath them.



Difference between ZigBee, Wi-Fi, Bluetooth

	ZigBee	Wi-Fi	Bluetooth
Application	Monitoring and Control	Email, Web, Video	Cable replacement
Physical/ MAC layers	IEEE 802.15.4	IEEE 802.11	IEEE 802.15.1
Data Rate	250 Kbits/s	11 & 54 Mbits/sec	1 Mbits/sec
Range	10-100 meters	50-100 meters	10 meters
Networking Topology	Mesh	Point to hub	Ad-hoc, very small networks, point to point
Operating Frequency	2.4 GHz	2.4 and 5 GHz	2.4 GHz
Complexity (Device and application impact)	Low	High	High
Security	128 bit AES and Application Layer user defined	WEP, WPA, SSID	Authentication, 64-128 bits encryption
Power Consumption	low	High	Medium
Number of devices for Network	64K	32 per access point	7
Network Latency of Sleeping slave changing to active	Devices can join an existing network in under 30ms	Device connection requires 3-5 seconds	Device connection requires up to 10 seconds
Typical Applications	Industrial control and monitoring, sensor networks, games, building automation, home control and automation, toys	Wireless LAN connectivity, broadband Internet access	Wireless connectivity between devices such as phones, PDA, laptops, headsets

. History

Revision	Date	Author	Comments
1.0	Aug 8 2011	Sai Kesineni	Initial version