## Zigbee:

Ref: Jean-Philippe Vasseur, Adam Dunkels, in Interconnecting Smart Objects with IP, 2010

Ref: https://nptel.ac.in/courses/106105166

ZigBee is a IEEE 802.15.4 based, **low power, low data rate supporting wireless networking standard**, which is basically used for two-way communication between sensors and control system. It is a short-range communication standard like Bluetooth and Wi-Fi, covering range of 10 to 100 meters. The difference being while Bluetooth and Wi-Fi are high data rate communications standard supporting transfer of complex structure like media, software etc.,

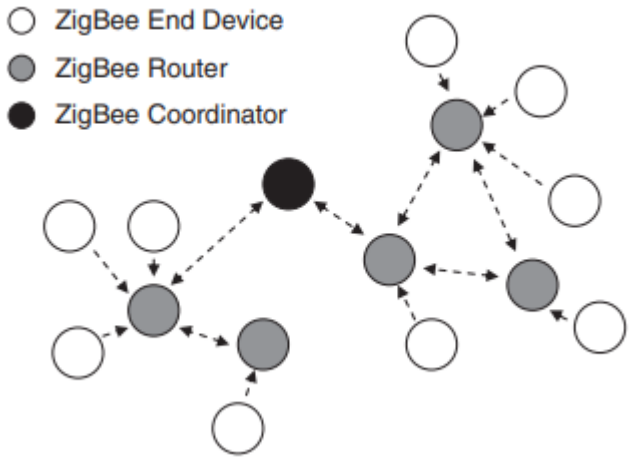
ZigBee Technology supports transfer of simple data like that from sensors. It supports low data rate of about 250 kbps. The operating frequencies are 868 MHz, 902 to 928 MHz and 2.4 GHz. ZigBee Technology is used mainly for applications requiring low power, low cost, low data rate and long battery life.

**ZigBee Architecture**

The ZigBee Network Protocol follows IEEE 802.15.4 standards for Physical and MAC layers, along with its own Network and Application layers. ZigBee is based on the IEEE 802.15.4 standard and does not provide any alternatives as underlying radios. The ZigBee protocols are defi ned around the concepts and addressing modes provided by the underlying IEEE 802.15.4 radio, making it difficult to adapt the ZigBee protocols to other radios.

ZigBee Device Type:

ZigBee specifies three different device types: the ZigBee Coordinator (ZC), the ZigBee Router (ZR), and the ZigBee End Device (ZED). These three devices play different roles in a ZigBee network as shown in Figure.




A ZigBee network has exactly one ZC device. The ZC coordinates the actions of the network as a whole and is responsible for bootstrapping the network. The ZRs build a network between themselves through which packets are exchanged. The ZEDs are logically attached to a ZR. ZEDs communicate only with their ZR, but cannot communicate between each other. ZED

contains just enough functionality to talk to the parent node, and it cannot relay data from other devices. This allows the node to be asleep a significant amount of the time thereby enhancing battery life. Memory requirements and cost of ZEDs are quite low, as compared to ZR or ZC. Each of the ZigBee device types has been designed for a specific deployment. ZCs and ZRs have a higher power requirement than ZEDs and cannot be battery-powered. The ZED has a lower power requirement and achieves a long lifetime on batteries

The ZC is responsible for bootstrapping the network. During the bootstrapping process, the ZC chooses the personal area network (PAN) identifier that will be used by the network, as well as the physical radio channel on which the network will operate.

After bootstrapping, the ZC acts as a normal ZR device.

ZEDs are off most of the time, thus they are not able to receive any traffic sent to them. Instead, they periodically wake up and check for messages at the ZR with which they are associated.

The ZR buffers data sent to their ZED nodes and sends these data whenever they get a poll request from a ZED.

The ZED transmits data to the ZR at any time, since the ZR is always awake. The wake-up schedule for ZED is defi ned by the application developer, not by the ZigBee specification. The number of ZEDs associated with a ZR is limited. In the ZigBee 2007 specification, a ZR can handle a maximum of 14 ZEDs.

**Layers in the ZigBee Stack**

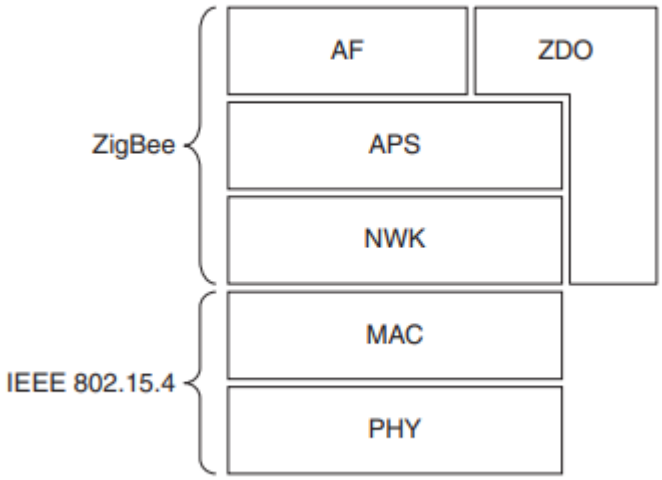
The ZigBee specification is divided into five layers, as shown in following figure: the physical (PHY) layer, the medium access control (MAC) layer, the network (NWK) layer, the application support (APS) layer, and the application framework (AF) layer.

In addition to the five layers, a cross-layer entity called the ZigBee Device Object (ZDO) is also present in the architecture.

Of these layers, PHY and MAC are not part of the ZigBee specification; they are taken from the IEEE 802.15.4 radio standard.

The NWK, APS, and AF layers are part of the ZigBee specification, as is the ZDO.

The layering of the ZigBee stack is reminiscent of the layers in the IP stack. Just like in the IP architecture, each layer in the ZigBee stack has a specific purpose. There is, however, one major difference between the layering in the IP architecture and the layering in the ZigBee stack: in the ZigBee stack, the layers cannot be changed. The IP architecture is built to allow multiple types of MAC and PHY layers. The same protocols can be used even if the specific radio standard changes. In contrast, the ZigBee specification is designed specifically for the IEEE 802.15.4 MAC and PHY layers. Also, the upper layer protocols make explicit use of mechanisms provided by the radio layer. For example, instead of providing its own NWK layer addressing scheme, ZigBee uses IEEE 802.15.4 MAC layer addresses even at the NWK layer. We will now discuss the ZigBee layers in more detail.




**PHY and MAC Layers**

The PHY layer transports bits across the physical radio medium.

The MAC layer mediates access to the medium so that multiple transmitters do not transmit at the same time.

Because ZigBee uses IEEE 802.15.4 for its MAC layer, ZigBee also uses the same addressing format at 802.15.4.

ZigBee supports the short addressing mode in which addresses are 16 bits wide. This allows each ZigBee network to support at most 65,536 nodes. In practice, the number of possible nodes is reduced because a number of addresses are reserved. In ZigBee 2004 and 2006, a network includes a maximum of 31,101 nodes, whereas in ZigBee 2007 and ZigBee Pro, the maximum number of nodes in a network is 65,540.

ZigBee uses a carrier sense multiple access with collision avoidance (CSMA/CA) scheme for its MAC layer. Before a packet is sent, the MAC queries the PHY for other current radio transmissions. If another node is currently sending a packet, the node refrains from sending its own packet. Instead, it sets a timer and tries to resend the packet at a later time.

The MAC layer does hop-by-hop acknowledgments for all ZigBee packets except broadcast packets.

The acknowledgment uses the standard IEEE 802.15.4 acknowledgment mechanism. If an acknowledgment is not received, the packet is retransmitted up to three times. ZigBee also performs end-to-end acknowledgments at the application support sublayer, as described next.

ZRs and ZCs have their radios constantly on, whereas ZDEs may keep their radio off all the time. Nodes that have their radio turned on all the time have a significantly higher energy consumption and therefore cannot be battery-operated. Only nodes that keep their radios turned off have a low enough power consumption to be battery-operated.

**NWK**

The NWK layer performs addressing and routing and is the equivalent of the IP layer in the IP architecture.

The ZigBee network layer provides two forms of data delivery: broadcast and unicast.

Multicast is also supported, but multicast data are delivered using broadcast with software filtering of the incoming packets at the receiver.

Broadcast delivery is a form of network flooding, which sends a packet to all nodes on the network.

The packet can be tagged with a maximum hop count that determines how far the packet can travel in the network. Because the broadcast packet reaches every node in the network, a broadcast is an expensive operation. Unicasts, on the other hand, are sent only to the node to which they are addressed.

Both broadcasts and unicasts can travel up to 30 hops.

The ZigBee stack has two schemes for routing unicast packets: network routing and source routing. In network routing, the network takes care of finding the best route for the packet to take through the network. In source routing, the sender must explicitly state through which nodes the message should pass to reach its destination.

Source routing is useful for large networks where each node in the network may not be able to maintain large routing tables for all nodes.

Instead, the ZC node, which is assumed to have significantly more memory than the other nodes, can maintain all routing information for all nodes. This reduces the memory load for the network at the expense of a slight overhead in each packet. But as node addresses are short in ZigBee, this overhead is small.

To keep the overhead to a bounded value, source routing is limited to five hops. Source routing is available only in the ZigBee Pro version.

There are two types of network routing: mesh and tree routing. Mesh routing builds a connected mesh between the ZR devices and transports data in a point-to-point fashion.

The tree routing scheme builds a tree where the ZC is the root of the tree and ZEDs are the leaf nodes. Tree routing is not available in ZigBee Pro.

The ZigBee mesh routing algorithm is an adaptation of the Internet Engineering Task Force (IETF) standard protocol Ad hoc On-demand Distance Vector (AODV) Protocol [194].

AODV is a reactive on-demand protocol, which means that routes are not established until they are needed; that is, nodes do not know about each other until the first packet is sent. When a packet is sent, the originating node broadcasts a routing request packet. This routing request reaches all nodes in the network. Nodes set up a reverse path to the originating node as part of the route request procedure. When a node receives a routing request packet, it adds an entry for the originating node in its routing table. The routing table entry is filled with the address of the originating node as well as the address of the node from which the route request came. This

packet should be sent to this node to reach the originator. Thus a reverse path is built in the network.

When the route request reaches the requested node, this node sends a unicast route reply back to the originator of the request. Since the nodes in the network have built a reverse path, the network knows how to reach the originator node. As the nodes on the path forward the unicast route reply, they add the destination node to their routing tables along with the node from which they received the route reply. When the route reply reaches the originator, the route is set up and the originator and the destination begin exchanging packets.

The network routing mechanism works well for small networks, but as the network grows, the amount of state each node has to maintain increases. In large networks with hundreds or thousands of nodes, the routing tables in the memory-constrained nodes begin to overflow. Additionally, the network flooding of the route request packets becomes problematic. In such situations, the source routing mechanism can be used instead.

**APS Sublayer**

The APS sublayer is equivalent to the transport layer in the IP architecture. It is a thin layer that acts as an intermediary between the NWK layer and the application layer. The purpose of the APS is to do end-to-end acknowledgments and to filter out duplicate packets. The APS layer has a connection between two nodes called a binding. A binding is unidirectional — a node is bound to another node, but the other node is not necessarily bound back to the first node.

**AF**

The ZigBee application layer is called application framework (AF) and runs on top of the APS layer.

The AF supports multiple applications and demultiplexes incoming data between the registered applications. Some of the applications are defined by the ZigBee specification, whereas others are implemented independently by vendors.

In ZigBee, an application is called a profile. ZigBee profiles are identified with an integer between 0 and 240, called an end point. This is the equivalent of the port number in the IP architecture.

When the AF layer processes a packet, it demultiplexes the packet based on the end point identifier. Applications register with an end point identifier at the AF layer. If a packet arrives for an end point identifier that is not registered, the packet is silently dropped. If the application has been registered, the packet is passed to the application layer. ZigBee profiles are used in cases for which the ZigBee technology is intended. For example, the ZigBee Alliance has defined a profile for home automation, smart energy management, building automation, and toys. There are two types of application profi les: public and vendor-specific. Each application profile is identified by an integer between 1 and 240. This integer is called a profile end point.

The profile with end point zero is the ZDO and it is used for network configuration and setup. Zig. Bee Device Object ZDO not only interacts with APS, but also interacts directly with the network layer. ZDO controls the network layer, telling it when to form or join a network, and when to leave, and provides the application interface to network layer management services

For example, ZDO can be configured to continue attempting to join a network until it is successful, or until a user-specified number-of-retries has occurred before giving up, and informing the application of the join failure. The ZDO profi le is responsible for network maintenance. It provides mechanisms for interacting with the NWK and APS layers, which is done during network configuration.

**Network Setup**

The ZigBee network setup process involves all layers of the ZigBee stack. This process establishes a physical communication link between the nodes in the network, distributes address information between the nodes in the network, and discovers and binds the services on the nodes. The network setup process begins at the PHY layer. The ZC starts by scanning the 16 available physical radio channels of the IEEE 802.15.4 radio to fi nd the channel that has the least current radio energy. This channel is assumed to be the one with the least interference from other equipment. Since IEEE 802.15.4 runs on the unlicensed 2.4 GHz band, there are several sources of interference such as WiFi networks and microwave ovens. The channel scan samples each channel for 0.5 s. Thus, the process takes eight seconds and gives only a snapshot of the channel activity. When the scan is complete, the ZC chooses the channel with the least activity for the network. This channel is retained through the lifetime of the network. After the PHY layer channel selection is complete, the MAC layer creates a new PAN ID for the network. The PAN ID is a 16-bit integer selected at random by the ZC. Once the ZC has selected a PAN ID, it begins to announce its presence on the selected channel and with the selected PAN ID through repeated beacon messages. When the physical channel and PAN ID have been selected, the network formation is said to be complete. Once the ZC has formed the network, ZRs and ZEDs begin to join it. Nodes join a network by sending out their own beacon messages. If a ZR or ZC hears a beacon from a node that is not part of a network, it responds by sending a beacon message back. The node collects all answers it receives and decides which network and ZR it should try to associate with. The process by which the node chooses its network and parent is application-specific. If network security is enabled, after a node has selected a network and a parent, it authenticates itself with the parent. Now the node is fully part of the network.

The Zigbee network setup involves coordination across all layers of the Zigbee stack and encompasses establishing communication links between nodes, distributing address information, and discovering and binding services within the network. Here's an overview of the process:

1. **Channel Selection at PHY Layer:** The Zigbee Coordinator (ZC) initiates the setup by scanning the 16 available physical radio channels to identify the channel with the least interference. This is crucial due to potential interference sources in the unlicensed 2.4 GHz band, like WiFi networks and microwave ovens. The ZC selects the channel with the least activity, which will persist throughout the network's lifetime.

2. **PAN ID Creation at MAC Layer:** Following channel selection, the MAC layer generates a new Personal Area Network ID (PAN ID), a 16-bit integer selected randomly by the ZC. This PAN ID is used to identify the network.

3. **Beacon Messages to Establish Network:** The ZC broadcasts its presence on the selected channel and PAN ID by repeatedly transmitting beacon messages. This marks the completion of network formation.

4. **Joining the Network by ZRs and ZEDs:** Other Zigbee Routers (ZRs) and End Devices (ZEDs) aim to join the network. They send out their beacon messages. When a ZR or ZC detects a beacon from a node not yet part of a network, it responds with a beacon message, allowing the node to decide which network and ZR to associate with.

5. **Authentication and Integration:** If network security features are enabled, after a node selects a network and a parent, it authenticates itself with the parent device. Following successful authentication, the node becomes a fully integrated part of the network.

The process involves meticulous steps at each layer, starting from channel selection to PAN ID creation, broadcasting presence, joining the network, and finally integrating and authenticating nodes. The goal is to establish a robust and functional Zigbee network while managing channel interference and ensuring