ZigBee Technology

ZigBee Standard: https://csa-iot.org/all-solutions/zigbee/

Dr. Manas Khatua
Associate Professor
Dept. of CSE, IIT Guwahati
E-mail: manaskhatua@iitg.ac.in

IoT Access Technologies

- there are many IoT technologies in the market today

Need of ZigBee

- Bluetooth and Wi-Fi are used to connect devices but not suitable for IoT applications.
- IoT applications require
  - Battery operated devices
  - Large number of connected device

- Wi-Fi working on IEEE 802.11 have high power consumption.
- Bluetooth network commonly known as Piconets, uses point-to-point connection. One master node can connect maximum up to 7 salve nodes.
- Need of something that can meet both requirements of IoT.
  - Solution is the Zigbee.

IEEE 802.15.4

- IEEE 802.15.4-2003 is a **wireless Access Technology** for
  - ✓ low-cost and low-data-rate devices
  - ✓ devices powered by batteries

- It enables easy installation using a compact protocol stack

- Several network communication stacks leverage this technology for many IoT use cases in both the consumer and business markets.
  - **ZigBee /** ZigBee IP
  - 6LoWPAN
  - WirelessHART
  - Thread
  - 6TiSCH

- **ZigBee** shows how 802.15.4 can be leveraged (at the PHY & MAC) independent of the protocol layers above.

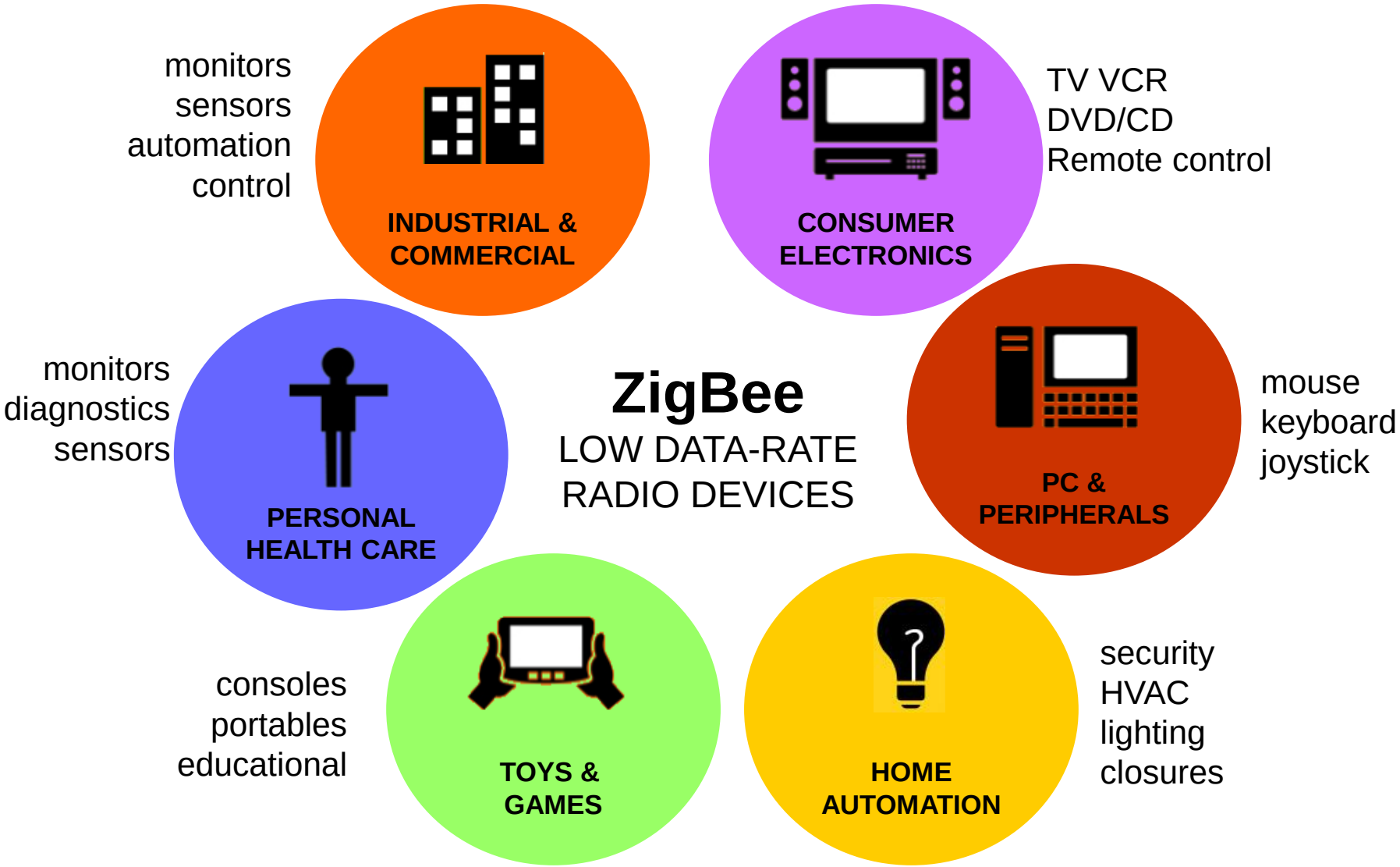
ZigBee

- First ZigBee specification was ZigBee-2004
- ZigBee technology follows
  - Low data rate
  - Low power consumption
  - Low cost
  - Wireless networking
  - Mesh networking topology
- Well-known application domains:

ZigBee in Digi's Xbee radio module

Industrial and Commercial Automation	Smart Home Applications	Smart Energy or Utility Applications
measuring temperature and humidity, and tracking assets	control lighting, thermostats, and security functions	monitor and control the use and delivery of utilities, such as electricity and water

Other ZigBee Applications

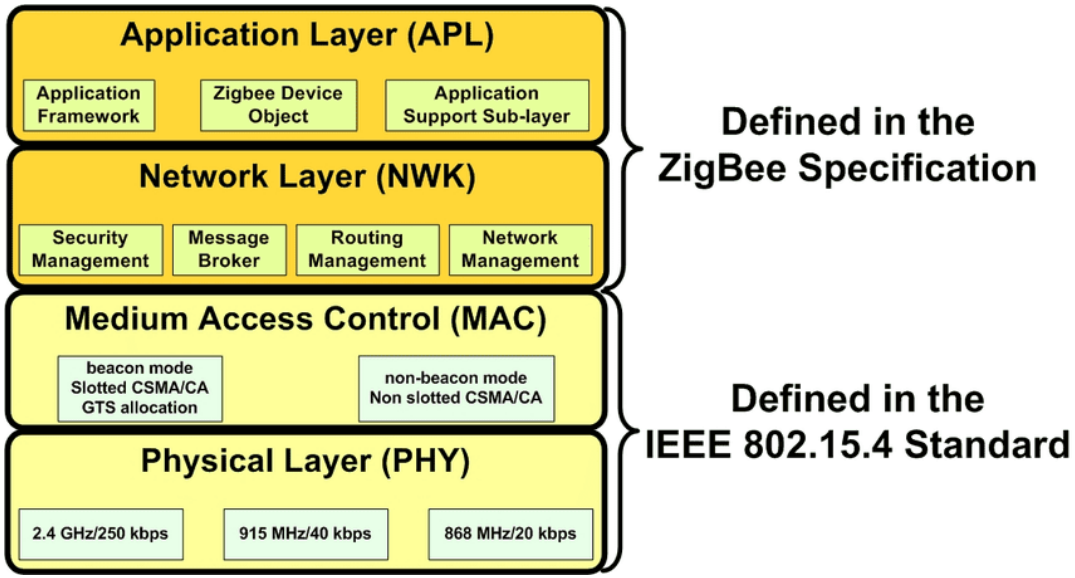


ZigBee Protocol Stack

IEEE and **ZigBee Alliance** jointly specifies the entire ZigBee protocol stack for communication

- ✓ IEEE 802.15.4 focuses on the specification of the lower two layers of the protocol (physical and data link layer)

- ✓ ZigBee Alliance aims to provide the upper layers of the protocol stack (from network to the application layer)



ZigBee Alliance

- An alliance of organizations with a **mission** to define
  - reliable,
  - cost effective,
  - low-power,
  - wirelessly networked,
  - monitoring and control products
  - based on an open global standard

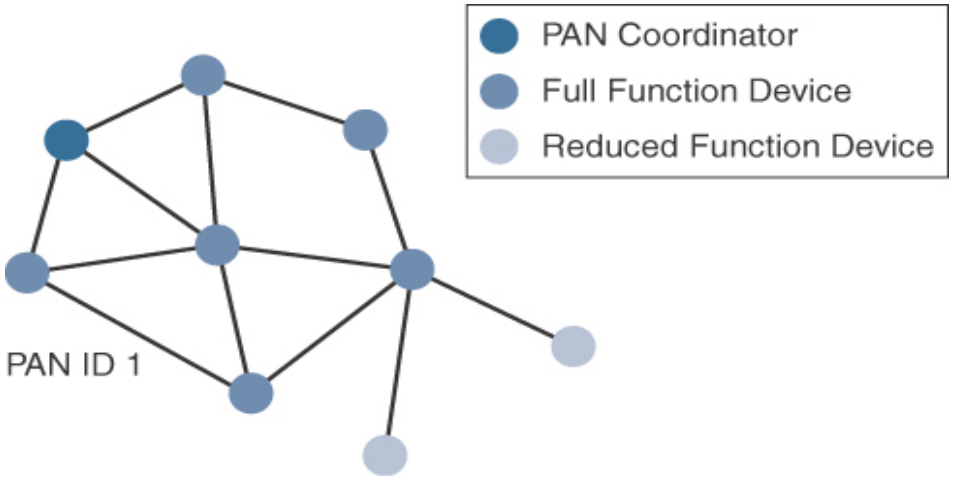
- Alliance **provides**
  - interoperable data networking,
  - interoperability compliance testing,
  - branding or marketing of the standard,
  - a range of wireless home and building control solutions,
  - security services
  - advanced engineering for the evolution of the standard

- ZigBee Alliance
  - 45+ companies: Semiconductor mfrs, IP providers, OEMs, etc.

Device Type

- The most basic component of a ZigBee system is the **device**
  - A device can be a full-function device (FFD) or reduced-function device (RFD).
  - The FFD can operate in three modes:
    - a personal area network (PAN) coordinator
    - a coordinator
    - a device.
  - An FFD can talk to RFDs or FFDs.
  - An RFD can only talk to an FFD.

A network shall include at least one FFD, operating as the PAN coordinator.



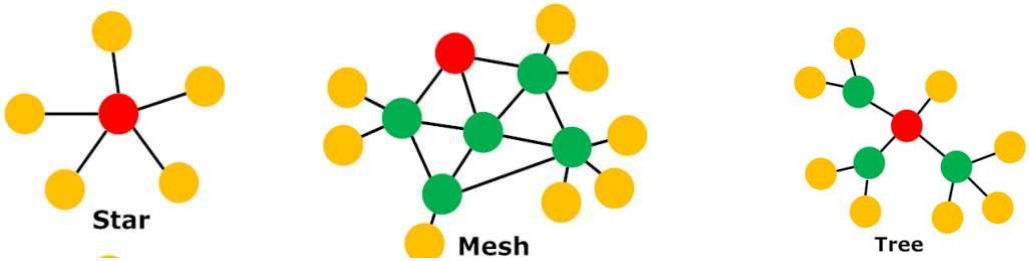
Network Topologies

Three types of topologies that ZigBee supports:

- ✓ Star topology
  - communication is established between devices and a single central controller (PAN coordinator).
  - each start network has an unique PAN identifier

- ✓ Peer-to-peer topology
  - there is also one PAN coordinator
  - unlike star, any device can communicate with any other device if they are in range of one another
  - peer-to-peer network can be ad hoc, self-organizing and self-healing
  - It allows multiple hops to route messages from any device to any other device in the network.
  - It can provide reliability by multipath routing

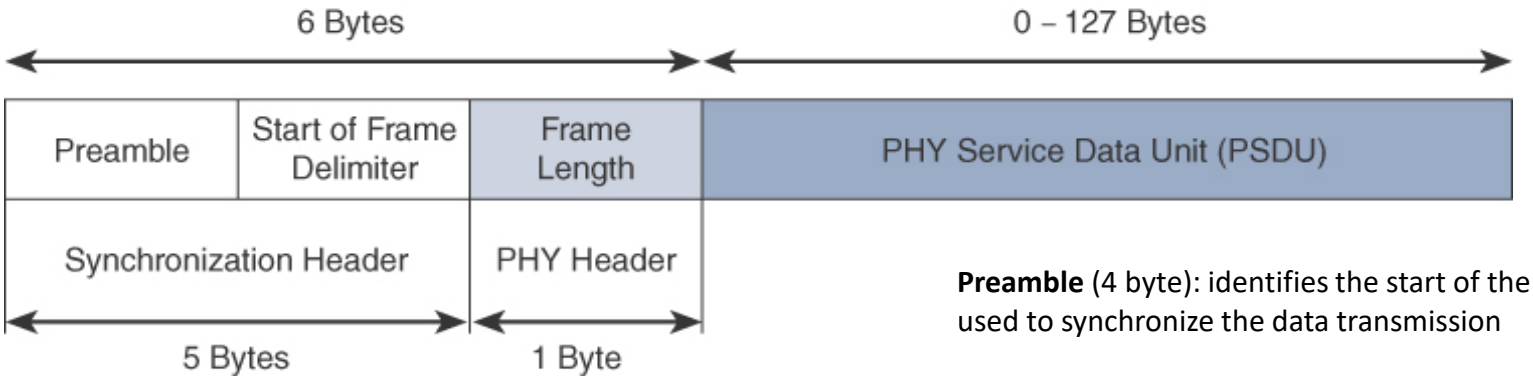
- ✓ Cluster tree
  - Cluster-tree network is a special case of a peer-to-peer network
  - The PAN coordinator forms the first cluster by establishing itself as the cluster head (CLH)
  - Devices join successively in multi-hop fashion i.e. successive clusters
  - If required, PAN coordinator may instruct a device to become the CLH of a new cluster



IEEE 802.15.4 PHY Layer

IEEE 802.15.4 PHY provides the PHY data service and PHY management services.

- The PHY data service enables the transmission and reception of PHY protocol data units (PPDU) across the physical radio channel.



PPDU Frame Format

Preamble (4 byte): identifies the start of the frame; used to synchronize the data transmission

SFD (1 byte): informs the receiver about the starting point of frame content

Services of PHY

- radio transceiver activation/deactivation,
- radio channel selection,
- energy level detection (ED) ,
- received signal quality (RSI) or link quality indicator (LQI),
- clear channel assessment (CCA),
- transmitting and receiving packets in 2.4-GHz band.

- Transmission options
  - **2.4 GHz**, with a data rate ~ 250 kbps
  - **915 MHz**, with a data rate ~ 40 kbps
  - **868 MHz**, with a data rate ~ 20 kbps
- Modulation schemes
  - Offset quadrature phase-shift keying (O-QPSK)
  - Binary phase-shift keying (BPSK)
  - Amplitude shift keying (ASK)

Key Features of ZigBee PHY

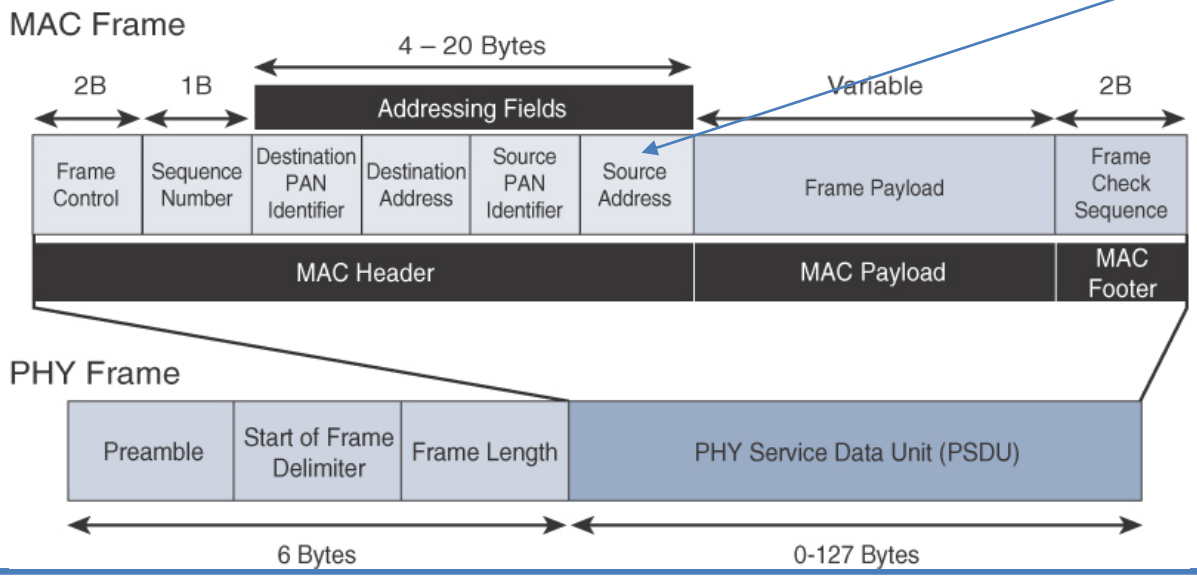
- Energy Detection (ED)
  - It is an estimate of the received signal power within the bandwidth of an IEEE 802.15.4 channel.
  - No attempt is made to identify or decode signals on the channel.
  - The ED time should be equal to 8 symbol periods.
  - The ED result shall be reported as an 8-bit integer
  - The ED measurement is intended for use by a network layer as part of channel selection algorithm.

- Link Quality Indication (LQI)
  - The LQI measurement is a characterization of the strength and/or quality of a received packet.
  - The measurement may be implemented using receiver ED, a signal-to-noise ratio (SNR) estimation or a combination of these methods.
  - The LQI shall be reported as an 8-bit integer
  - The use of LQI result is up to the network or application layers.

- Clear Channel Assessment (CCA)
  - CCA is performed according to at least one of the following three methods:
    - Energy above ED threshold.
    - Carrier sense only (i.e. based upon the detection of a signal with modulation and spreading characteristics)
    - Carrier sense with energy above ED threshold.

IEEE 802.15.4 MAC layer

- IEEE 802.15.4 MAC provides the MAC data service and MAC management services.
  - The **MAC data service** enables transmission of MAC protocol data units (MPDU) across the PHY data service.
  - The **MAC sublayer features** include
    - beacon management,
    - channel access,
    - GTS management,
    - frame validation,
    - ACK frame delivery, and
    - association and disassociation.

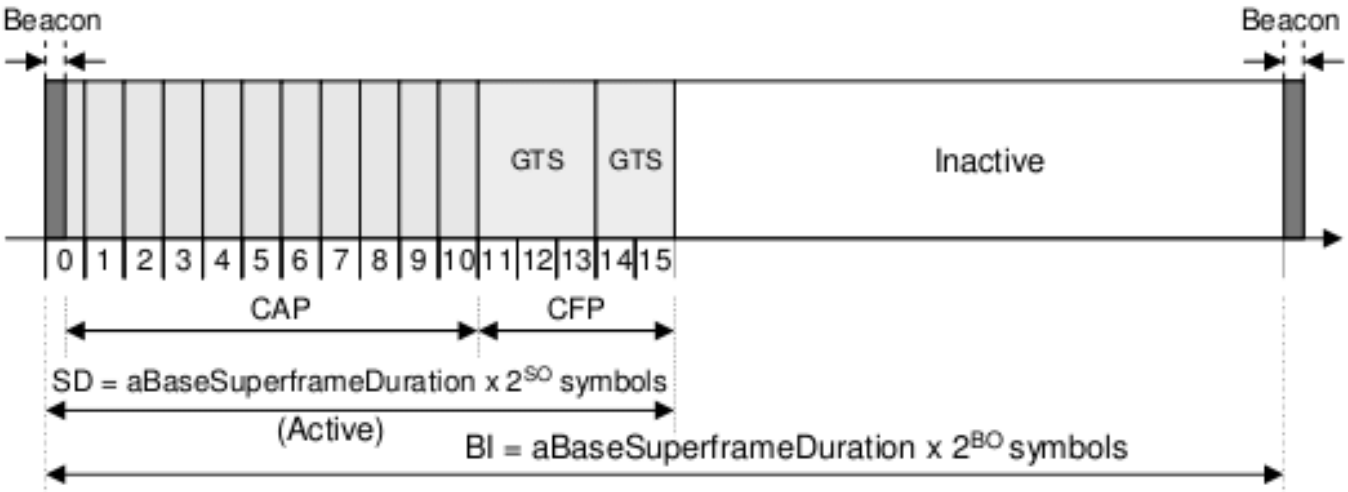


16-bit short address
OR
64-bit extended address

- MAC frame types:
  - Data frame
  - Beacon frame
  - ACK frame
  - Command frame

MAC Features

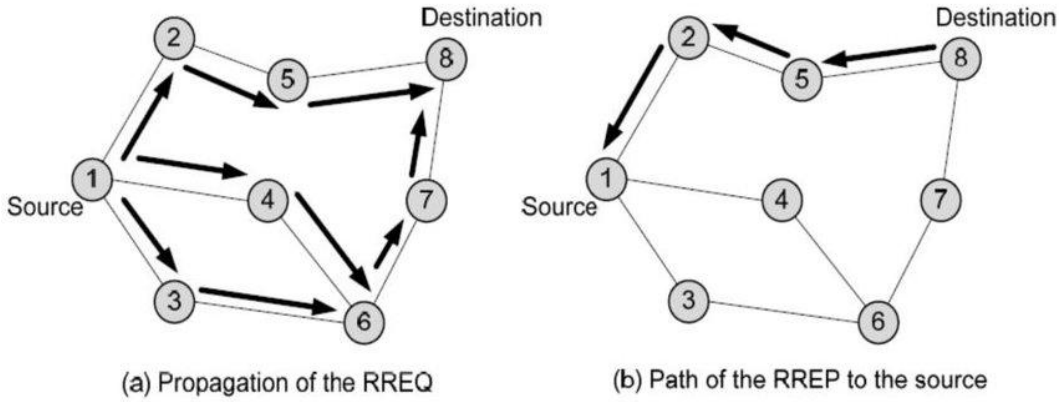
- Superframe Structure for data transmission
- Beacon Generation



- Slotted / Unslotted CSMA-CA as channel access mechanism
- Starting and Maintaining PANs
- Association and Disassociation
- Synchronization
- GTS Allocation and Management

ZigBee Routing Layer

- Routing Algorithms: (i) AODV, (ii) Cluster Tree Algorithm, (iii) Few others….
- AODV (Ad-hoc On-demand Distance Vector)
  - It is a pure on-demand route acquisition algorithm
    - Nodes do not lie on active paths, neither maintain any routing information nor participate in any periodic routing table exchanges
    - A node does not discover and maintain a route to another node until the two need to communicate



- RREQ is broadcasted
- RREP is unicasted

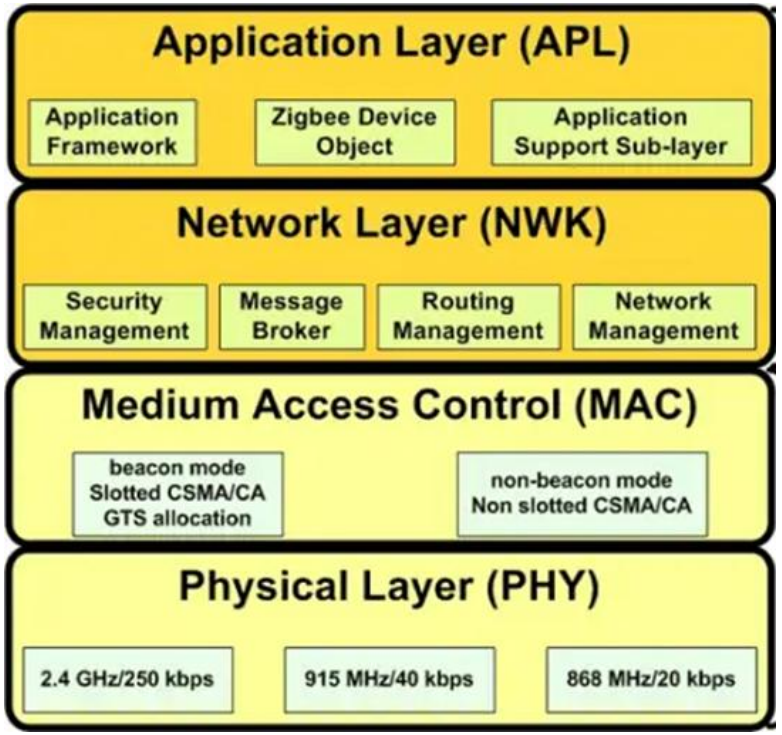
- Routing table entry:
  - Dest. Node
  - Next Hop
  - No. of hops
  - Seq. no. for the dest.
  - Active neighbours for this route / dest.
  - Expiration time

Route Request Packet = {*source addr, source seq. no., broadcast id, dest. addr, dest. seq. no., hop count*}

Route Reply Packet = {*source addr, dest. addr, dest. seq. no., hop count, lifetime*}

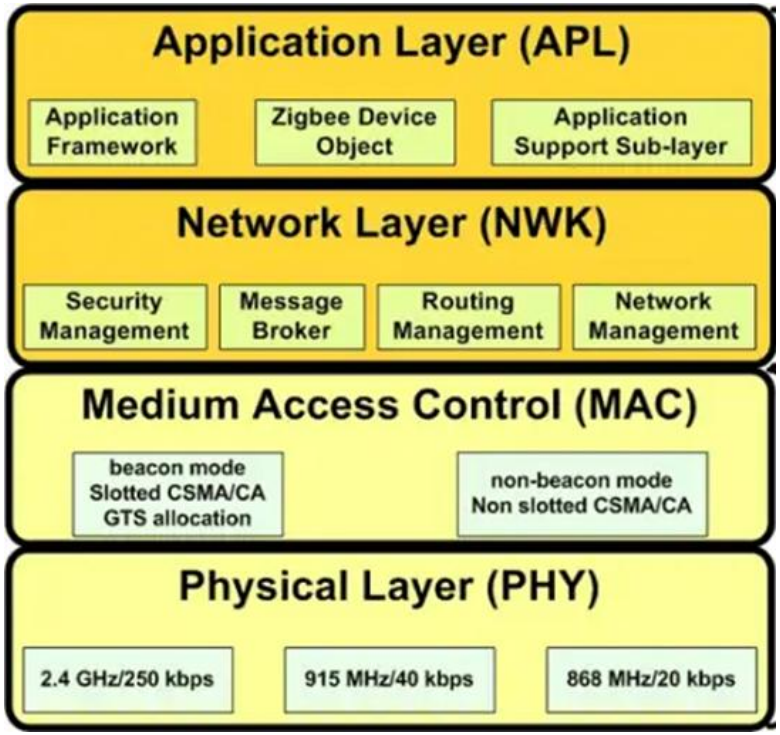
ZigBee Application Layer

- The Application Layer in Zigbee architecture consists of sub layers namely:
  - ❖ Application Support Sub Layer
  - ❖ Application Framework
  - ❖ Zigbee Device Object



- **Application Support sub layer (APS)** responsible for :
  - ✓ Maintaining binding tables
    - ✓ Binding is the connection between the endpoint on a node to one or more endpoints on other nodes.
  - ✓ Address definition, mapping and management.
    - ✓ address mapping associates a 64-bit MAC address with a ZigBee 16-bit Network address.
  - ✓ Filtering out packets
    - ✓ Coming form non-registered end devices, or
    - ✓ device profiles that don't match
  - ✓ Reassembling of the packets.
  - ✓ Providing data service to the applications
  - ✓ Performs automatic retries wherever applicable

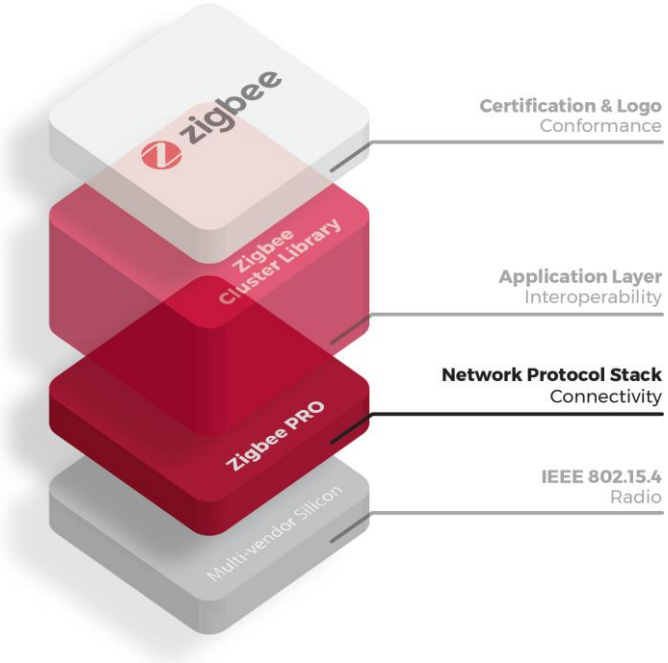
Cont…



At the application level, the standardization of functionality is addressed per market sector through application profiles (e.g., Home Automation, Smart Energy, Health Care), with the aim of allowing interoperability.

- **Application Framework**
  - ✓ Provides a framework for building and running application
  - ✓ It describes how to build an application profile on to the zigbee stack for an application
  - ✓ End points are provided with mechanism to distinguish one application from another.
- **ZigBee device object**
  - ✓ Defining role of a device within a network
  - ✓ provides local network management and over-the-air (OTA) network management
  - ✓ provides services to discover other nodes & services in the same network automatically

ZigBee Cluster Library



ZigBee Cluster Library (ZCL) is introduced in ZigBee-2006.

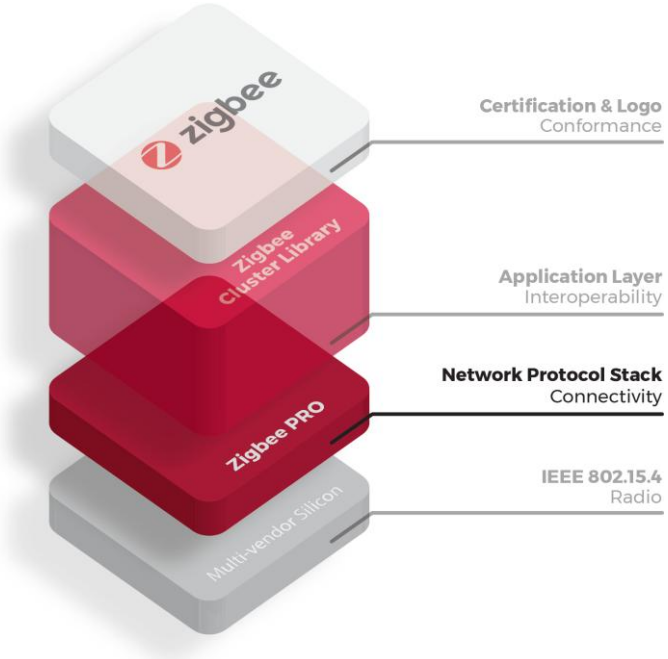
The ZCL is intended to act as a repository for cluster functionality that is developed by ZigBee

Need of ZCL: A developer constructing a new application SHOULD use the ZCL to find relevant cluster functionality that can be incorporated into the new application so as not to "re-invent the wheel"

Examples of ZCL

- *Door Lock Cluster* : provides an interface to set values representing the states of door lock.
- *Thermostat Cluster* : provides an interface for configuring and controlling the functionality of a thermostat.
- *Fan Control Cluster* : used to control the speed of a fan
- *Temperature Measurement Cluster* : provides an interface to an temperature measuring device, allowing the configuration of measuring and the reporting of measurements.

ZigBee PRO



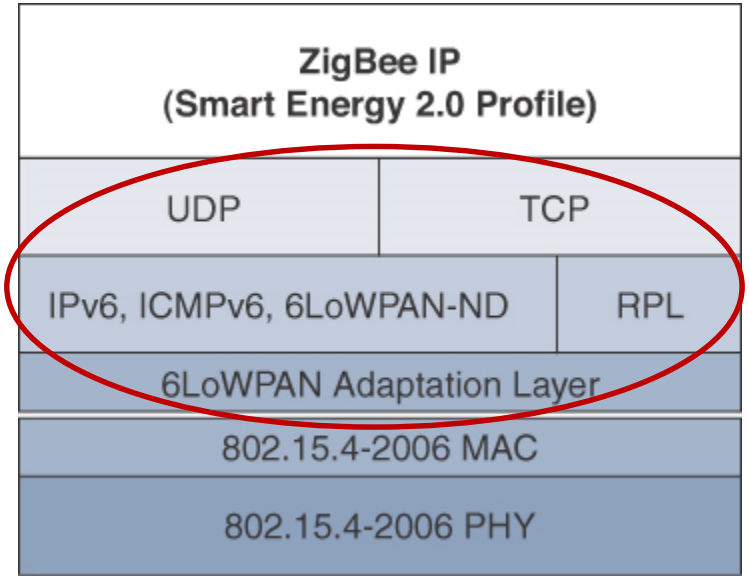
ZigBee PRO is the enhanced version of ZigBee-2006. Initially published in 2007.

ZigBee PRO Features:

- Multi-band communication across 2.4GHz and sub-GHz bands with multi PHY support
- Incorporates power saving mechanisms for all device classes,
- Discovery mechanism , Pairing mechanism with full application confirmation
- Various transmission options -- broadcast, groupcast and unicast
- Security key generation mechanism
- Utilizes the industry standard AES-128 security scheme
- Sub-GHz channels transmission ranges up to 1km.

ZigBee IP

- Initially, ZigBee did not provide interoperability with other IoT solutions or open standards
- ZigBee IP was created to embrace the open standards at the Network and Transport layers
- Open standards designed by IETF's work on LLNs, such as 6LoWPAN and RPL.
- **ZigBee IP** optimizes the standard for IPv6-based full wireless mesh networks, offering internet connections to control low-power, low-cost devices.
- ZigBee IP routes standard IPv6 traffic over IEEE 802.15.4 using 6LoWPAN header compression.



- ZigBee IP nodes support
  - ✓ IPv6,
  - ✓ ICMPv6,
  - ✓ 6LoWPAN,
  - ✓ Neighbour Discovery (ND), and
  - ✓ RPL for the routing of packets.

ZigBee RF4CE

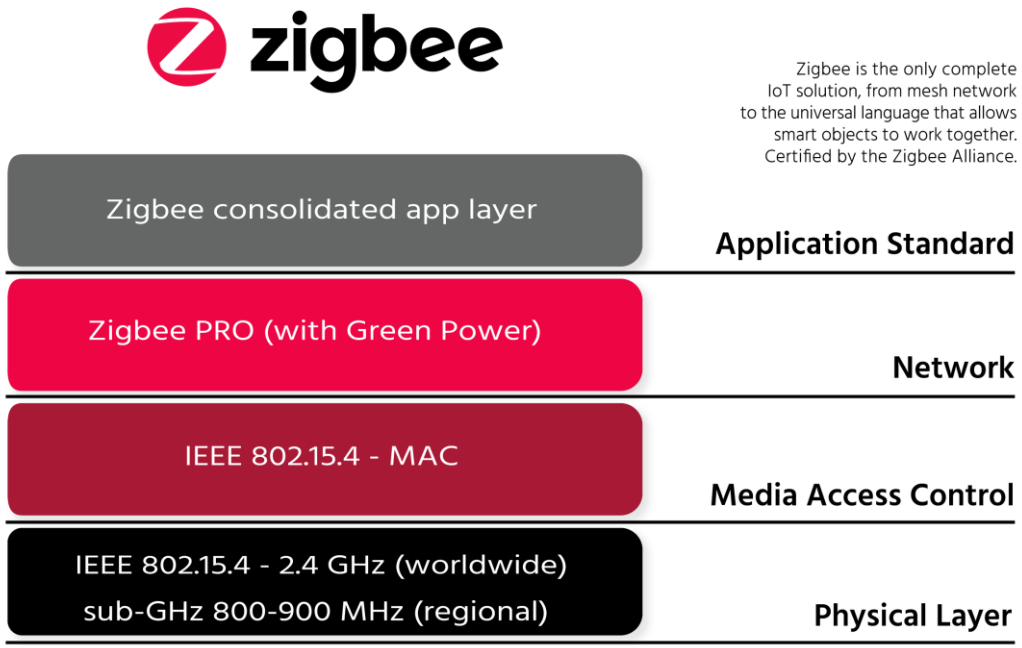
- In 2009, the Radio Frequency for Consumer Electronics (RF4CE) consortium and ZigBee Alliance agreed to deliver jointly a standard for radio frequency remote controls

- consumer electronics products, such as TVs and set-top boxes.

- Advantages:
  - richer communication,
  - increased reliability,
  - enhanced features and flexibility,
  - interoperability,
  - no line-of-sight barrier,
  - can run on smaller memory configurations in lower-cost devices

ZigBee Green Power

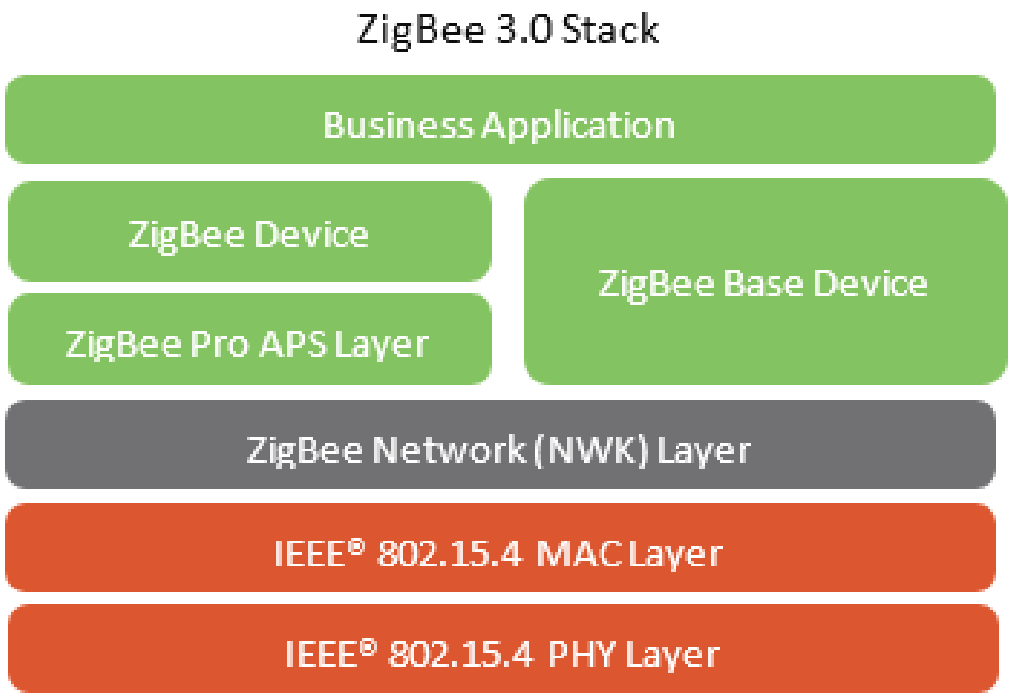
- Zigbee Green Power (ZGP) is included in the Zigbee specification
- ZGP **enables battery-less** (energy-harvesting) or ultra-long battery devices to securely join Zigbee PRO networks.
- Common ZGP devices include switches, sensors, detectors, and buttons.
- ZGP uses a new compact packet format that minimizes the amount of energy used to transmit data



- GPDF (Green Power Device Frame) is shorter than a standard ZigBee frame. This allows a GPD (Green Power Device) to transmit a GPDF using less power than a standard ZigBee frame.

ZigBee 3.0

- Aims to break the barriers between low-power wireless devices from different market sectors, to allow fully integrated networks as well as Internet connectivity
- So, it removes restrictions that prevent nodes in different application areas from participating in the same network.
- ZigBee 3.0 **redefines ZigBee PRO** to allow increased interoperability
- ZigBee 3.0 provides enhanced network security
- ZigBee 3.0 supports with large local networks of greater than 250 nodes.



The ZigBee 3.0 software stack **incorporates** a 'base device' feature that provides consistent behaviour for commissioning nodes into a network.

Source: https://www.nxp.com/docs/en/brochure/75017677.pdf

Thanks!