University of Colorado Boulder

ZigBee Protocol

Subir Kumar Padhee

Subir.Padhee@colorado.edu

Abhilash Manjunath

Abhilash.Manjunath@colorado.edu

University of Colorado Boulder

What is ZigBee?

- Wireless mesh network standard intended for use in Embedded applications
- Low-cost, Low-power, Low latency
- Operates in the industrial, scientific and medical (ISM) radio band frequencies- 2.4 GHz(Worldwide), 915 MHz(USA) and 868 MHz (Europe)
- Data rates vary from 20 kbit/s (868 MHz band) to 250 kbit/s (2.4 GHz band).
- At 2.4 GHz, the transmission range varies between 10–20 m, with obstacles between the transmitter and receiver. With direct line-of-sight, the range may go up to 1500 m.

The ZigBee Network

University of Colorado Boulder

Nodes

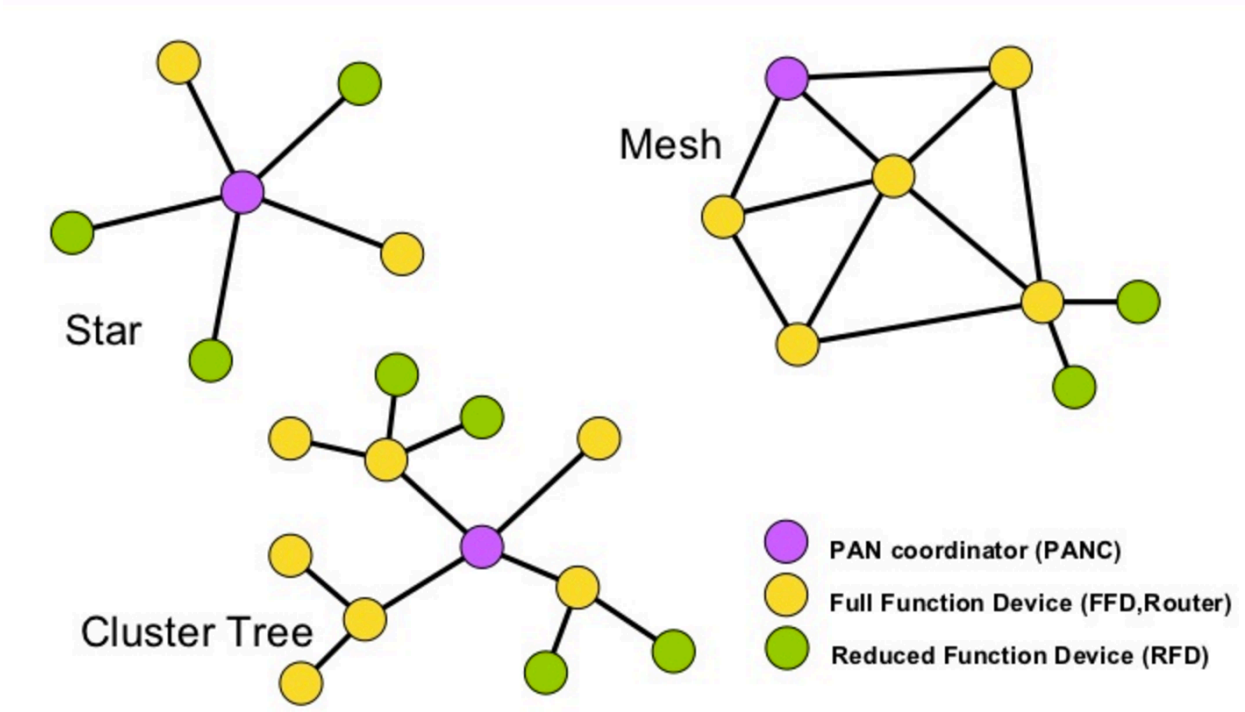
Two different device types:

- A full function device (FFD)
- A reduced function device (RFD)

FFDs can operate in three modes serving

- End device
- Router
- PAN coordinator

RFDs can only operate in one mode serving a END device



The ZigBee Network

University of Colorado Boulder

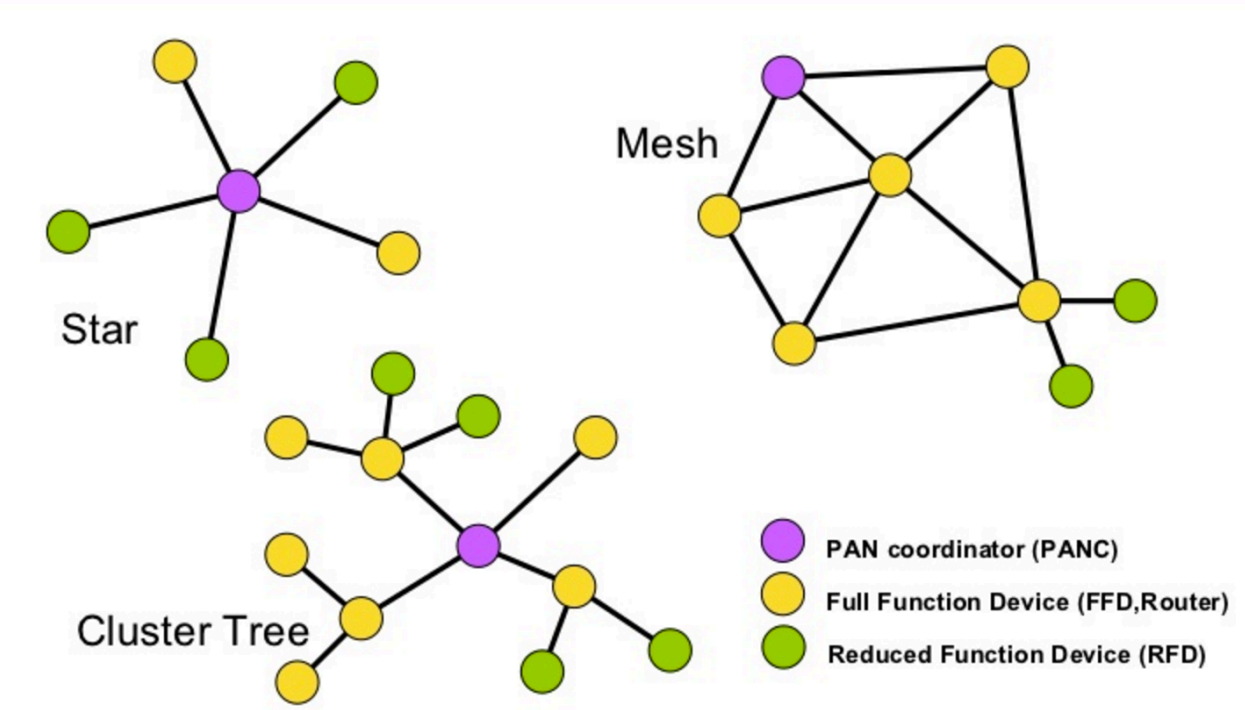
Nodes

Full function device (FFD)

- Any topology
- Network coordinator capable
- Talks to any other device

Reduced function device (RFD)

- Limited to star topology
- Cannot become a network coordinator
- Talks only to a network coordinator

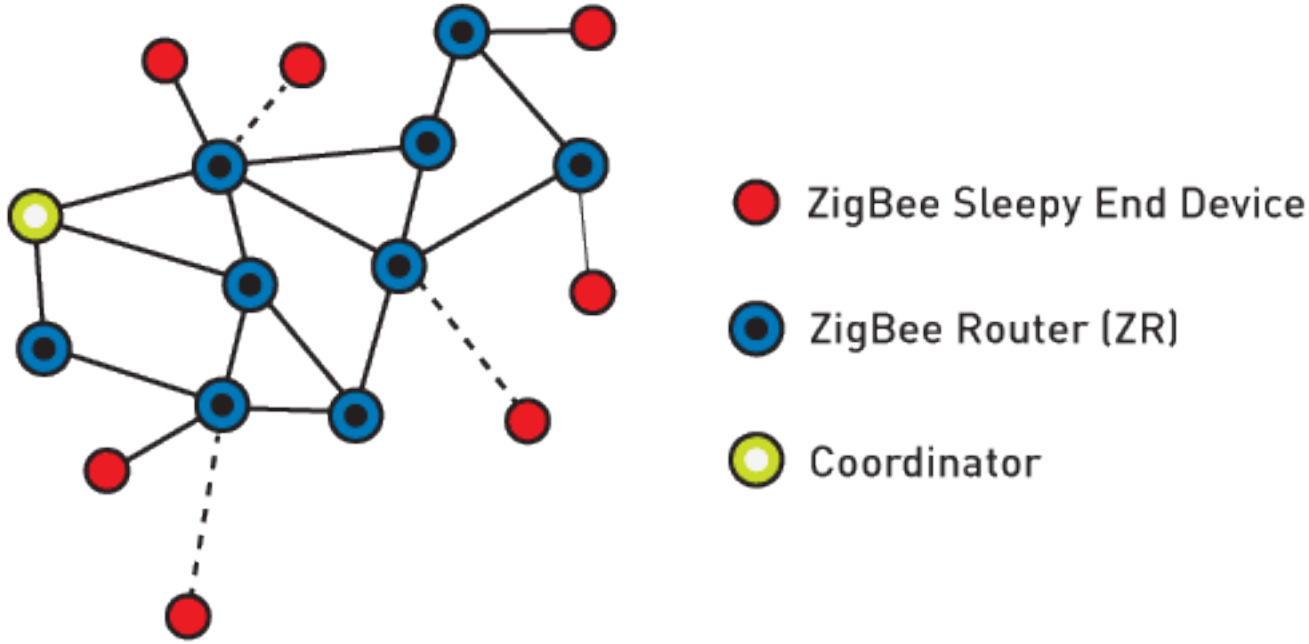


The ZigBee Network

University of Colorado Boulder

ZigBee Coordinator

- The Coordinator forms the root of the network tree and bridges to other networks.
- There is one ZigBee Coordinator in each network since it is the device that started the network.
- Stores information about the network and acts as the Trust Center & repository for security keys.

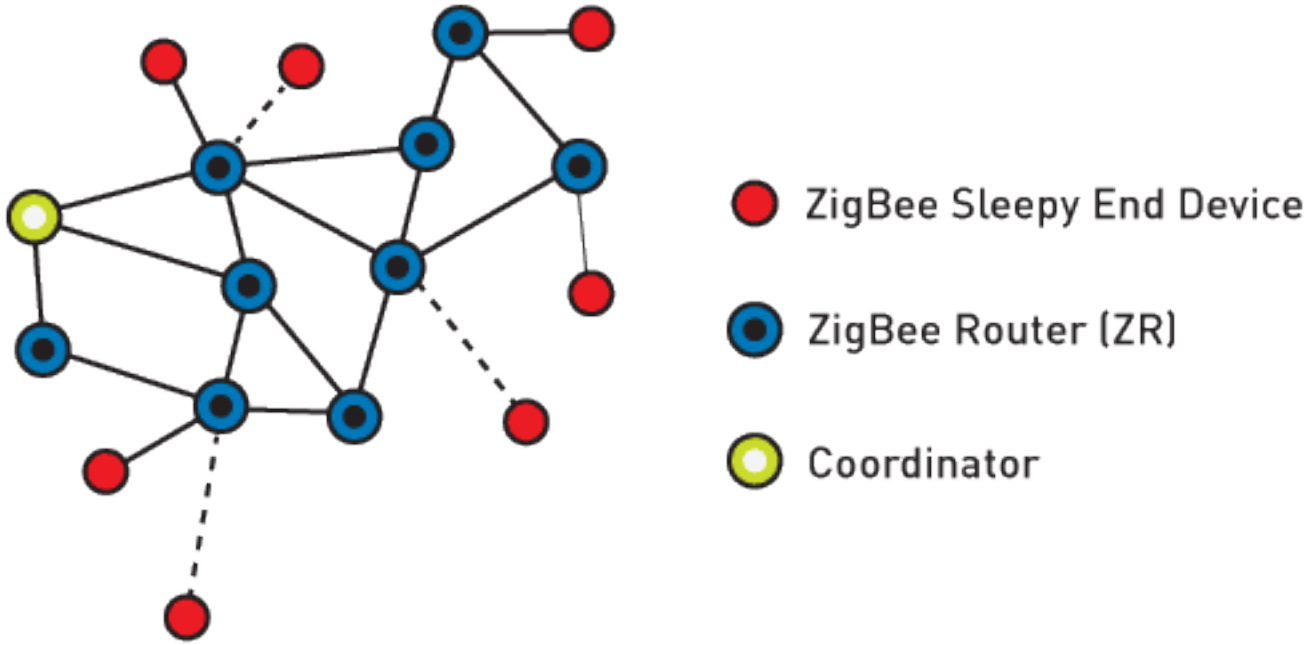


The ZigBee Network

University of Colorado Boulder

ZigBee Router

- Runs an application function, also acts as an intermediate router, passing on data from other devices.

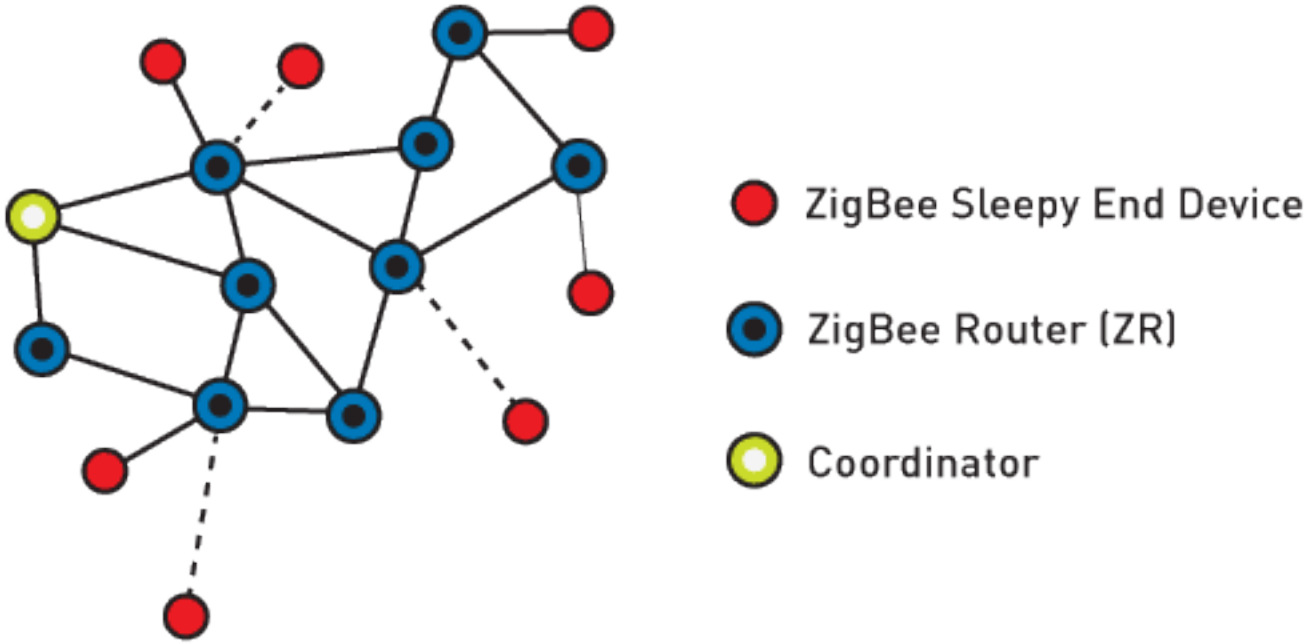


The ZigBee Network

University of Colorado Boulder

ZigBee End Device

- Talks to the parent node (Coordinator or Router).
- Cannot relay data from other devices.
- This Network architecture allows the node to be asleep a significant amount of time giving a long battery life. It also requires least amount of memory, hence is less expensive to manufacture than a Coordinator or Router.



Forming The ZigBee Network

University of Colorado Boulder

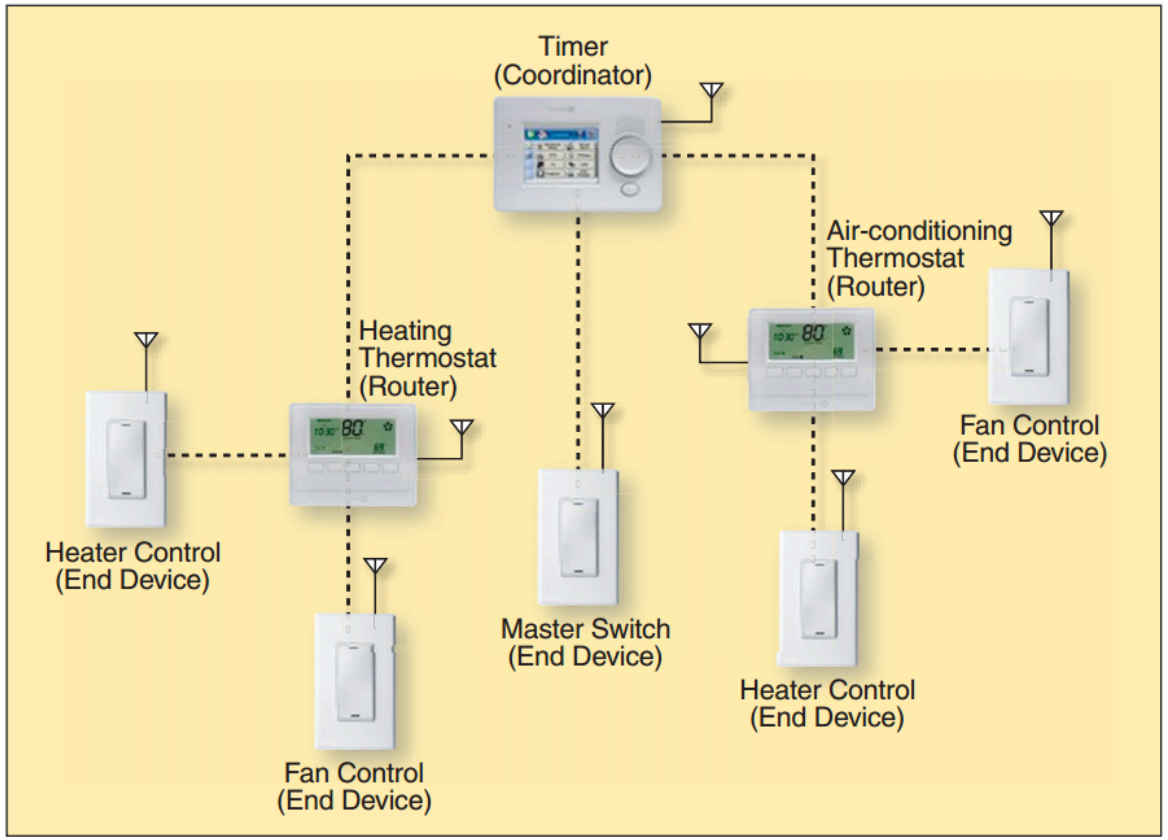
- The Coordinator searches for a suitable RF channel on all 16 channels to check which is usable and not interfering with Wireless LAN frequencies in use.
- Coordinator assigns a PAN ID to the network.
  - Manual or dynamic- obtained by checking other PAN IDs of networks already in operation nearby so that PAN ID does not conflict .
- Coordinator sends a broadcast beacon request frame on the channel (PAN scan). Coordinator receives PAN ID of routers and end devices present nearby. It also comes to know whether the Routers or End devices allow join or not.
- Routers or End devices can join by sending association request to Coordinator depending on
  - Permit joining attribute.
  - Number of end device children it already has.

The ZigBee Network- Example

University of Colorado Boulder

Home Automation Network

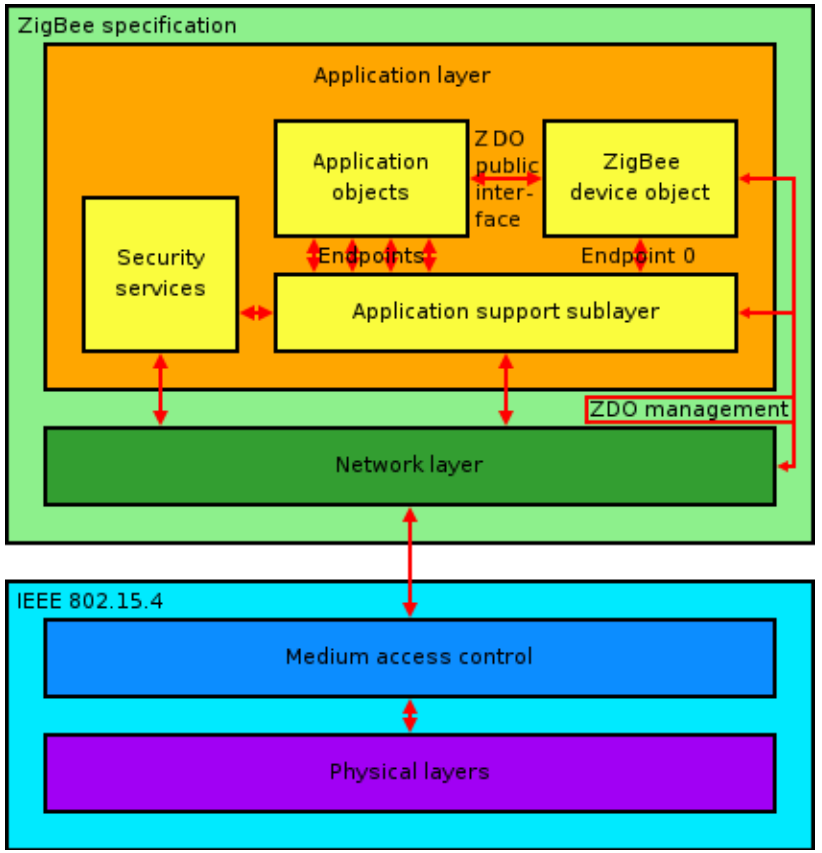
- Coordinator- Timer
- Router- Thermostats
- End devices-switches



ZigBee Protocol Stack

University of Colorado Boulder

- ZigBee builds on the physical layer and media access control defined in IEEE standard 802.15.4 for low-rate WPANs.
- While IEEE 802.15.4 governs the lower two layers, i.e. Physical and MAC Layer, ZigBee forms the logical network and application software.



ZigBee Protocol Stack

University of Colorado Boulder

Physical Layer

- The physical layer performs modulation on outgoing signals and demodulation on incoming signals.
- It transmits information and receives information from a source.
- The table shows the physical layer frequency band, data rate, and channel numbers in different Geographical regions.

Frequency Band	Country	Data Rate	Channel Numbers
868.3MHz	European countries	20Kbps	0
902-928 MHz	United States	40Kbps	1-10
2.405GHz	Worldwide	250Kbps	11-26

ZigBee Protocol Stack

University of Colorado Boulder

Media Access Control (MAC) Layer

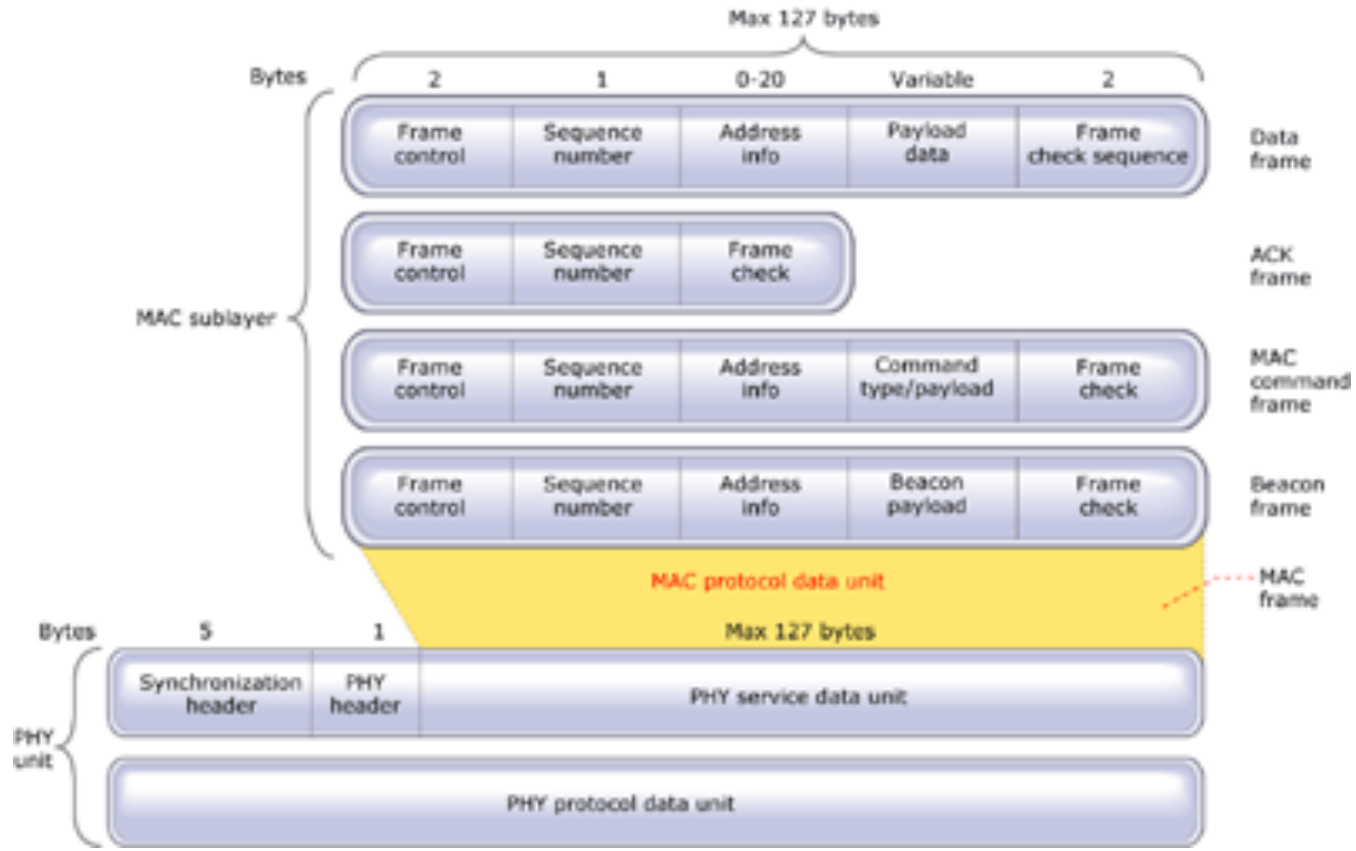
- The function of the MAC layer is to access the network by using carrier-sense multiple access with collision avoidance (CSMA/CA), to transmit frames.
- **Carrier sense multiple access with collision avoidance** (**CSMA/CA**) is a network multiple access method in which carrier sensing is used, but nodes attempt to avoid collisions by transmitting only when the channel is sensed to be "idle".
- **Carrier Sense**: prior to transmitting, a node first listens to the shared medium to determine whether another node is transmitting or not.
- **Collision Avoidance**: if another node is heard, we wait for a period of time for the node to stop transmitting before listening again for a free communications channel.

ZigBee Protocol Stack

University of Colorado Boulder

Media Access Control (MAC) Layer

- **Data frame** provides a payload of up to 104 bytes. The frame is numbered to ensure that all packets are tracked. A frame-check sequence ensures that packets are received without error. This frame structure improves reliability in difficult conditions.
- **Acknowledgment *(ACK) frame*** provides feedback from the receiver to the sender confirming that the packet was received without error.



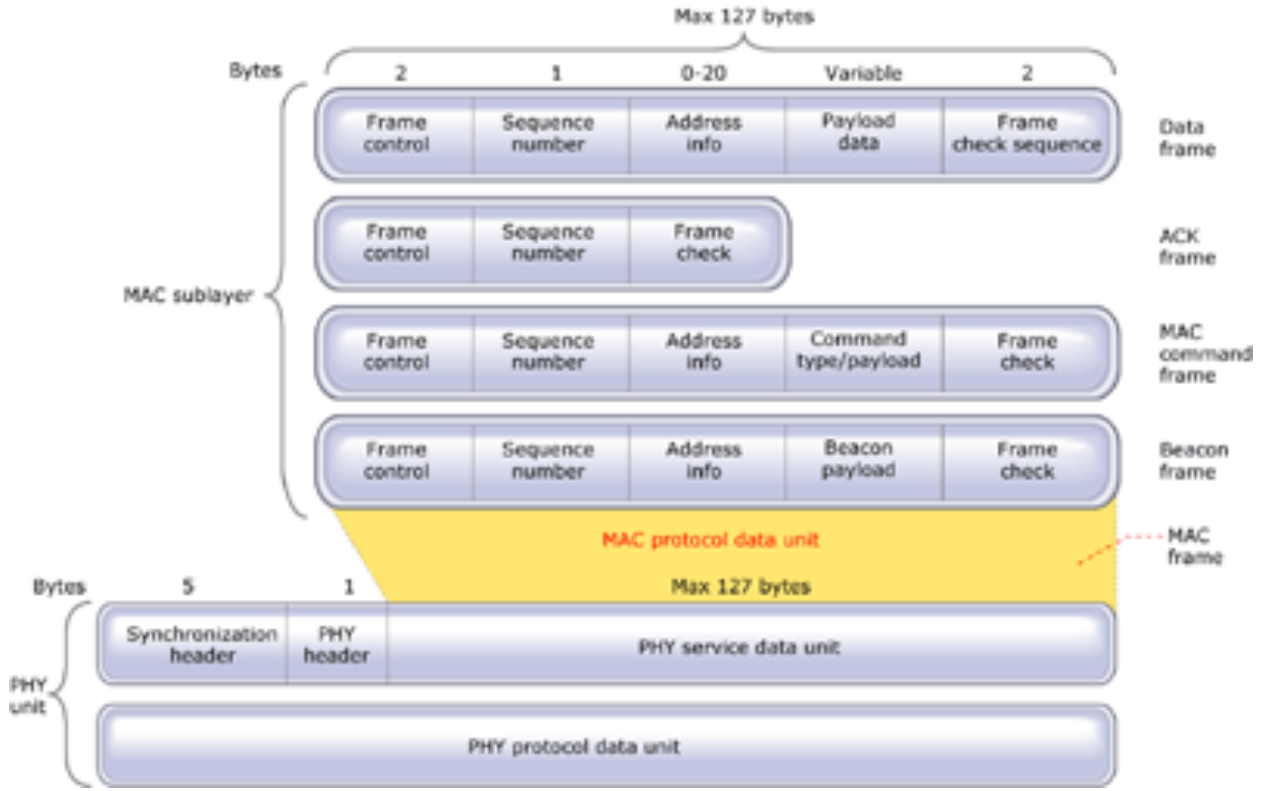
ZigBee Protocol Stack

University of Colorado Boulder

Media Access Control (MAC) Layer

- **MAC command frame** provides the mechanism for remote control and configuration of client nodes.

- **Beacon frame** wakes up client devices, which listen for their address and go back to sleep if they don't receive it.

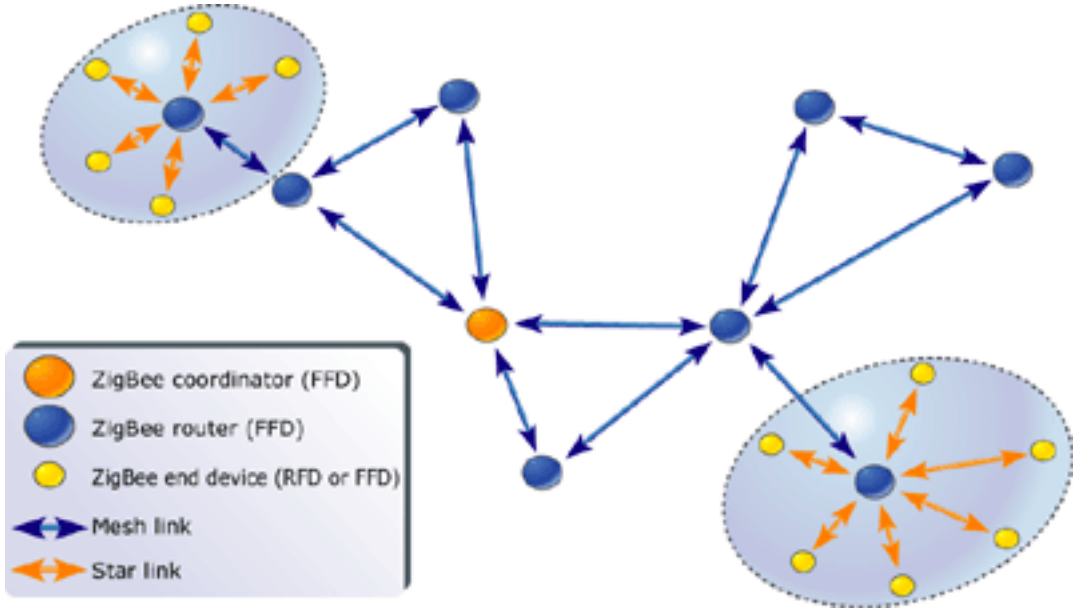


ZigBee Protocol Stack

University of Colorado Boulder

Network Layer

- The NWK layer associates or dissociates devices using the network coordinator, implements security, and routes frames to their intended destination. In addition, the NWK layer of the network coordinator is responsible for starting a new network and assigning an address to newly associated devices.
- The Network layer supports multiple network topologies including star, cluster tree, and mesh

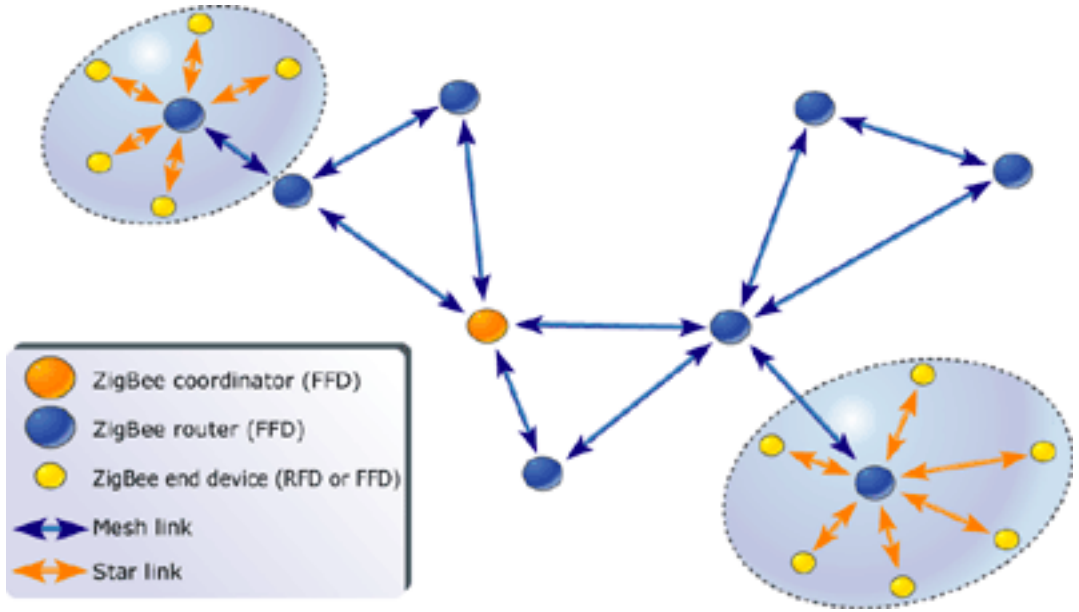


ZigBee Protocol Stack

University of Colorado Boulder

Network Layer

- The NWK layer associates or dissociates devices using the network coordinator, implements security, and routes frames to their intended destination. In addition, the NWK layer of the network coordinator is responsible for starting a new network and assigning an address to newly associated devices.
- The Network layer supports multiple network topologies including star, cluster tree, and mesh.



ZigBee Protocol Stack

University of Colorado Boulder

Application layer

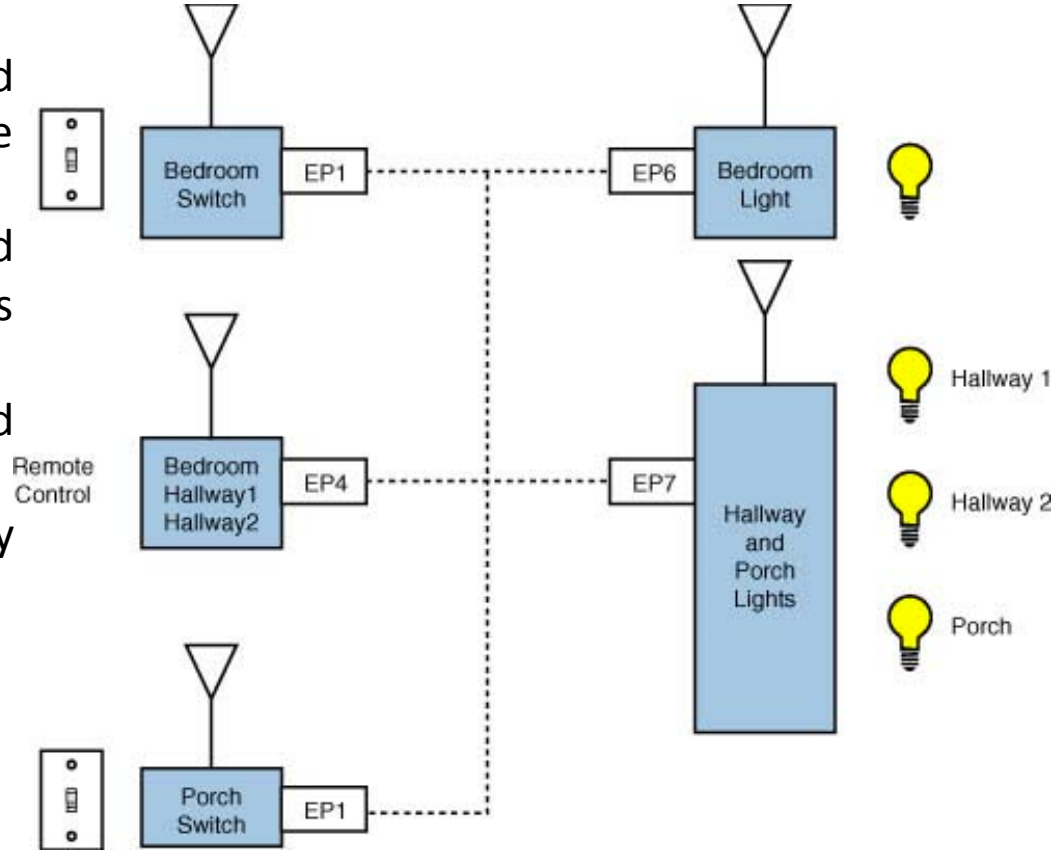
- **Application support sub layer (APS)** provides the services necessary for application objects (endpoints) and the ZigBee device object (ZDO) to interface with the network layer for data and management services.
  - Services provided by the APS to the application objects for data transfer are request, confirm, and response.

ZigBee Protocol Stack

University of Colorado Boulder

Application layer

- **Application object (endpoint):** It defines input and output to the APS. Each node can have 240 separate application objects.
- **ZigBee device object (ZDO):** It performs control and management of application objects. The ZDO performs the overall device management tasks such as
  - Determining the type of device in a network (End device, Router, or Coordinator)
  - Initializes the APS, network layer, and security service provider
  - Performs device and service discovery
  - Initializes coordinator for establishing a network
  - Security management
  - Network management



An example of home control lighting.

ZigBee Protocol Stack

University of Colorado Boulder

Application layer

ZigBee leverages the security model of the IEEE 802.15.4 MAC sublayer which specifies four security services:

- Access control—the device maintains a list of trusted devices within the network.
- Data encryption, which uses symmetric key 128-bit advanced encryption standard.
- Frame integrity to protect data from being modified by parties without cryptographic keys.
- Sequential freshness to reject data frames that have been replayed—the network controller compares the freshness value with the last known value from the device and rejects it if the freshness value has not been updated to a new value

The actual security implementation is specified by the implementer using a standardized toolbox of ZigBee security software.

ZigBee Protocol Stack

University of Colorado Boulder

Application layer

- **Router:** Each router can have multiple Application objects, each of which contains an application profile, such as home automation, and can be used to control multiple devices or a single device.
  - Actual application profiles are defined in the individual profiles of the IEEE's working groups. Each ZigBee device can support up to 30 different profiles.
  - Currently, only one profile, Commercial and Residential Lighting, is defined.
  - It includes switching and dimming load controllers, corresponding remote-control devices, and occupancy and light sensors.

ZigBee Protocol Stack

University of Colorado Boulder

Addressing

- **ZigBee addressing mode:** ZigBee uses direct, group, and broadcast addressing for transmission of information.
  - In direct addressing, two devices communicate directly with each other. This requires that the source device has both the address and endpoint of the destination device.
  - Group addressing requires that the application assign a group membership to one or more devices. A packet is then transmitted to the group address in which the destination device lies.
  - The broadcast address is used to send a packet to all devices in the network.

References

1. ZigBee™: WirelessControl Made Simple Wireless & Mobile WorldExpo NTC Toronto, CanadaMatt MaupinTechnical Marketer TMFreescale Semiconductor

2. https://www.silabs.com/products/wireless/zigbee/Pages/zigbee-software.aspx

3. http://www.embedded.com/design/connectivity/4006430/Home-networking-with-Zigbee

4. http://www.science.smith.edu/~jcardell/Courses/EGR328/Readings/ZigbeeLightSwitch.pdf

5. http://www.zigbee.org/zigbee-for-developers/network-specifications/

6. https://en.wikipedia.org/wiki/IEEE_802.15.4

7. https://en.wikipedia.org/wiki/ZigBee

8. http://www.rfwireless-world.com/Tutorials/Zigbee_tutorial.html

9. http://www.informit.com/articles/article.aspx?p=1409785&seqNum=7

10. http://www.drhdmi.eu/dictionary/ieee-802-15-4.html

11. http://www.csie.nuk.edu.tw/~lhyen/wn/zigbee_802_15_4.pdf

12. ZigBee Wireless Sensor and Control Network By Ata Elahi, Adam Gschwender Published Oct 29, 2009 by Prentice Hall.