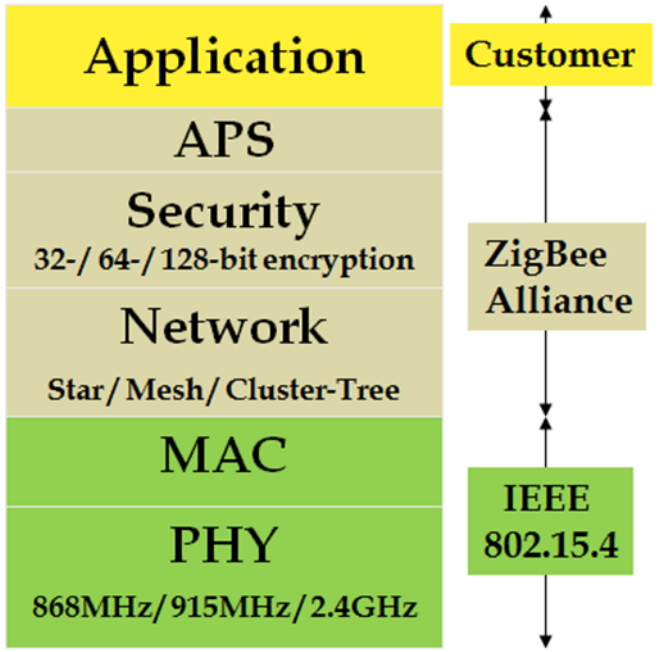
Introduction to Wireless Sensor Network Technology
IEEE 802.15.4 ZigBee Standard

Melvyn U Myint Oo
T16620
68970688
melvyn_oo@sp.edu.sg

Content

- Introduction
- ZigBee Hardware Devices
- ZigBee Logical Devices
- ZigBee Protocol Stack
- Physical (PHY) Layer
- Medium Access Control (MAC) Layer
- Network (NWK) Layer
- ZigBee Networks
- Address Assignment
- Security
- Application Layer



Introduction

- Personal Area Network (PAN)
- Short range operation, low cost sensors, low power consumption (Long battery life)
- Network Topology: Star, Mesh (Peer to Peer), Cluster tree
- Access control: Beacon or CSMA/CA
- Reliable data transfer and self healing
- Data rates: 250 kb/s (2450 MHz band), 40 kb/s (915 MHz), 20 kb/s (868 MHz)
- IEEE 802.15.4 compliance (Can be used globally)
- Promoter: ZigBee Alliance

What is ZigBee Alliance?

- An organization with a mission to define reliable, cost effective, low-power, wirelessly networked, monitoring and control products based on an open global standard
- Alliance provides interoperability, certification testing, and branding

ZigBee™ Alliance
Wireless Control That Simply Works

ZigBee Hardware Devices

Full Function Device (FFD)

- Can communicate with every type of device. A FFD can operate in three different modes
- Acts as coordinator/router
- Normal device.

Reduced Function Device (RFD)

- Can only talk to a single FFD
- Limited to star topology
- Lower power
- low cost

ZigBee Logical Devices

ZigBee Coordinator (ZC) (FFD)

- One and only one required for each ZB network
- Initiates network formation
- May act as router once network is formed
- Can communicate with every type of device and perform applications
- Sends beacon frames, provides routing information, manages short, network-specific addresses to maintain and control the network
- AC power could not sleep

ZigBee Logical Devices

ZigBee Router (ZR) (FFD)

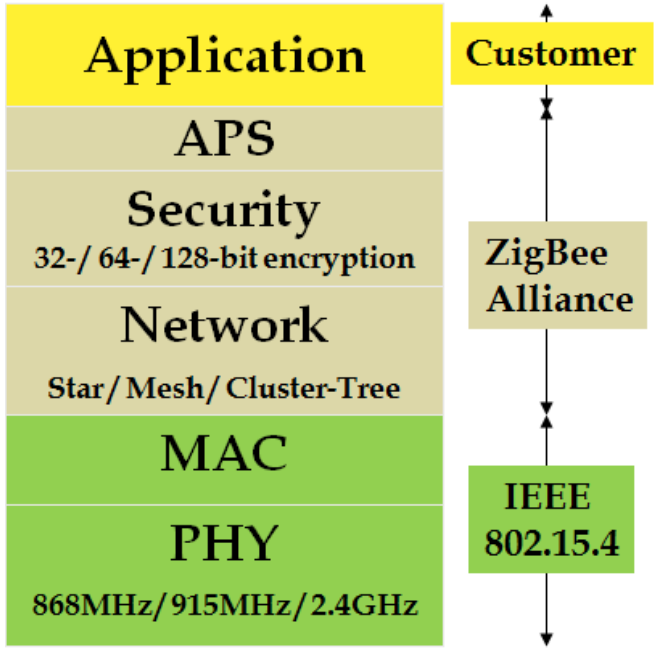
- May associate with ZC or with previously associated ZR
- Participates in multi-hop routing of messages
- Looks after its own ZEDs (broadcasting/routing)
- AC power , could not sleep

ZigBee End Device (ZED) (RFD)

- Must be connected to coordinator/router
- Shall not participate in routing
- Low power operation; put to sleep by parent

ZigBee Protocol Stack

- The IEEE 802.15.4 standard describes the physical and MAC layer.
- ZigBee Alliance builds on the IEEE standard and defines Network, Security & Application support layers, Brand management



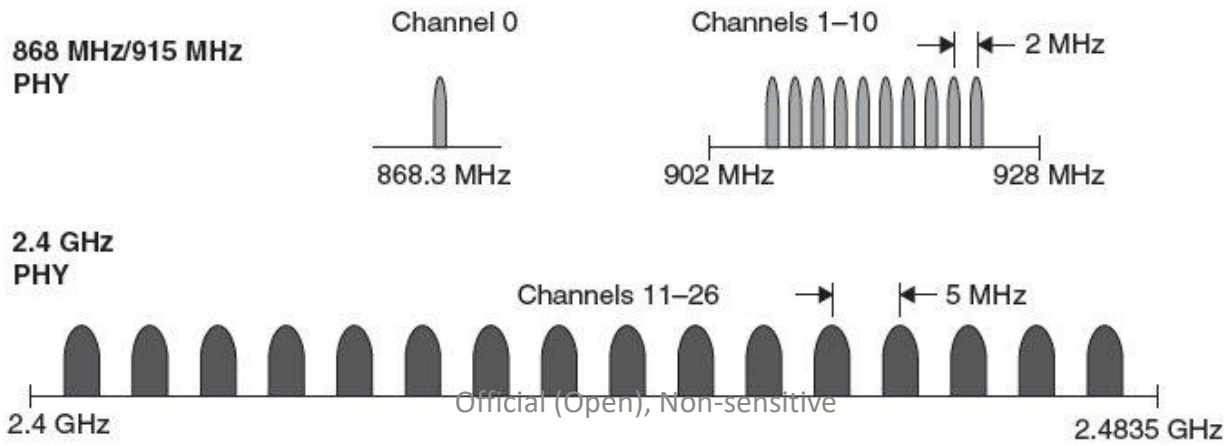
Physical (PHY) Layer

The physical layer is responsible for:

- Activation/Deactivation of transceiver.
- estimate signal strengths (energy detection) as part of CSMA mechanism
- compute link quality indicators (LQI, or SINR)
- Channel selection, assessment
- Transmission and reception of packets
- Frequency bands: 2.4 GHz (worldwide), 868.3 MHz (EU), 916 MHz (US)

Physical (PHY) Layer (cont.)

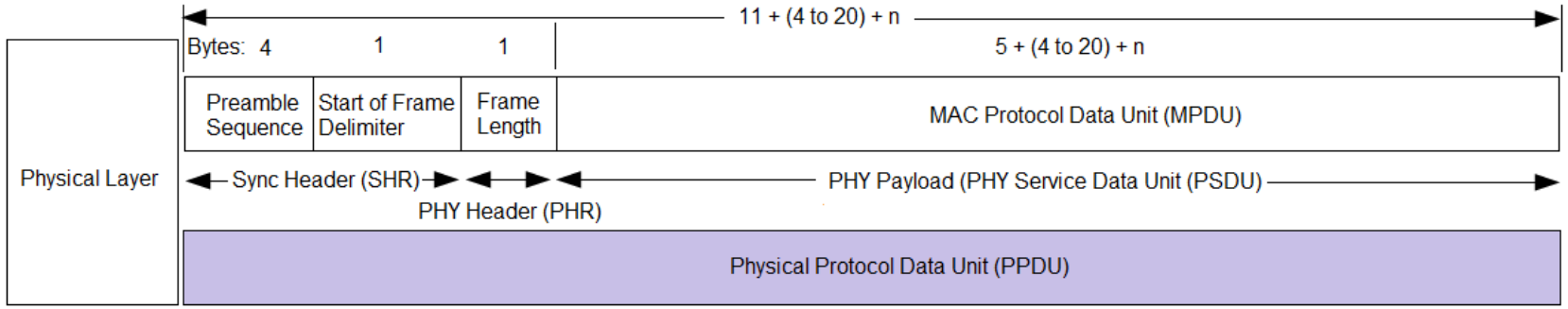
Frequency Band	Channel Number	Modulation Techniques	Physical layer Protocol	Bit Rate
868.3 MHz	0	BPSK	DSSS	20 kbps
902-928 MHz	1 to 10	BPSK	DSSS	40 kbps
2.4 – 2.4835 GHz	11 to 26	O-QPSK	DSSS	250 kbps



Physical (PHY) Layer (cont.)

PHY Frame Structure

- Preamble (32 bits) – synchronization
- Start of packet delimiter (8 bits) – signify end of preamble and shall be formatted as “11100101”
- PHY header (8 bits) – specify length of PSDU
- PSDU (≤ 127 bytes) – PHY layer payload

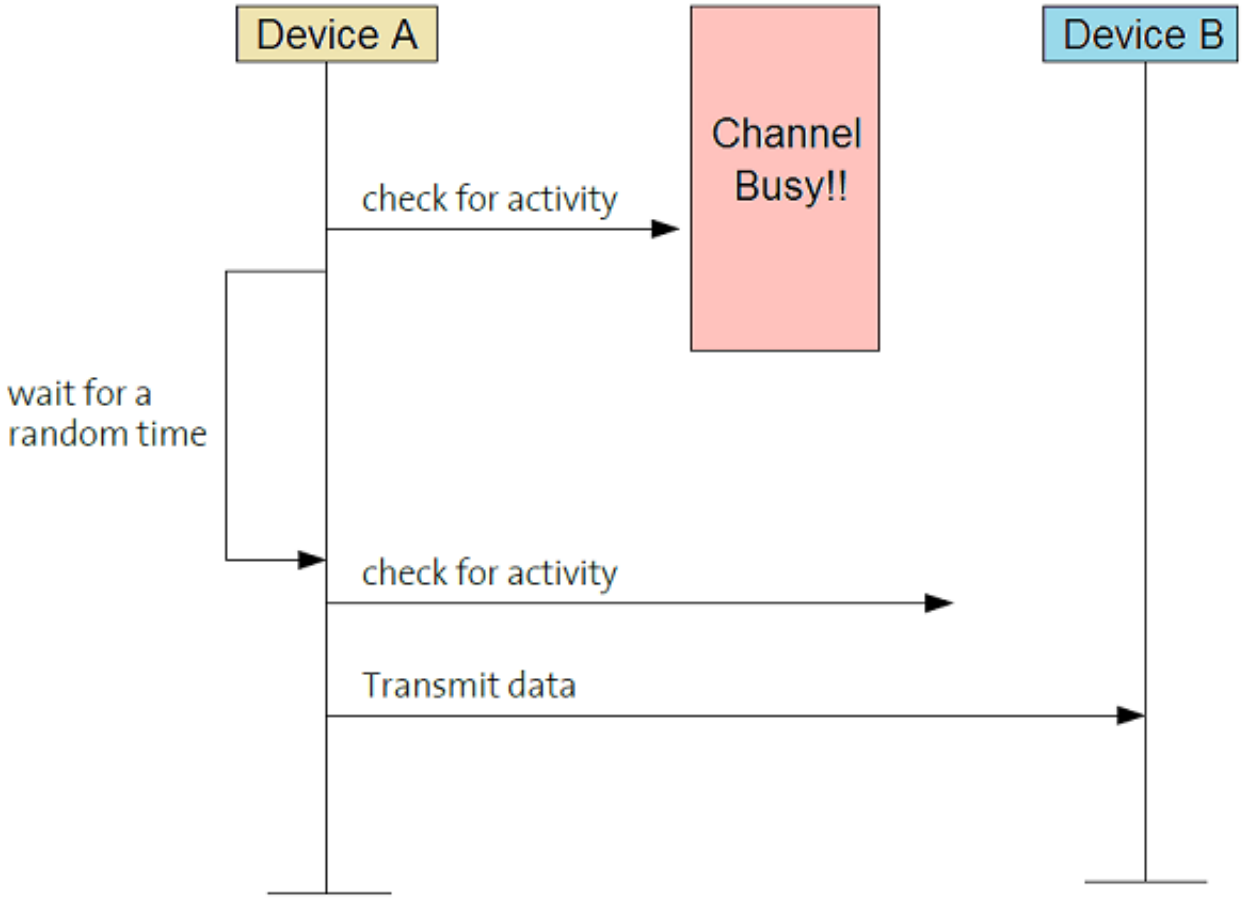


Medium Access Control (MAC) Layer

The following services are provided by the MAC layer:

- Beacon management by PAN coordinator for synchronisation
- Provide channel access to nodes in non-beacon mode using CSMA-CA
- Manage Guaranteed Time Slot (GTS) mechanism in beacon-enabled mode
- Frame Acknowledgment and validation through ARQ, CRC
- Association, disassociation

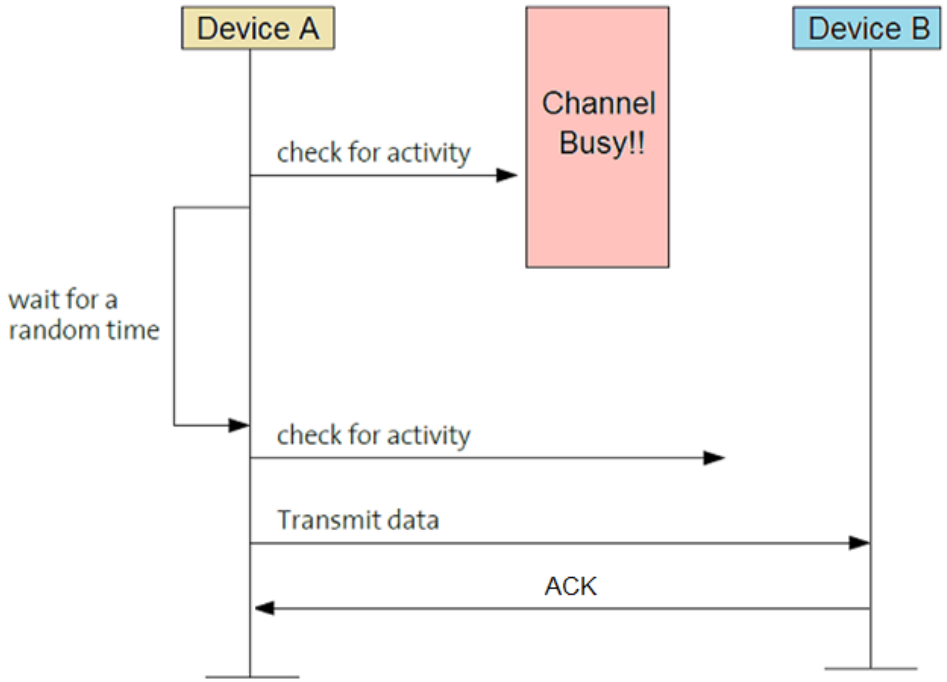
What is Media Access (CSMA/CA)?



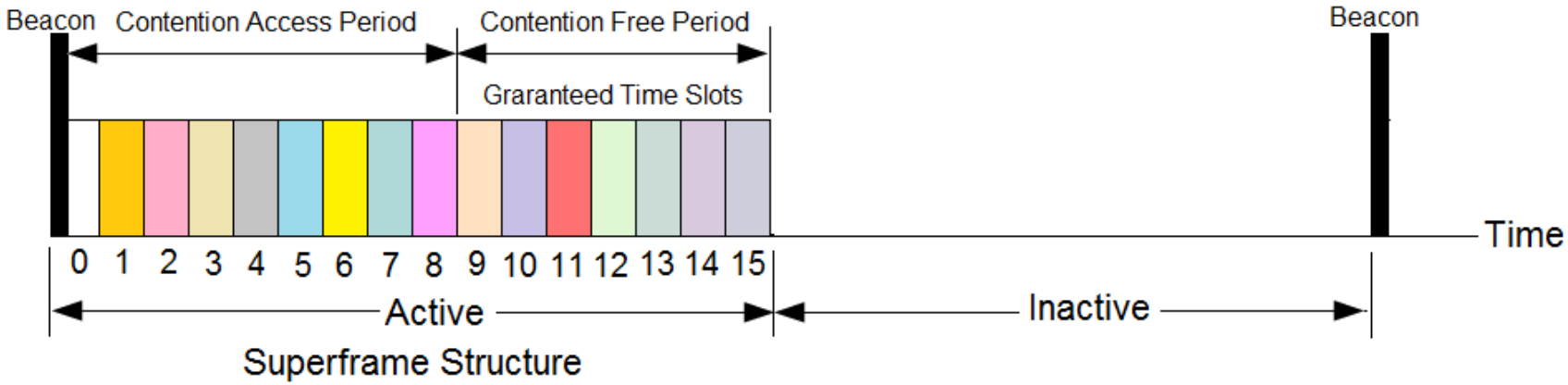
What is Media Access (CSMA/CA)?

The IEEE 802.15.4 standard describes the CSMA/CA mechanism to access the wireless channel:

- A device that wishes to transmit data frames waits for a random back-off.
- If the channel is clear after the back-off, the data is transmitted.
- If the channel is busy, the device waits for another random period.
- Acknowledgment frames are sent immediately after the corresponding data frames without using the CSMA/CA mechanism.

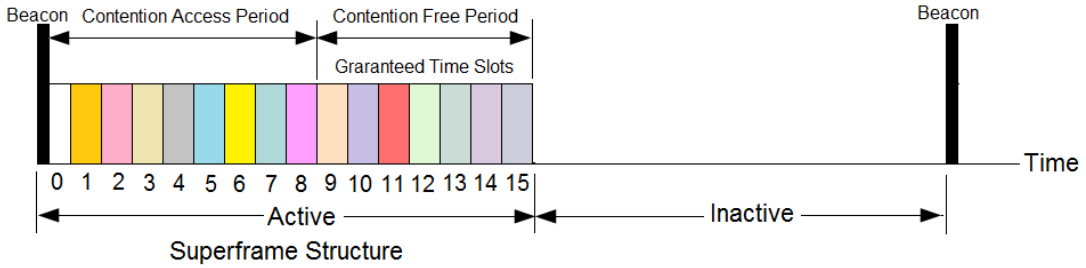


Superframe Structure in Beacon Mode



- A superframe is divided into two parts
  - Inactive: all station sleep
  - Active:
    - Active period will be divided into 16 slots
    - 16 slots can further divided into two parts
      - Contention access period
      - Contention free period

Beacon Mode



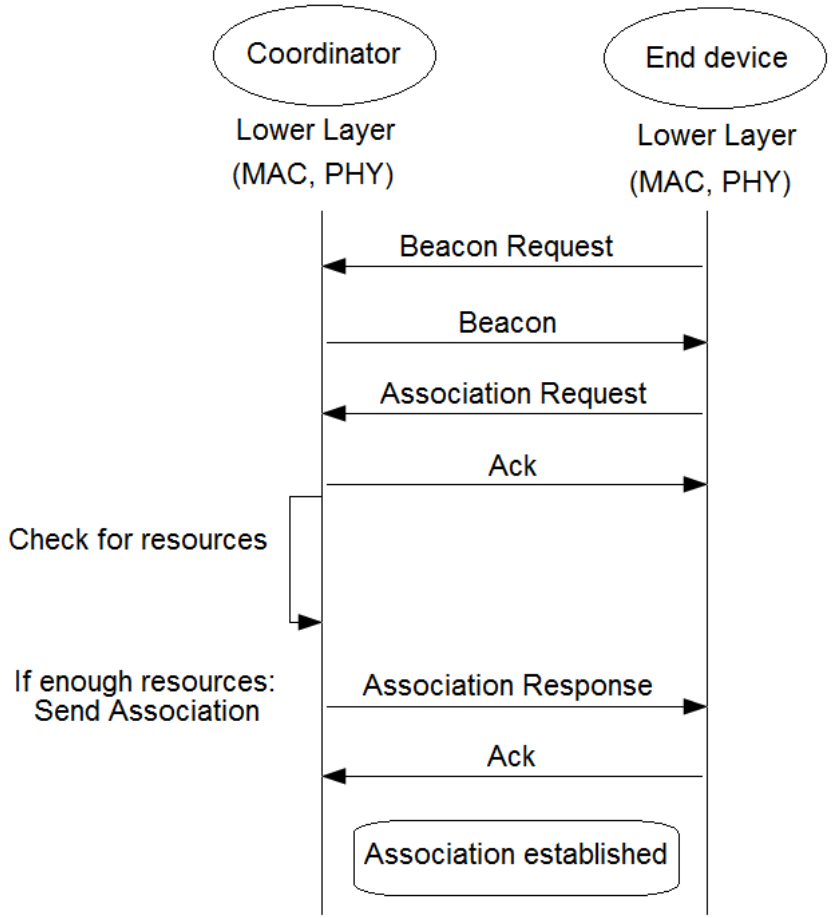
The network may also utilize the so-called beacon mode:

- Coordinator regularly sends beacon frames in the first slot.
- The beacon frames are used to synchronize the attached devices, identifies the PAN, and describes the superframe structure.
- Any device that wishes to send data uses the CSMA/CA mechanism, but aligns the sent frames to the slots (slotted CSMA/CA).
- The PAN coordinator may assign guaranteed time slots (GTS) to devices for low-latency or fixed data bandwidth.
- Up to 7 GTS can be allocated in this way at the end of the superframe.

MAC layer Association process (Active) Beacon

A device becomes a member of a PAN by associating with its coordinator:

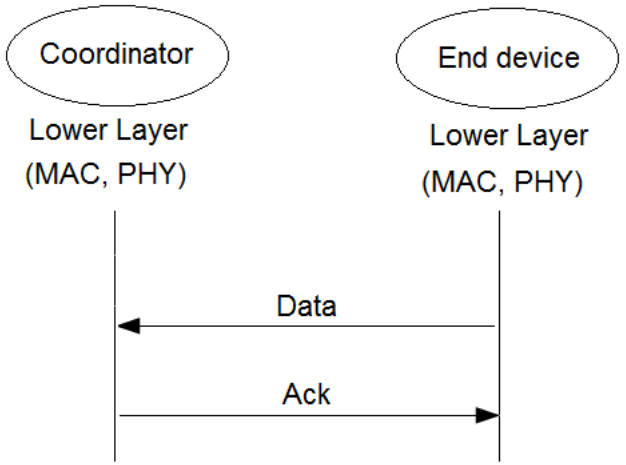
- A coordinator responds to association requests by appending devices' long addresses in beacon frames
- After associating to a coordinator, a device will be assigned a 16-bit short address



MAC layer Data transfer process (non-beacon)

Data transferred from device to coordinator:

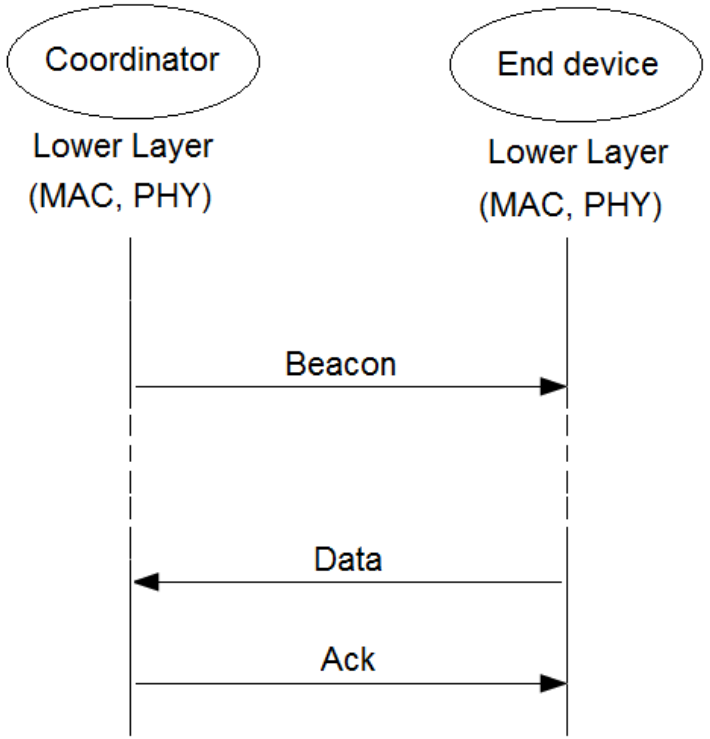
- In a non-beacon-enabled network, device simply transmits its data using unslotted CSMA/CA



MAC layer Data transfer process (beacon)

Data transferred from device to coordinator:

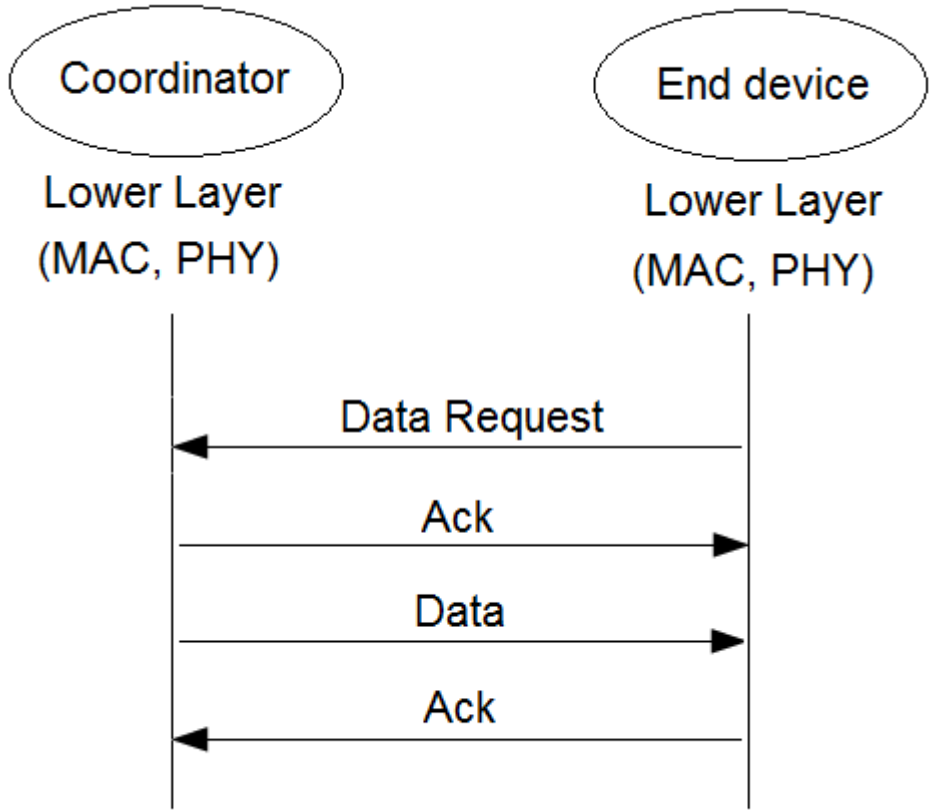
- In a beacon-enabled network, a device finds the beacon to synchronize to the superframe structure. Then it uses slotted CSMA/CA to transmit its data



MAC layer Data transfer process (non-beacon)

Data transferred from coordinator to device in a non-beacon-enabled network:

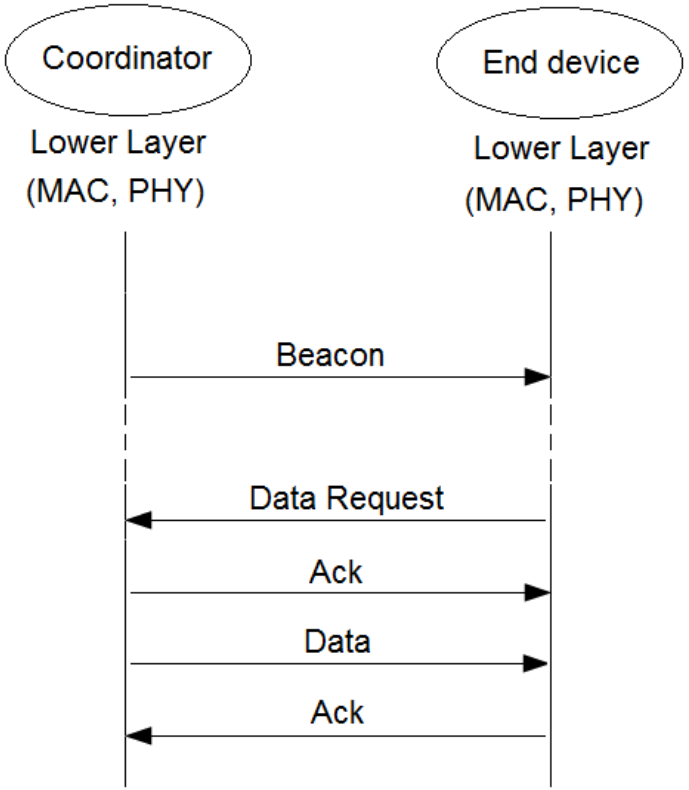
- The device transmits a Data Request using unslotted CSMA/CA.
- If the coordinator has its pending data, an ACK is replied.
- Then the coordinator transmits Data using unslotted CSMA/CA.
- If there is no pending data, a data frame with zero length payload is transmitted.



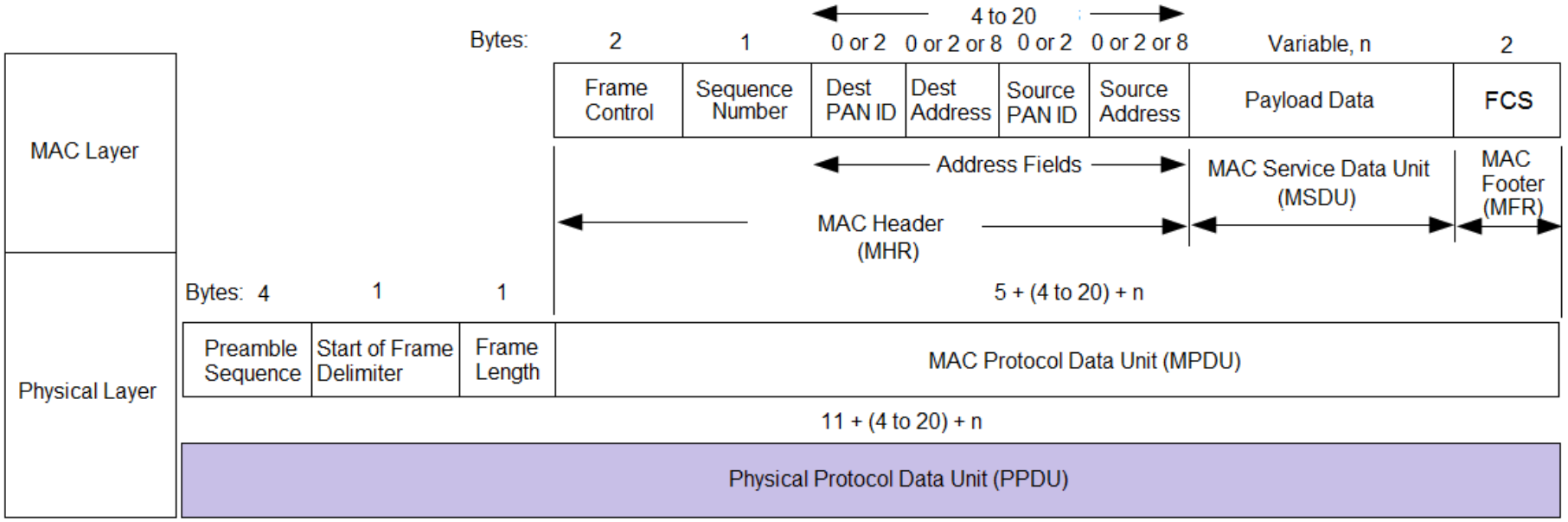
MAC layer Data transfer process (beacon)

Data transferred from coordinator to device in a beacon-enabled network:

- The coordinator indicates in the beacon that some data is pending.
- A device periodically listens to the beacon and transmits a Data Request command using slotted CSMA/CA.
- Then ACK, Data, and ACK follow …



ZigBee Packet Structure



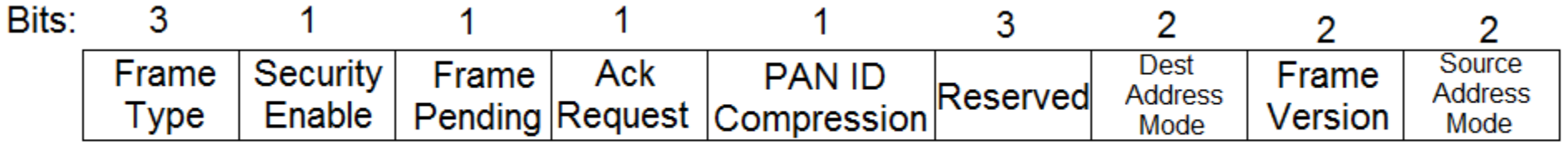
- Designed for minimum complexity
- 4 different MAC Fames <= 127 bytes
- Data frame is the most important
- Up to 104 bytes payload
- FCS : Frame Check Sequence for error detection

Frame Type (3 bits in Frame control fields)

- 000 Beacon Frame (Generated by coordinator for synchronisation)
- 001 Data frame (Used for transferring data)
- 010 Acknowledge frame (Acknowledges successful reception of the frame, No payload)
- 011 Command frame (Used by MAC layer management)
- 00 -111 Reserved

Frame Control Field

- Indicates the type of MAC frame being transmitted.
- Specifies the format of the address field and controls the acknowledgment.
- Multiple address types: 64 bit physical address and short 16 bit network address are provided.
- Address field size may vary from 0 to 20 bytes.



Frame Control Field

Frame Types

The IEEE 802.15.4 standard defines four different frame types:

- A beacon frame: Sent by the coordinator to announce the network and contains the superframe structure.
- A data frame: Used for data transfer
- An acknowledgment frame: To confirm the successful reception of a frame.
- A MAC command frame: For handling MAC peer entity control transfers.

Network (NWK) Layer

The lower level of the ZigBee protocol builds on the MAC layer of IEEE 802.15.4.

- Topology specific routing
- Security
- New device configuration
- Network startup

Network (NWK) Layer (cont.)

Joining/leaving a network

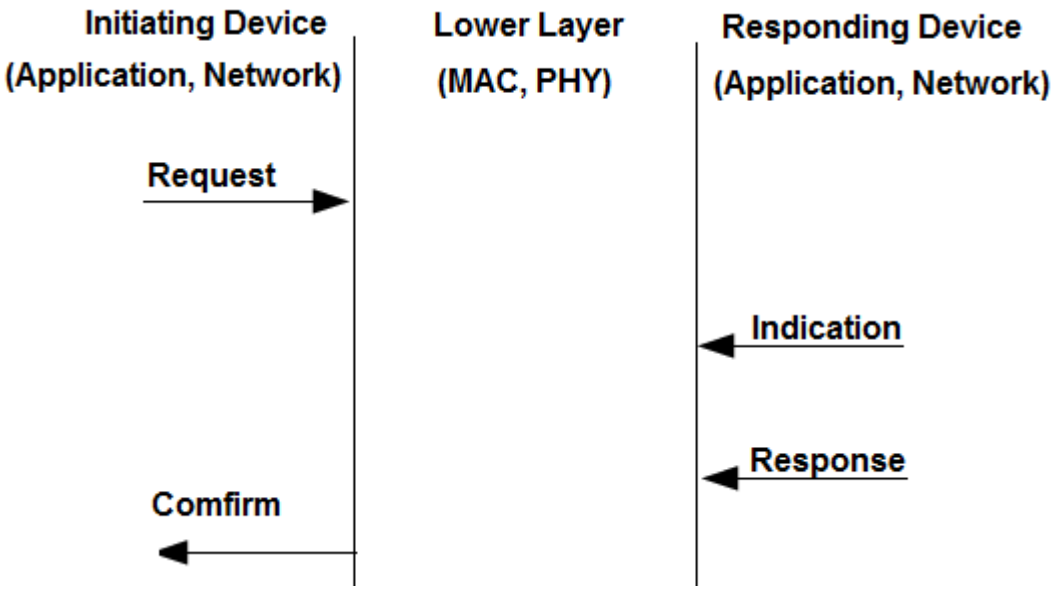
- Addressing
- Neighbour discovery
- Route discovery
- Reception control

Service Primitives

Defines the communication between different layers of the protocol:

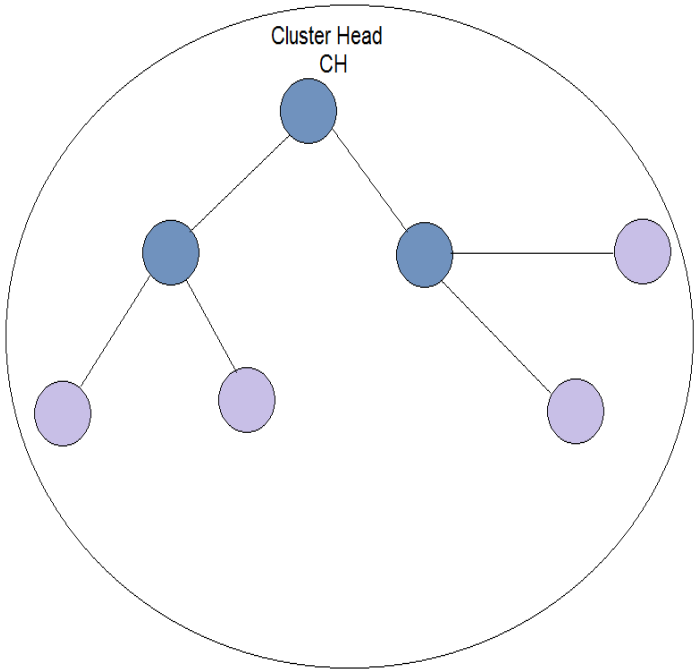
- Request: Passed from user to the underlying layer to initiate a service.
- Indication: To indicate an internal event that is significant to the user.
- Response: To complete a procedure invoked by an Indication primitive.
- Confirm: Passed to the user application to convey the results of a previous service request.

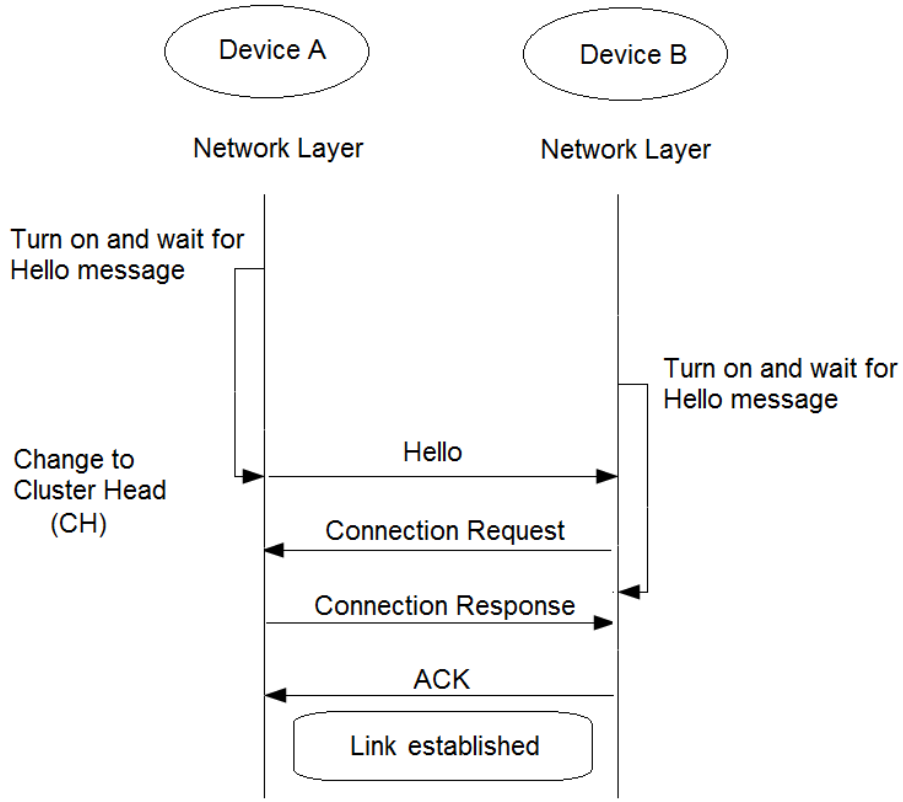
Service Primitives (cont.)



Network layer

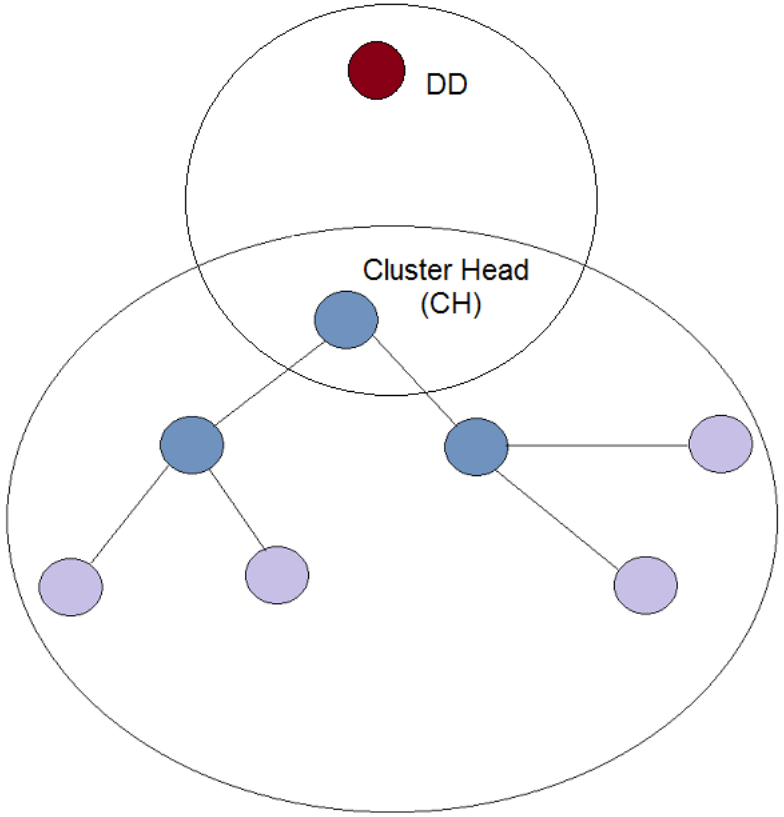
Routing for Single Cluster Network

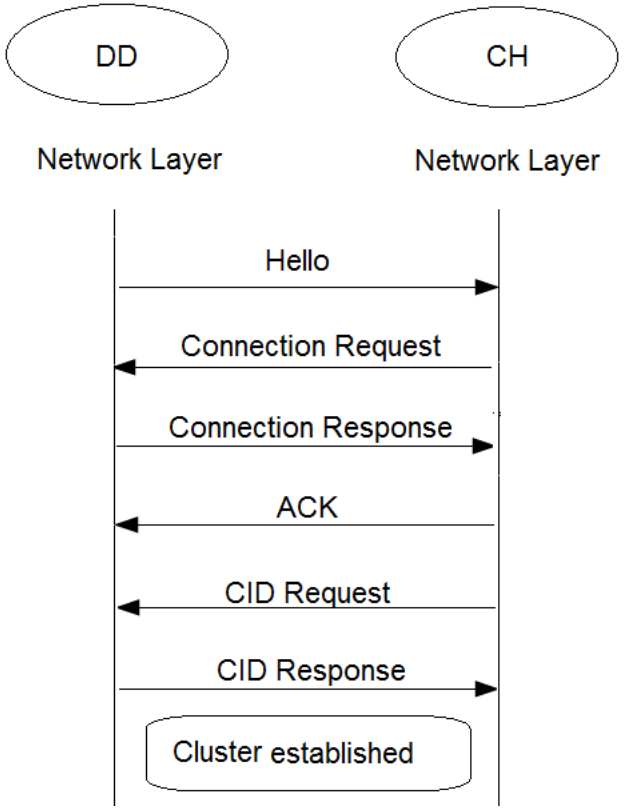




Network layer

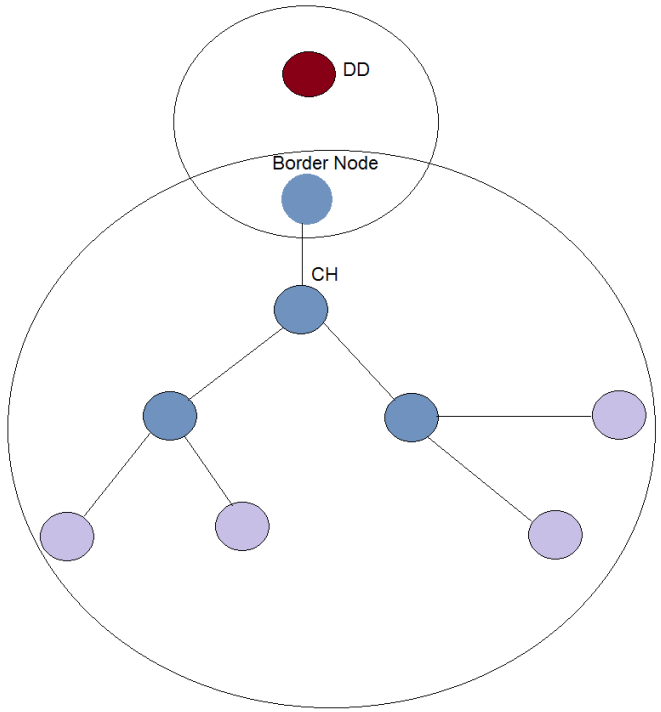
Routing for Multi Cluster Network

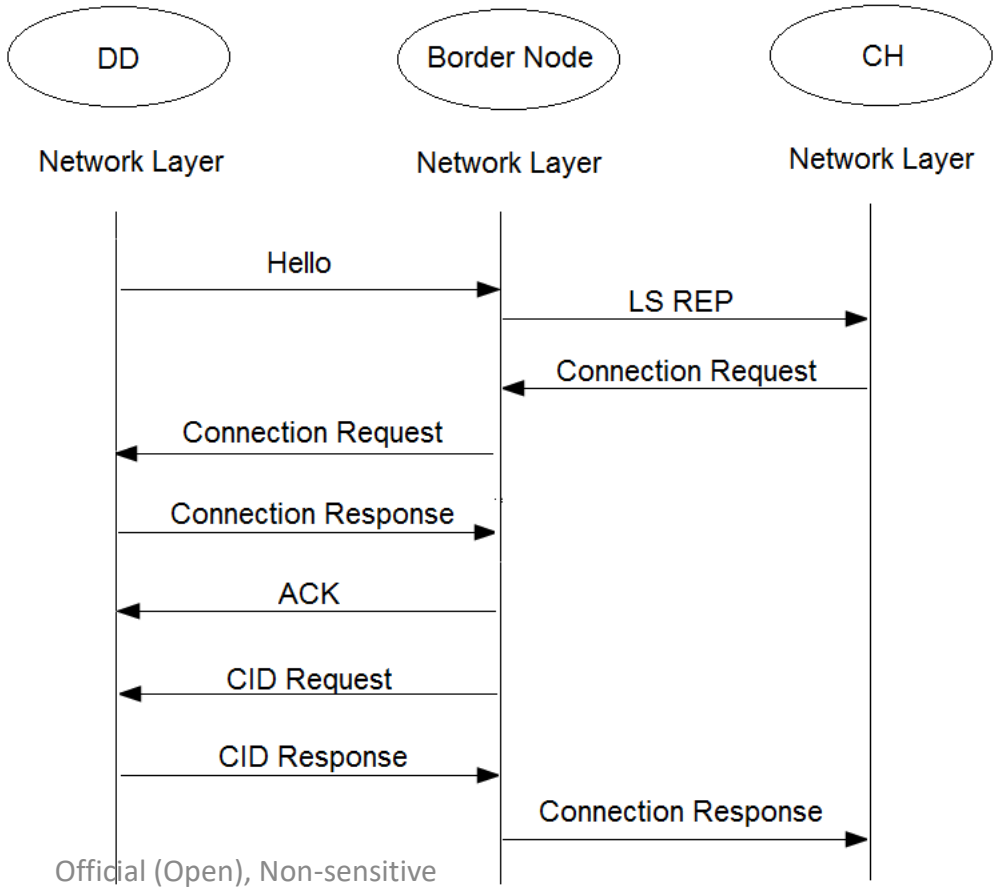




Network layer

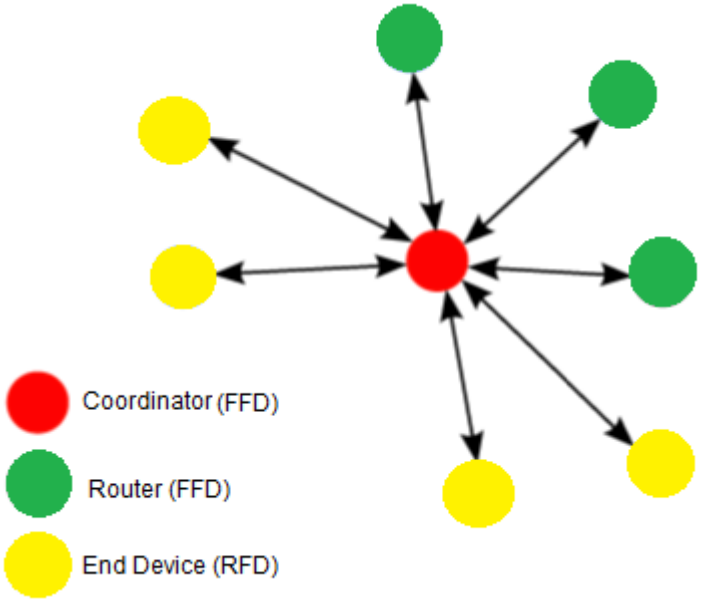
Routing for Multi Cluster Network





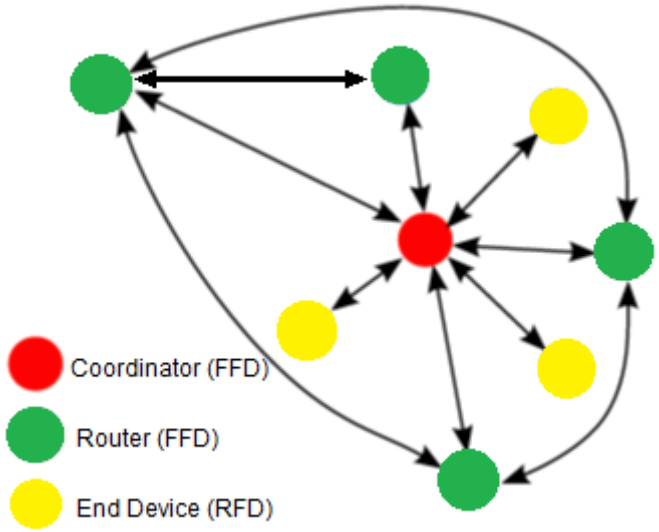
Star Network

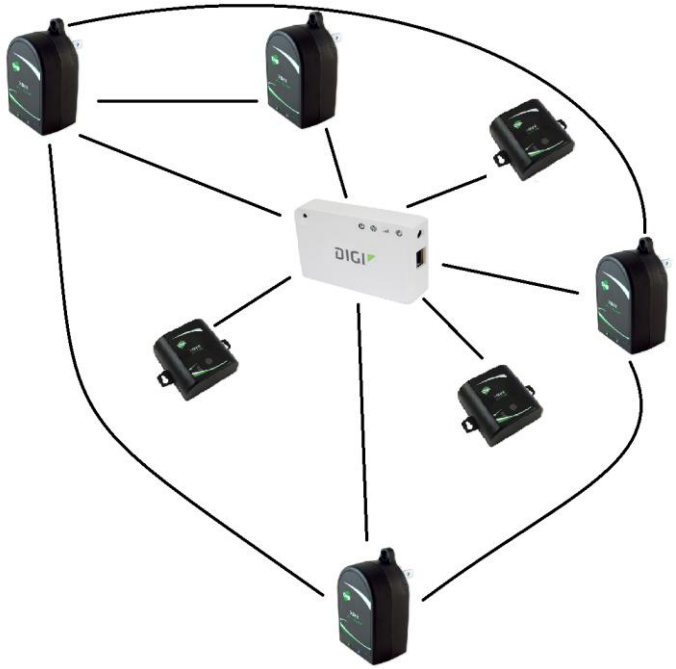
- In the star topology, the PAN coordinator chooses a unique (within its radio sphere of influence) PAN id. All attached nodes can only talk to the central PAN coordinator.



Mesh (Peer-to-Peer) Network

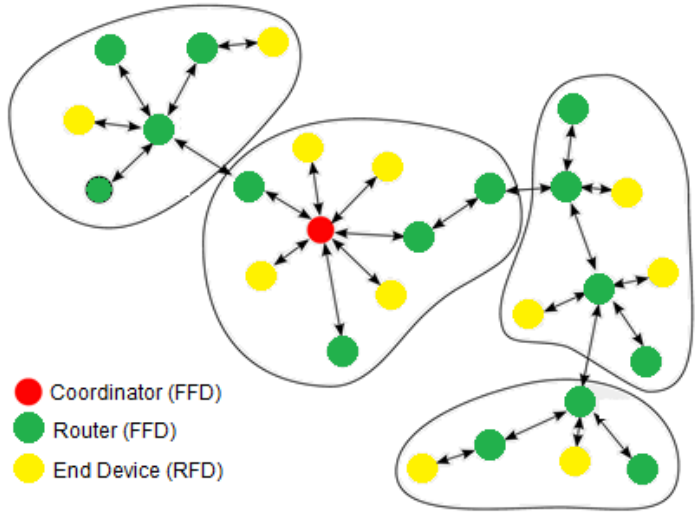
- Within a peer-to-peer topology, each FFD can communicate with any other device within its range. A RFD may only communicate with a single FFD at a given time.

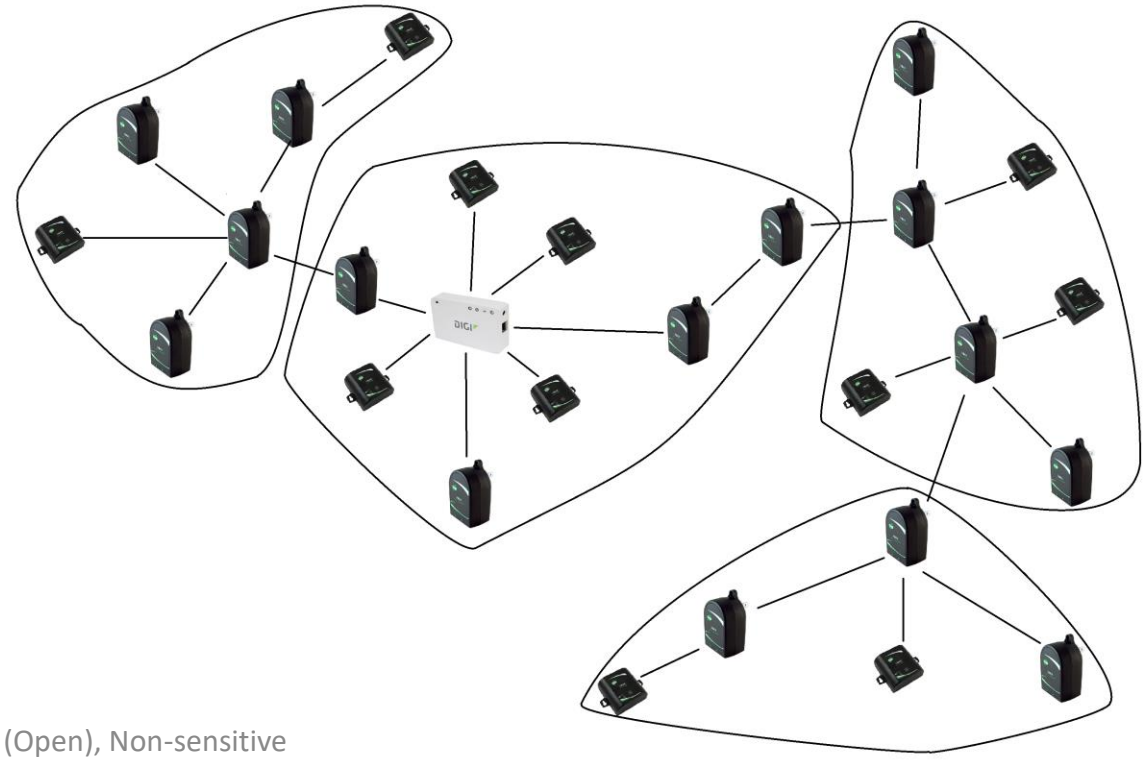




Cluster Tree Network

- Larger networks may be established by forming multi-cluster topologies. Each cluster has a single cluster head that is responsible for coordination within the cluster.





Comparison among ZigBee Networks

	Pros	Cons
Star	1. Easy to synchronize 2. Support low power operation 3. Low latency	1. Small scale 2. Solely Dependent on Coordinator as network master
Tree	1. Low routing cost 2. Can form superframes to support sleep mode 3. Allow multihop communication	1. Route reconstruction is costly 2. Latency may be quite long
Mesh	1. Robust multihop communication 2. Network is more flexible 3. Lower latency	1. Cannot form superframes (and thus cannot support sleep mode) 2. Route discovery is costly 3. Needs storage for routing table

Addressing

- Each ZigBee node has a unique 64 bit MAC address
- Additionally the Coordinator maintains a table to map the 64 bit addresses to network-specific 16 bit addresses
- Within each node, the application can define up to 240 Application endpoints.

ZigBee Security

3 Security Levels

- Insecure
- Access control list (ACL)
- Symmetric Encryption

Advanced Encryption Standards (AES) 128 bit

- Confidentiality
- Integrity
- Authenticity

Application Support Layer

The application layer provides the following services:

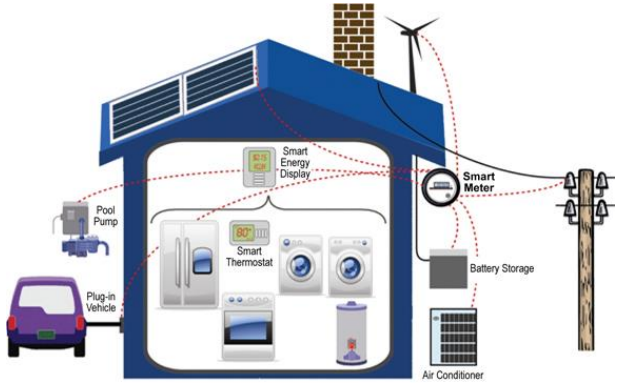
- Maintain tables for binding
- Fragmentation, reassembly and reliable data transport
- Provide communication endpoints for the application
- Discovering devices and application services.
- Initiating/responding to binding requests between endpoints

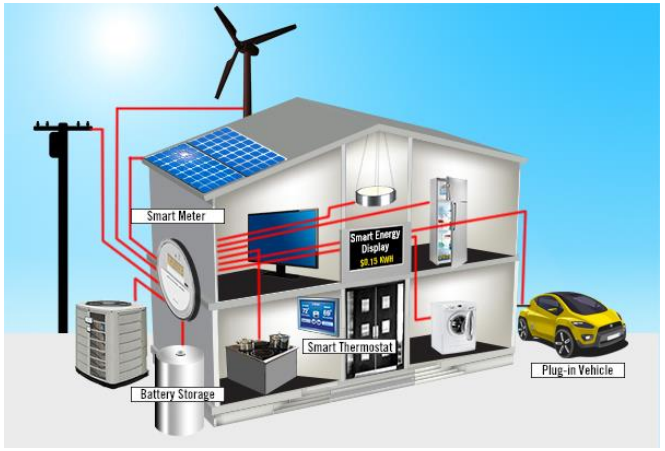
ZigBee Application Examples

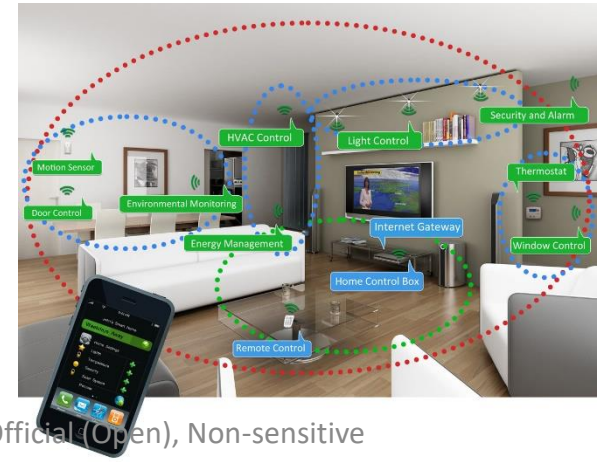
Building automation
- Lighting control (light sensors, dimmers)
- Heating control
- Air-condition control

Smart Home control

Remote Control for consumer electronic







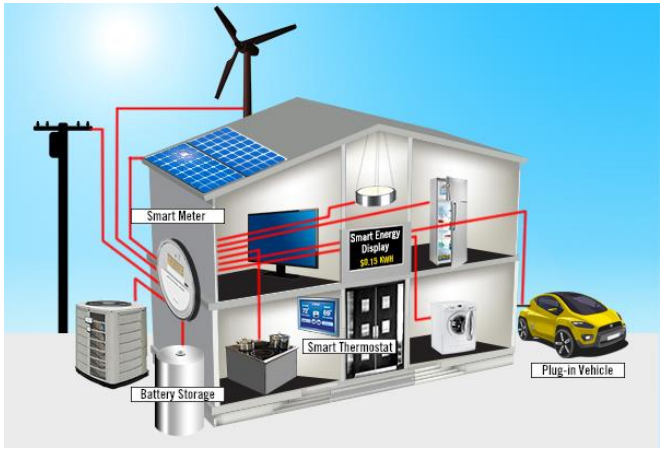
ZigBee Application Areas

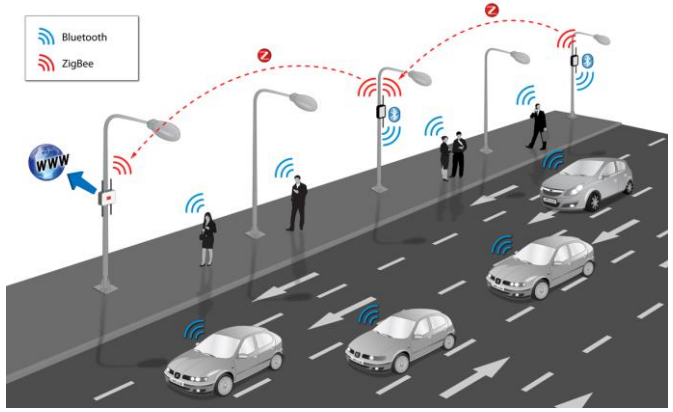
Industrial and Commercial
- Monitors
- Movement Sensors
- Automation

Personal Healthcare
- Patient monitors
- Remote Diagnosis
- Data loggers

Building Automation
- Security
- Lighting
- Fire and Safety systems

Automotive
- Service controls
- Inventory tracking





References

ZigBee Wireless Sensor and Control Network, Ata Elahi, Ph.D. with Adam Gschwender, Prentice Hall, 2010, Call No. TK5103.485 Ela.

http://zigbeewiki.anaren.com/index.php/Channel

http://www.digikey.com/en/articles/techzone/2012/apr/modular-choices-simplify-and-futureproof-m2m-wifi-and-zigbee-connectivity

http://www.dcg.ethz.ch/lectures/ws0506/seminar/materials/zb_slides.pdf

http://people.cs.nctu.edu.tw/~yctseng/papers.pub/book-zigbee.pdf

Design, deployment and performance of 4G-LTE networks : a practical approach / Ayman ElNashar, Mohamed A. El-saidny, Mahmoud Sherif, Call No. TK5103.2 Eln, Johon Wiley & Sons, Ltd, 2014.