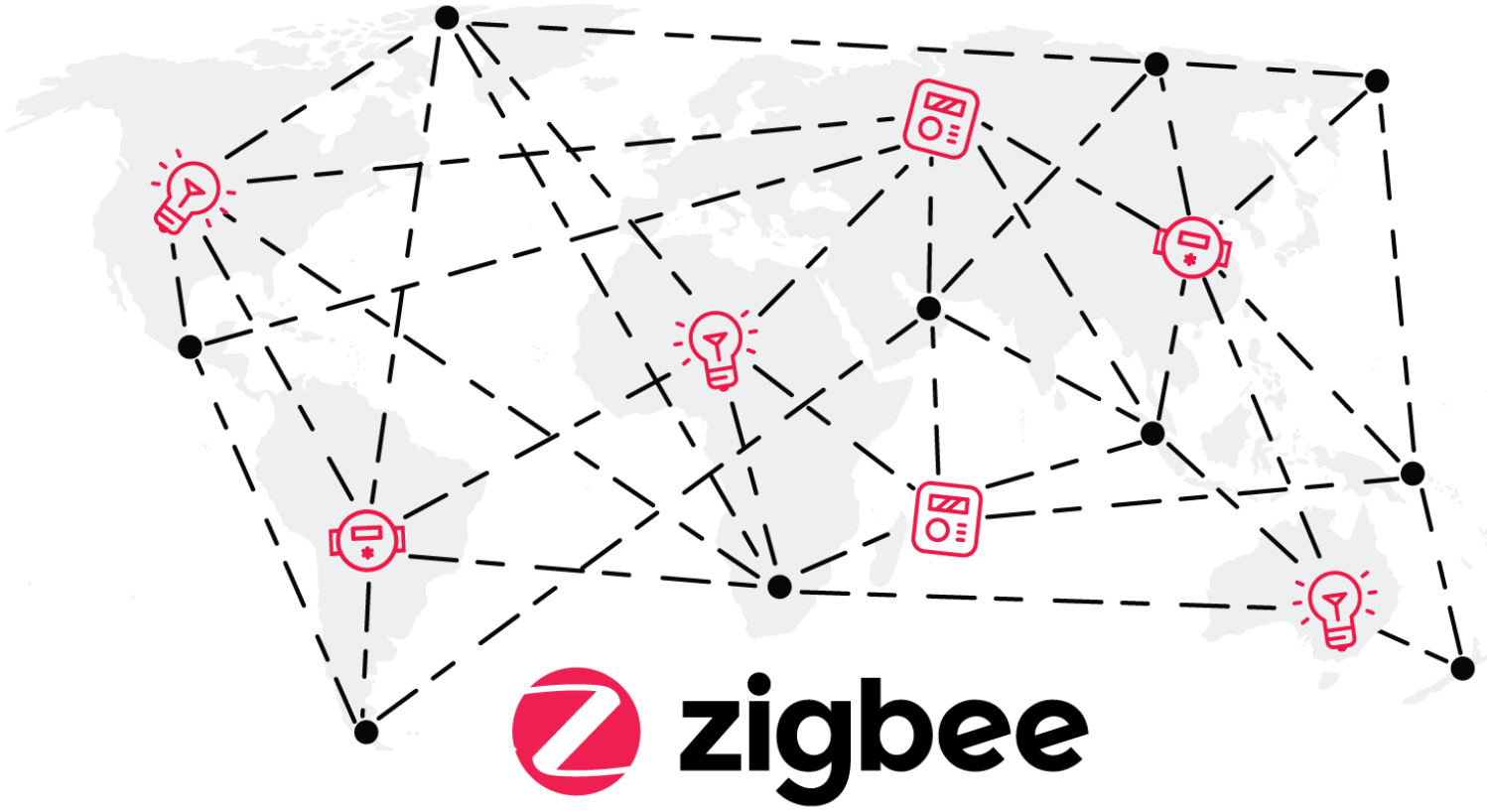
무선데이터통신연구실

전 용 석

ysjeon741@gmail.com



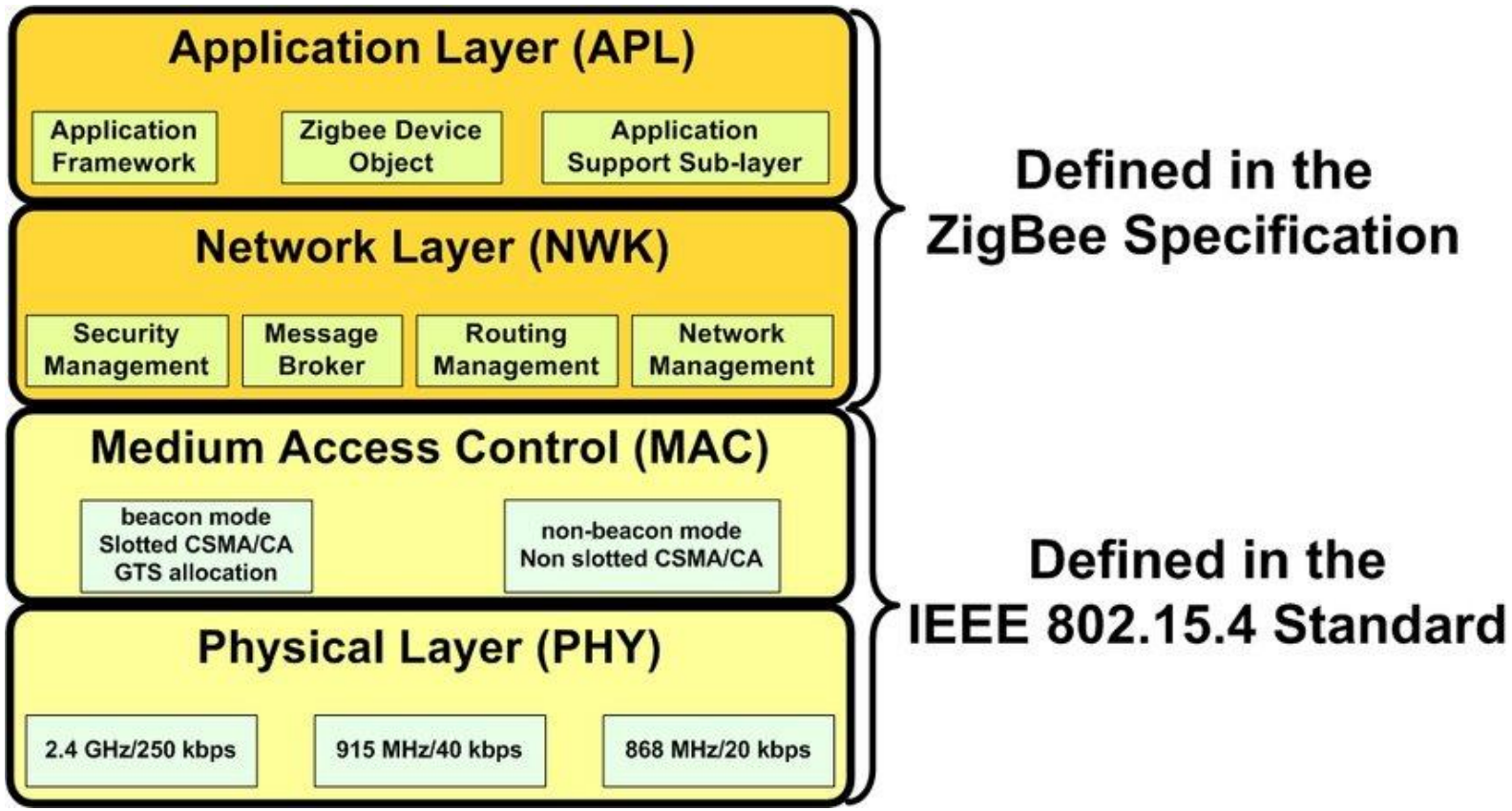
What is ZigBee?



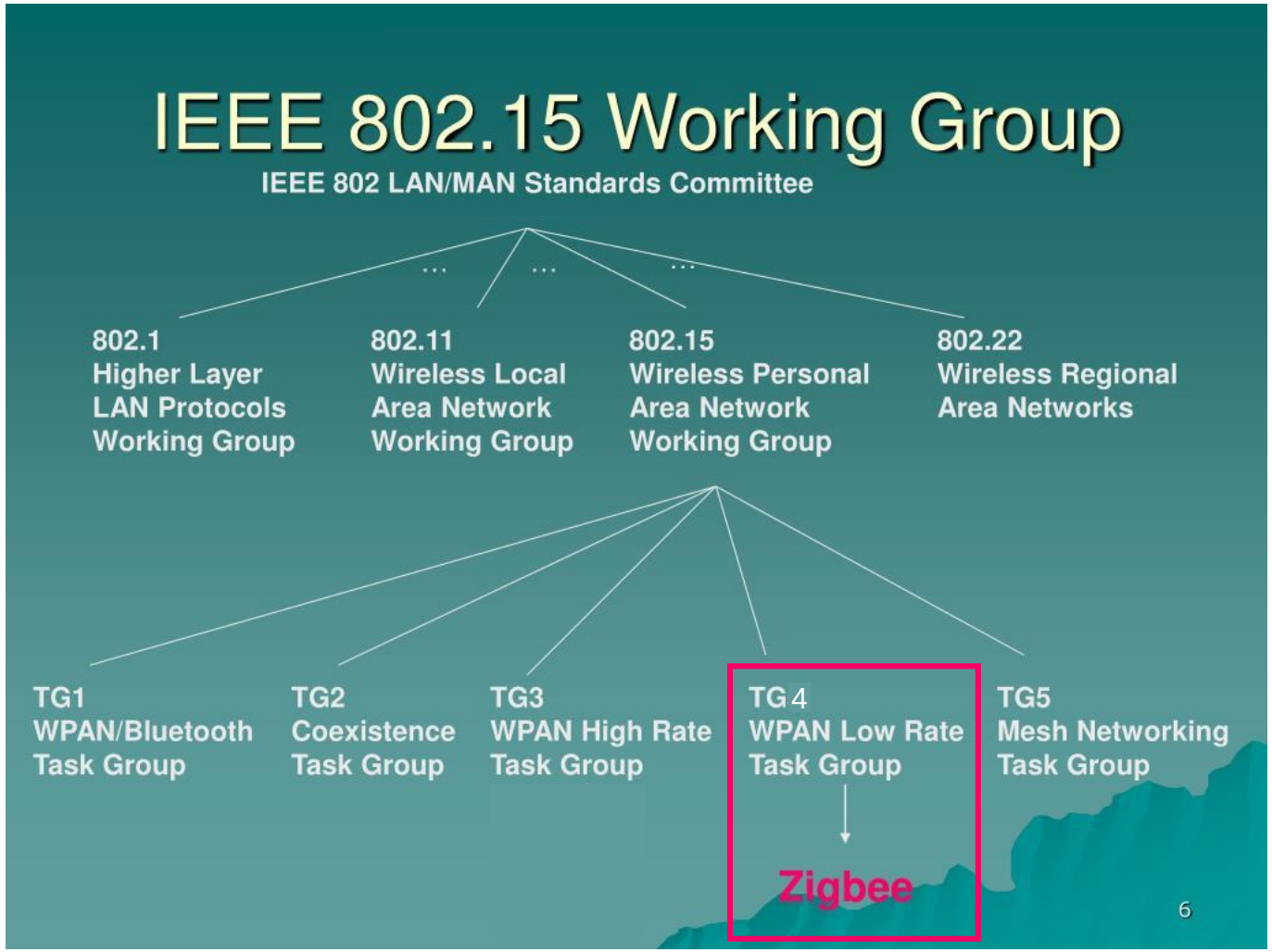


- IEEE 802.15.4–based specification for a suite of high–level communication protocols
- Used to create personal area networks (PAN) with small, low–power digital radios
  - Home automation, medical device data collection, etc.
- ZigBee is a low–power, low data rate, and close proximity wireless ad hoc network

Protocol Stack Architecture



IEEE 802.15 Working Group



Comparison Between WPAN

Project	Data Rate	Range	Configuration	Other Features
802.15.1 (Bluetooth)	1 Mbps	10M (class 3) 100M (class 1)	8 active device Piconet/ Scatternet	Authentication, Encryption, Voice
802.15.3 High Rate	22, 33, 44, 55 Mbps	10M	256 active device Piconet/ Scatternet	FCC part 15.249 QoS, Fast Join Multi-Media
802.15.4 Low Rate	up to 250Kbps	10M nominal 1M-100M based on settings	Master/Slave (256 Devices or more) Peer to Peer	Battery Life: multi-month to infinite
802.15.2 Coexistence	Develop a Coexistence Model and Mechanisms Document as a Recommended Practice			

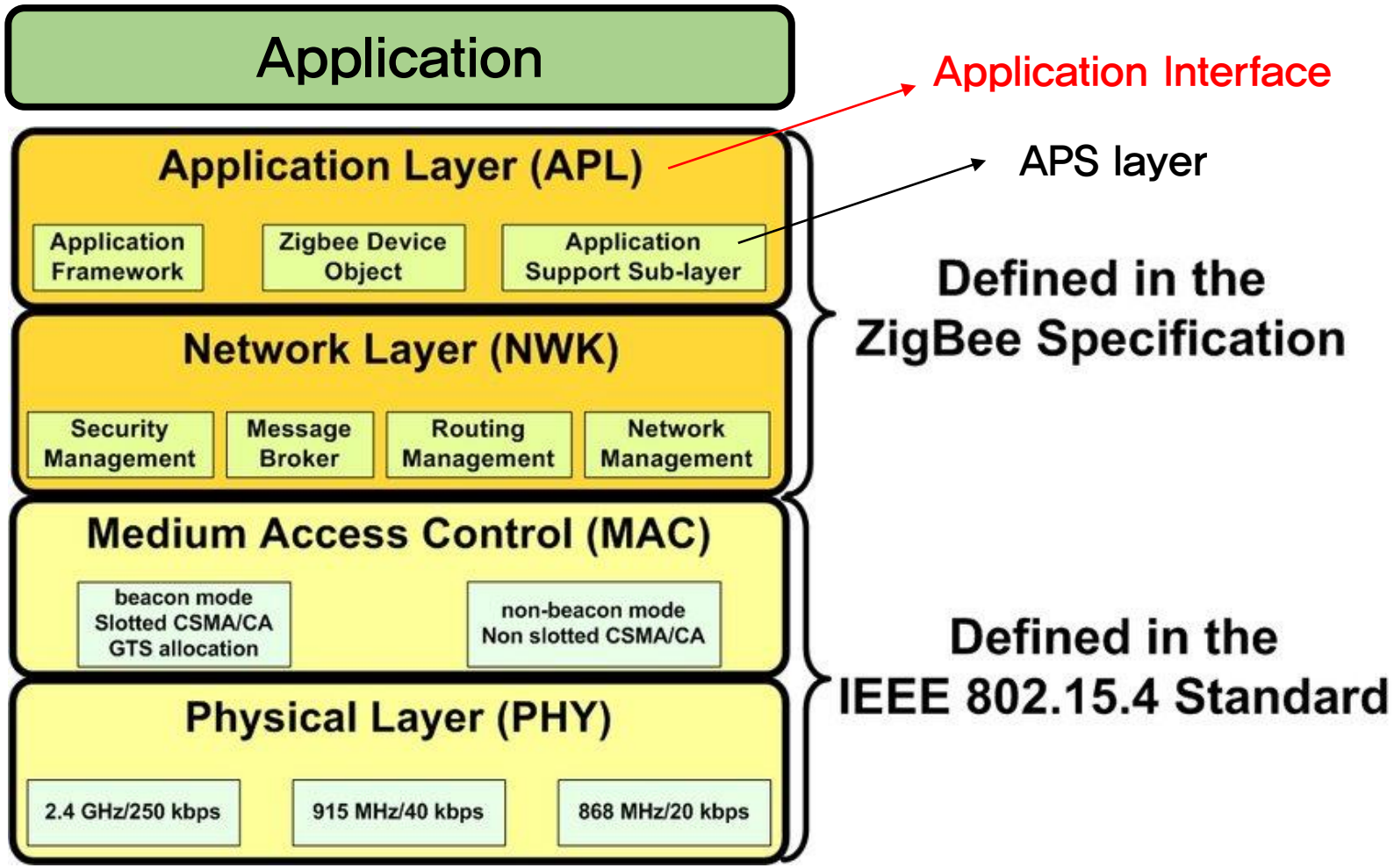
ZigBee Alliance

- A group of companies that maintain and publish the ZigBee standard
- The Alliance publishes application profiles that allow multiple OEM vendors to create interoperable products
- The relationship between IEEE 802.15.4 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance
- https://zigbee.org/

Our Mission

The Zigbee Alliance ignites creativity and collaboration in the Internet of Things, by creating, evolving, and promoting universal open standards that enable all objects to securely connect and interact.

Protocol Stack Architecture



Basic Features

- Low power consumption
- Low cost
- Low offered message throughput
- Support large network orders (<= 65k nodes)
- Low to no QoS guarantees
- Flexible protocol design suitable for many applications

IEEE 802.15.4

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Multi–level security
  - Works well for
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable devices

IEEE 802.15.4 Device Types

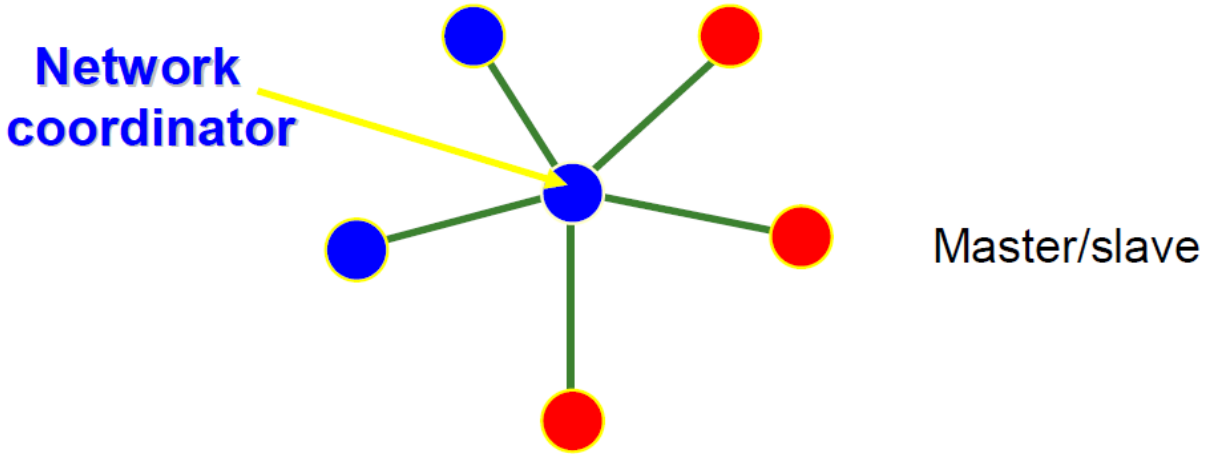
- There are two different device types:
  - Full function device (FFD)
  - Reduced function device (RFD)
- Full function device (FFD)
  - Any topology
  - Operate in any modes serving
    - Device, coordinator (router), PAN coordinator
  - Talks to any other devices
- Reduced function device (RFD)
  - Limited to star topology
  - Cannot become a network coordinator
  - Very simple implementation





Network Topology

- Star topology



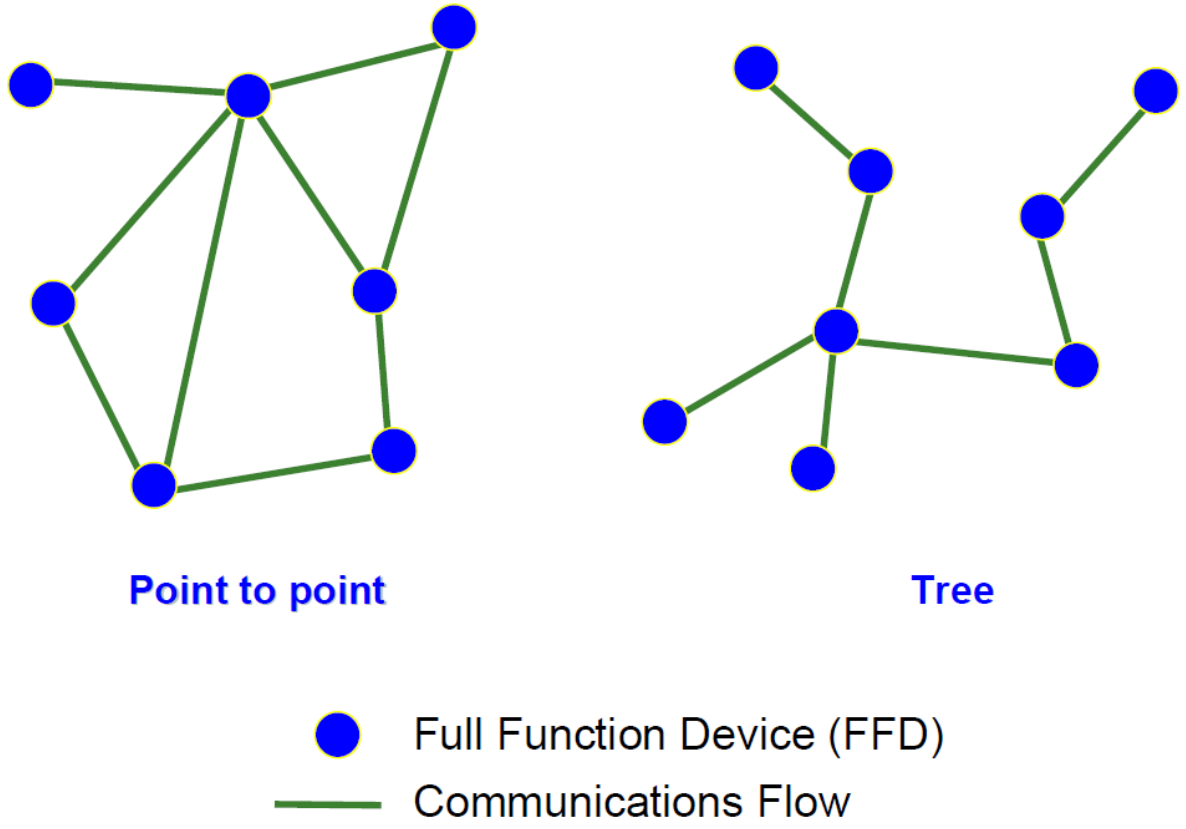
Full Function Device (FFD)

Reduced Function Device (RFD)

Communications Flow

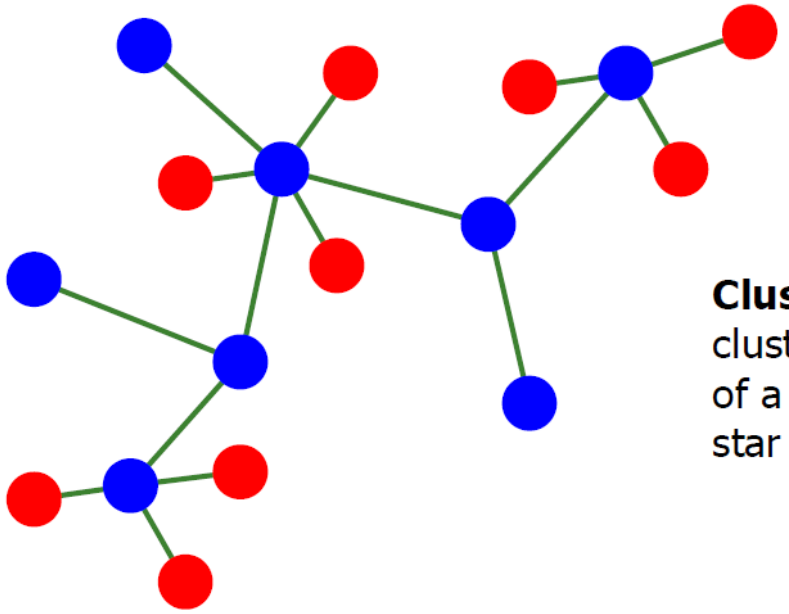
Network Topology

- Peer–Peer topology



Network Topology

- Combined topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

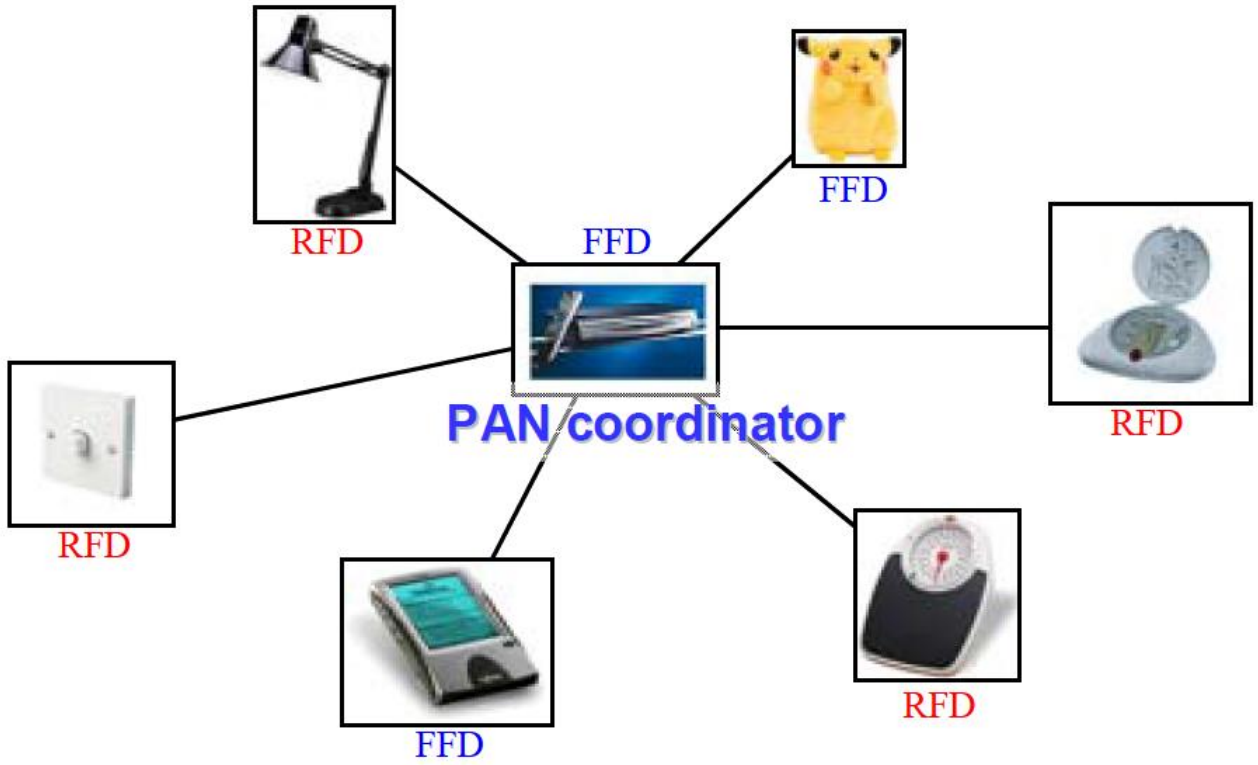
Full Function Device (FFD)

Reduced Function Device (RFD)

Communications Flow

Network Topology

- Example network

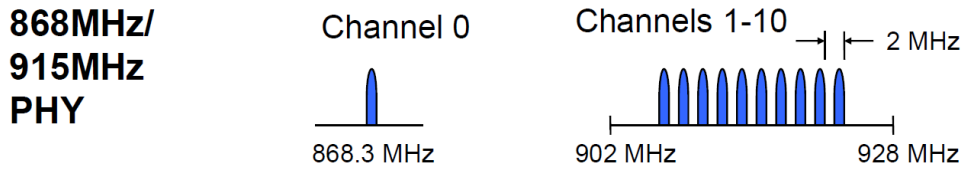


IEEE 802.15.4 PHY Overview

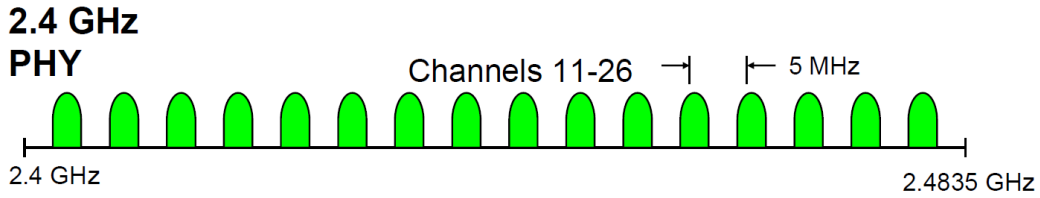
- PHY functionalities
  - Activation and deactivation of the radio transceiver
  - Energy detection within the current channel
  - Link quality indication for received packets
  - Clear channel assessment for CSMA/CA
  - Channel frequency selection
  - Data transmission and reception

IEEE 802.15.4 PHY Frequency Bands

- Operating Frequency Bands
  - 868 MHz/915 MHz direct sequence spread spectrum (DSSS) PHY (11 channels)
    - 1 channel (20 kb/s) in European 868 MHz band
    - 10 channels (40 kb/s) in 915 (902–928) MHz ISM band



  - 2.4 GHz direct sequence spread spectrum (DSSS) PHY (16 channels)
    - 16 channels (250 kb/s) in 2.4 GHz band

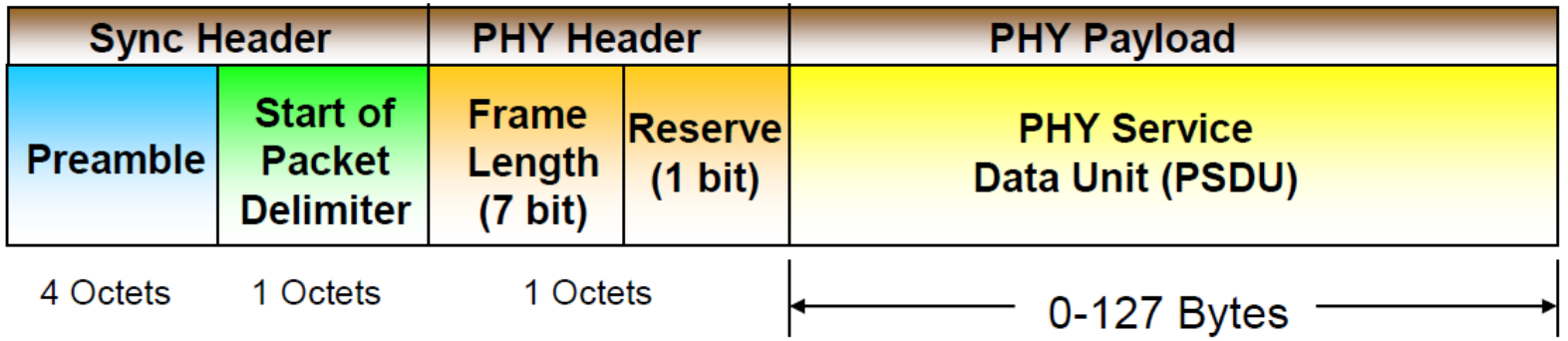


IEEE 802.15.4 PHY Spec.

PHY (MHz)	Frequency band (MHz)	Spreading parameters		Data parameters		
		Chip rate (kchip/s)	Modulation	Bit rate (kb/s)	Symbol rate (ksymbol/s)	Symbols
868/915	868–868.6	300	BPSK	20	20	Binary
	902–928	600	BPSK	40	40	Binary
868/915 (optional)	868–868.6	400	ASK	250	12.5	20-bit PSSS
	902–928	1600	ASK	250	50	5-bit PSSS
868/915 (optional)	868–868.6	400	O-QPSK	100	25	16-ary Orthogonal
	902–928	1000	O-QPSK	250	62.5	16-ary Orthogonal
2450	2400–2483.5	2000	O-QPSK	250	62.5	16-ary Orthogonal

IEEE 802.15.4 PHY Frame Structure

- PHY packet fields



  - Preamble (32 bits) – synchronization
  - Start of packet delimiter (8 bits) – shall be formatted as “11100101”
  - PHY header (8 bits) – PSDU length
  - PSDU (0 to 127 bytes) – data field

IEEE 802.15.4 MAC Overview

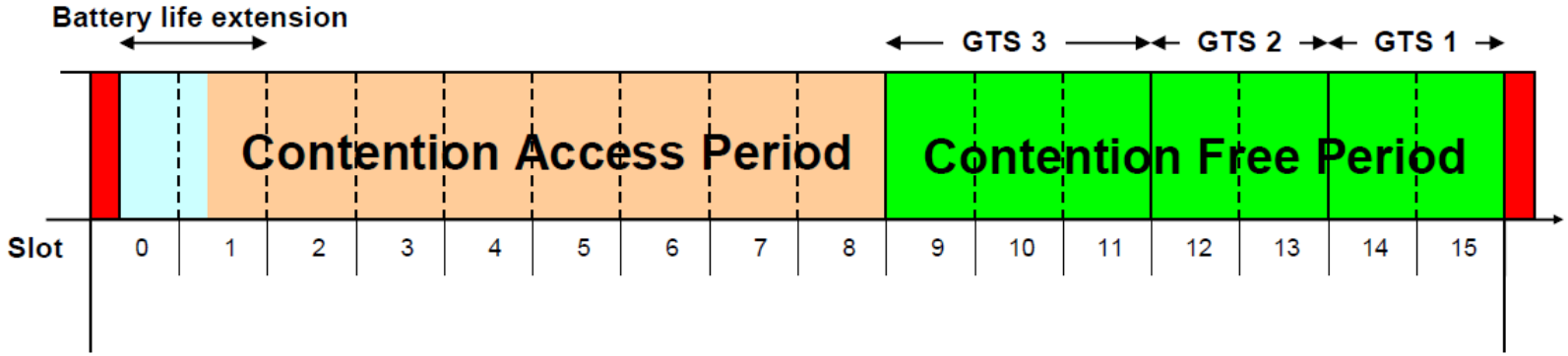
- Simple frame structure
- Association/disassociation
- AES-128 security
- CSMA/CA channel access
- GTS mechanism

IEEE 802.15.4 MAC

- Traffic types
  - Periodic data
    - Application defined rate (e.g. sensors)
  - Intermittent data
    - Application/external stimulus defined rate (e.g. light switch)
  - Repetitive low latency data
    - Allocation of time slots (e.g. mouse)

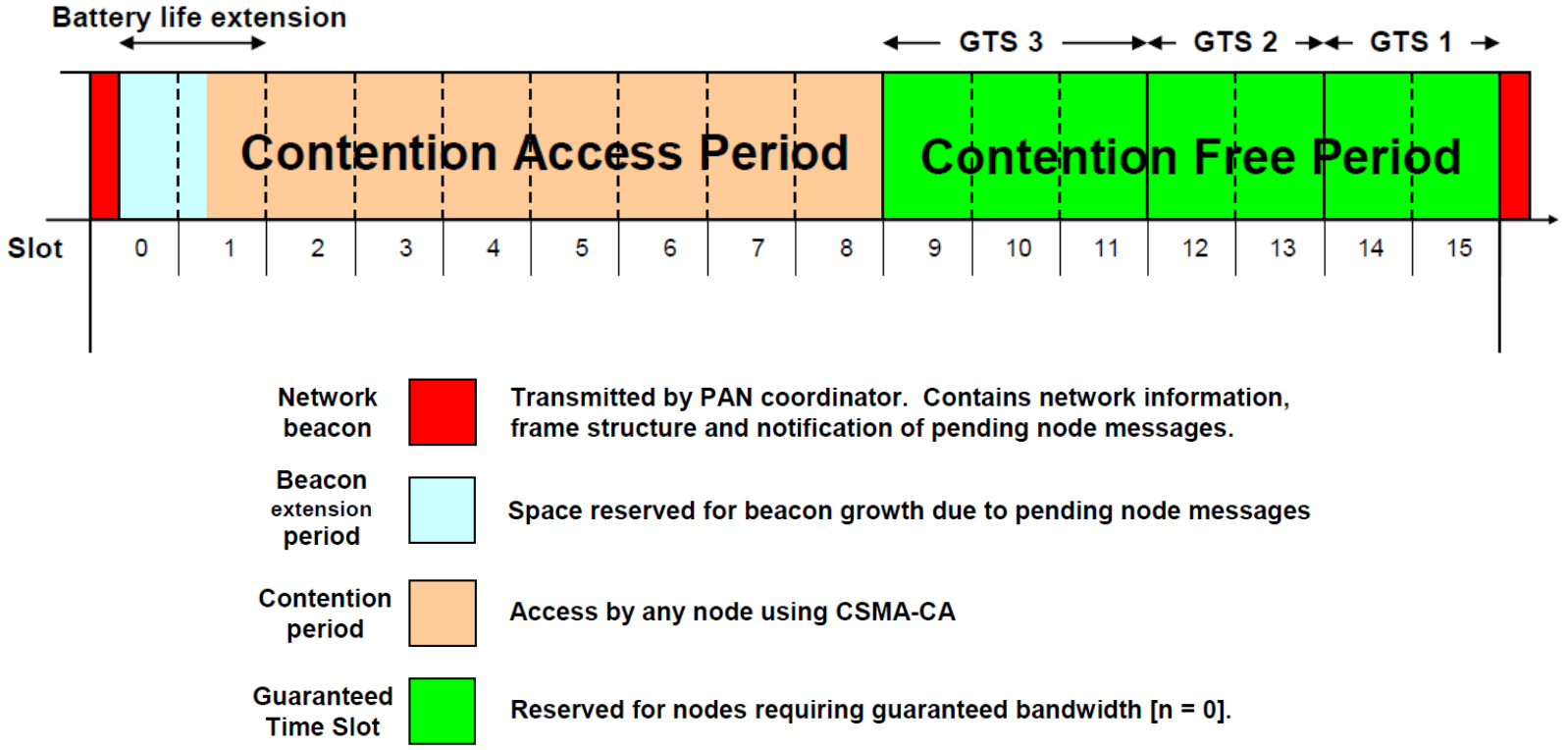
Frame Structure

- Data transport concepts
  - Frames are the basic unit of data transport
  - Four fundamental types:
    - Data, acknowledgement, beacon, and MAC command frames
  - Superframe structure
    - Defined by the coordinator
    - Two beacons act as its limits and provide synchronization to other device
    - Consists of sixteen equal-length slots



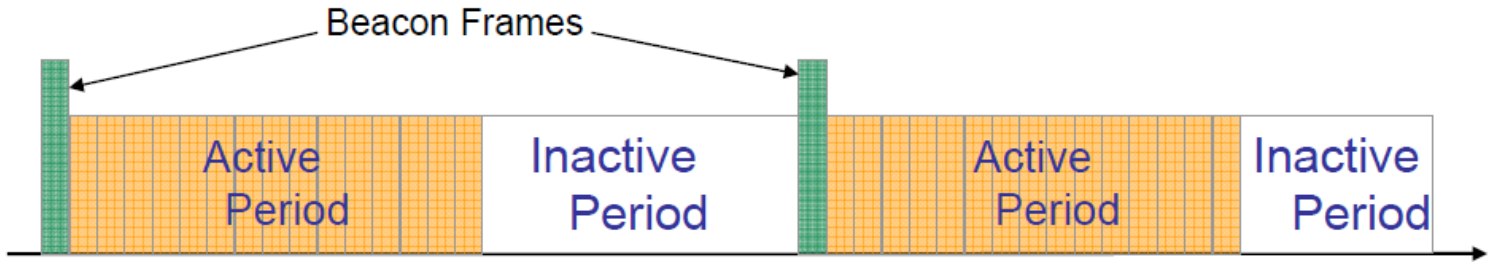
Frame Structure

- Data transport concepts
  - Superframe structure (cont'd)



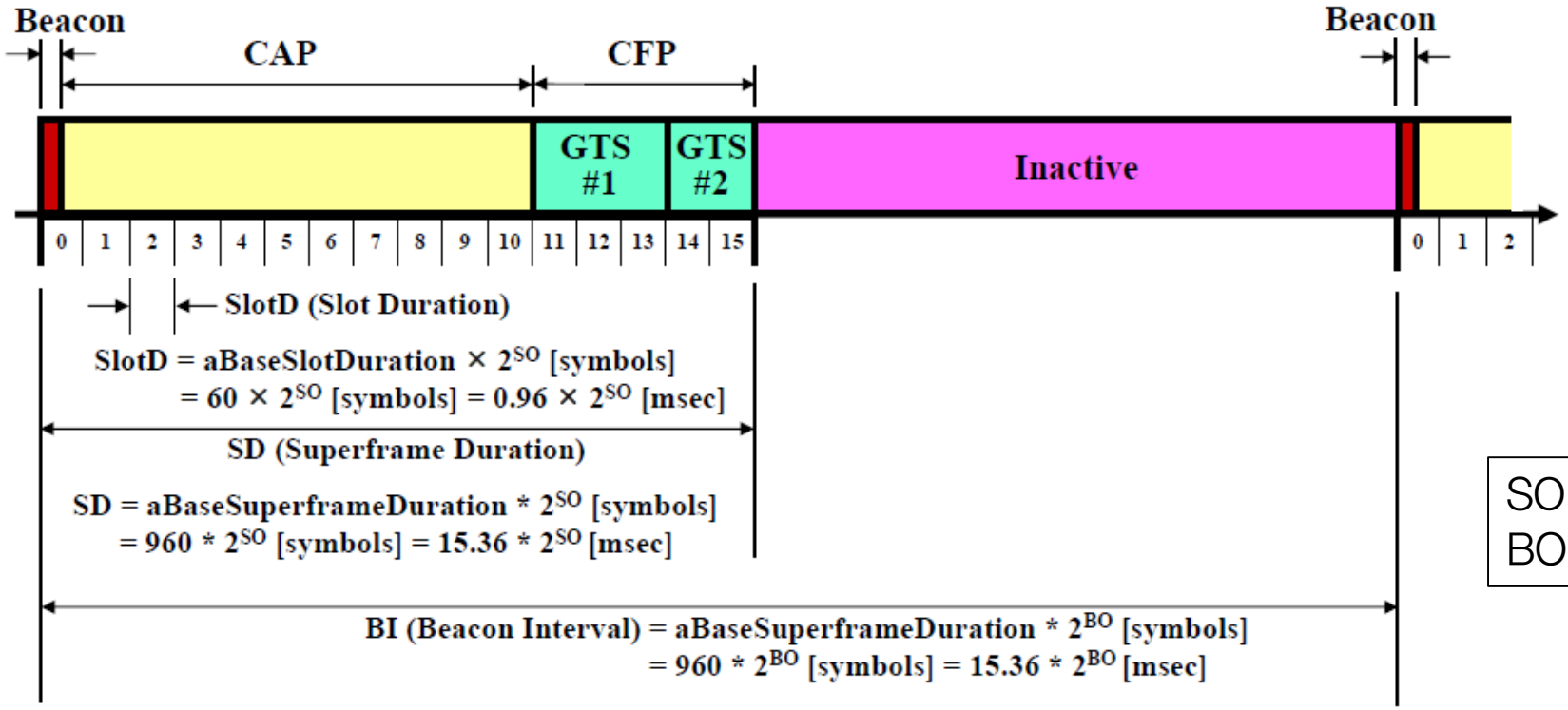
Frame Structure

- Data transport concepts
  - Superframe structure (cont'd)
    - Every transmission must end before the arrival of the second beacon
    - Applications can use up to seven domains of one or more contentionless guaranteed time slots, trailing at the end of the superframe
    - Superframe can be further devided into an active part and inactive part
      - During inactive period, the coordinator may enter power saving mode



Frame Structure

- Data transport concepts
  - Superframe structure (cont'd)



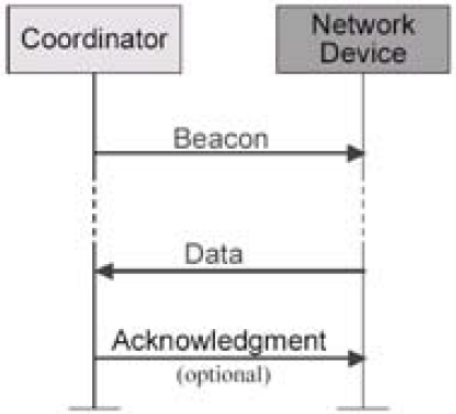
SO: slot order
BO: Beacon order

Data Transfer Model

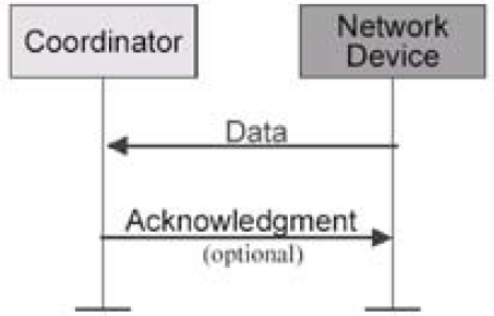
- Network coordinator
  - Transmits network beacons
  - Sets up a network
  - Manages network nodes
  - Stores network node information
  - Routes messages between paired nodes
  - Receives constantly
- Network node
  - Is generally battery powered
  - Searches for available networks
  - Transfer data from tis application as necessary
  - Determines whether data is pending
  - Requests data from the network coordinator
  - Can sleep for extended periods

Data Transfer Model

- Data transferred from device to coordinator (Uplink)
  - Beacon-enable network
    - Device finds the beacon to synchronize to the superframe structure
    - Slotted CSMA/CA
  - Non beacon-enable network
    - Device simply transmits its data
    - Unslotted CSMA/CA



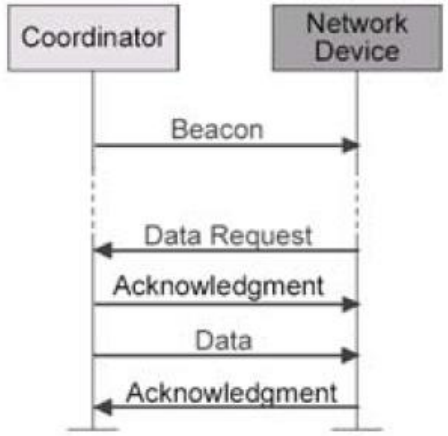
Communication to a coordinator
In a beacon-enabled network



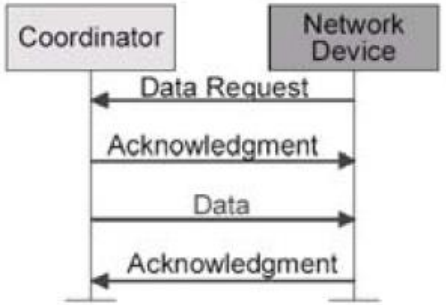
Communication to a coordinator
In a non beacon-enabled network

Data Transfer Model

- Data transferred from coordinator to device (Downlink)
  - Beacon-enable network
    - The coordinator indicates in the beacon that "data is pending."
    - Device periodically listens to the beacon and transmits a request using slotted CSMA/CA
  - Non beacon-enable network
    - A device transmits a MAC command request using CSMA/CA
      - Similar to unslotted ALOHA



Communication from a coordinator
In a beacon-enabled network

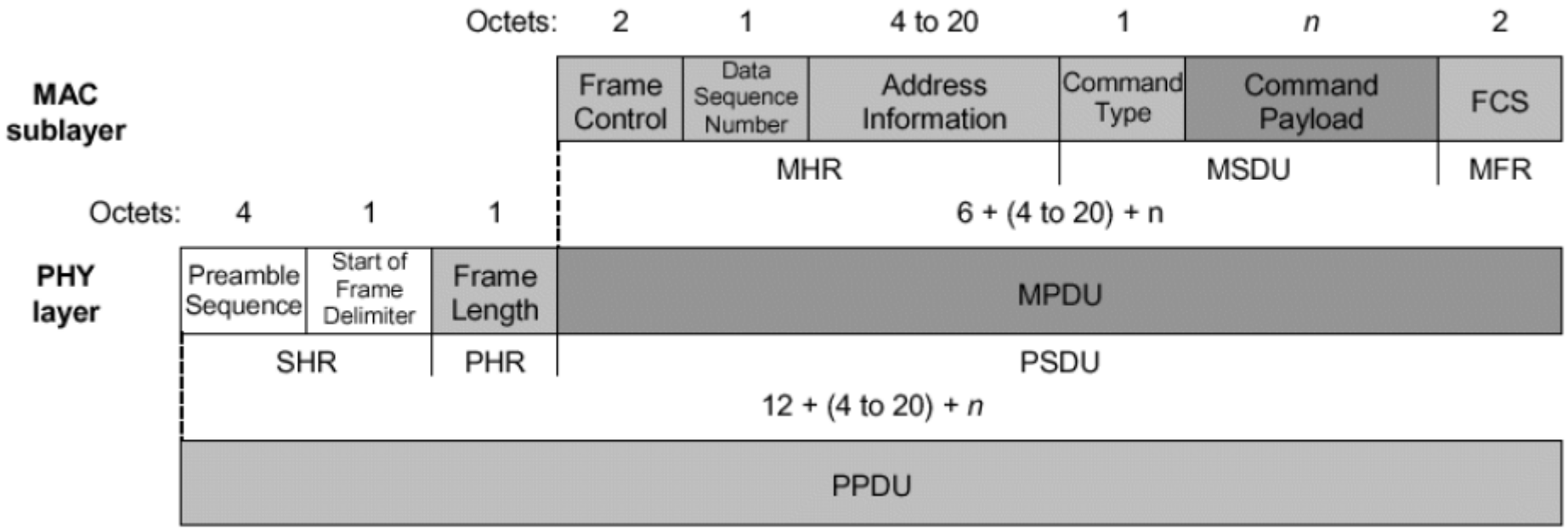


Communication from a coordinator
in a non beacon-enabled network

Security

- Device can have the ability to:
  - Maintain an access control list
  - Use symmetric cryptography (AES-128)
- Security modes
  - Unsecured mode
  - Access control list mode
  - Secured mode
- Security done in the higher layer

IEEE 802.15.4 MAC Frame Structure



Network Layer Overview

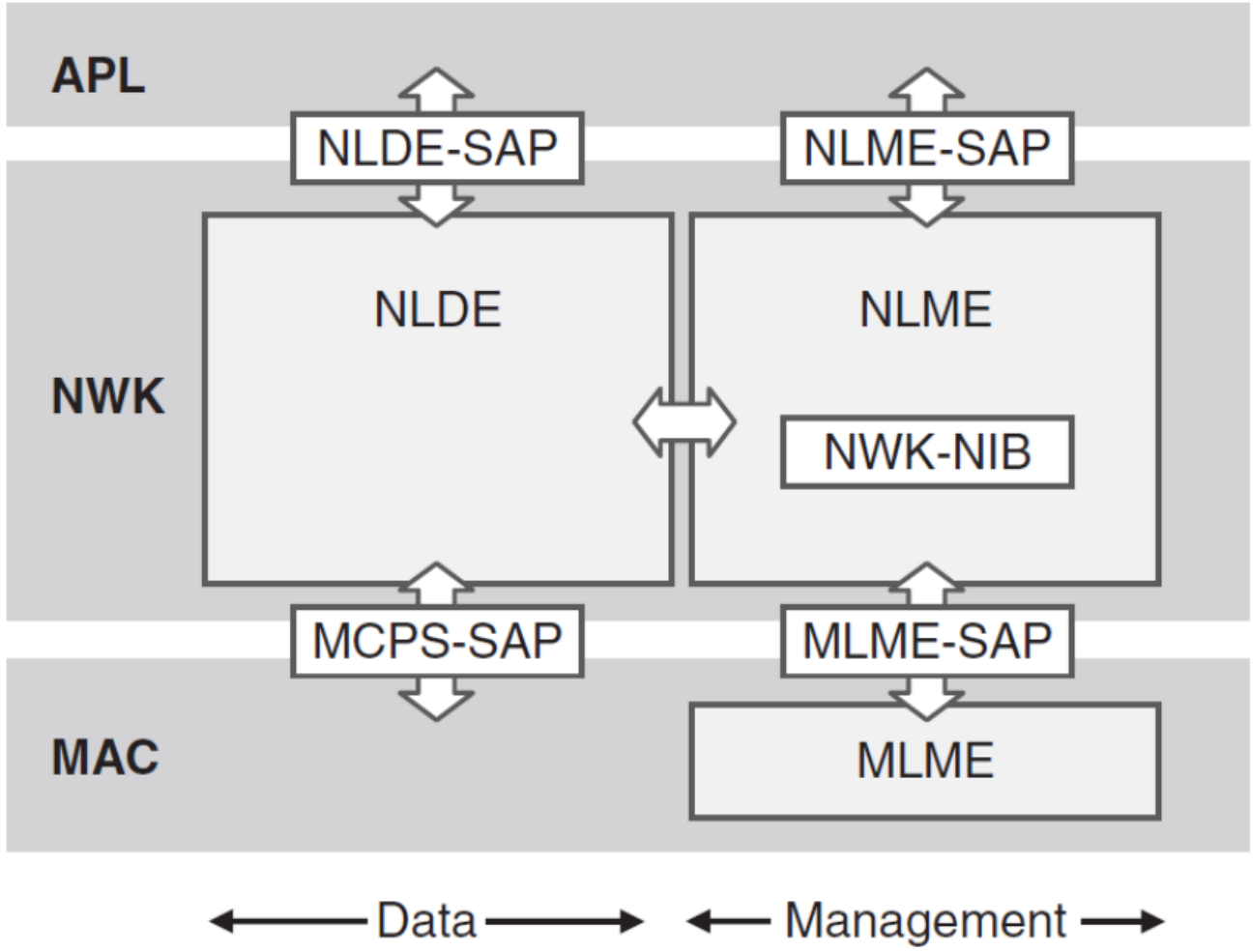
- Network Layer (NWL) overview
  - Network management
  - Routing management
  - Security management
  - Message broker

Network Layer

- Network layer function vs. ZigBee device types

ZigBee Network Layer Function	Coordinator	Router	End Device
Establish a ZigBee network	O		
Permit other device to join or leave the network	O	O	
Assign 16-bit network address	O	O	
Discover and record paths for efficient message delivery	O	O	
Discover and record list of one-hop neighbors	O	O	
Route network packets	O	O	
Receive or send network packets	O	O	O
Join or leave the network	O	O	O
Enter sleep mode			O

Network Layer



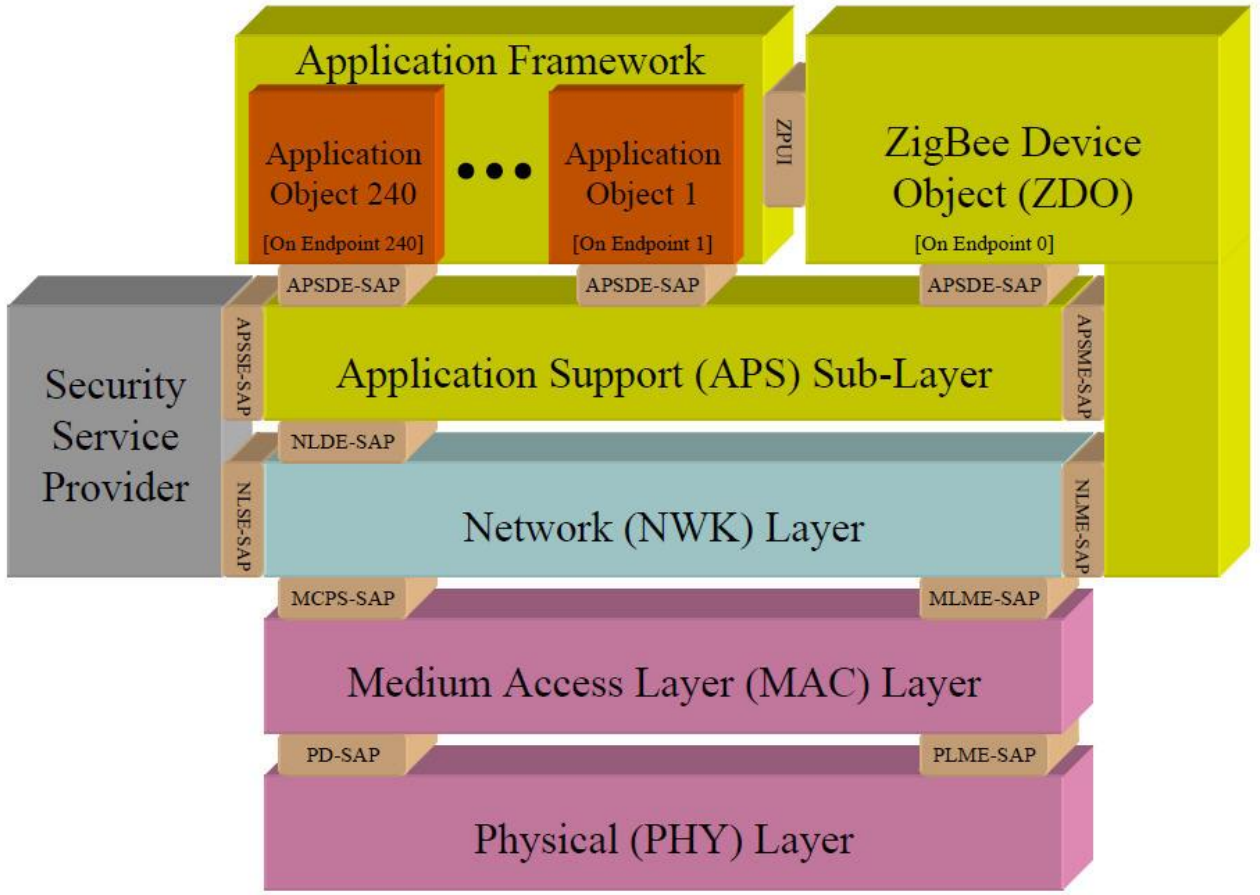
Network Layer

- ZigBee coordinator and routers define and maintain tables
  - Routing table
  - Route discovery table (temporary)
- ZigBee devices maintain neighbor table

Field Name	Description
Extended address	64-bit IEEE 802.15.4 address
Network address	16-bit network address
Device type	ZigBee coordinator, router, or end device
RxOnWhenIdle	If the device keeps its receiver ON during idle mode, this field is set to TRUE
Relationship	This field determines the relationship of the neighbor to the device as parent, child, sibling, previous child, or none of the above
Transmit failure	A high value in this field indicates that many of the previous transmission attempts resulted in failure
LQI	The estimated link quality
Incoming beacon timestamp	The time that the last beacon was received (optional field)
Potential parent	This field determines whether this neighbor is a potential parent (optional field)

Application Layer

- Application Support Sublayer (APS)
- Application Framework (APF)
- ZigBee Device Object (ZDO)



Application Support Sublayer (APS)

- APS sublayer is responsible for:
  - Binding tables
  - Message forward between bound devices
  - Group address definition and management
  - Address mapping from 64–bit extended addresses to 16–bit NWK addresses
  - Fragmentation and reassembly of packets
  - Reliable data transport

Application Framework

- The application framework is an execution environment for application objects to send and receive data
- Application objects are defined by the manufacturer of the ZigBee-enabled device
- As defined by ZigBee, an application object is at the top of the application layer and is determined by the device manufacturer
- An application object actually implements the application
- The application profile is run by the application objects

Application Framework

- Each application object is addressed through its corresponding endpoint
- Endpoint numbers range from 1 to 240
  - Endpoint 0 is the address of the ZigBee Device Object (ZDO)
  - Endpoint 255 is the broadcast address
  - Endpoints 241 through 254 are reserved for future use
- ZigBee defines function primitives, not an application programming interface (API)

ZigBee Device Object (ZDO)

- The ZDO is responsible for overall device management, specifically it is responsible for:
  - Initializing the APS sublayer and the NWK layer
  - Defining the operating mode of the device (i.e., coordinator, router, or end device)
  - Device discovery and determination of which application services the device provides
  - Initiating and/or responding to binding requests
  - Security management

ZigBee Stack

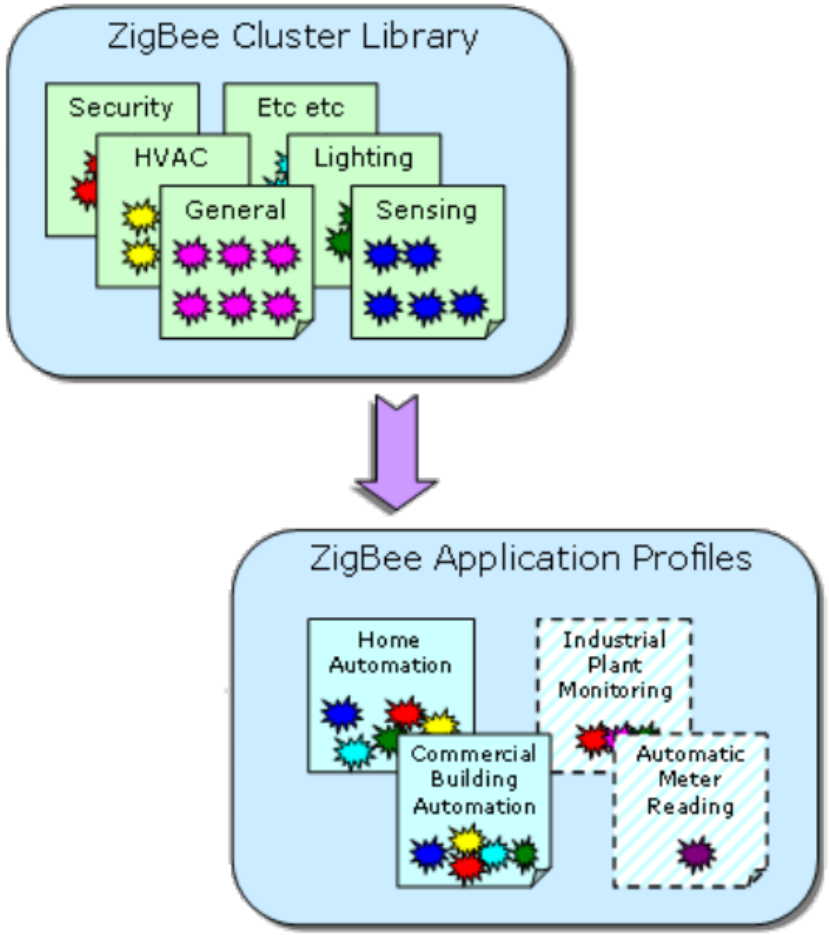
- ZigBee provides several separate stacks
  - ZigBee 2004
    - was released in 2004 and supported a home control lighting profile
    - This stack was never extensively deployed with customers and is no longer supported
  - ZigBee 2006
    - was released in 2006 and supports a single stack known as the ZigBee stack
  - ZigBee 2007
    - was released in Q4 2007
    - It has two feature sets, ZigBee and ZigBee PRO

ZigBee Cluster Library (ZCL)

- ZCL is a set of messages used to send and receive related commands and data over a ZigBee network
- These clusters are further grouped into functional domains
  - HVAC, security, lighting, etc.
- The ZigBee common application layer then references which clusters are used within certain applications, and specifies which clusters are supported by different devices–some clusters are mandatory, others optional

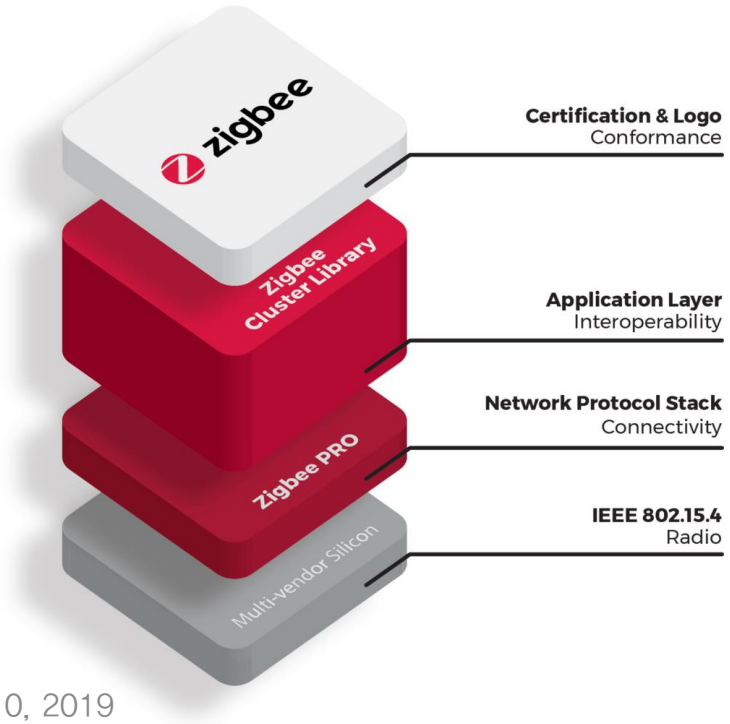
ZigBee Cluster Library (ZCL)

- Functional domains
  - General
  - Closures
  - HVAC
  - Lighting
  - Measurement & Sensing
  - Security & Safety
  - Protocol Interfaces
  - Smart Energy
  - etc.



ZigBee 3.0

- ZigBee 3.0 unites all of the different application profiles into one common application layer
- Released on November, 2014



Lighting

On/Off light switch
Dimmable plug-in unit
Dimmable light
Color dimmable light
Dimmer switch
Light sensor
Color temperature light
Extended color light
Color controller
Color scene controller
Non-color controller
Non-color scene controller
Scene selector
Light level sensor

Generic Devices

Configuration tool
Remote control
Combined interface
Range extender
Mains power outlet
Control bridge
Level control switch
On/off switch
On/off sensor
On/off output

HVAC

Heating/cooling unit
Humidity sensor
Thermostat
Temperature sensor

Security

Access Control (fobs)
Occupancy sensor
Door lock
Door lock controller
Fobs

Green Power Devices

Proxy Basic
Combo Basic
Green Power (Energy Harvesting) Device

Intruder Alarm System

IAS control & indicating equipment
IAS ancillary control equipment
IAS zone
IAS warning device

Closure Devices

Shade controller
Window covering devices

ZigBee 3.0

Solution	Description
Network Protocol	Zigbee PRO 2015 (or newer)
Network Topology	Self-Forming, Self-Healing MESH
Network Device Types	Coordinator (routing capable), Router, End Device, Zigbee Green Power Device
Network Size (# of nodes)	Up to 65,000
Radio Technology	IEEE 802.15.4-2011
Frequency Band / Channels	2.4 GHz (ISM band) 16-channels (2 MHz wide)
Data Rate	250 Kbits/sec
Security Models	Centralized (with Install Codes support) Distributed
Encryption Support	AES-128 at Network Layer AES-128 available at Application Layer
Communication Range (Average)	Up to 300+ meters (line of sight) Up to 75-100 meters indoor
Low Power Support	Sleeping End Devices Zigbee Green Power Devices (energy harvesting)
Legacy profile support	Zigbee 3 devices can join legacy Zigbee profile networks. Legacy devices may join Zigbee 3 networks (based on network's security policy)
Logical device support	Each physical device may support up to 240 end-points (logical devices)