ITMC412 PAN
شبكات المنطقة الشخصية

LR-WPAN L5
(IEEE802.15.4, ZigBee)

By: Dr. Abdussalam Nuri Baryun
abaryun.teaching@gmail.com
abaryun.classhub@gmail.com

Mobile Computing Department, Faculty of Information Technology, University of Tripoli

IEEE802.15.4 and ZigBee

- As with many IEEE networking standards, the 802.15.4 standard only defines the PHY and MAC layers for Low Rate WPAN (LR-WPAN). The ZigBee standard extends 802.15.4 to provide Bluetooth like interoperability features.

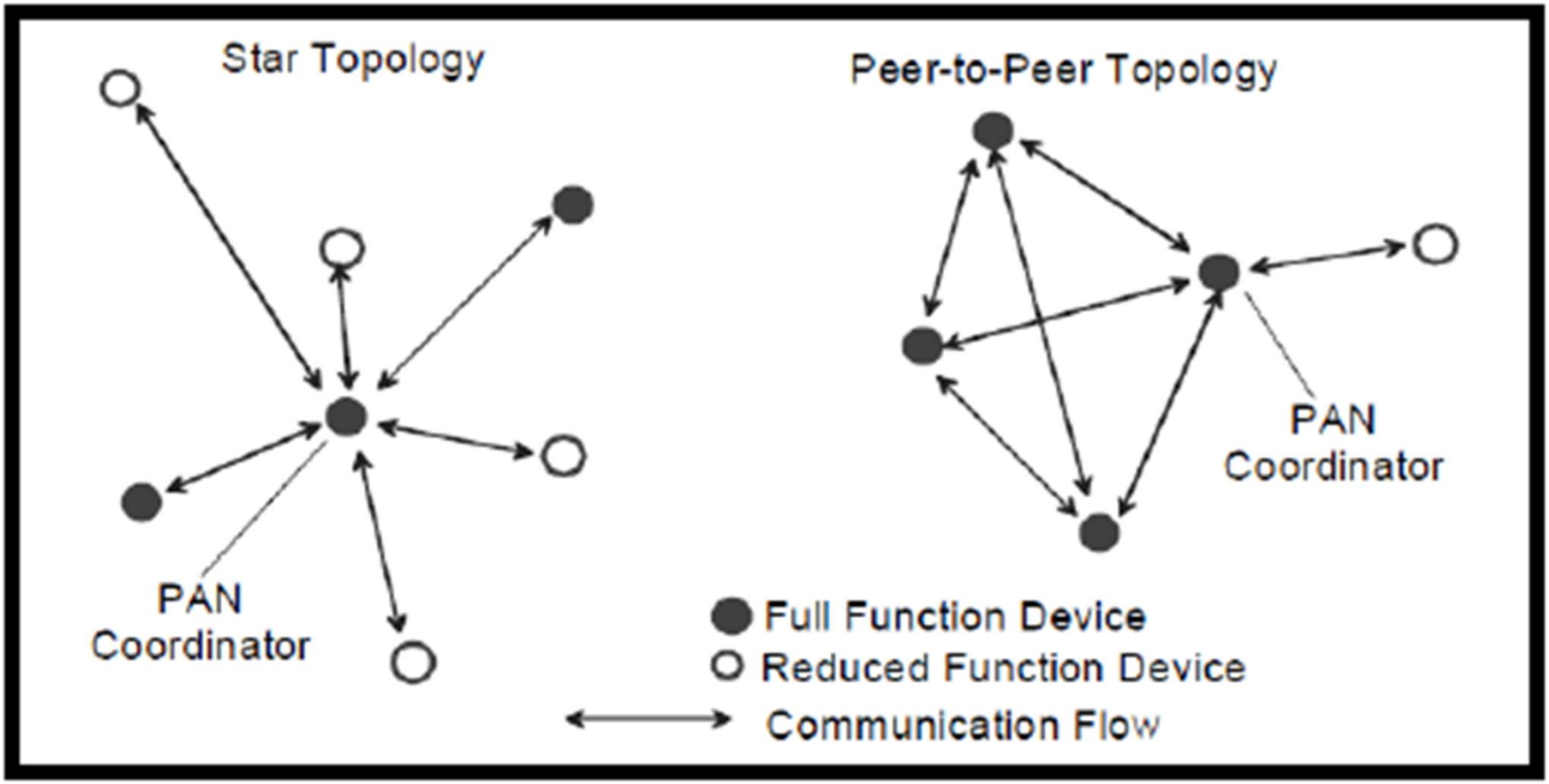
- ZigBee builds on top of 802.15.4's radio layer, specifying network, security , and application layers.

- Devices that implement the 802.15.4 standard are not necessarily ZigBee compatible.

IEEE802.15.4

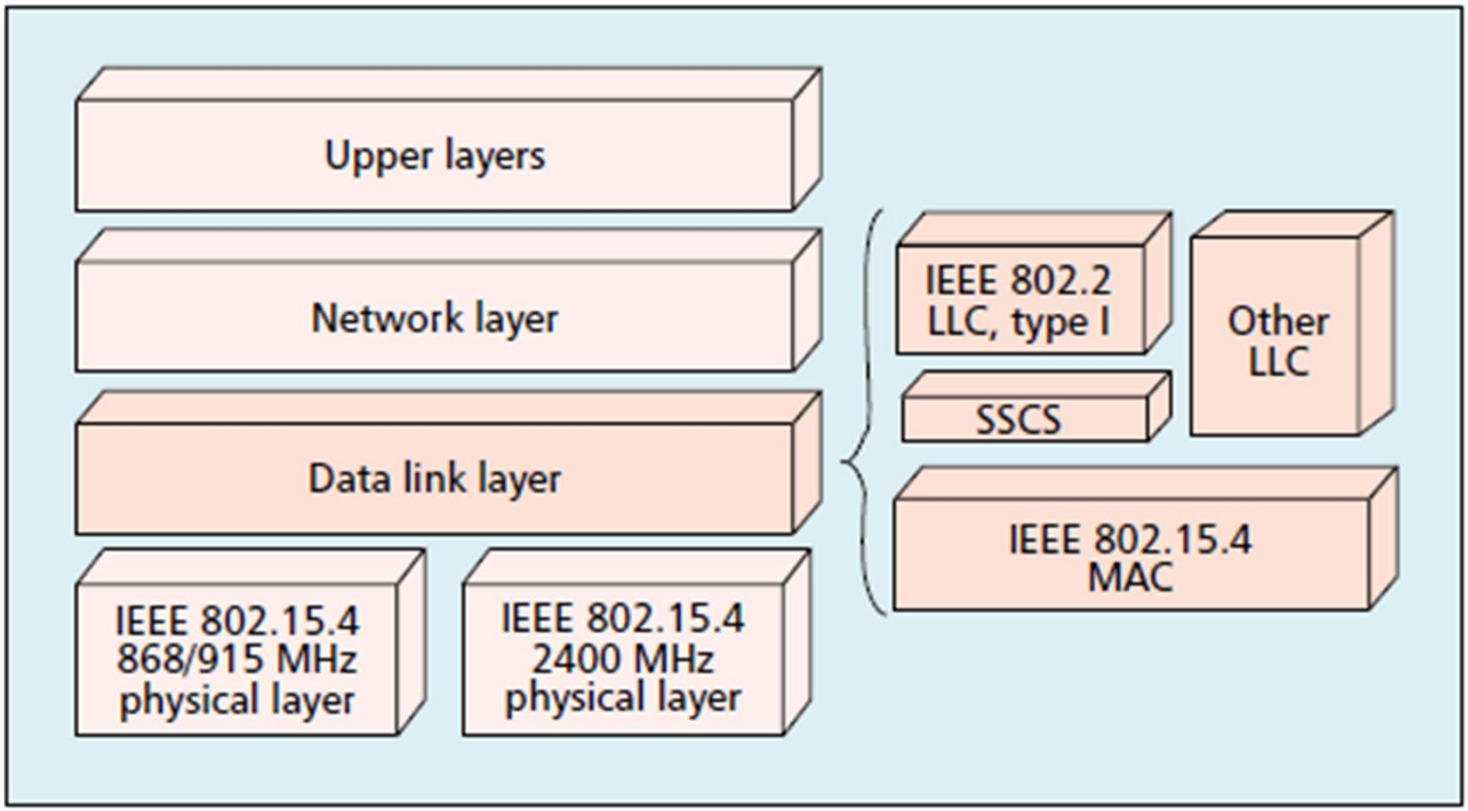
- Although Bluetooth's power requirements are much lower than of 802.11b, it is still requires to be charged every few days. This 802.15.4 standard is intended for deployment on *long lived systems*, with low data rate requirements, where devices must be able to operate autonomously for months or even years without recharging the battery.
- The IEEE 802.15.4 standard defines the PHY and MAC for very low-power, low duty network links.
- Provides Two topologies: Star or peer-to-peer operation

IEEE802.15.4 PAN Topology



IEEE802.15.4 standard Topology [Ref.1]

LR-WPAN System Architecture



The IEEE802.15.4 has two PHY layers that serve same MAC layer [Ref.3]
SSCS: service-specific convergence sublayers
LLC: Link Logic Control

IEEE802.15.4 Devices

- 802.15.4 devices can be divided into two categories, which determine the topology and media access used by the network.
  - **Full function devices (FFDs)** can communicate directly with any other devices in the network.
  - **Reduced function devices (RFDs)** can only communicate with FFDs.
- The 802.15.4 standard allows networks to form rather a one hop star topology, or a multi hop peer to peer topology. The former is most appropriate in networks with few FFDs, whereas the latter is more resilient to node failure when many FFDs are available.
- The FFD may operate in three modes serving as a personal area network (PAN) coordinator, a coordinator, or a device.

IEEE802.15.4 capability

Some of the capabilities provided by IEEE802.15.4 standard are as follows:

— Unique 64-bit extended address or allocated 16-bit short address

— Optional allocation of guaranteed time slots (GTSs)

— Carrier sense multiple access with collision avoidance (CSMA-CA) or ALOHA channel access

— Fully acknowledged protocol for transfer reliability

— Low power consumption

— Energy detection (ED)

— Link quality indication (LQI)

— IEEE 802.15.4 uses two methods of addressing ; short addressing 16 bit and extended addressing 64bit

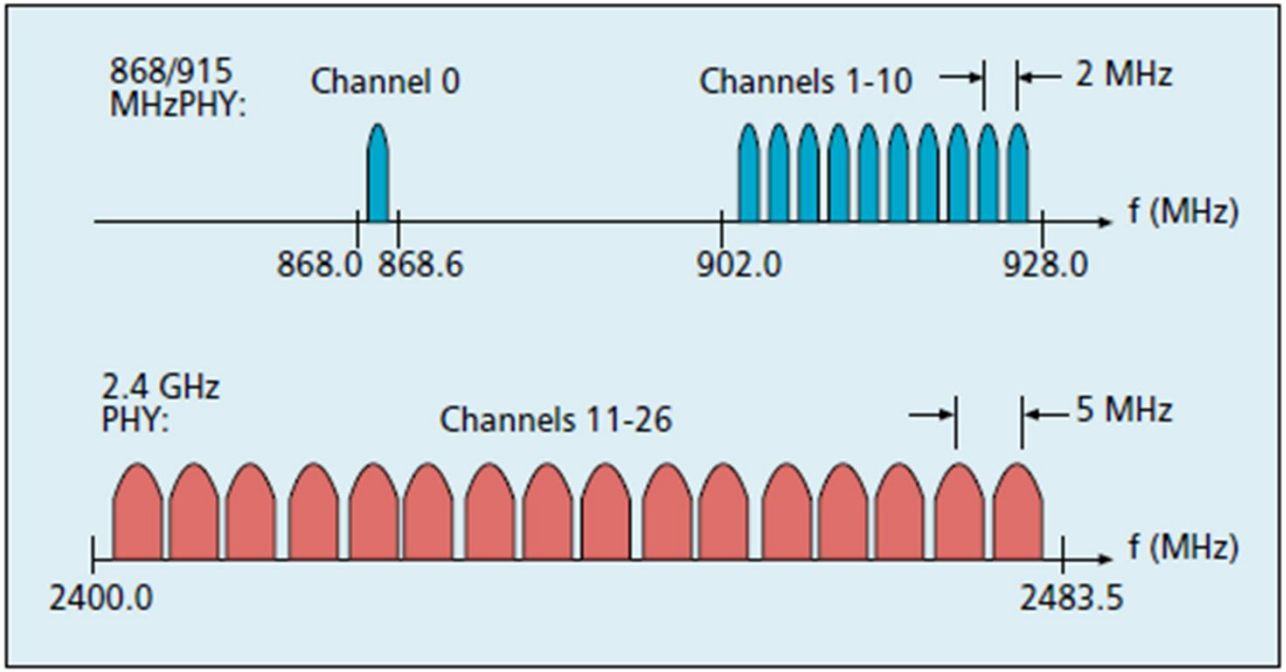
FFD and RFD capability

- FFD device
  - Any topology
  - PAN coordinator capable
  - Talks to any other devices
- RFD device
  - Limited to star topology
  - Not capable of PAN coordination
  - Talks only to PAN coordination
  - Very simple implementation

IEEE802.15.4 PHY

- 802.15.4 offers twenty-seven channels spread across three different areas of license exempt spectrum:
  - One channel is available at 868 MHz,
  - Ten channels are available from 902 MHz to 928 MHz, with a separation of 2 MHz between channels.
  - Sixteen channels are available from 2.4 GHz to 2.4835 GHz, with a channel separation of 5 MHz.
- Direct sequence spread spectrum (DSSS) modulation is used to minimize data loss due to noise and interference.
- Like Bluetooth these channels are used to avoid interference with neighboring PANs, each PAN uses a single unique channel.
- Unlike Bluetooth, devices do not hop across frequencies during the network's life time.

IEEE802.15.4 PHY Channels [3]



The IEEE 802.15.4 channel structure.

Frequency band	Bit rate (kb/s)	Modulation
868.0–868.6 MHz	20	BPSK
902.0–928.0 MHz	40	BPSK
2.4–2.4835 GHz	250	O-QPSK

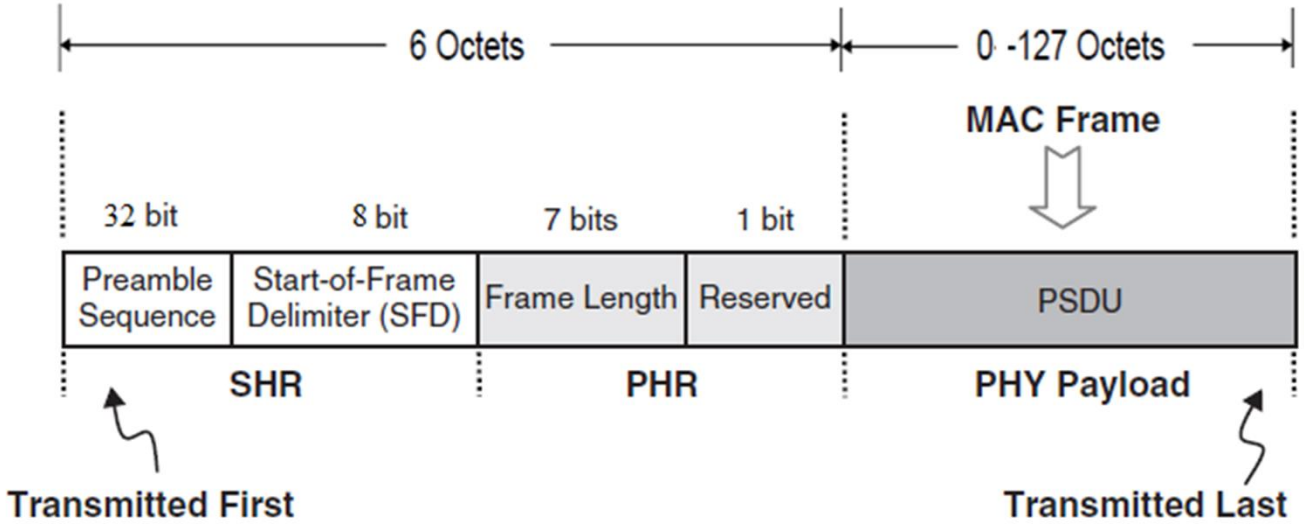
Each frequency_band with different low data rate

Channel number	Channel center frequency (MHz)
$k = 0$	868.3
$k = 1, 2, \ldots, 10$	$906 + 2(k - 1)$
$k = 11, 12, \ldots, 26$	$2405 + 5(k - 11)$

IEEE 802.15.4 Channel frequencies (total of 27 channels)

IEEE802.15.4 PHY Packet

- SHR: Synchronization Header
- PHR: PHY Header



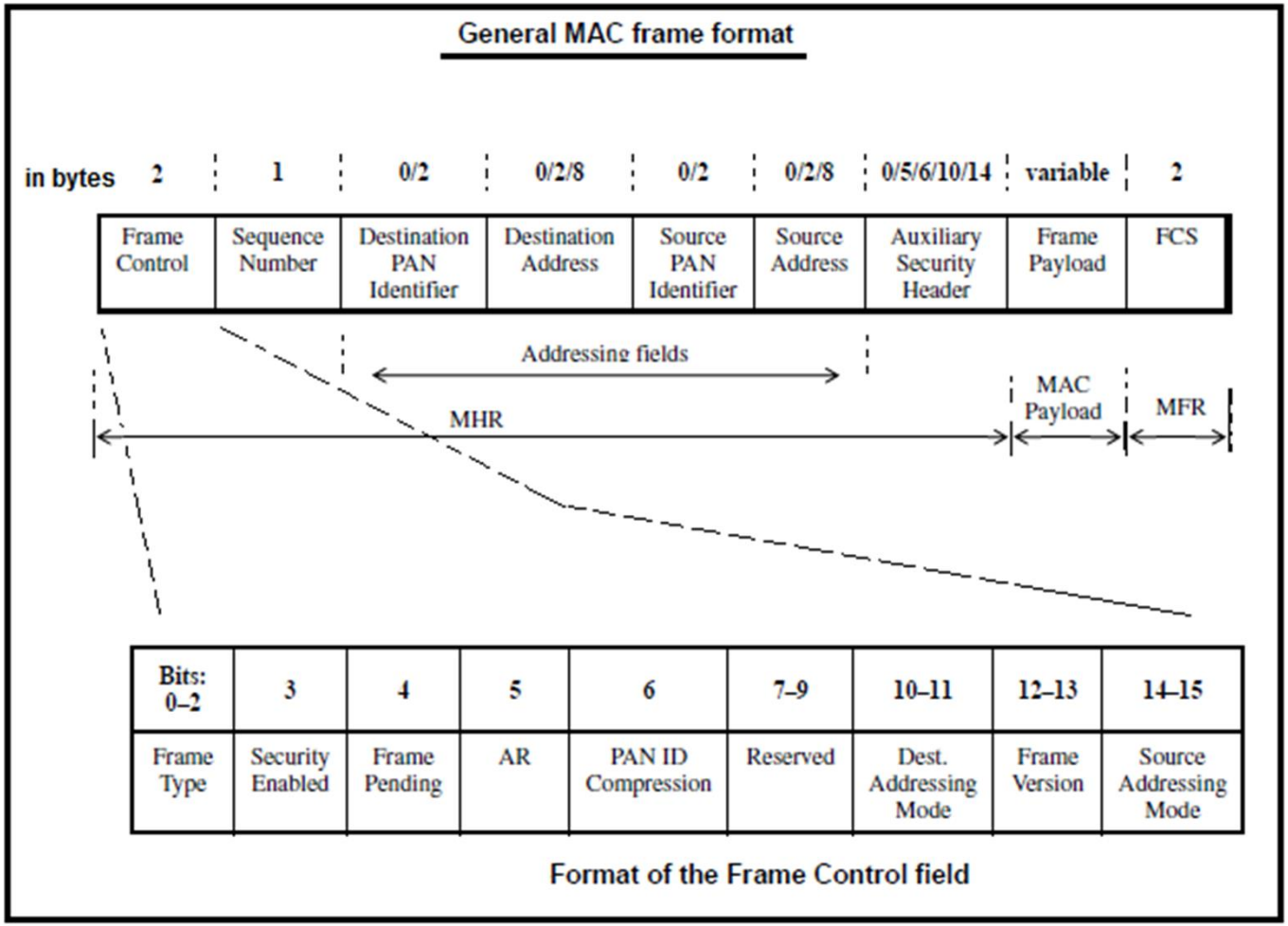
[Ref.1]

IEEE802.15.4 MAC Frame Structures

IEEE802.15.4 defines four MAC frame structures:

- Beacon frame (for beacon enabled PAN only)
  - Sent by coordinator only
- Data frame
- Acknowledge frame
- MAC command frame

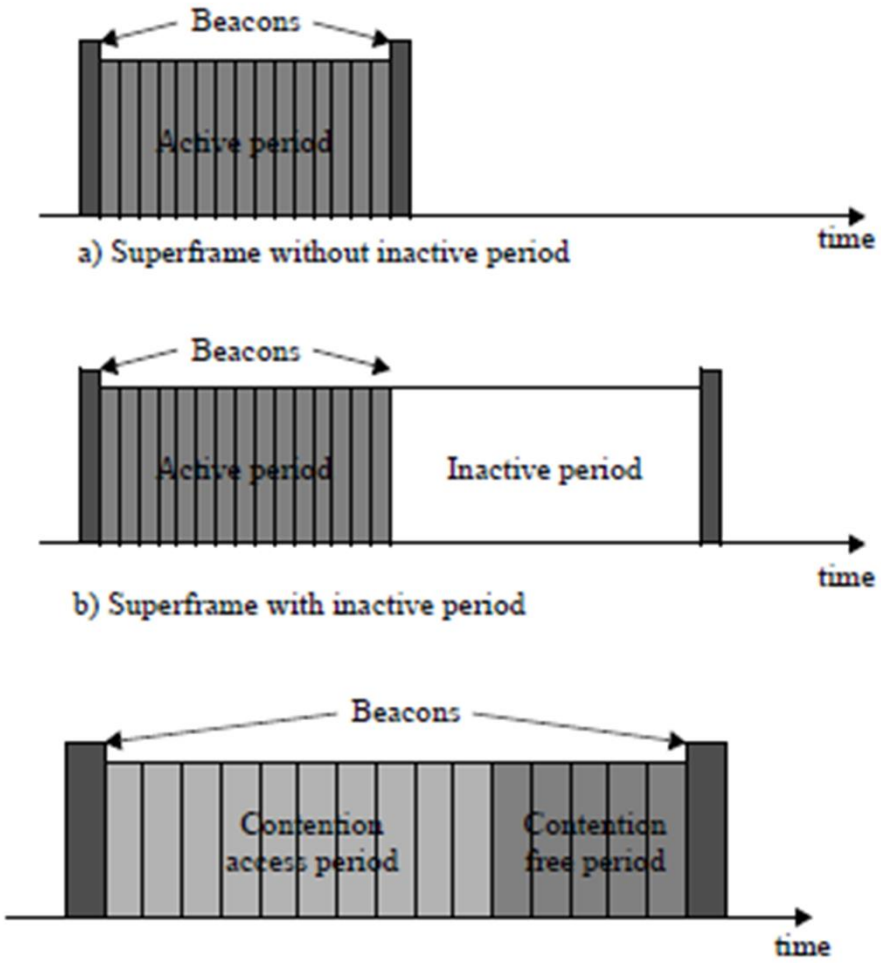
MAC frame format



[Ref.1]

IEEE802.15.4 MAC Superframe (optional)

- The *superframe: is a frame bounded by* two beacon frames, defined by coordinator.
- The superframe is optionally used only in a beacon-enabled PAN and helps define GTSs.



[Ref.1]

- The format of the superframe is defined by the PAN coordinator, by using the network beacons which bound the superframe structure.
- The superframe is composed of 16 equally sized time slots grouped in two sections: the contention access period (CAP) and the contention free period (CFP).

PAN and Coordinator

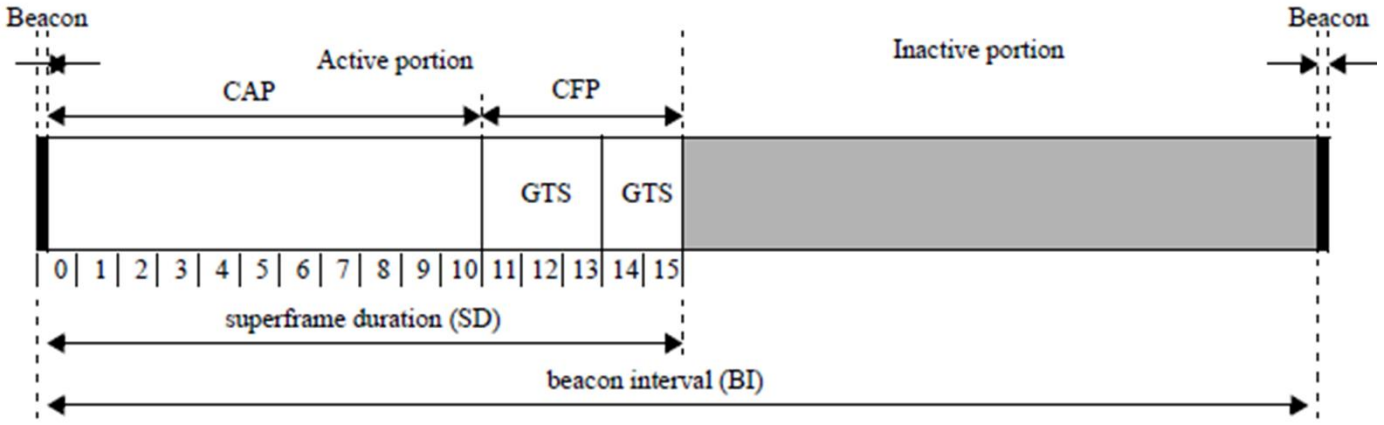
- One FFD can optionally act as a coordinator node. Which regulates media access. This node periodically sends beacons that identify the PAN it is coordinating.
- The interval between these beacons is constant but user selectable, any multiple of 15.38 ms, may separate these beacons up to 252s.
- Two beacons form a superframe that is partitioned into 16 equally sized timeslots. Members of the PAN may request guaranteed time slots (GTSs) in the contention free period (CFP) at the end of the superframe.
- All other slots from the contention access period (CAP), which is accessed using CSMA-CA scheme, and the media is always subject to contention.

Contention Access Period (CAP)

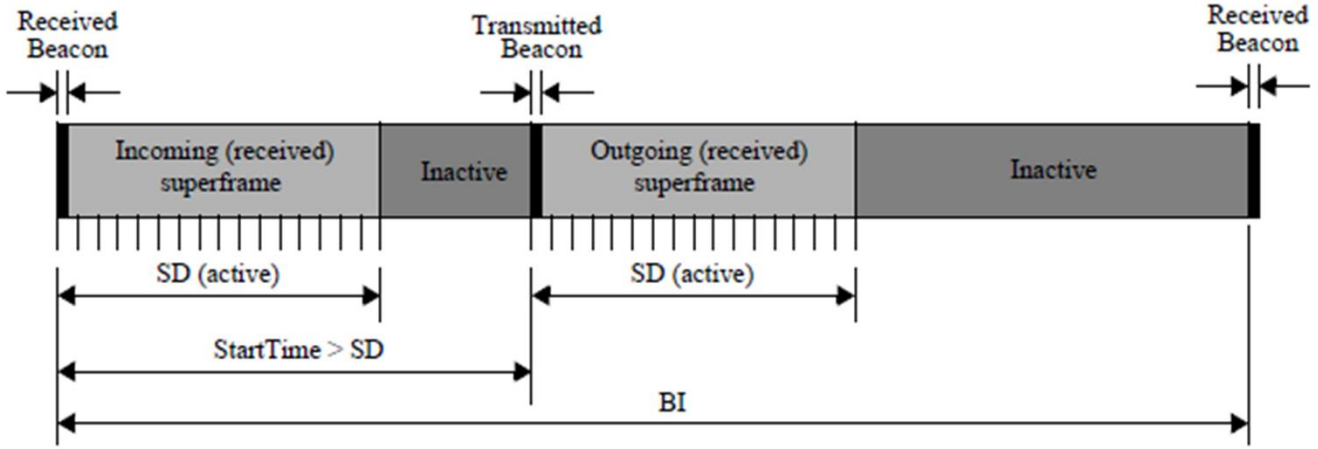
- Any device wishing to communicate during the **CAP** between two beacons competes with other devices using a slotted CSMA-CA or ALOHA mechanism, as appropriate.
- There are two types of CSMA-CA: slotted and unslotted. *Slotted CSMA-CA is referred* to as performing CSMA-CA while there is a superframe structure in place. A superframe divides the active period into 16 equal time slots.
- A nonbeacon-enabled PAN always uses the unslotted CSMA-CA algorithm for channel access.

Superframe Structure

- **CAP**: Contention Access Period.
- **CFP**: Contention Free Period.
- **BI**: Beacon Interval
- **GTS**: Guarantee Time Slot
- **SD**: Superframe Duration



a) superframe structure showing frame duration and beacon interval

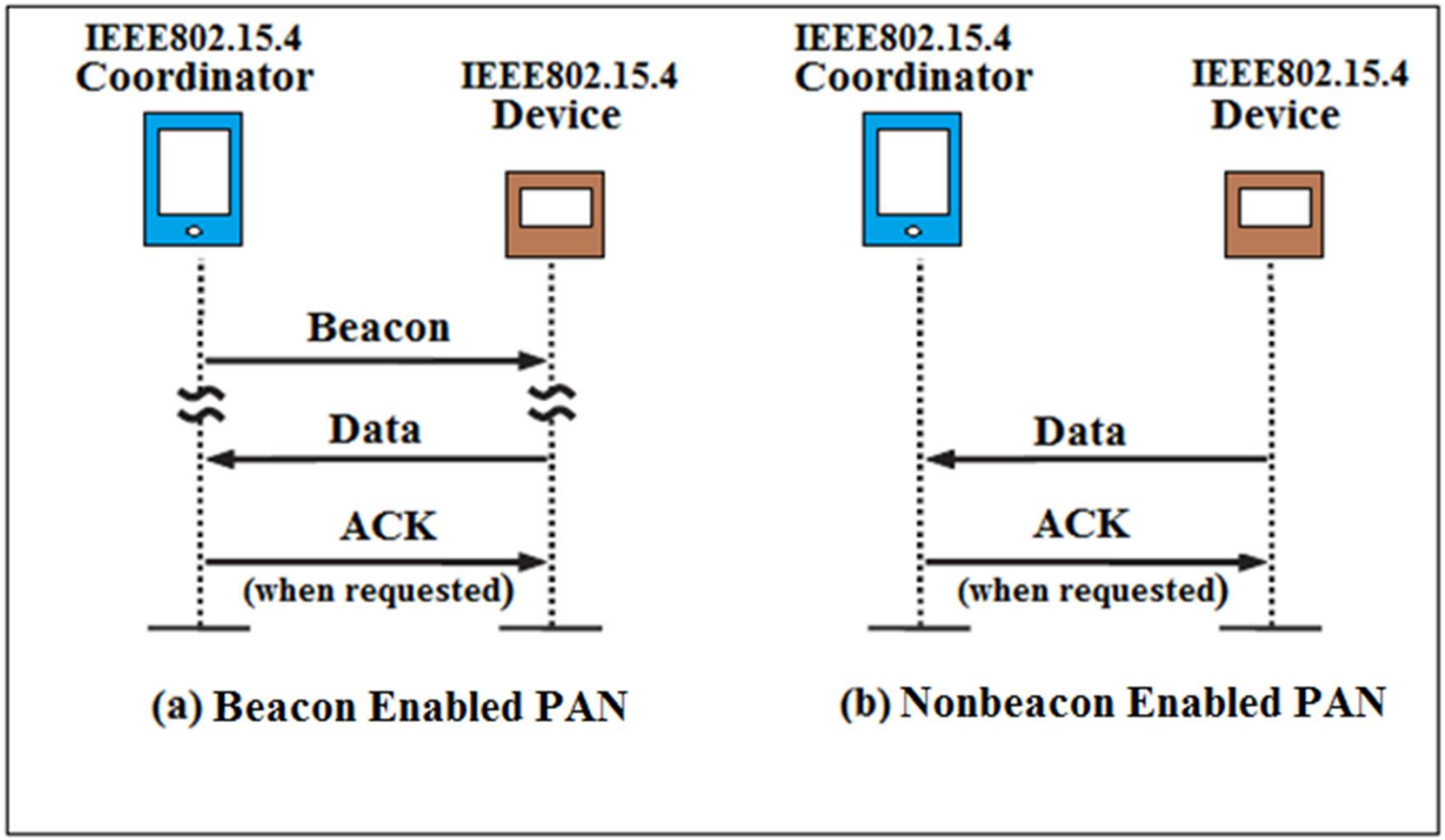


b) two superframes showing the relationship between incoming and outgoing beacons [Ref.1]

The Basic Communication

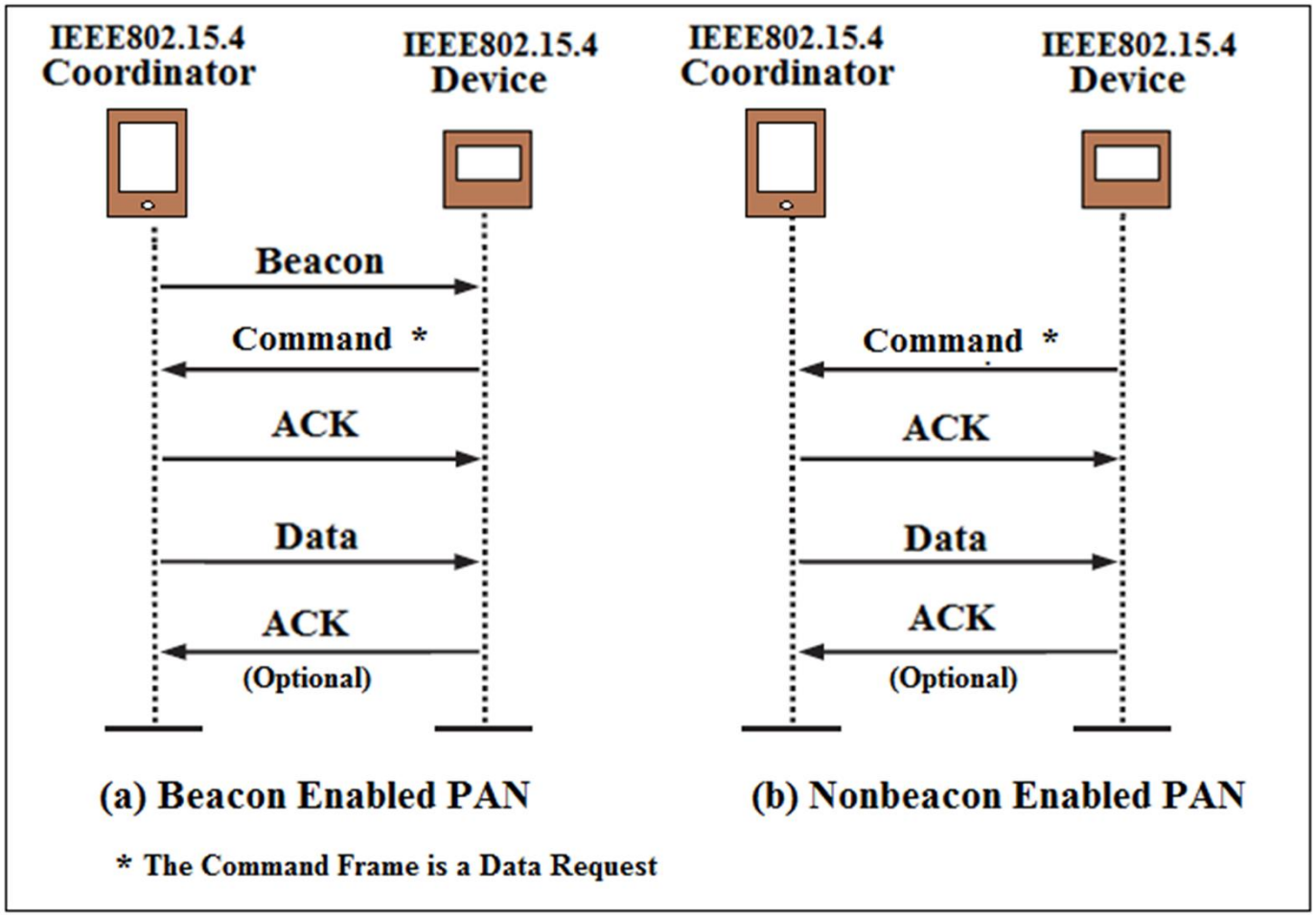
- There are three types of data transfer in IEEE 802.15.4:-
  - Data transfer to a coordinator from a device.
  - Data transfer from a coordinator to a device.
  - Data transfer between two peer devices.

Sending Data to a coordinator



IEEE802.15.4 Communication to the Coordinator

Sending Data to a Device



IEEE802.15.4 Communication To the Device

IEEE802.15.4 Security

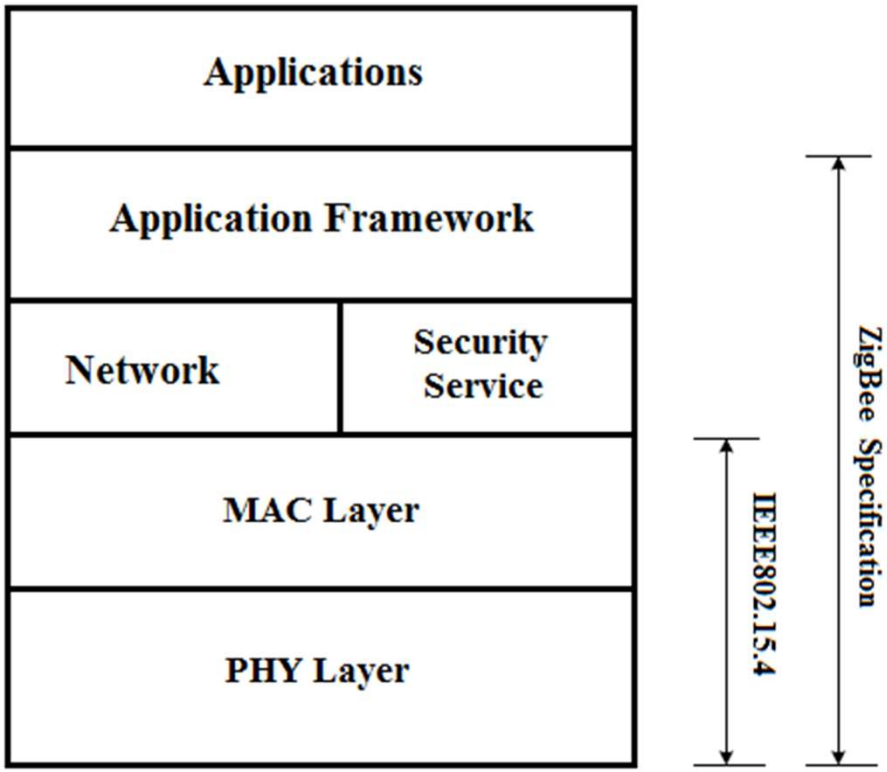
- 802.15.4 compliant MAC layers are required to encrypt packets using the AES-128 algorithm when a private key is provided by the upper layers.

- 802.15.4 does not define how AES keys are to be distributed and selected throughout the PAN. This decision is left to the discretion of the upper layers.

- This does not inherently protect nodes from replay attacks. Application and/or device developers must manually build replay protection on top of 802.15.4's AES encryption.

ZigBee System Architecture

- ZigBee built on top of IEEE802.15.4 to extend it and provide bluetooth like interoperability and applications with low power consumption.



ZigBee Architecture [Ref.2]

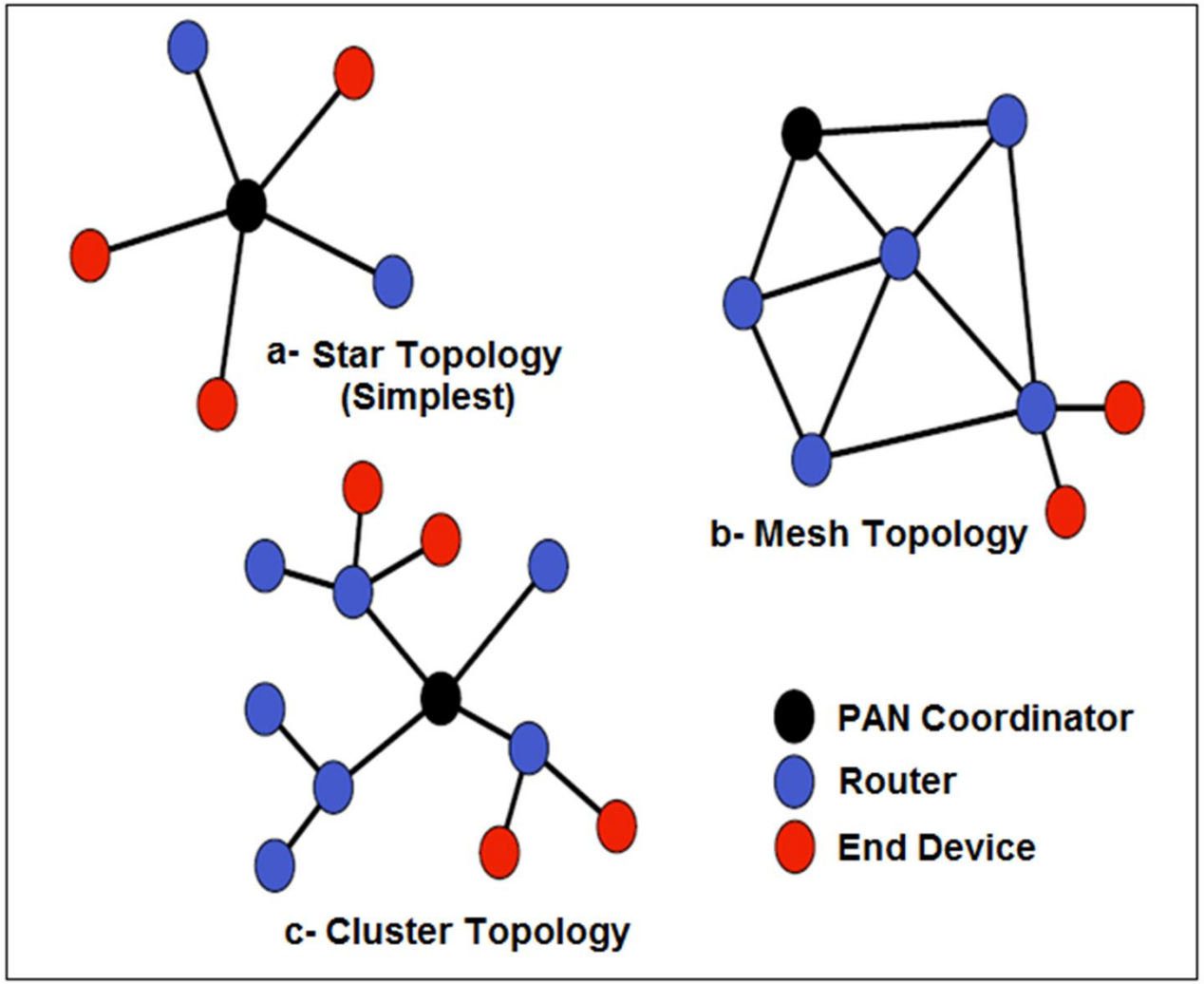
Three ZigBee Devices

ZigBee refines 802.15.4's two device categories into three hierarchical device roles:-

- *Coordinators:* are 802.15.4 FFDs that act as 802.15.4 coordinator nodes and maintain ZigBee-specific information about the PAN (master encryption keys, etc.).
- *Routers:* are 802.15.4 FFDs that participate in ZigBee's routing protocols.
- *End devices:* are analogous to 802.15.4's RFDs: they must communicate with each other by way of an intermediary coordinator or router.

- ZigBee devices can perform unicast or broadcast queries to discover other devices and/or perform service matchmaking.

ZigBee Topology



Three ZigBee Topologies [Ref.2]

Three Topologies

- ZigBee maintains 802.15.4's star topology, but divides the peer-to-peer topology into mesh and cluster topologies.
- Mesh topologies maintain a relatively fixed routing infrastructure, using a simplified version of the Ad-hoc On-demand Distance Vector (AODV) routing scheme.
- Cluster topologies create links between routers and coordinators opportunistically using a beaconing scheme.

ZigBee

- Network size: up to 65,535 nodes. Typical network join time 30 milliseconds.
- Manufactures describe a device's role and capabilities using a static device object.
- Device objects contain descriptions of the device's type, power, and communication endpoints, as well as optional complex fields describing device or manufacture specific information.
- Each device's service is described using an application object that encapsulates its attributes and capabilities.
- ZigBee does not define the format of application objects, this is left to the discretion of manufacturers.
- Each application object has a unique endpoint address (endpoint 1 to endpoint 240).

ZigBee Security [4]

- Has two security modes:
  - Residential mode: uses a single pre deployed key for the entire PAN and all applications, and hence very little overhead is involved.
  - Commercial mode: Two master keys are pre deployed in a trust center that resides on the coordinator node. Other devices negotiate with the trust center to derive per link keys from one of these two master keys.

Applications and Future Outlook

- 802.15.4 has been rapidly adopted by the sensor network community, where battery life is at a premium.
- Industry is using 802.15.4 or ZigBee enabled sensors joined by a Bluetooth or 802.11b backbone to create powerful system for healthcare monitoring and industrial automation.
- ZigBee has also been positioned as a standard for communication among home automation devices, such as wireless electrical switches.

References

[1] WG home page: http://www.ieee802.org/15/

[2] ZigBee Alliance: http://www.zigbee.org

[3] Ed Callaway, Paul Gorday, Lance Hester, Jose A. Gutierrez, Marco Naeve, Bob Heile, Home Networking with IEEE 802.15.4: Developing Standard for Low-Rate Wireless Personal Area Networks, *IEEE Communications Magazine, August 2002.*

[4] Hackmann, 802.15 PAN, scientific paper