Contents

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
  - Physical Layer Issues
  - Communication Technologies Criteria
  - Communication Technologies and Protocols

Mostly adopted from Chapters 4, 5, and 6 of IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Communication Technologies Criteria-Summary

- These criteria include: range, frequency bands, power consumption, network topology, the presence of constrained devices and/or networks, and data throughput.

- From a network engineer perspective, you must make sure an architecture is developed with the proper abstraction for a particular access technology.
  - This is especially true for constrained network nodes, where quite often your choices of protocols and solutions can be limited.

- The next section reviews the main IoT access technologies dedicated to constrained networks.

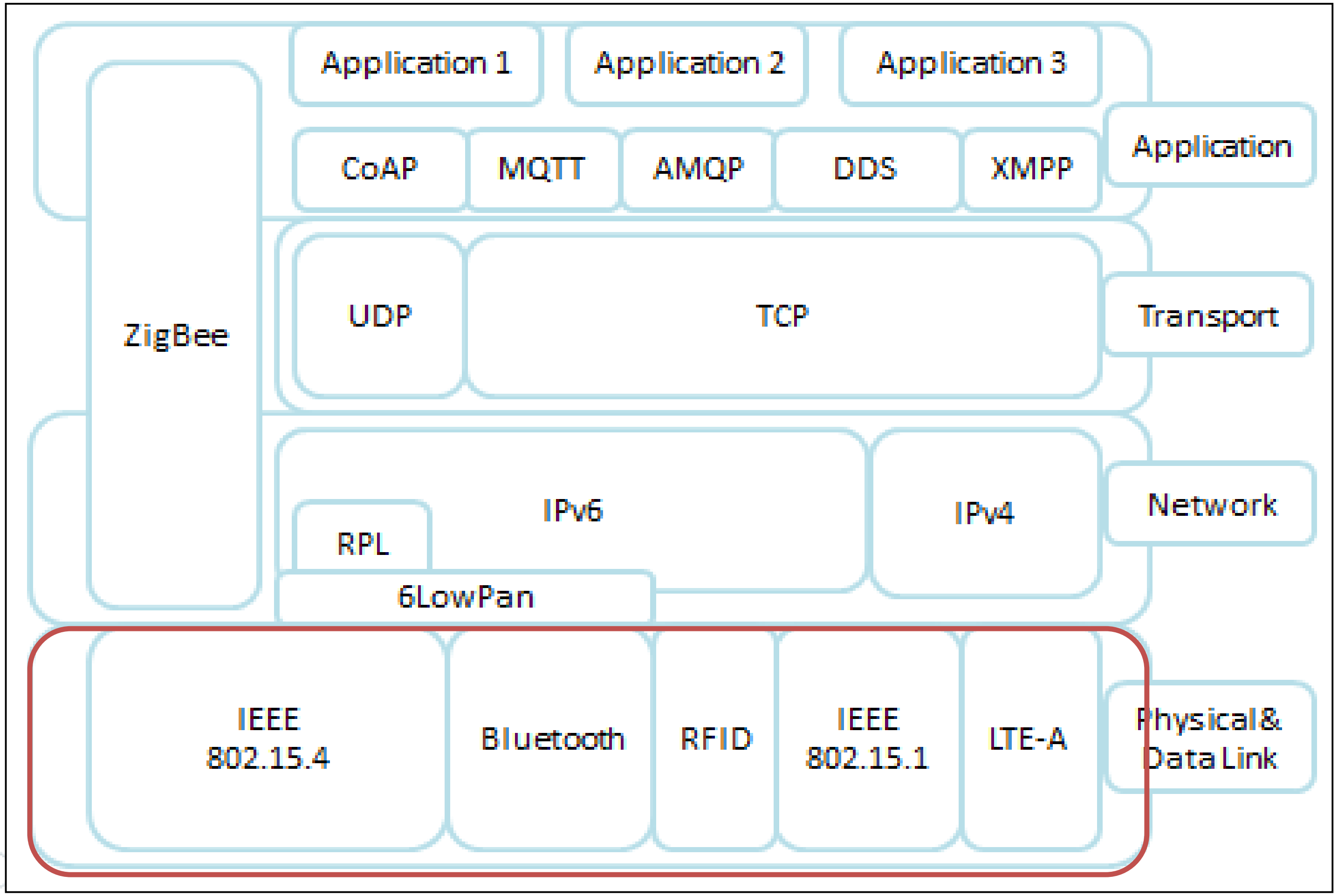
* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IoT Protocol Stack- Physical and Link Layers Protocols

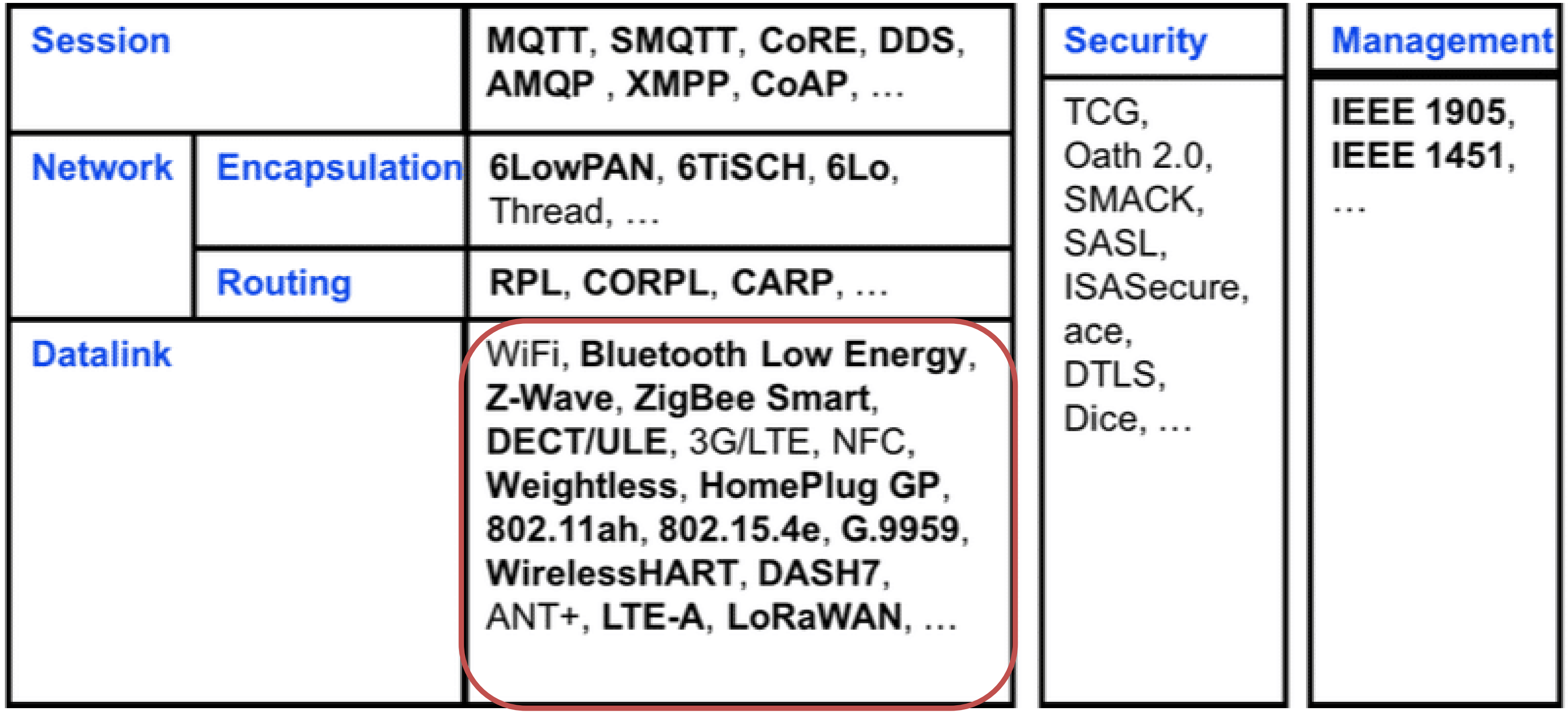
- IEEE 802.15.4
- IEEE 802.11
- ZigBee
- Bluetooth Low Energy (BLE)
- low-power Wi-Fi
- LoRaWAN
- NB-IoT
- power line communications (PLC)

* Internet of Things Architectures, Protocols and Standards, Wiley press, 2019
* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IoT Protocol Stack- Physical and Link Layers Protocols



IoT Protocol Stack- Physical and Link Layers Protocols



Session		MQTT, SMQTT, CoRE, DDS, AMQP , XMPP, CoAP, …
Network	Encapsulation	6LowPAN, 6TiSCH, 6Lo, Thread, …
	Routing	RPL, CORPL, CARP, …
Datalink		WiFi, Bluetooth Low Energy, Z-Wave, ZigBee Smart, DECT/ULE, 3G/LTE, NFC, Weightless, HomePlug GP, 802.11ah, 802.15.4e, G.9959, WirelessHART, DASH7, ANT+, LTE-A, LoRaWAN, …

Security
TCG, Oath 2.0, SMACK, SASL, ISASecure, ace, DTLS, Dice, …

Management
IEEE 1905, IEEE 1451, …

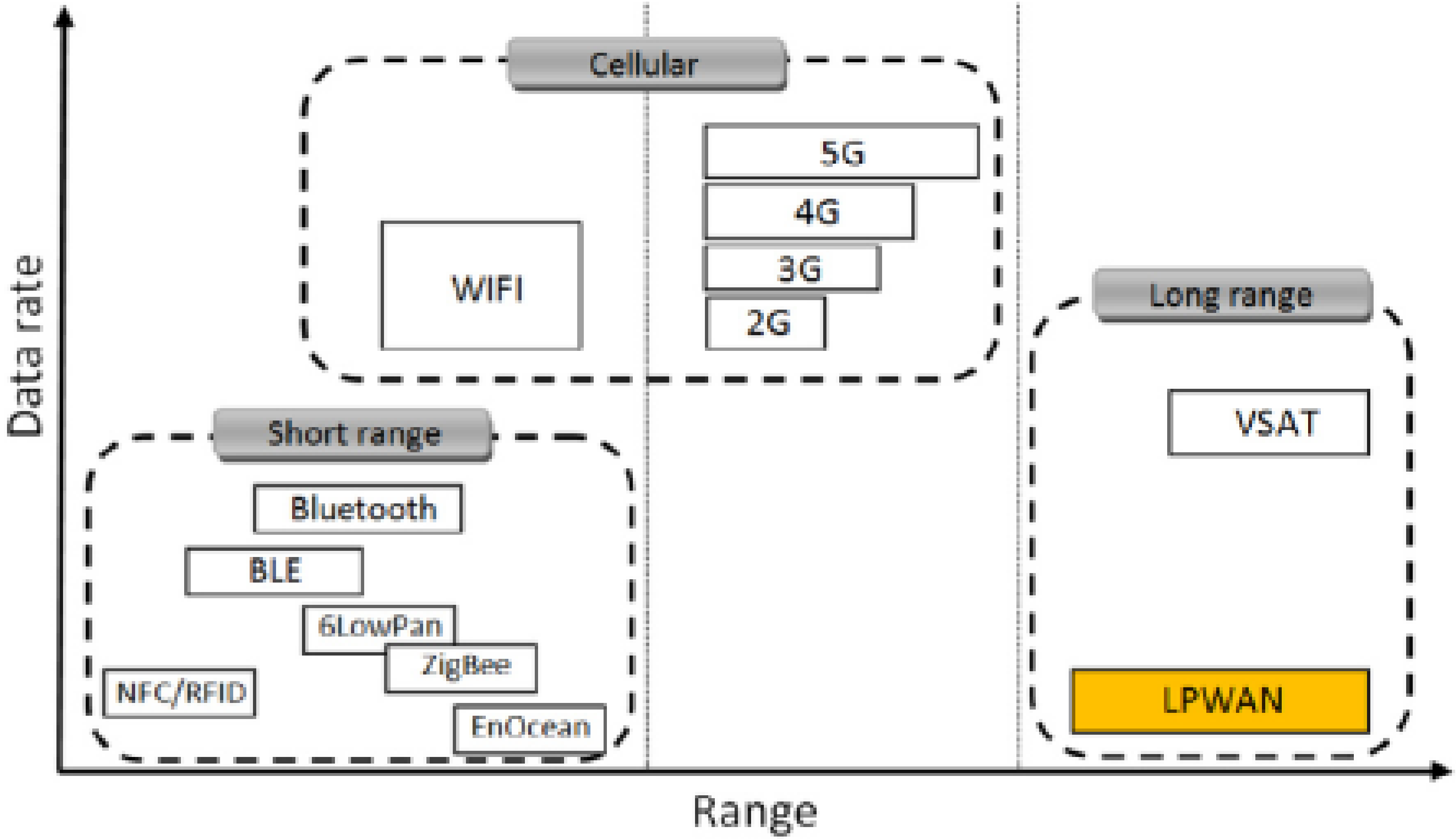
IoT Protocol Stack- Physical and Link Layers Protocols

- Short-range and low-power wireless networks:
  - Low Power BAN, PAN, Low power LAN
    - 802.15.4
    - Bluetooth Low Energy
    - 802.11h
    - NFC
    - …

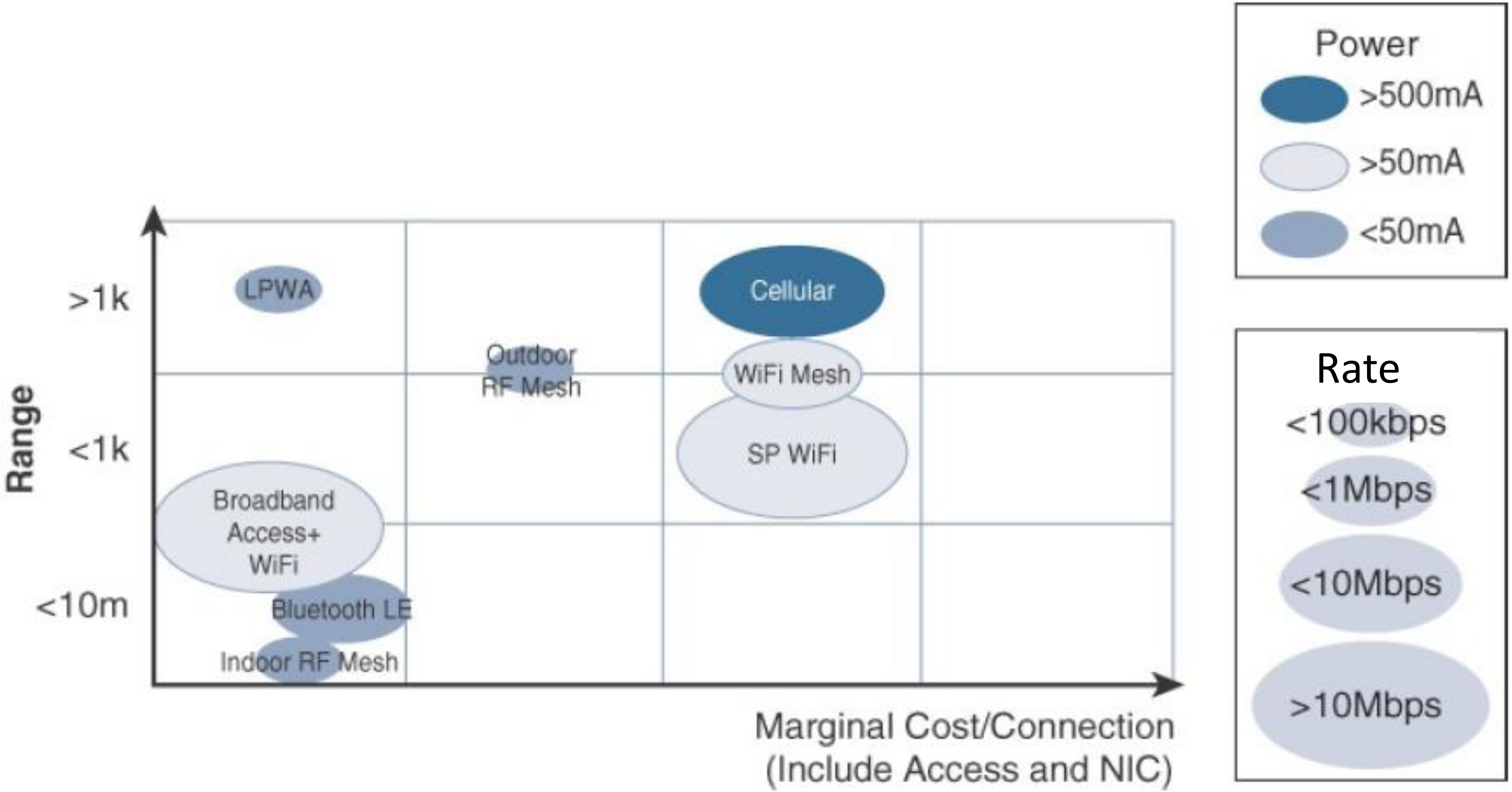
- Long-range and low-power wireless networks:
  - Low Power WAN (LPWAN)
    - LoRaWAN
    - NB-IoT
    - SigFox

IoT Protocol Stack- Physical and Link Layers Protocols

Required Data Rate vs. Range

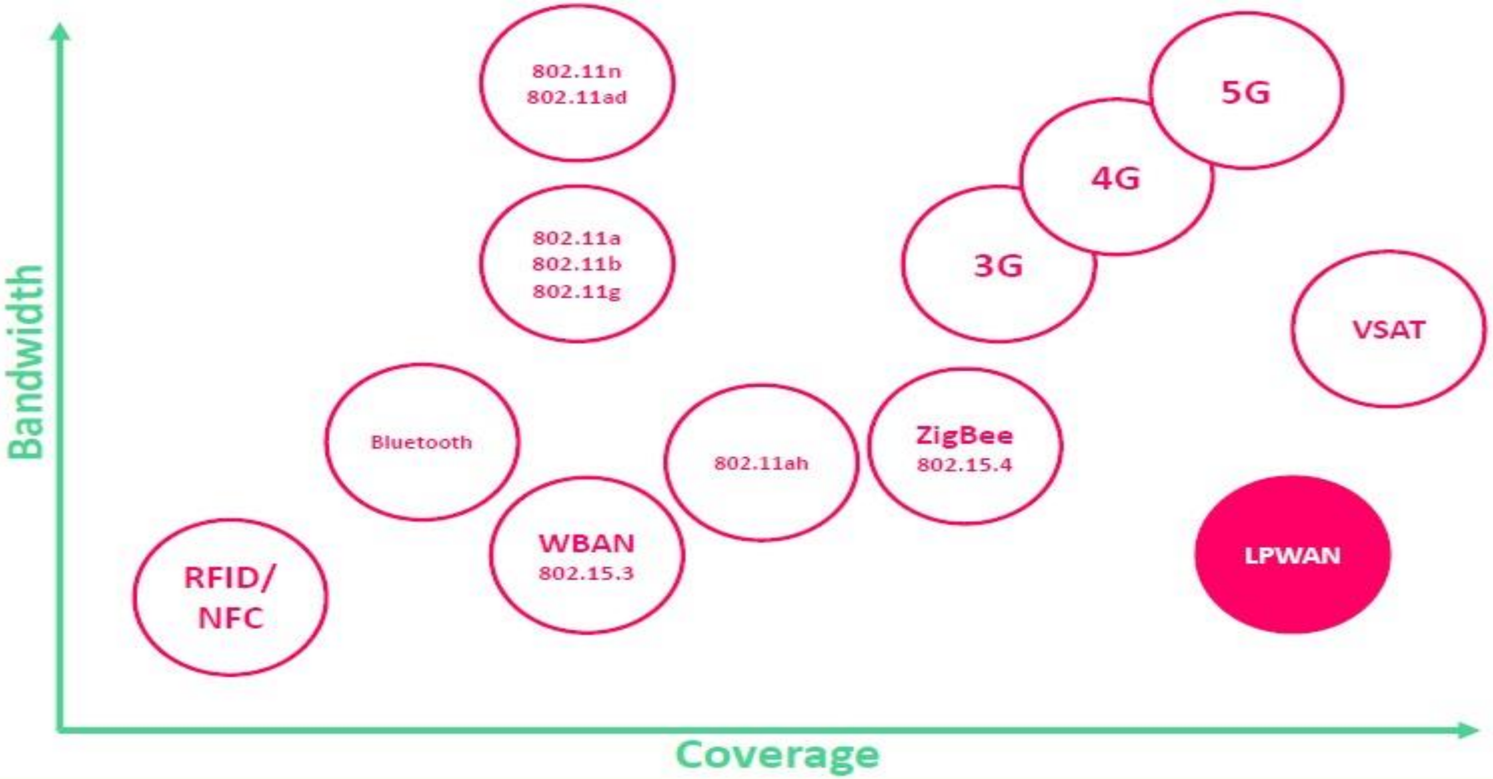


Comparison Between Common Access Technologies in Terms of Range Versus Power, Rate and Cost



Communication Technologies Comparison

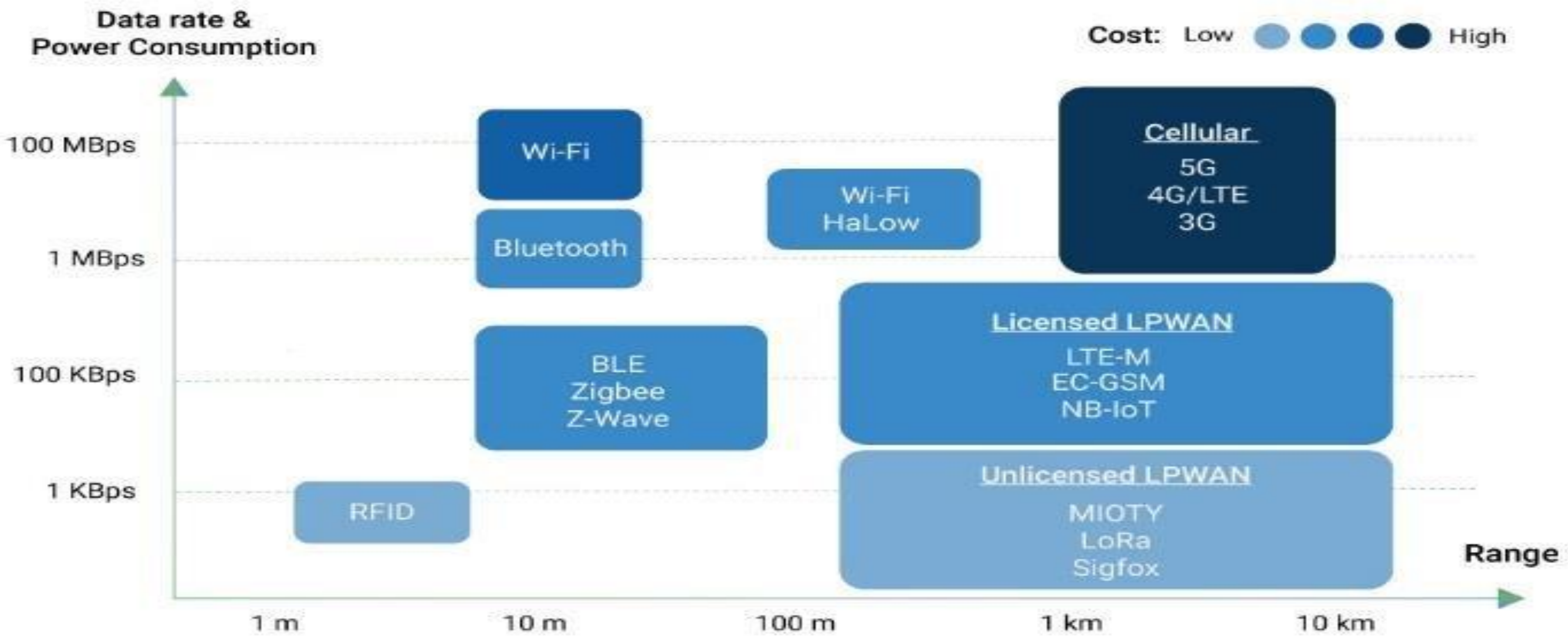
- Range vs Bandwidth



* Introduction to the Internet of Thing, Telecommunication Department, Monenco Iran

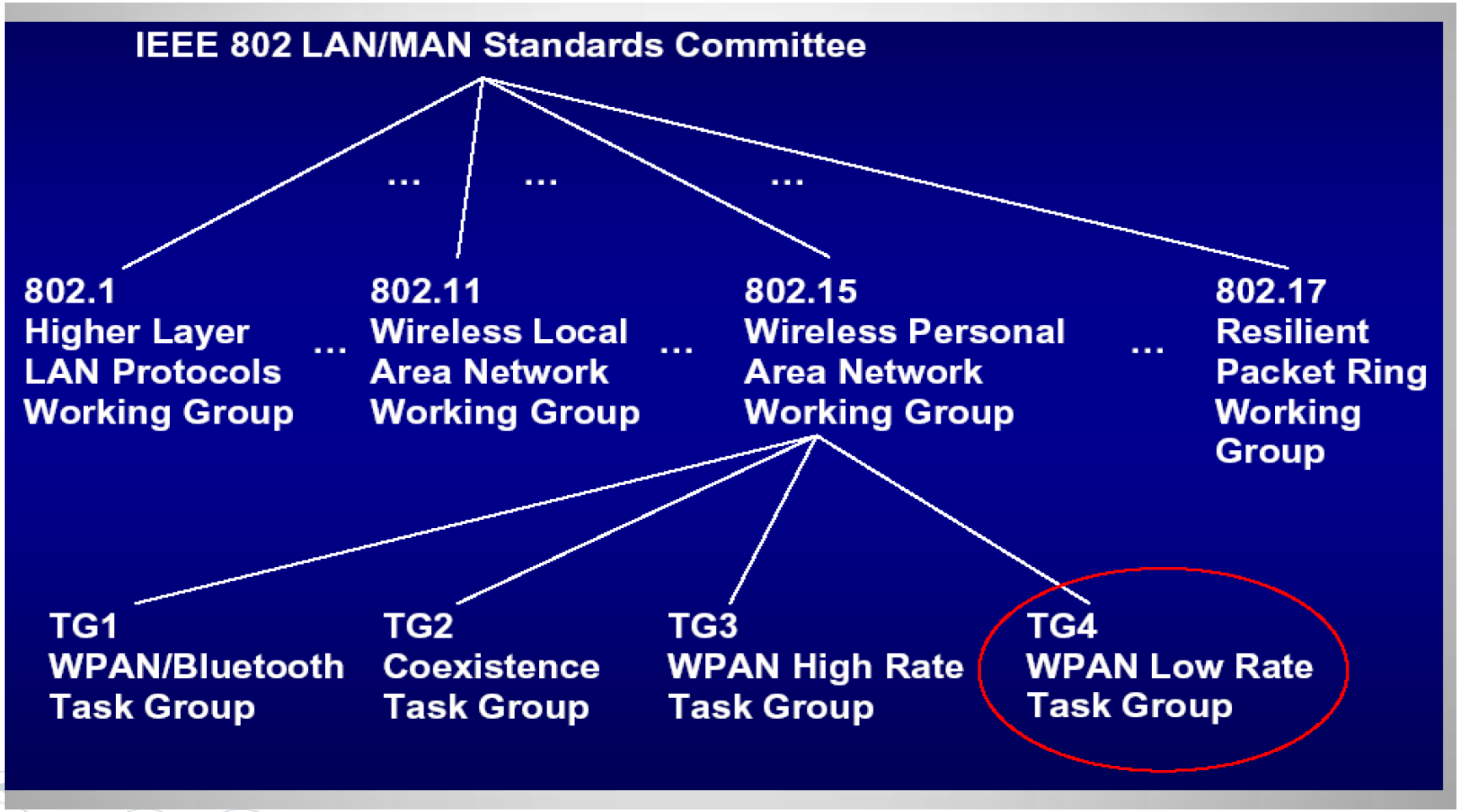
Communication Technologies Comparison

- Data Rate vs Range and Power consumption



* https://behrtech.com/blog/6-leading-types-of-iot-wireless-tech-and-their-best-use-cases/

IoT Protocol Stack- Physical and Link Layers Protocols



IoT Protocol Stack- Physical and Link Layers Protocols

- For each of the IoT access technologies, a common information set is being provided:
  - **Standardization and alliances:** The standards bodies that maintain the
  - protocols for a technology
  - **Physical layer:** The wired or wireless methods and relevant
  - frequencies
  - **MAC layer:** Considerations at the Media Access Control (MAC) layer,
  - which bridges the physical layer with data link control
  - **Topology:** The topologies supported by the technology
  - **Security:** Security aspects of the technology
  - **Competitive technologies:** Other technologies that are similar and may be suitable alternatives to the given technology

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Contents

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
  - Physical Layer Issues
  - Communication Technologies Criteria
  - Communication Technologies and Protocols
    - Short Range Access technologies (PHY and Link Layer Protocols)
    - Long Range Access technologies (PHY and Link Layer Protocols)
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

Mostly adopted from Chapters 4, 5, and 6 of IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Contents

- Introduction
- Physical and Link Layers Protocols (IoT Access Technologies)
  - Physical Layer Issues
  - Communication Technologies Criteria
  - Communication Technologies and Protocols
    - – Short Range Access technologies (PHY and Link Layer Protocols)
    - – Long Range Access technologies (PHY and Link Layer Protocols)
- Network Layer Protocols (IP as the IoT Network Layer)
- Transport Layer Protocols
- Application Layer Protocols

Mostly adopted from Chapters 4, 5, and 6 of IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices powered or run on batteries.

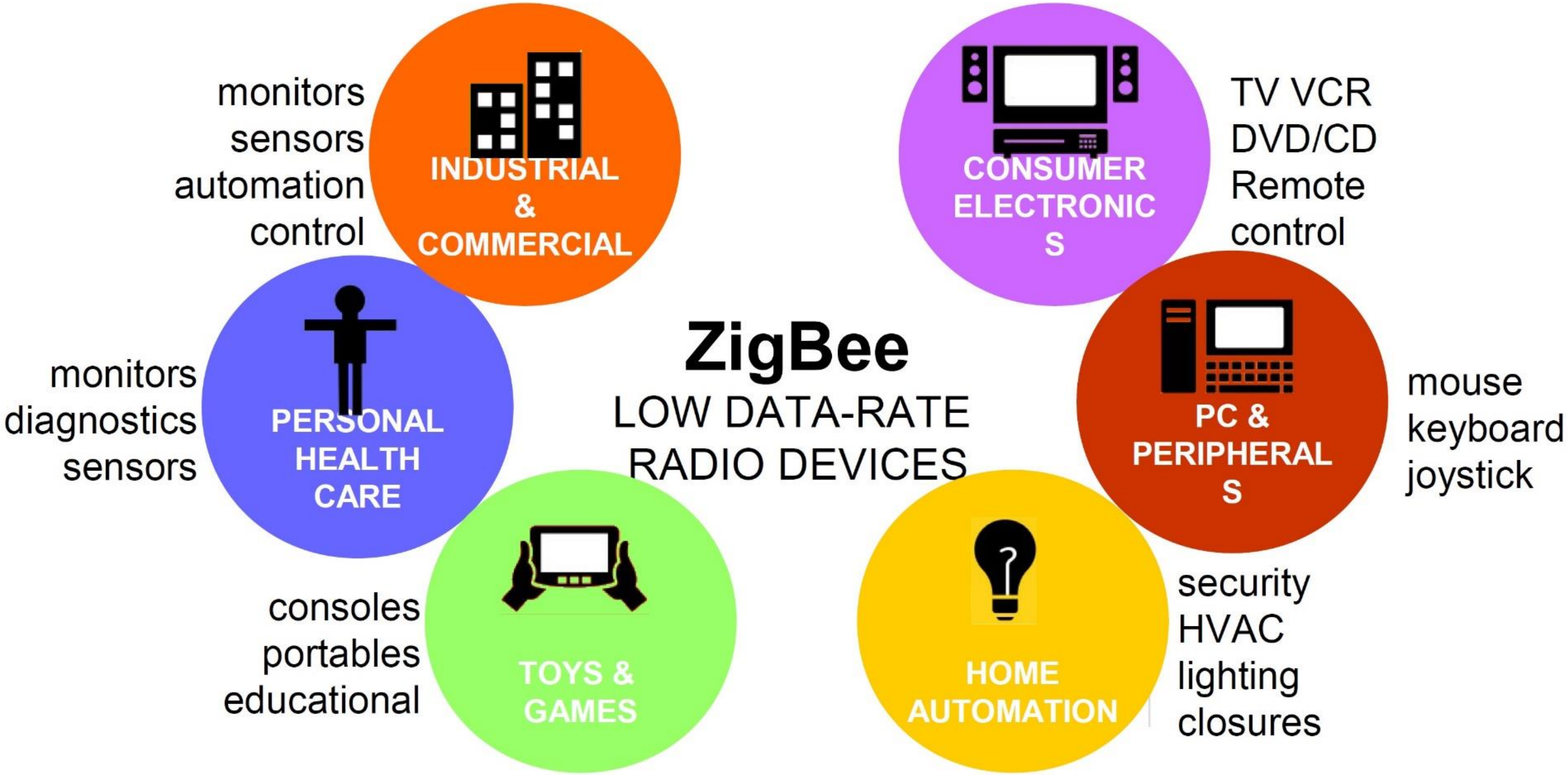
- IEEE 802.15.4 (or IEEE 802.15 Task Group 4)
  - Defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN).
  - For low complexity wireless devices with low data rates that need many months or even years of battery life.

- Used in following types of deployments:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4

- Application Sector



Heating, Ventilation and Air Conditioning systems (HVAC)

Physical and Link Layers Protocols- IEEE 802.15.4

- Since 2003, the IEEE has published several iterations of the IEEE 802.15.4 specification, each labeled with the publication's year:
  - IEEE 802.15.4-2003
  - 802.15.4-2006,
  - 802.15.4-2011 and 802.15.4-2015.

- Newer releases typically supersede older ones, integrate addendums, and add features or clarifications to previous versions

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- IEEE 802.15.4

- IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks.

- These protocol stacks make use of 802.15.4 at the physical and link layer levels, but the upper layers are different:
  - ZigBee
  - ZigBee IP
  - 6LoWPAN
  - ISA100.11a
  - WirelessHART
  - Thread

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

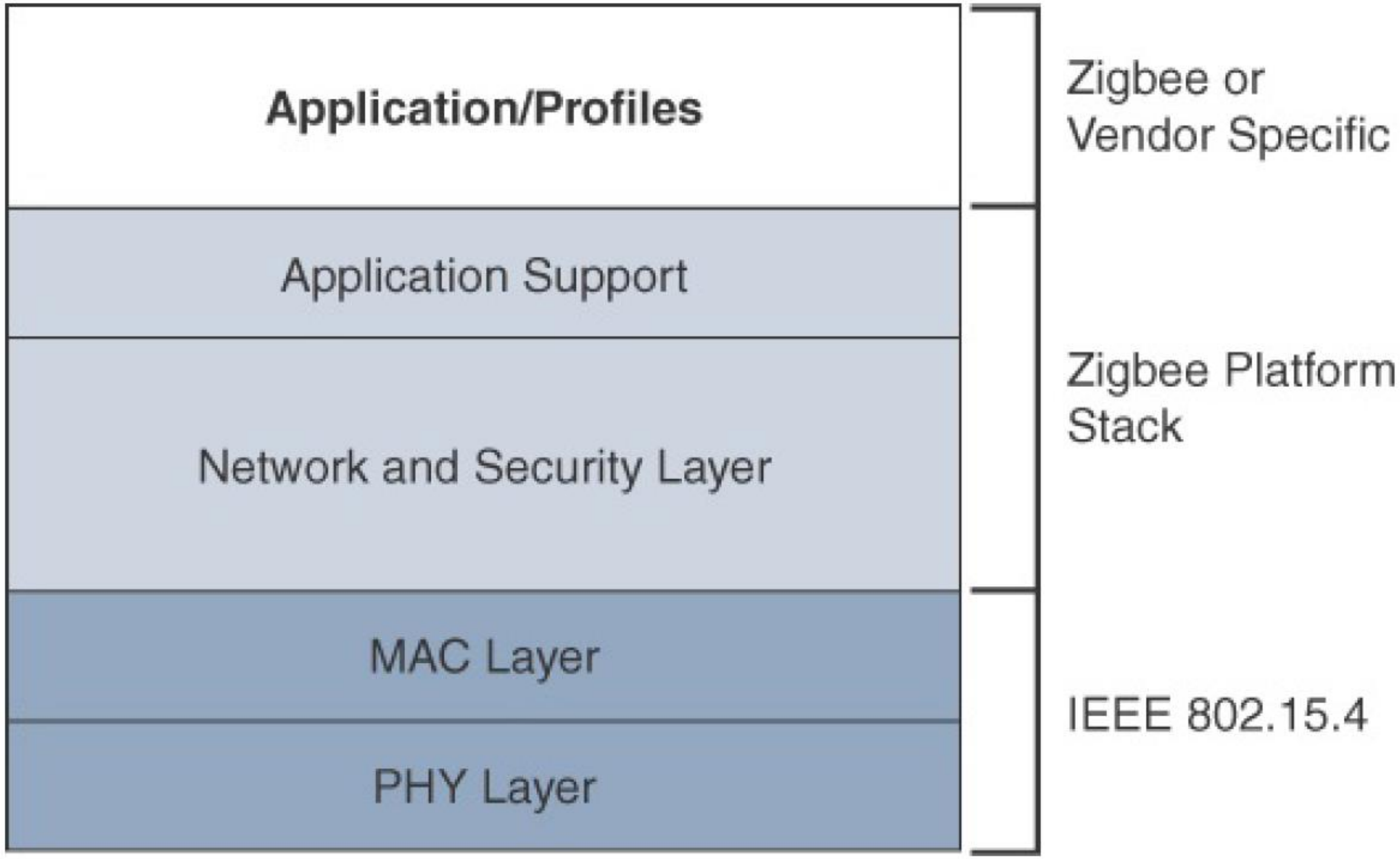
Protocol Stacks Using 802.15.4: ZigBee

- ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers.
  - ZigBee specifies the network and security layer and application support layer that sit on top of the lower layers.
- The first ZigBee specification was ratified in 2004,
  - shortly after the release of the IEEE 802.15.4 specification the previous year.
- While not released as a typical standard, like an RFC, ZigBee still had industry support from more than 100 companies upon its initial publication.
  - This industry support has grown to more than 400 companies that are members of the ZigBee Alliance.

* *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing*, Cisco press, 2017

Protocol Stacks Using 802.15.4: ZigBee

- High-Level ZigBee Protocol Stack



Protocol Stacks Using 802.15.4: ZigBee

- On top of the 802.15.4 PHY and MAC layers, ZigBee specifies its own network and security layer and application profiles.
- While this structure has provided a fair degree of interoperability for vendors with membership in the ZigBee Alliance, it has not provided interoperability with other IoT solutions.
- However, this has started to change with the release of ZigBee IP, which is discussed next.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Protocol Stacks Using 802.15.4: ZigBee IP

- With the introduction of ZigBee IP, the support of IEEE 802.15.4 continues, but the IP and TCP/UDP protocols and various other open standards are now supported at the network and transport layers.

- The ZigBee-specific layers are now found only at the top of the protocol stack for the applications.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

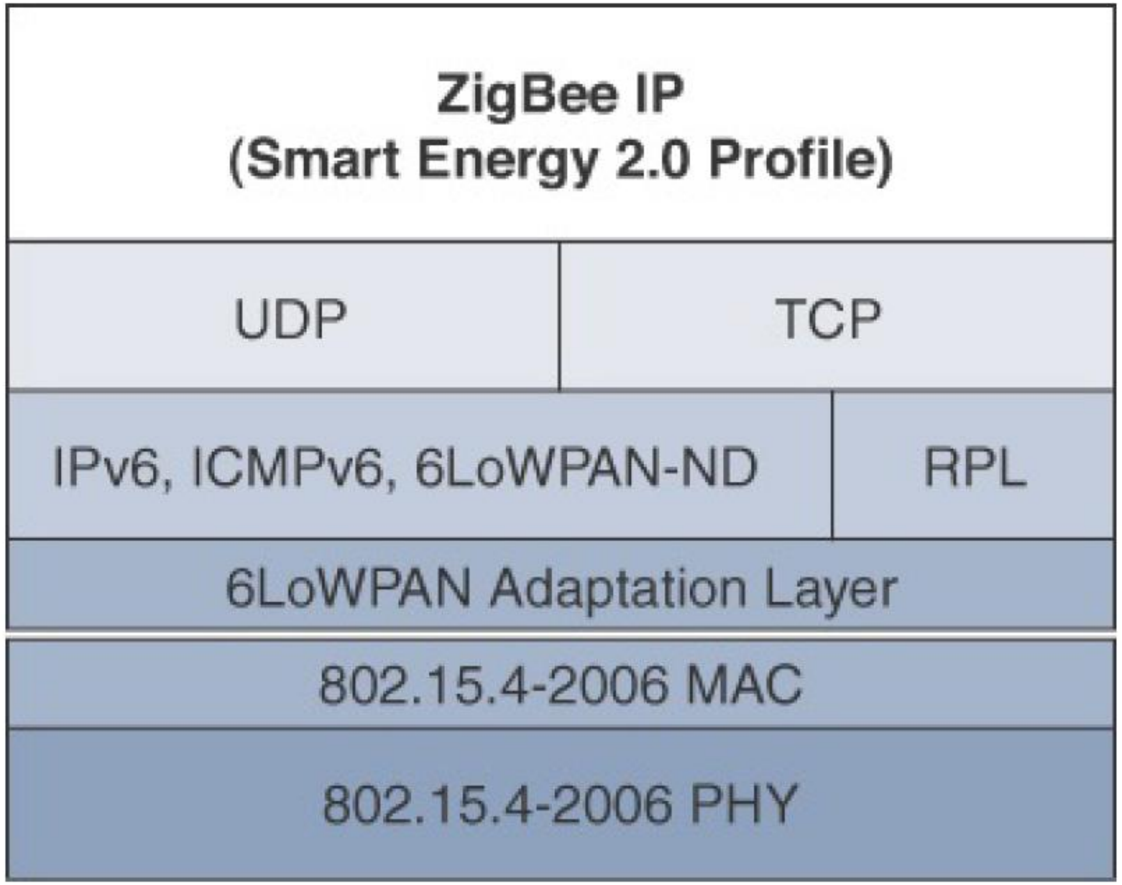
Protocol Stacks Using 802.15.4: ZigBee IP

- ZigBee IP was created to embrace the open standards coming from the IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL.
- They provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.
- ZigBee IP is a critical part of the Smart Energy (SE) Profile 2.0 specification from the ZigBee Alliance.
  - SE 2.0 is aimed at smart metering and residential energy management systems.
  - In fact, ZigBee IP was designed specifically for SE 2.0 but it is not limited to this use case. Any other applications that need a standards-based IoT stack can utilize Zigbee IP.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Protocol Stacks Using 802.15.4: ZigBee

- The ZigBee IP stack



ZigBee IP
(Smart Energy 2.0 Profile)

UDP | TCP

IPv6, ICMPv6, 6LoWPAN-ND | RPL

6LoWPAN Adaptation Layer

802.15.4-2006 MAC

802.15.4-2006 PHY

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Physical and Link Layers Protocols- ZigBee

- ZigBee
  - ZigBee is aimed at smart objects and sensors that have low bandwidth and low power needs.
  - Functions for a device
    - Metering
    - Temperature
    - Lighting control

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

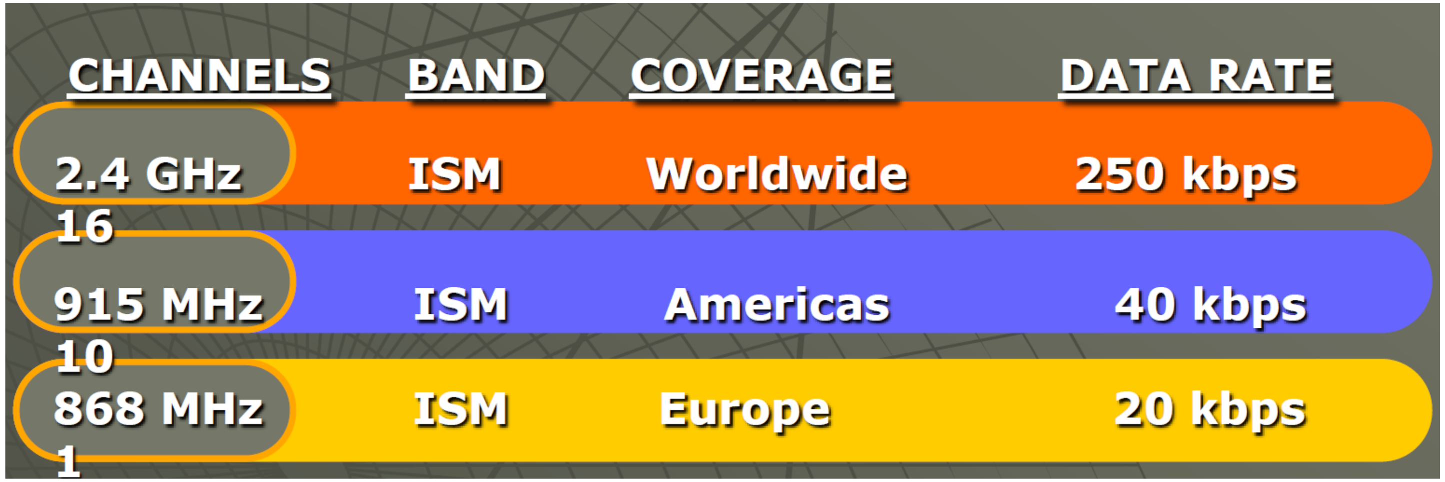
IEEE 802.15.4: Physical Layer

- IEEE 802.15.4- Physical layer
  - The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands.
  - The original physical layer transmission options were as follows:
    - 2.4 GHz, 16 channels, with a data rate of 250 kbps
    - 915 MHz, 10 channels, with a data rate of 40 kbps
    - 868 MHz, 1 channel, with a data rate of 20 kbps
  - only the 2.4 GHz band operates worldwide.
  - The 915 MHz band operates mainly in North and South America, and the 868 MHz frequencies are used in Europe, the Middle East, and Africa.

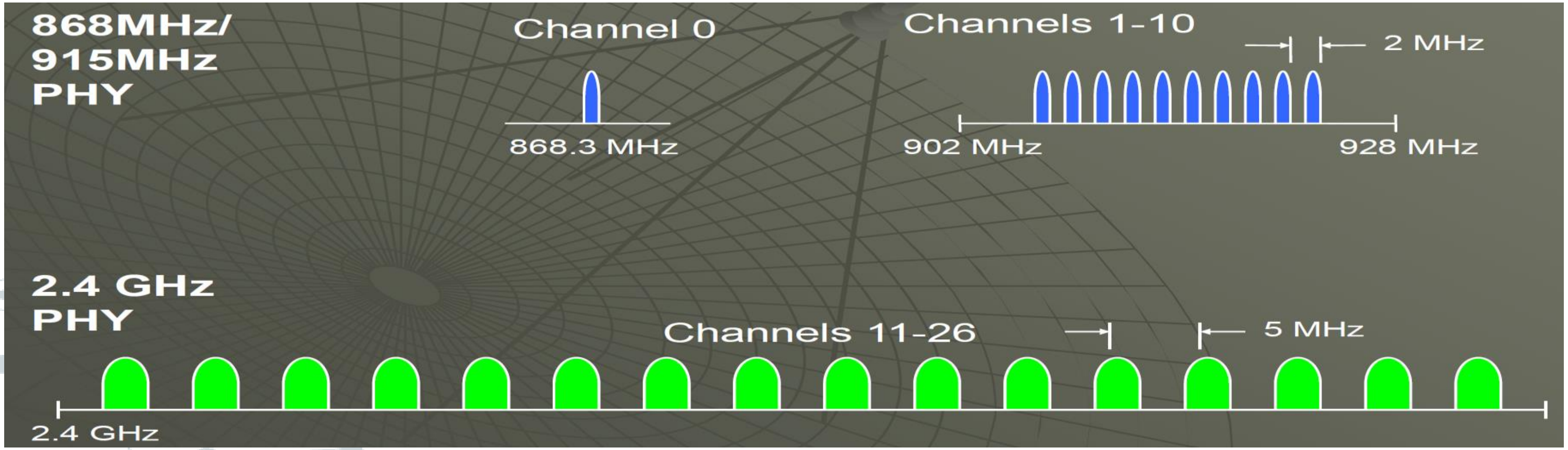
* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: Physical Layer

- Frequency and Channels



CHANNELS	BAND	COVERAGE	DATA RATE
2.4 GHz 16	ISM	Worldwide	250 kbps
915 MHz 10	ISM	Americas	40 kbps
868 MHz 1	ISM	Europe	20 kbps



IEEE 802.15.4: Physical Layer

- The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation.

- DSSS is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: Physical Layer

- IEEE 802.15.4-2006, 802.15.4-2011, and IEEE 802.15.4-2015 introduced additional PHY communication options, including the following:
  - **OQPSK PHY**
    - This is DSSS PHY, employing offset quadrature phase shift keying (OQPSK) modulation. OQPSK is a modulation technique that uses four unique bit values that are signaled by phase changes.
    - An offset function that is present during phase shifts allows data to be transmitted more reliably.
  - **BPSK PHY**
    - This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation.
    - BPSK specifies two unique phase shifts as its data encoding scheme.
  - **ASK PHY**
    - This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation.
    - PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS.
    - ASK uses amplitude shifts instead of phase shifts to signal different bit values.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: Physical Layer

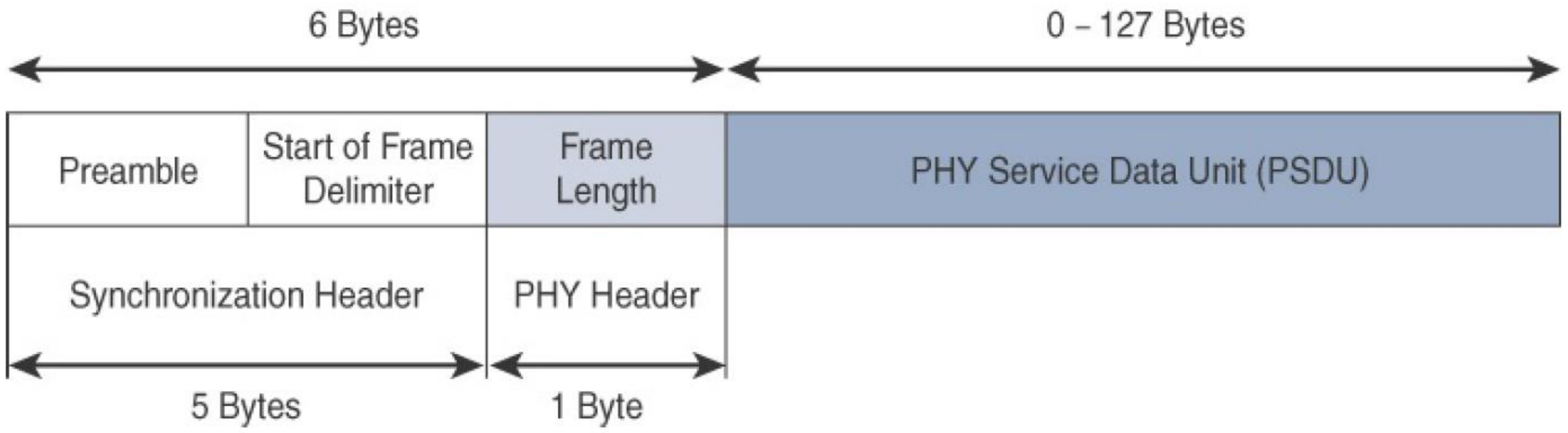
- These improvements increase the maximum data rate for both 868 MHz and 915 MHz to 100 kbps and 250 kbps, respectively.

- The 868 MHz support was enhanced to 3 channels, while other IEEE 802.15.4 study groups produced addendums for new frequency bands. For example, the IEEE 802.15.4c study group created the bands 314–316 MHz, 430–434 MHz, and 779–787 MHz for use in China.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: Physical Layer

- *IEEE 802.15.4 PHY Format:*



- The synchronization header (to synchronize the data transmission) for this frame is composed of
  - The Preamble
  - The Start of Frame Delimiter fields.

- The Preamble field is a 32-bit 4-byte (for parallel construction) pattern that identifies the start of the frame and is used to synchronize the data transmission.
  - The Start of Frame Delimiter field informs the receiver that frame contents start immediately after this byte

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: Physical Layer

- Pay attention to which versions of 802.15.4 particular devices support.
  - The various versions and addendums to 802.15.4 over the years through various working groups have been made

- When providing details on the physical layer implementation, products and solutions must refer to:
  - Proper IEEE 802.15.4 specification,
  - Frequency band,
  - Modulation,
  - Data rate.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

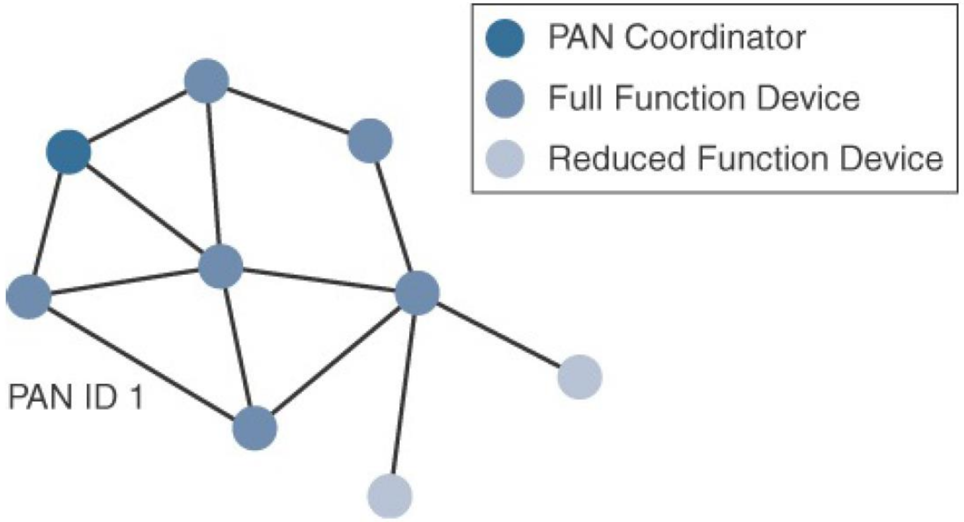
IEEE 802.15.4: MAC Layer

- IEEE 802.15.4
  - Topology
    - Star
    - Peer-to-Peer
    - Mesh

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

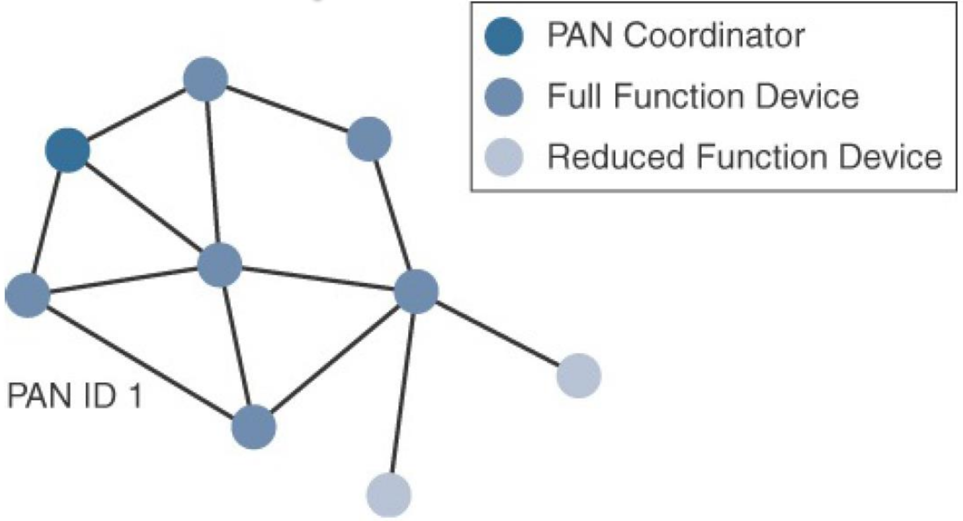
IEEE 802.15.4: MAC Layer

- Two types of nodes:
  - – Full-function devices (FFDs)
    - Any topology
    - Network coordinator capable
    - Talks to any other device
  - – Reduced-function devices (RFDs)
    - Limited to star topology
    - Cannot become a network coordinator
    - Talks only to a network coordinator
    - Very simple implementation (and is low cost)



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer



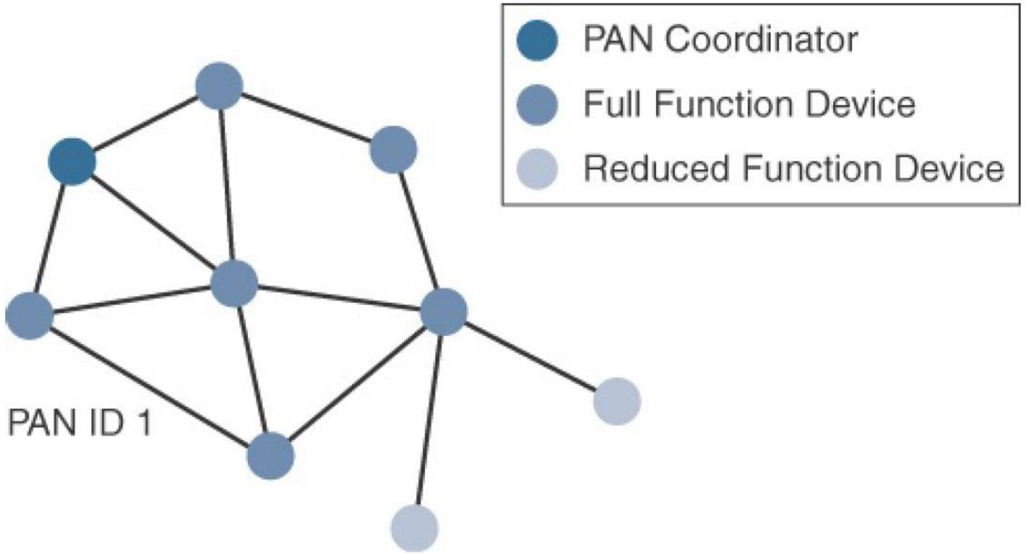
- A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN.

- FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

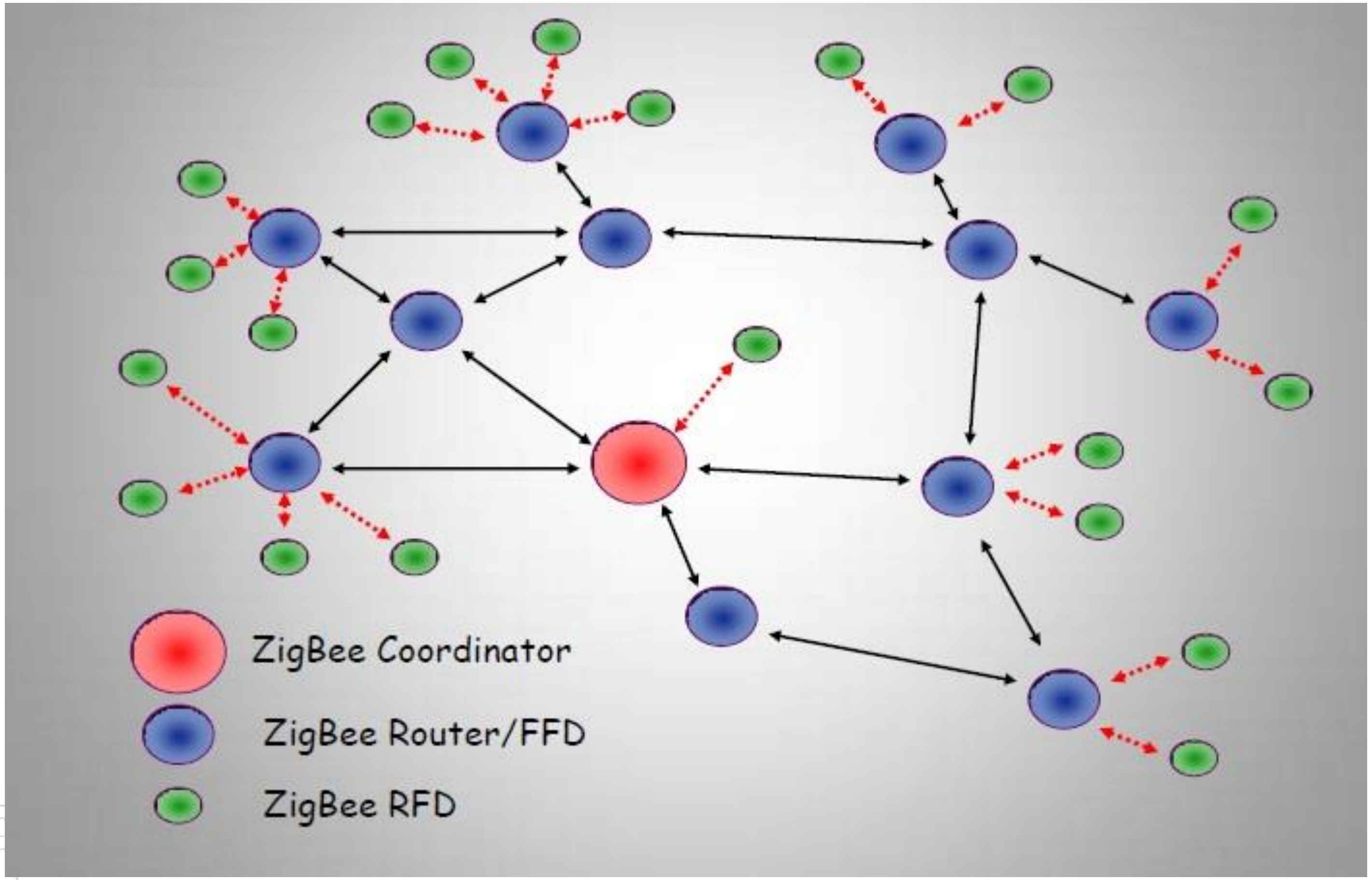
IEEE 802.15.4: MAC Layer

- Every 802.15.4 PAN should be set up with a unique ID.
  - All the nodes in the same 802.15.4 network should use the same PAN ID.
- This figure shows an example of an 802.15.4 mesh network with a PAN ID of 1.



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer



IEEE 802.15.4: MAC Layer

- IEEE 802.15.4- MAC layer
  - manages access to the PHY channel by defining how devices in the same area will share the frequencies
  - the scheduling and routing of data frames are also coordinated.
  - The 802.15.4 MAC layer performs the following tasks:
    - Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
    - PAN association and disassociation by a device
    - Device security
    - Reliable link communications between two peer MAC entities

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

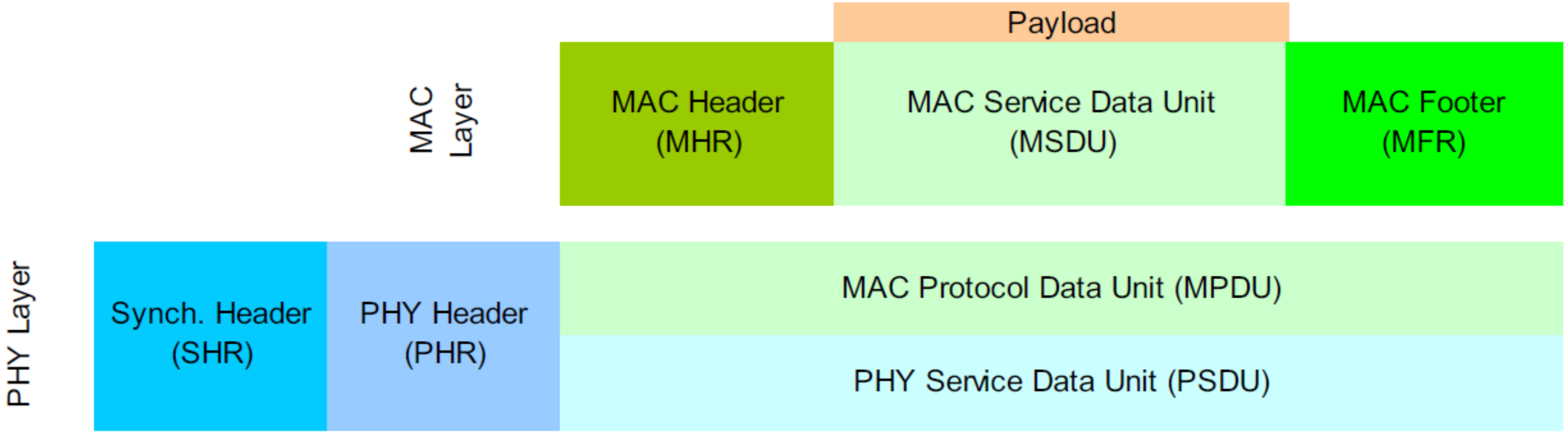
- To do MAC layer’s tasks, four types of MAC frames are specified in 802.15.4 :
  - **Data frame:** Handles all transfers of data
  - **Beacon frame:** Used in the transmission of beacons from a PAN coordinator
  - **Acknowledgement frame:** Confirms the successful reception of a frame
  - **MAC command frame:** Responsible for control communication between devices

- Each of these four 802.15.4 MAC frame types follows the frame format shown next.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

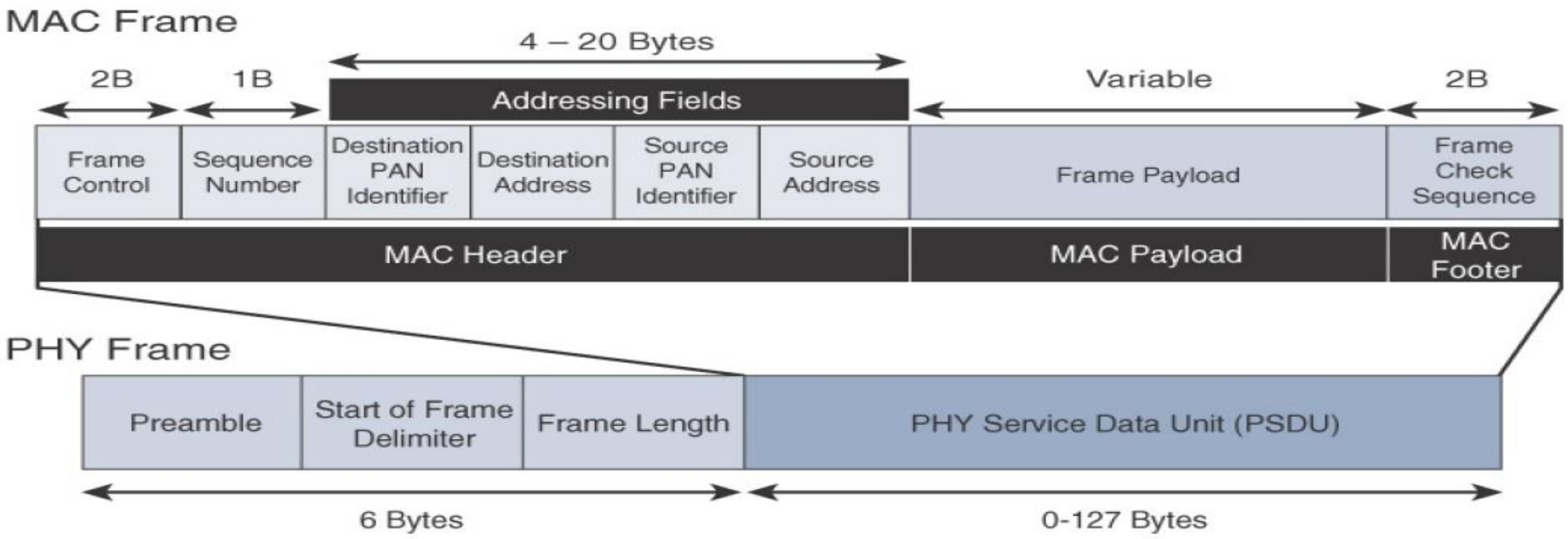
IEEE 802.15.4: MAC Layer

- IEEE 802.15.4 MAC layer frame format
  - – The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.



IEEE 802.15.4: MAC Layer

- IEEE 802.15.4 MAC layer frame format
  - The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.

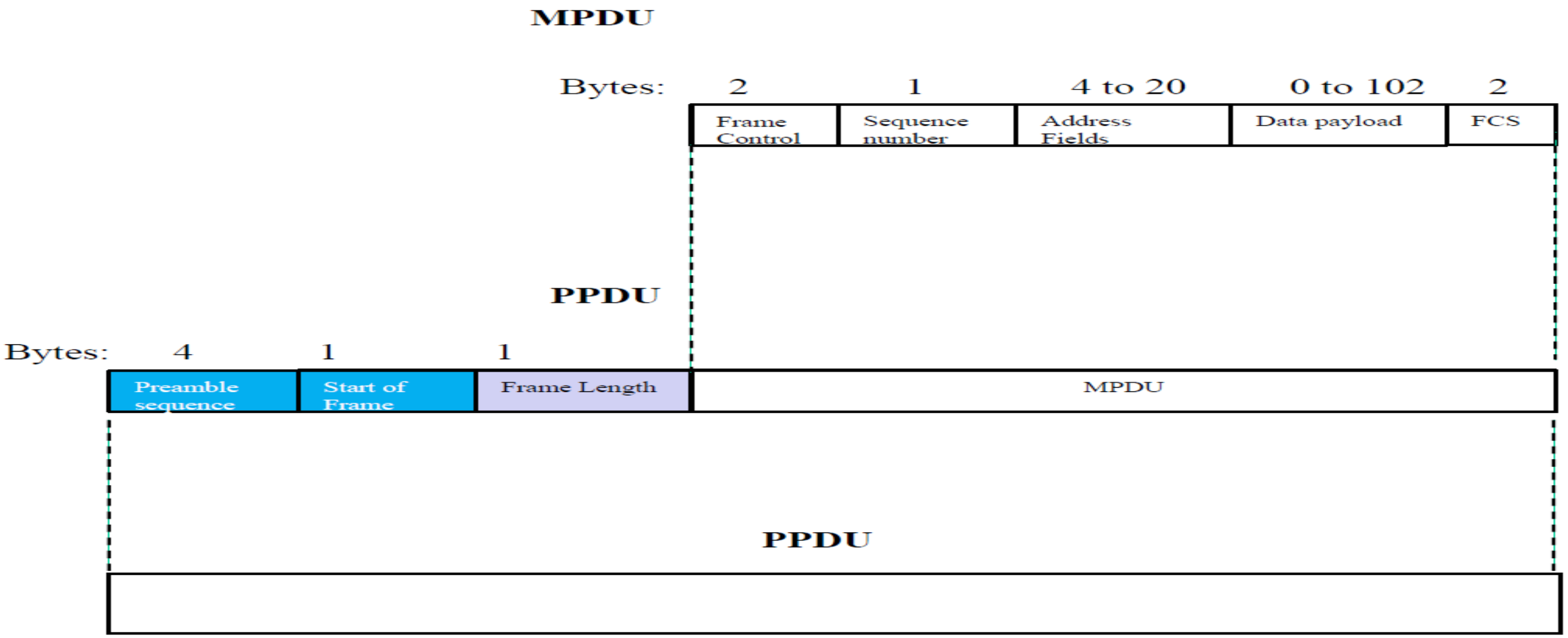


- ıe

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

- IEEE 802.15.4 MAC layer frame format



MPDU

Bytes:	2	1	4 to 20	0 to 102	2
	Frame Control	Sequence number	Address Fields	Data payload	FCS

PPDU

Bytes:	4	1	1	
	Preamble sequence	Start of Frame	Frame Length	MPDU

PPDU

- The MAC Footer field is nothing more than a frame check sequence (FCS).
  - An FCS is a calculation based on the data in the frame that is used by the receiving side to confirm the integrity of the data in the frame.

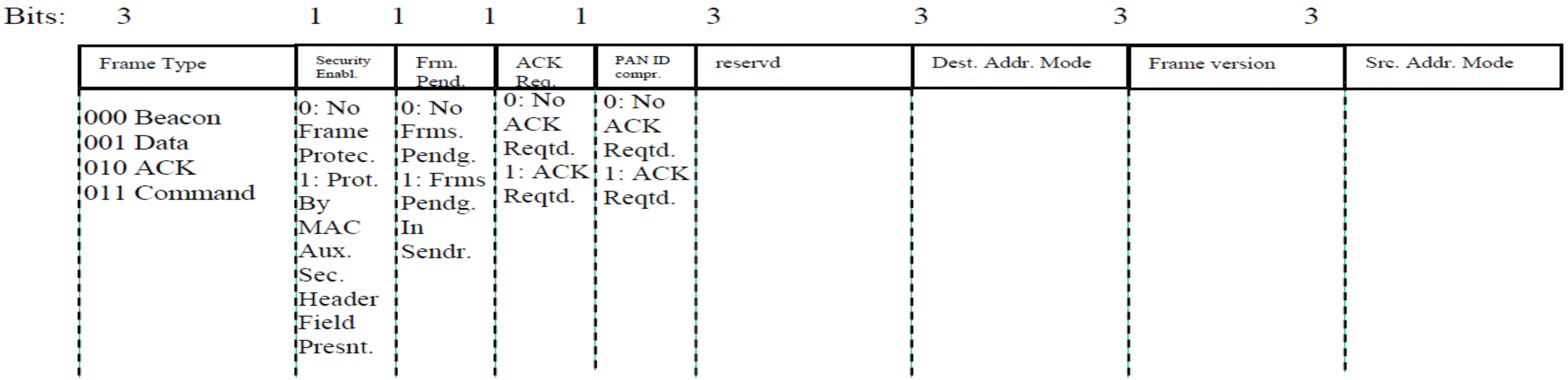
IEEE 802.15.4: MAC Layer

- The MAC Header field is composed of the
  - Frame Control
    - defines attributes such as **frame type**, **addressing modes**, and other control flags
  - Sequence Number
    - indicates the sequence identifier for the frame.
  - Addressing fields:
    - specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

- Frame Control: **frame type**, **addressing modes**, and other control flags



Bits:	3	1	1	1	1	3	3	3	3
	Frame Type	Security Enabl.	Frm. Pend.	ACK Req.	PAN ID compr.	reservd	Dest. Addr. Mode	Frame version	Src. Addr. Mode
	000 Beacon 001 Data 010 ACK 011 Command	0: No Frame Protec. 1: Prot. By MAC Aux. Sec. Header Field Presnt.	0: No Frms. Pendg. 1: Frms Pendg. In Sendr.	0: No ACK Reqtd. 1: ACK Reqtd.	0: No ACK Reqtd. 1: ACK Reqtd.				

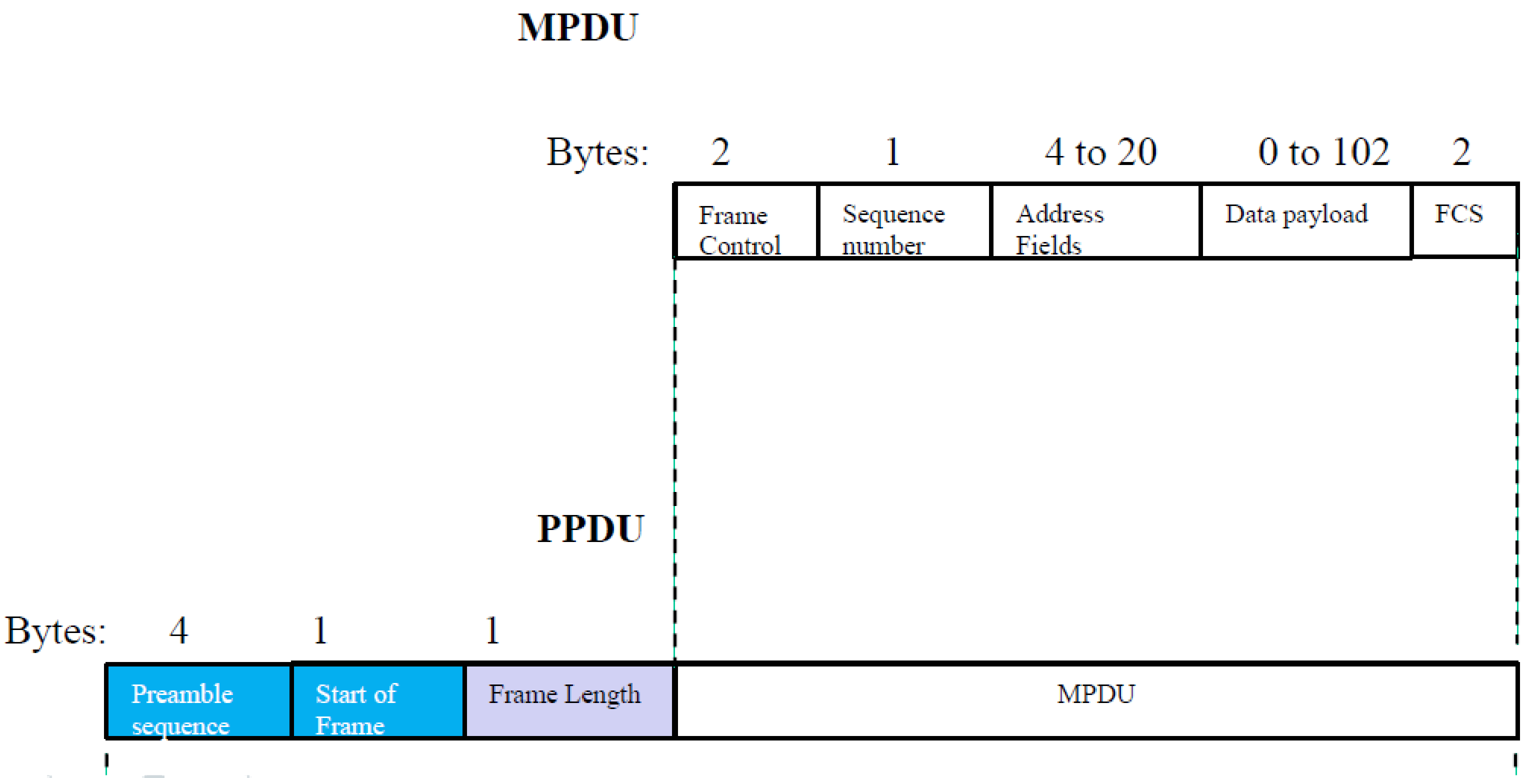
IEEE 802.15.4: MAC Layer

- The MAC Payload field varies by individual frame type. For example:
  – Beacon frames have specific fields and payloads related to beacons,
  – MAC command frames have different fields present

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

- Data frame structure:



MPDU

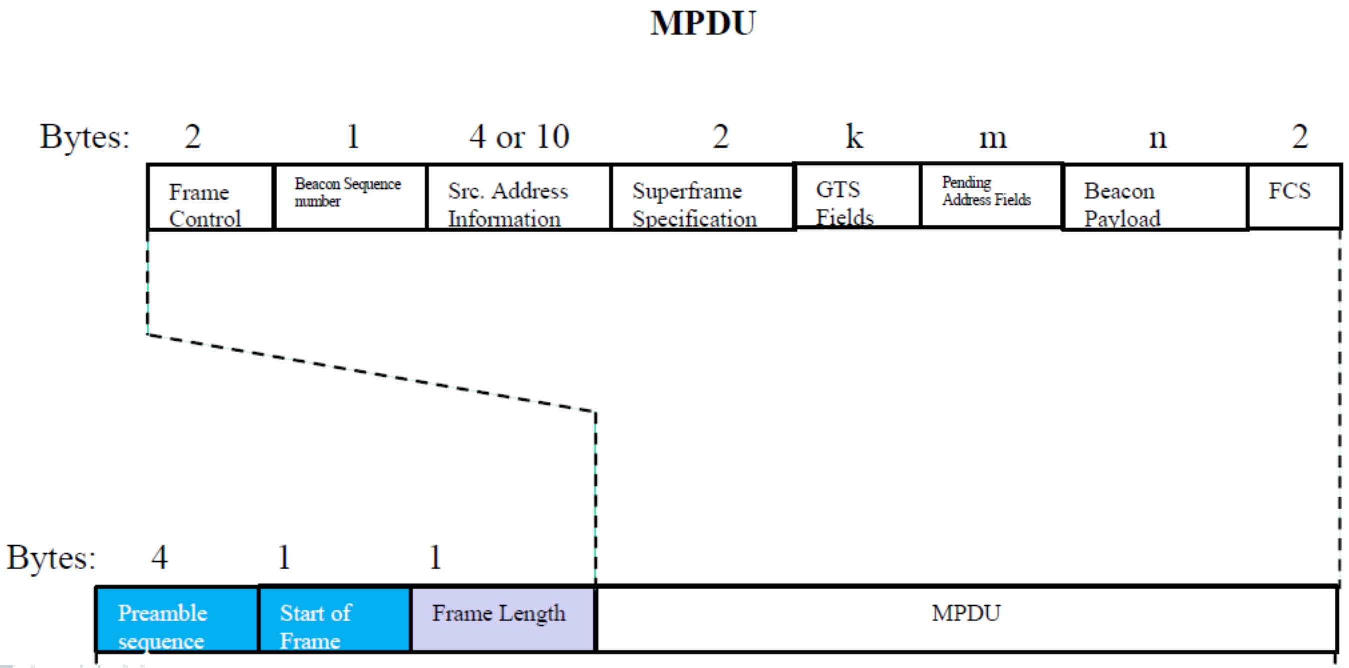
Bytes:	2	1	4 to 20	0 to 102	2
	Frame Control	Sequence number	Address Fields	Data payload	FCS

PPDU

Bytes:	4	1	1	
	Preamble sequence	Start of Frame	Frame Length	MPDU

IEEE 802.15.4: MAC Layer

- Beacon frames structure



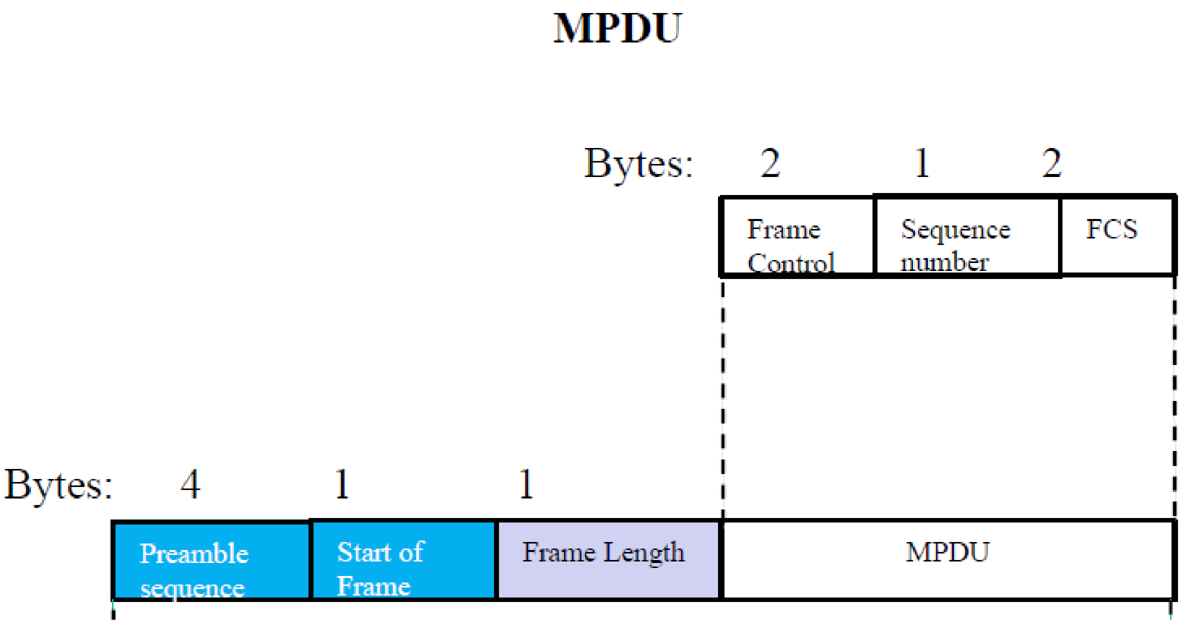
MPDU

Bytes:	2	1	4 or 10	2	k	m	n	2
	Frame Control	Beacon Sequence number	Src. Address Information	Superframe Specification	GTS Fields	Pending Address Fields	Beacon Payload	FCS

Bytes:	4	1	1	
	Preamble sequence	Start of Frame	Frame Length	MPDU

IEEE 802.15.4: MAC Layer

- ACK frame structure



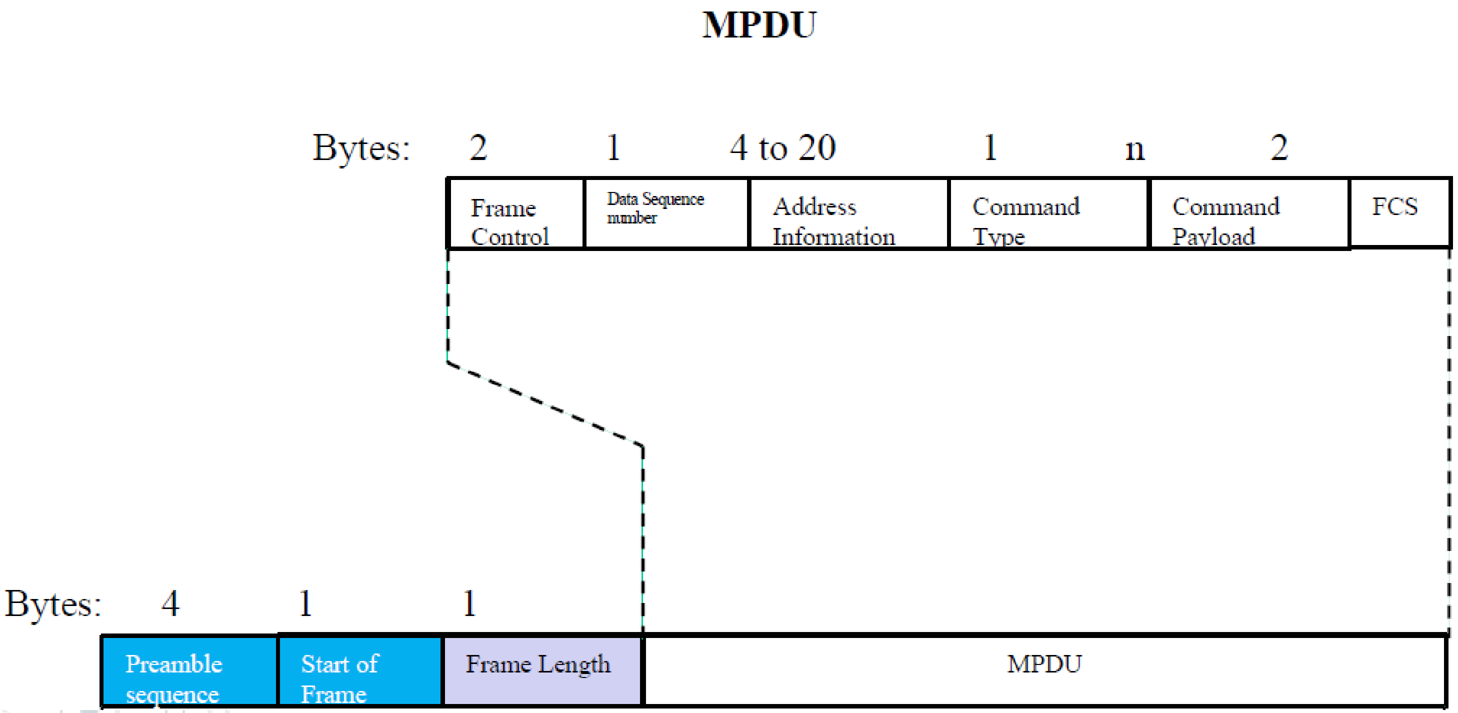
MPDU

Bytes:	2	1	2
	Frame Control	Sequence number	FCS

Bytes:	4	1	1	
	Preamble sequence	Start of Frame	Frame Length	MPDU

IEEE 802.15.4: MAC Layer

- AC command frames structure:



MPDU

Bytes:	2	1	4 to 20	1	n	2
	Frame Control	Data Sequence number	Address Information	Command Type	Command Payload	FCS

Bytes:	4	1	1	
	Preamble sequence	Start of Frame	Frame Length	MPDU

IEEE 802.15.4: MAC Layer

- IEEE 802.15.4 requires all devices to support a unique 64-bit extended MAC address, based on EUI-64.

- However, because the maximum payload is 127 bytes, 802.15.4 also defines how a 16-bit “short address” is assigned to devices.
  - This short address is local to the PAN and substantially reduces the frame overhead compared to a 64-bit extended MAC address.
  - However, you should be aware that the use of this short address might be limited to specific upper-layer protocol stacks.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

- **Three Channel Access Mechanisms**
  - 1. Slotted CSMA/CA
  - 2. CSMA/CA
  - 3. Contention Free (Guaranteed Time Slots)

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

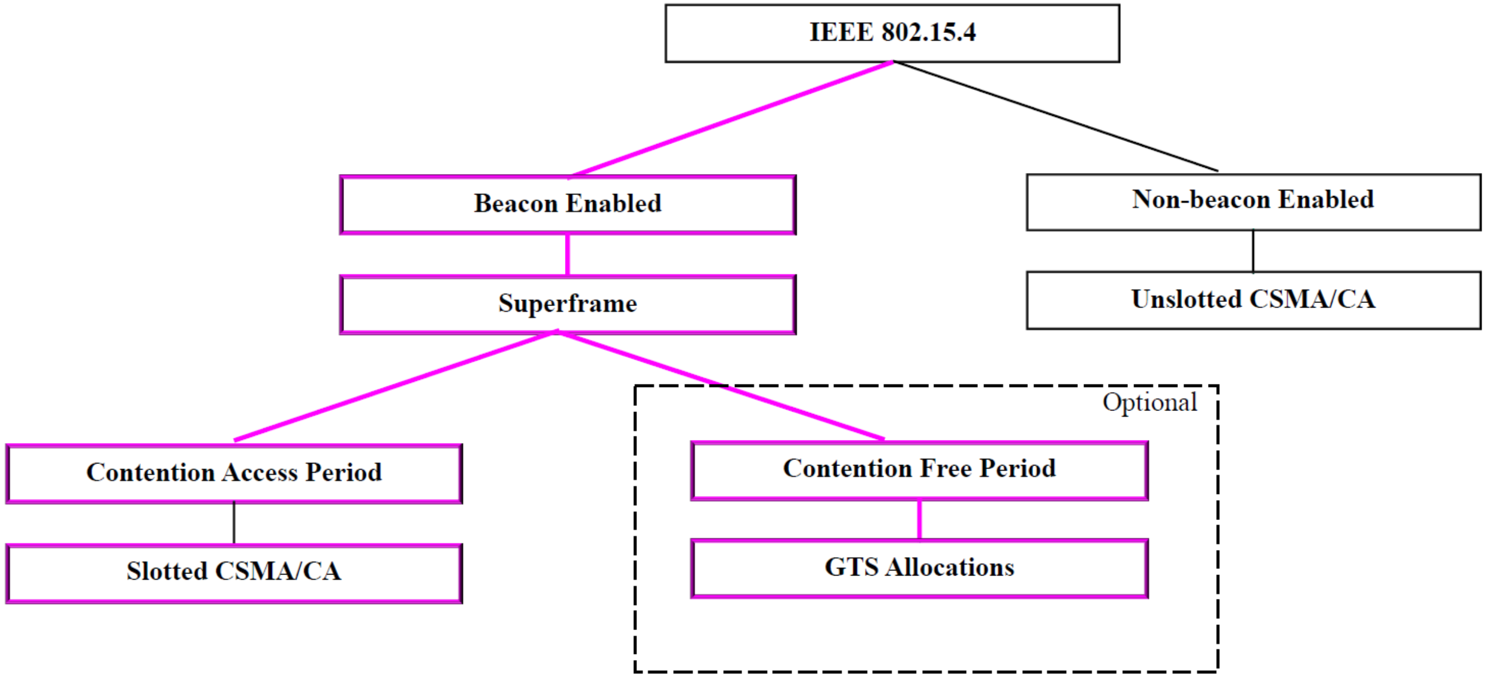
- Channel access within a piconet is based on a combination of random access and scheduled access:
  - 1. Slotted CSMA/CA
  - 2. CSMA/CA
  - 3. Contention Free (Guaranteed Time Slots)

- Channel access is controlled by the PAN coordinator that may choose between two different modalities:
  - beacon-enabled
  - nonbeacon-enabled

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: MAC Layer

- **Three Channel Access Mechanisms**



IEEE 802.15.4: MAC Layer

- In the beacon-enabled modality, the PAN coordinator broadcasts a periodic beacon containing information about the PAN.
  - The period between two consecutive beacons defines a superframe structure divided in 16 slots.
  - The first slot is always occupied by the beacon, while the other slots are used for
    - data communication by means of random access,
    - and form the so called Contention Access Period (CAP).

- The beacon contains information related to PAN identification, synchronization, and superframe structure.

- The beacon-enabled modality is adopted only when the PAN has a star topology

IEEE 802.15.4: MAC Layer

- **Beacon Enabled 802.15.4 Mode:** Beacons are transmitted periodically by the coordinator used to:
  - Synchronize associated nodes
  - Identify the PAN
  - Delimit the beginning of a superframe
  - Channel access mostly by Slotted CSMA/CA
  - Also possible to allocate contention free
  - Guaranteed Time Slots (GTSs).

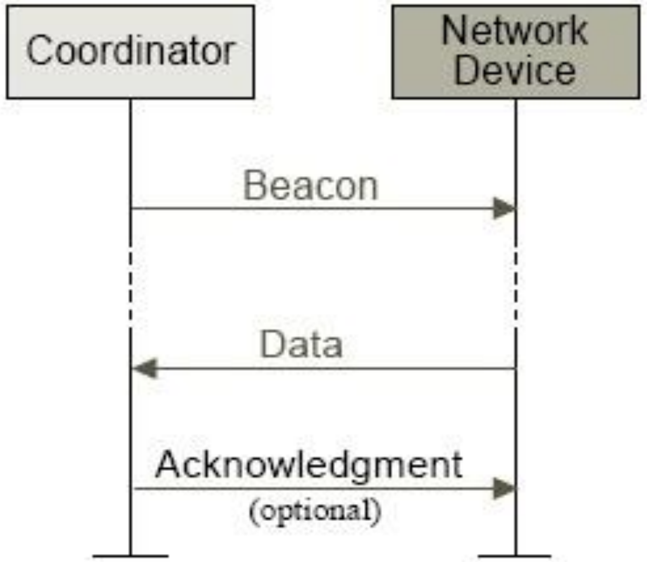
IEEE 802.15.4: MAC Layer

- In beacon-enabled case, two data transfer modes exist:
  - 1) Transfer from a device to the coordinator
    - A device willing to transfer data to the coordinator uses a slotted Carrier Sensing Multiple Access with Collision Avoidance (CSMA-CA):
      - The coordinator may confirm the successful data reception with an optional acknowledgment message within the same slot.
  - 2) Transfer from the coordinator to a device
    - when the coordinator has data pending for a device, it announces so in the beacon.
    - The interested device selects a free slot and sends a data request to the coordinator, indicating that it is ready to receive the data.
    - Slotted CSMA-CA is adopted to send the request.
    - When the coordinator receives the data request message, it selects a free slot and sends data using slotted CSMA-CA as well.

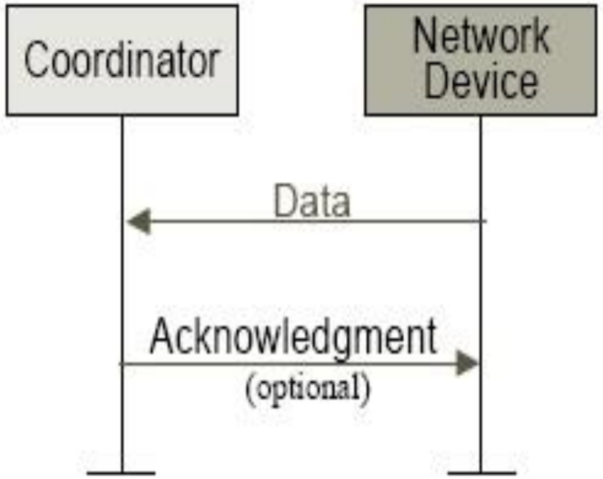
IEEE 802.15.4: MAC Layer

- In non-beacon-enabled case:
  - In the *nonbeacon-enabled* modality there is no explicit synchronization provided by the PAN coordinator.
  - This modality is particularly suited for PANs adopting the peer-to-peer topology, but can be adopted in a star network as well.
  - Data transferred from device to coordinator
    - In a non-beacon-enable network, device simply transmits its data using unslotted CSMA/CA

Communication Mechanisms-I

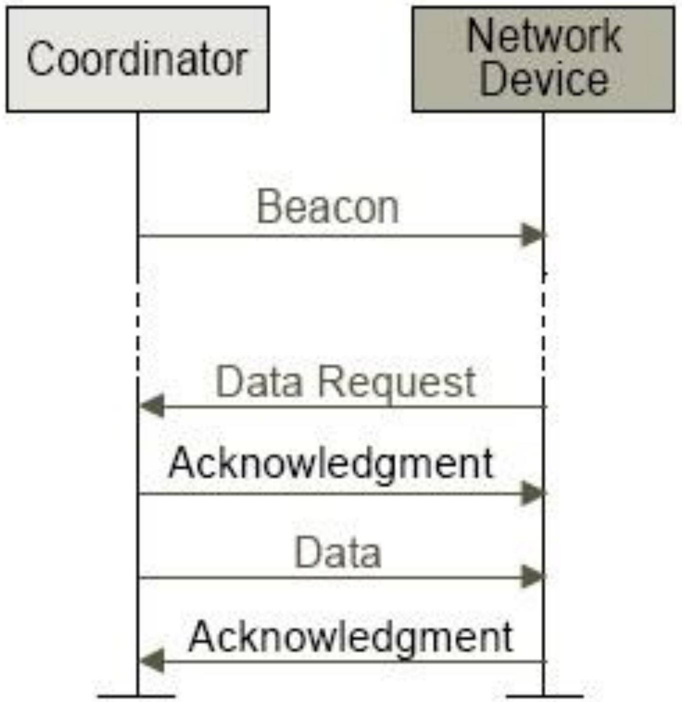


·Communication to a coordinator in a beacon-enabled network

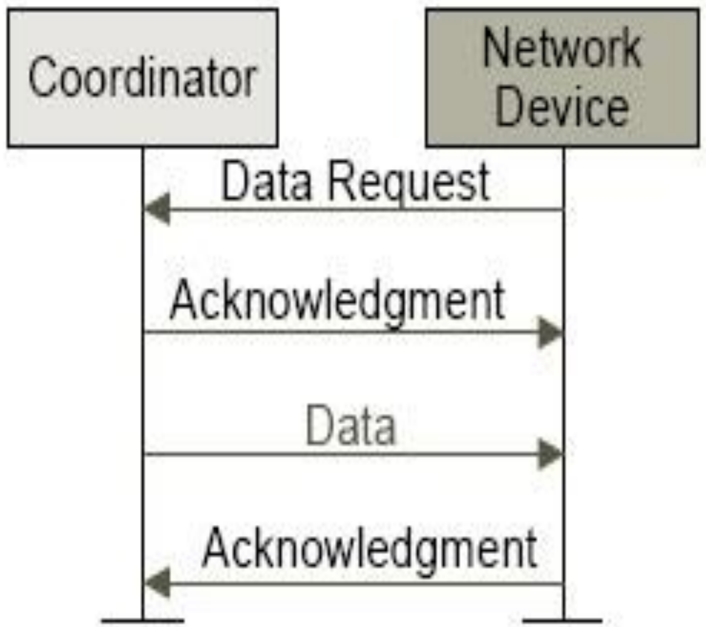


·Communication to a coordinator in a nonbeacon-enabled network

Communication Mechanisms-II



Communication from a coordinator a beacon-enabled network

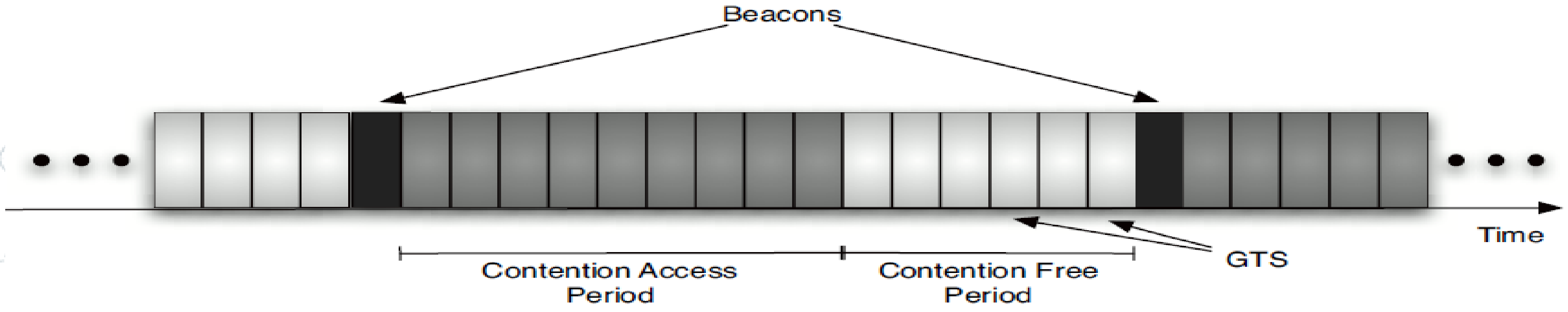


Communication from a coordinator in a nonbeacon-enabled network

IEEE 802.15.4: MAC Layer

- In order to support low-latency applications, the PAN coordinator can reserve one or more slots that are assigned to devices running such applications without need for contention with other devices.
- Such slots are referred to as Guaranteed Time Slots (GTS), and they form the Contention Free Period (CFP) of the superframe.

- An example of superframe with both CAP and CFP



IEEE 802.15.4: MAC Layer

- It should be noted that the peer-to-peer topology allows for a third transfer mode: the *peer-to-peer data transfer*, in which devices exchange data without involving the PAN coordinator, thus allowing more complex topologies and larger networks.

- Since there is no superframe defined in the non-beacon-enabled modality, no GTS can be reserved, and only random access is used.

- Furthermore, since no slot synchronization is available, random access is adopted for medium sharing in all transfer modes.

- In the random access phase devices adopt a CSMA-CA protocol to access the medium, either slotted on un-slotted depending on the selected PAN operation modality.

IEEE 802.15.4: MAC Layer

- Establishing a WPAN
  - 1. WPAN Coordinator selects an available channel
  - 2. Association procedure for devices to associate with it

- Channel selection
  - 1. Use energy detection scan over all the channels in the appropriate frequency band
  - 2. Find a channel which is free from interference

- Association procedure
  - 1. Search for available WPANs
  - 2. Select the WPAN to join
  - 3. Start the association procedure with the WPAN coordinator or with another FFD device, which has already joined the WPAN.

IEEE 802.15.4: MAC Layer

- Association procedure
  - 1. Search for available WPANs
    - Passive scan:
      - In beacon-enabled networks: eavesdrop on beacons transmitted periodically by associated devices
    - Active scan:
      - In non beacon-enabled networks: beacons are explicitly requested by the device through beacon request command frames.
  - 2. Select the WPAN to join
    - No logic is given in the standard 80215.4
    - This is, therefore, implementation dependent
  - 3. Start the association procedure with the WPAN coordinator or with another FFD device, which has already joined the WPAN.
    - Device sends an association request frame
    - An association response command frame is sent to the requesting device
    - The MAC association is referred to as a parent-child relationship

IEEE 802.15.4: Security

- Within the Frame Control portion of the 802.15.4 header is the Security Enabled field.
- When this field is set to a value of 0, the frame format matches the previous Figure.
- Beginning with the 802.15.4-2006 specification, when this field is set to a value of 1, an Auxiliary Security Header field is added to the 802.15.4 frame, will be shown later.

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4- Security

- The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data.

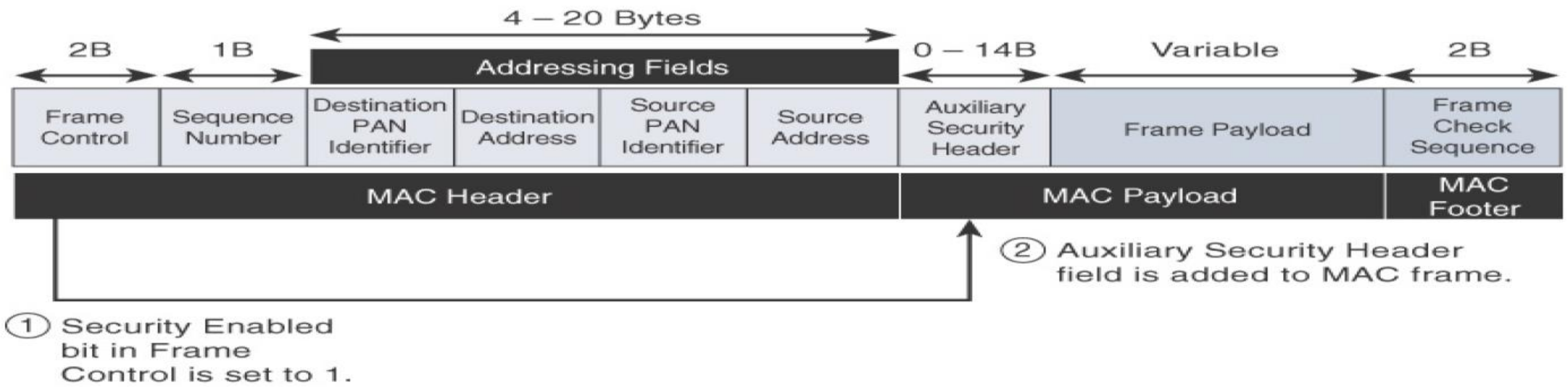
- AES: Established by the US National Institute of Standards and Technology in 2001, and is one of the most popular algorithms used in symmetric key cryptography.
    - A *symmetric key* means that the same key is used for both the encryption and decryption of the data.

- AES is a block cipher,
    - which means it operates on fixed-size blocks of data

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4- Security

- Enabling these security features for 802.15.4 changes the frame format slightly and consumes some of the payload.
- The Security Enabled field in the Frame Control portion of the 802.15.4 is a single bit that is set to 1 for security.
  - a field called the Auxiliary Security Header is created after the Source Address field, by stealing some bytes from the Payload field.
- Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions:



* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

IEEE 802.15.4: Routing

- The IEEE 802.15.4 specification does not define a path selection within the MAC layer for a mesh topology.
  - *Mesh-under:* can be done at Layer 2 and is based on a proprietary solution.
  - *Mesh-over: T*he routing function can occur at Layer 3, using a routing protocol, such as the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL) which will be discussed in network protocol section

* IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing, Cisco press, 2017

Exercises

- 1. The payload in data frames for data applications is typically 30 to 60 bytes long. Calculate the transmission time for the Data frame with a 45-byte payload if the transmission rate is 250 kbps

- 2. Calculate the maximum transmission time for the Data frame if the transmission rate is 250 kbps

- 3. Calculate the transmission time for an ACK frame

* *IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Thing*, Cisco press, 2017