

**MODULE-2**

**Chapter 4**

**Connecting Smart Objects**

# Communications Criteria

- In the world of connecting “things,” a large number of wired and wireless access technologies are available or under development.
- Wireless communication is prevalent in the world of smart object connectivity, mainly because it eases deployment and allows smart objects to be mobile, changing location without losing connectivity.

# Communications Criteria

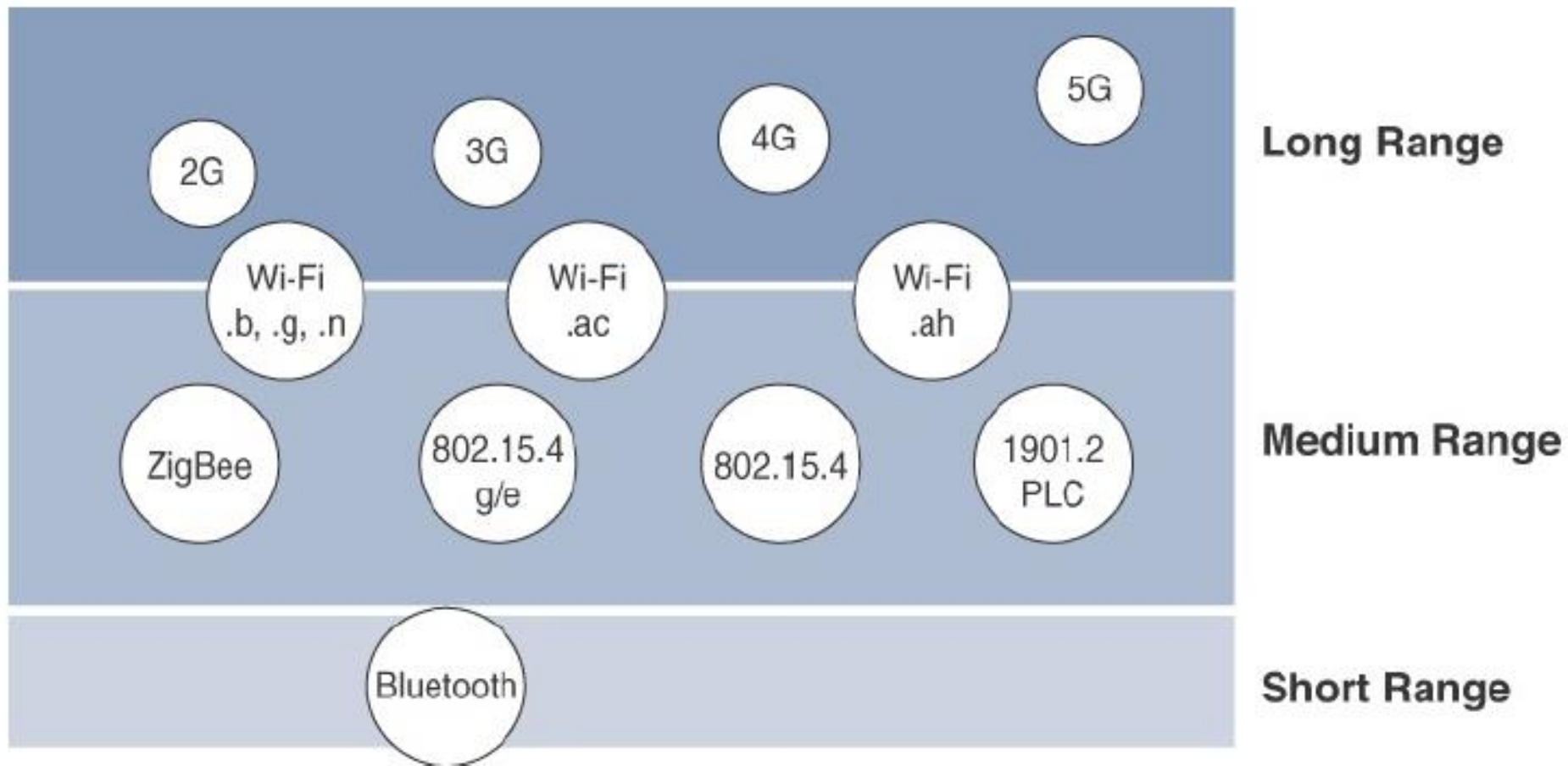
\* The various criteria used in the evaluation of various use cases and system solutions are as follows:

1. **Range**
2. **Frequency Bands**
3. **Power Consumption**
4. **Topology**
5. **Constrained Devices**
6. **Constrained-Node Networks**

# Range

## RANGE:

- The most commonly asked questions when wireless communication is deployed for smart object are :
  - How far does the signal need to be propagated?
  - what will be the area of coverage for a selected wireless technology?
- The simplest approach to answering these types of questions is to categorize these technologies as shown in Figure 4.1 breaking them down into the following ranges:



**Figure 4.1** : Wireless Access Landscape

## ➤ Short Range

- The classical wired example is a serial cable. Wireless short range technologies are often considered as an alternative to a serial cable, supporting tens of meters of maximum distance between two devices.
- Examples of short-range wireless technologies are IEEE 802.15.1 Bluetooth and IEEE 802.15.7 Visible Light Communications (VLC).
- These short-range communication methods are found in only a minority of IoT installations. In some cases, they are not mature enough for production<sup>6</sup> deployment.

## ➤ Medium Range

- This range is the main category of IoT access technologies. In the range of tens to hundreds of meters, many specifications and implementations are available.
- The maximum distance is generally less than 1 mile between two devices, although RF technologies do not have real maximum distances defined, as long as the radio signal is transmitted and received in the scope of the applicable specification.
- Examples of medium-range wireless technologies include IEEE 802.11 Wi-Fi, IEEE 802.15.4, and 802.15.4g WPAN. Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC) may also be classified as medium range, depending on their physical media characteristics.

## ➤ Long Range

- Distances greater than 1 mile between two devices require long-range technologies.
- Wireless examples are cellular (2G, 3G, 4G) and some applications of outdoor IEEE 802.11 Wi-Fi and Low-Power Wide-Area (LPWA) technologies.
- LPWA communications have the ability to communicate over a large area without consuming much power. These technologies are therefore ideal for battery-powered IoT sensors.
- Found mainly in industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications are classified as long range but are not really considered IoT access technologies



# Frequency Bands

- Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).
- These groups define the regulations and transmission requirements for various frequency bands.

- Focusing on IoT access technologies, the frequency bands leveraged by wireless communications are split **between licensed and unlicensed bands.**
- **Licensed spectrum** is generally applicable to IoT **long-range access technologies.**
- They are allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.

- In case if IoT access infrastructures wishes to utilize the **licensed spectrum** then users must **subscribe** to services when connecting their IoT devices.
- This adds **more complexity** to a large scale deployment of sensors and IoT devices. but in exchange for the subscription fee, the network operator can **guarantee Quality of Service(QoS)** and exclusive frequency usage over a target area.

- \* Examples of licensed spectrum commonly used for IoT access are cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.
- \* **Unlicensed spectrum** is usually simpler to deploy than licensed because it **does not** require a **service provider**. However, it can suffer from more interference because other devices may be competing for the same frequency in a specific area.

- Unlicensed means that no guarantees or protections are offered in the ISM bands for device communications.
- For IoT access, these are the most well-known ISM bands:
  - 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi
  - IEEE 802.15.1 Bluetooth
  - IEEE 802.15.4 WPAN

# Power Consumption

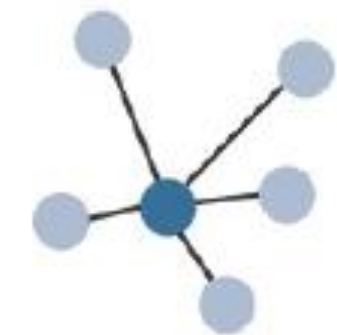
- **A powered node** has a direct connection to a power source, and communications are usually not limited by power consumption criteria.
- **Battery-powered nodes** bring much more flexibility to IoT devices. These nodes are often classified by the required lifetimes of their batteries

- IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes.
- This has led to the evolution of a new wireless environment known as **Low-Power Wide-Area(LPWA)**.

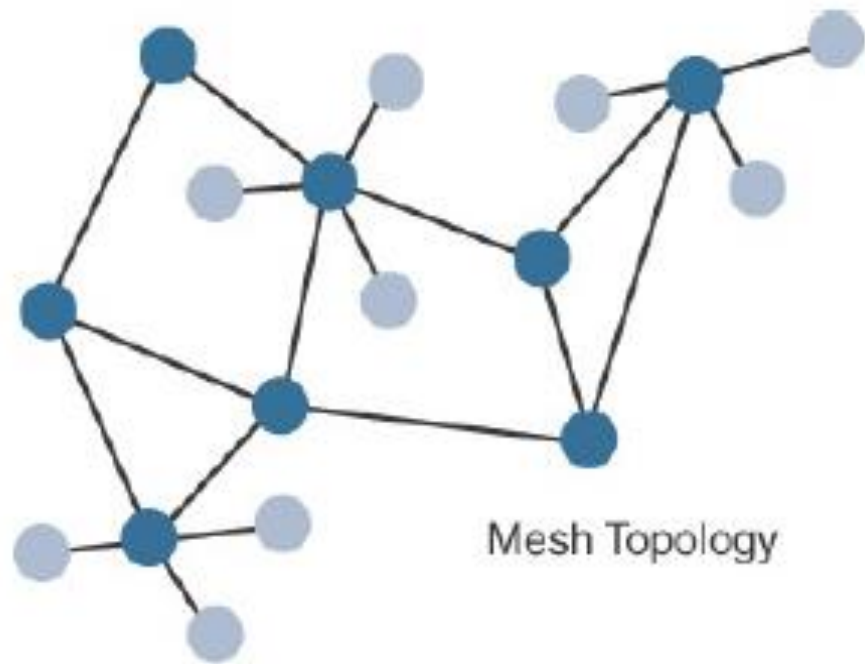
# Topology

- Among the access technologies available for connecting IoT devices, three main topology schemes are dominant: **star**, **mesh**, and **peer-to-peer**.
- Star topologies utilize a single central base station or controller to allow communications with endpoints.
- For medium-range technologies, a star, peer-to-peer, or mesh topology is common, as shown in Figure 4.2

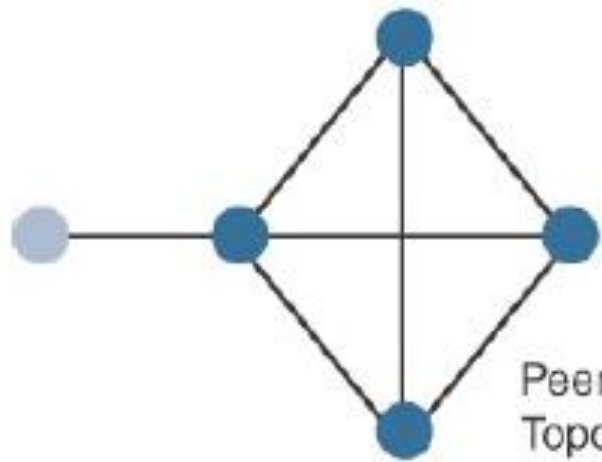




Star Topology



Mesh Topology



Peer-to-Peer Topology


- Full Function Device
- Reduced Function Device

**Figure 4.2 : Star, Peer-to-Peer and Mesh Topologies**

# Constrained Devices

- The categorization of IoT nodes into a specific class is a perilous exercise, with computing, memory, storage, power, and networking continuously evolving and improving.
- Constrained nodes have **limited resources** that impact their networking feature set and capabilities.
- Therefore, some classes of IoT nodes do not implement an IP stack.

Class	Definition
Class 0	<p>This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms. An example for class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.</p>
Class 1	<p>While greater than Class 0, the processing and code space characteristics (approximately 10KB RAM and approximately 100KB flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol(CoAP) . This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.</p>



Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of flash, so they can be fully integrated in IP networks. A smart power meter is an example of a Class 2 node.
---------	--

**Table 4.1** : Classes of Constrained Nodes, as defined by RFC 7228

# Constrained-Node Networks

- While several of the IoT access technologies, such as Wi-Fi and cellular, are applicable to laptops, smart phones, and some IoT devices, some IoT access technologies are more suited to specifically connect constrained nodes.

- Constrained-node networks are often referred to as low-power and lossy networks (LLNs).
- **Low-power** in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes.
- **Lossy networks** indicates that network performance may suffer from interference and variability due to harsh radio environments

- Layer 1 and Layer 2 protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability:
  - Data rate and throughput
  - Latency and determinism
  - Overhead and payload

# IoT Access Technologies

- Now, let us see the overview of the main IoT access technologies.
- For each of the IoT access technologies, a common information set is being provided.
- Particularly, the following topics are addressed for each IoT access technology:
  - **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

- 1. IEEE 802.15.4**
- 2. IEEE 802.15.4g and IEEE 802.15.4e**
- 3. IEEE 1901.2a**
- 4. IEEE 802.11ah**
- 5. LoRaWAN**
- 6. LTE Variations**

# IEEE 802.15.4

- \* a wireless access technology for **low-cost** and **low-data-rate** devices that are powered or run on batteries. this access technology enables easy installation
- \* **IEEE 802.15.4** is commonly found in the following types of deployments:
  1. Home and building automation
  2. Automotive networks
  3. Industrial wireless sensor networks
  4. Interactive toys and remote controls

# 1. Standardization and Alliances

- \* IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines **low-data-rate PHY and MAC layer specifications for WPAN.**
- \* This standard is a well-known solution **for low complexity wireless devices with low data rates** that need many months or even years of battery life

- the 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.
- These protocol stacks are promoted separately through various organizations and often commercialized.
- Some of the most well-known protocol stacks based on 802.15.4 are highlighted in Table 4.2



\* well-known protocol stacks based on 802.15.4 are

1. ZigBee
2. 6LoWPAN
3. ZigBee IP
4. ISA100.11a
5. Wireless HART
6. Thread

<b>Protocol</b>	<b>Description</b>
Zigbee	Promoted through Zigbee Alliance , Zigbee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation and healthcare. Zigbee also defines device object functions, such as device role, device discovery, network join and security.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers.
Zigbee IP	An evolution of the Zigbee protocol stack, Zigbee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security.
ISA 100.11a	ISA 100.11a is developed by the International Society of Automation(ISA) as “Wireless Systems for Industrial Automation: Process Control and Related Applications”. It based on IEEE 802.15.4-2006 and specifications were published in 2010 and then as IEC 62734.

WirelessHART	WirelessHART, promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band.
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home.

**Table 4.2** : Protocol Stacks Utilizing IEEE 802.15.4

- ZigBee has continued to evolve over time as evidenced by the release of Zigbee IP and is representative of how IEEE 802.15.4 can be leveraged at the PHY and MAC layers, independent of the protocol layers above.

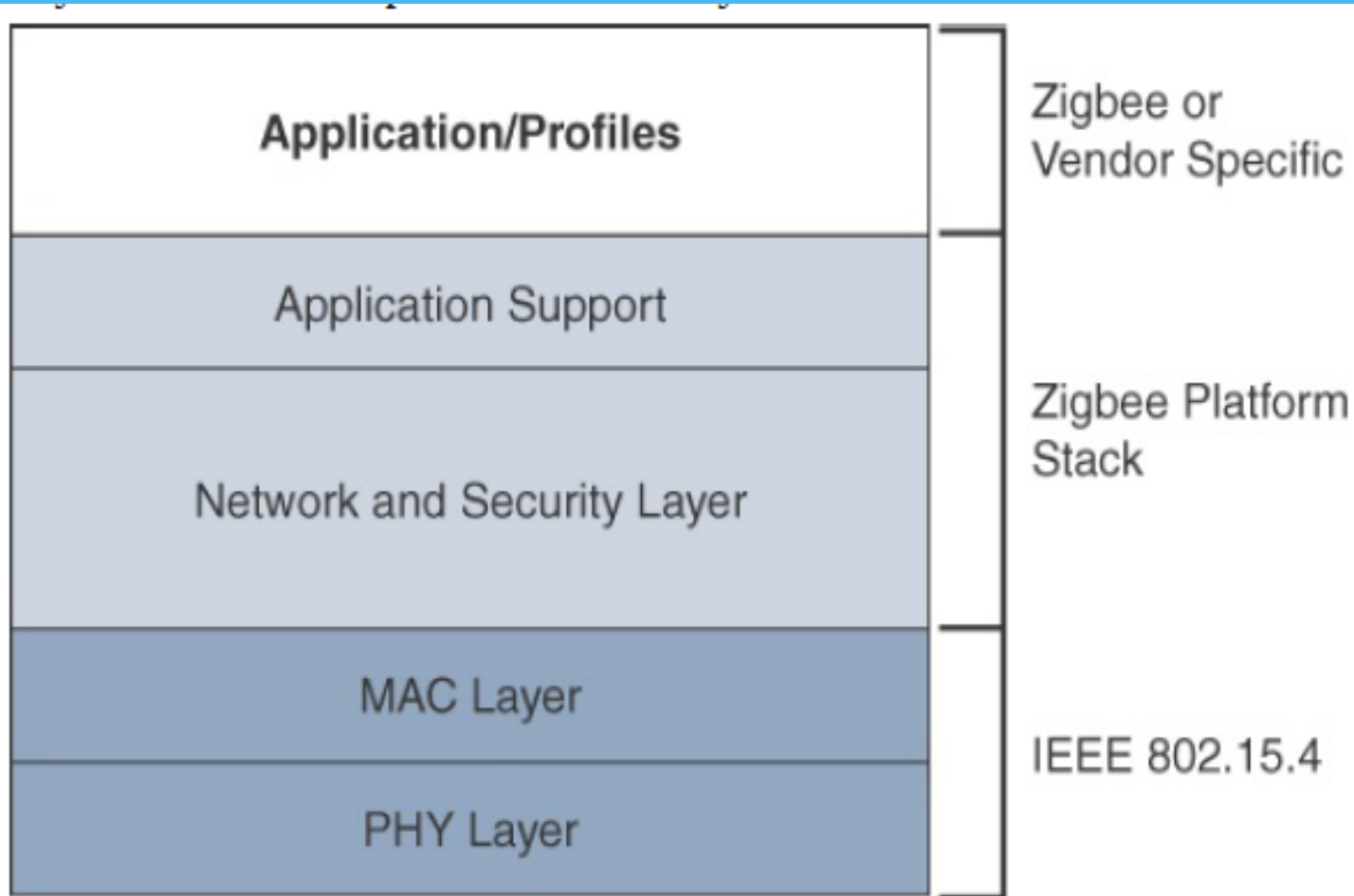


# ZigBee

- Based on the idea of ZigBee-style networks in the late 1990s, the first ZigBee specification was ratified in 2004, shortly after the release of the IEEE 802.15.4 specification the previous year.
- Similar to the Wi-Fi Alliance, the Zigbee Alliance is an industry group formed to certify interoperability between vendors and it is committed to driving and evolving ZigBee as an IoT solution for interconnecting smart objects.
- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs

- The Zigbee specification has undergone several revisions. In the 2006 revision, sets of commands and message types were introduced, and increased in number in the 2007 (called Zigbee pro) iteration, to achieve different functions for a device, such as metering, temperature, or lighting control.
- These sets of commands and message types are called clusters. Ultimately, these clusters from different functional domains or libraries form the building blocks of Zigbee application profiles.
- The main areas where ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy.

The traditional ZigBee stack is illustrated in Figure 4.3. ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers.



**Figure 4-3** High-Level ZigBee Protocol Stack

- ZigBee specifies the **network and security layer and application support layer** that sit on top of the lower layers.
- The ZigBee **network and security layer** provides mechanisms for network startup, configuration, routing, and securing communications.
- This includes calculating routing paths in what is often a changing topology, discovering neighbors, and managing the routing tables as devices join for the first time.

- The **network layer** is also responsible for forming the appropriate topology, which is often a **mesh** but could be a star or tree as well.
- From a security perspective, ZigBee utilizes 802.15.4 for security at the MAC layer, using the **Advanced Encryption Standard (AES)** with a 128-bit key and also provides security at the network and application layers.

- The **application support layer** in Figure 4.3 interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications.
- ZigBee is one of the most **well-known protocols built on an IEEE 802.15.4 foundation**. On top of the 802.15.4 PHY and MAC layers, **ZigBee specifies its own network and security layer and application profiles**.

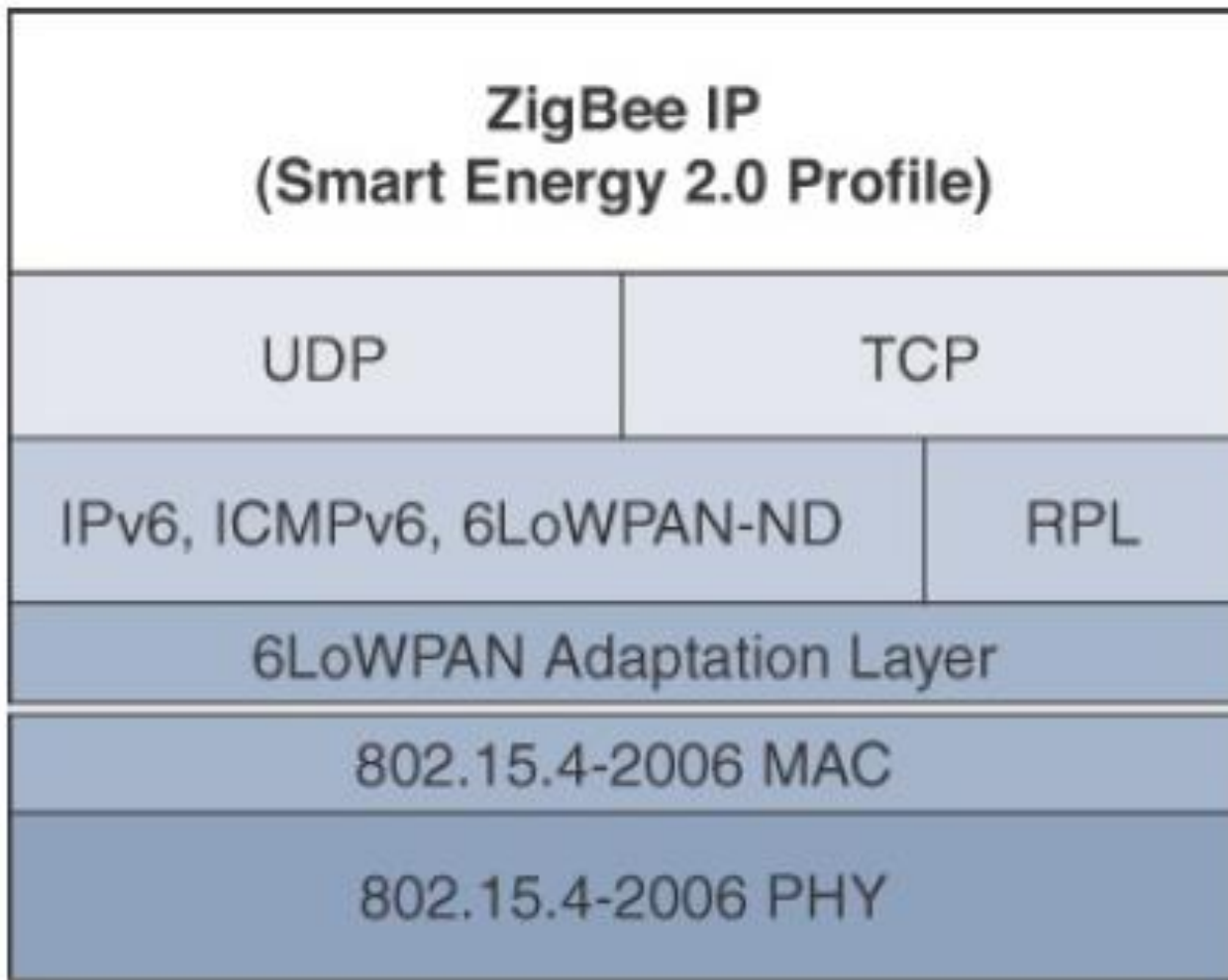
# ZigBee IP

- 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.
- 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.
- **ZigBee IP** supports **6LoWPAN** as an **adaptation layer**. The 6LoWPAN mesh addressing header is not required as ZigBee IP utilizes the mesh-over or route-over method for forwarding packets.




**Figure 4.4** : High-Level ZigBee Protocol Stack

- **ZigBee IP** requires the support of **6LoWPAN's fragmentation and header compression schemes**.
- At the **network layer**, all ZigBee **IP nodes** support **IPv6, ICMPv6, and 6LoWPAN Neighbor Discovery (ND)**, and utilize **RPL** for the routing of packets across the mesh network.
- Both **TCP and UDP** are also supported, to provide both connection-oriented and connectionless service.

# 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 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.

- 
- 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
  - 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.

- 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**

- **BPSK PHY**

- **ASK PHY**

## ➤ **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 signalled by phase changes.
- An offset function that is present during phase shifts allows data to be transmitted more reliably.

## ➤ **BPSK PHY**

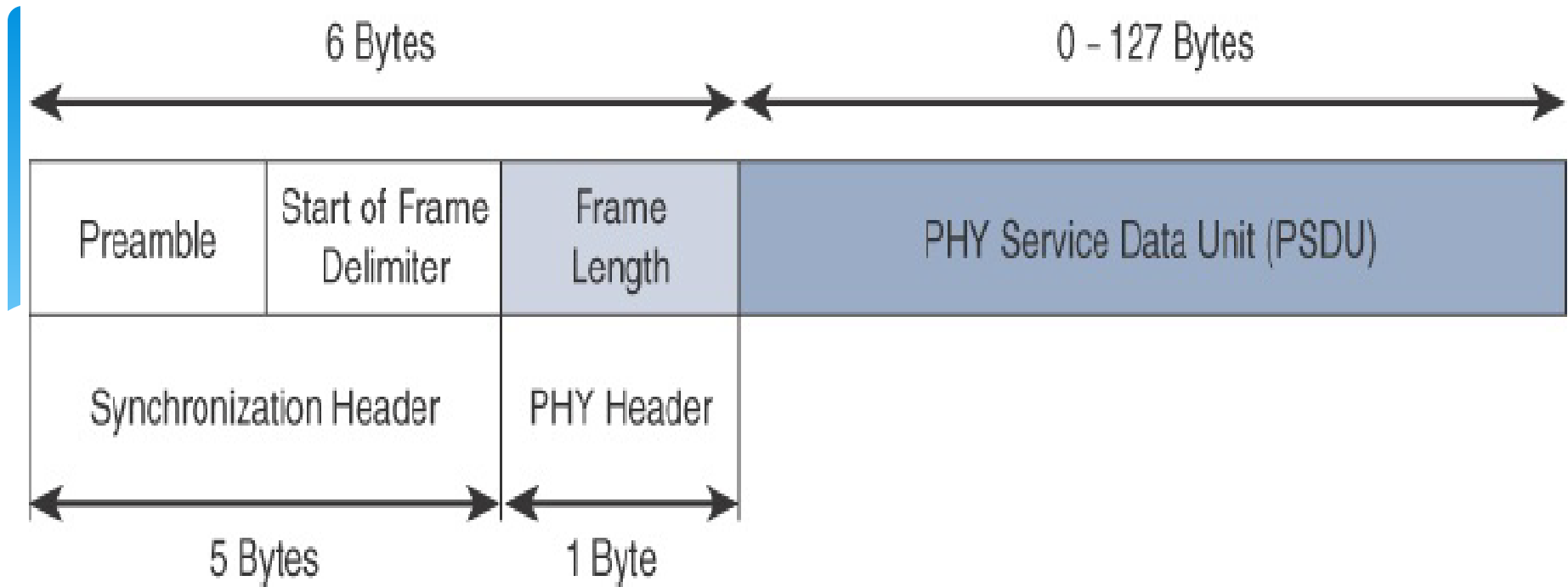
- This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation.
- BPSK specifies two unique phase shifts as its data encoding scheme.

## ➤ **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.

- 
- Figure 4.5 shows the frame for the 802.15.4 physical layer.
  - The **synchronization header** for this frame is composed of the Preamble and 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.





**Figure 4.5** : IEEE 802.15.4 PHY Format

- The **Start of Frame Delimiter** field informs the receiver that frame contents start immediately after this byte.

- **The PHY Header portion** of the PHY frame shown in Figure 4.5 is simply a frame length value. It lets the receiver know how much total data to expect in the PHY service data unit (PSDU) portion of the 802.4.15 PHY.
- The **PSDU** is the data field or payload.

# MAC Layer

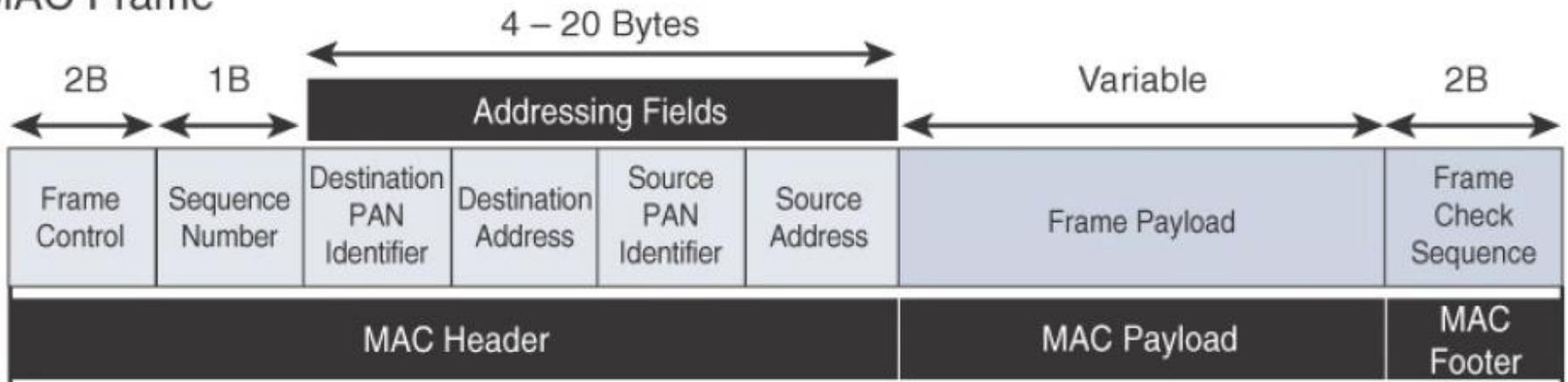
- The IEEE 802.15.4 MAC layer manages **access to the PHY channel by defining how devices in the same area will share the frequencies allocated.**
- At this layer, the **scheduling and routing of data frames are also coordinated.** The 802.15.4 MAC layer performs the following tasks:
  - Network beaconing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

- The MAC layer achieves these tasks by using various predefined frame types. In fact, 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

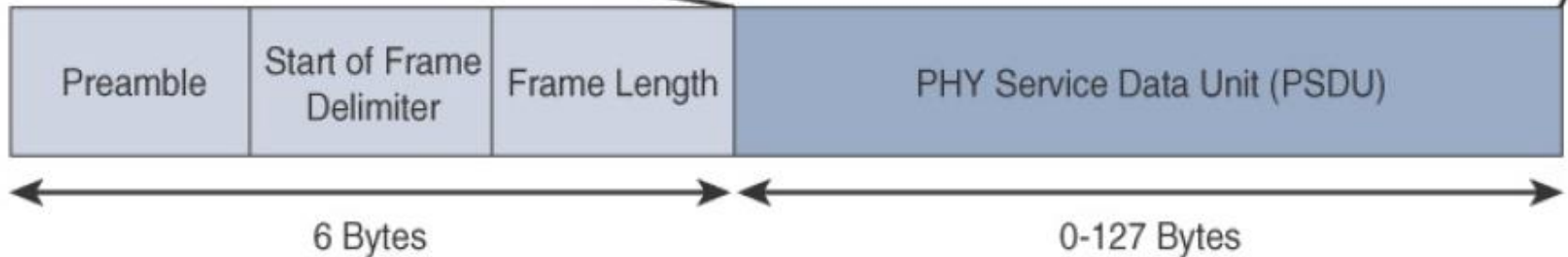
- Each of these four 802.15.4 MAC frame types follows the frame format shown in Figure 4.6.
- As shown in the Figure 4.6 the MAC frame is carried as the PHY payload. The 802.15.4 MAC frame can be broken down into the **MAC Header**, **MAC Payload**, and **MAC Footer** fields.

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

## MAC Frame



## PHY Frame



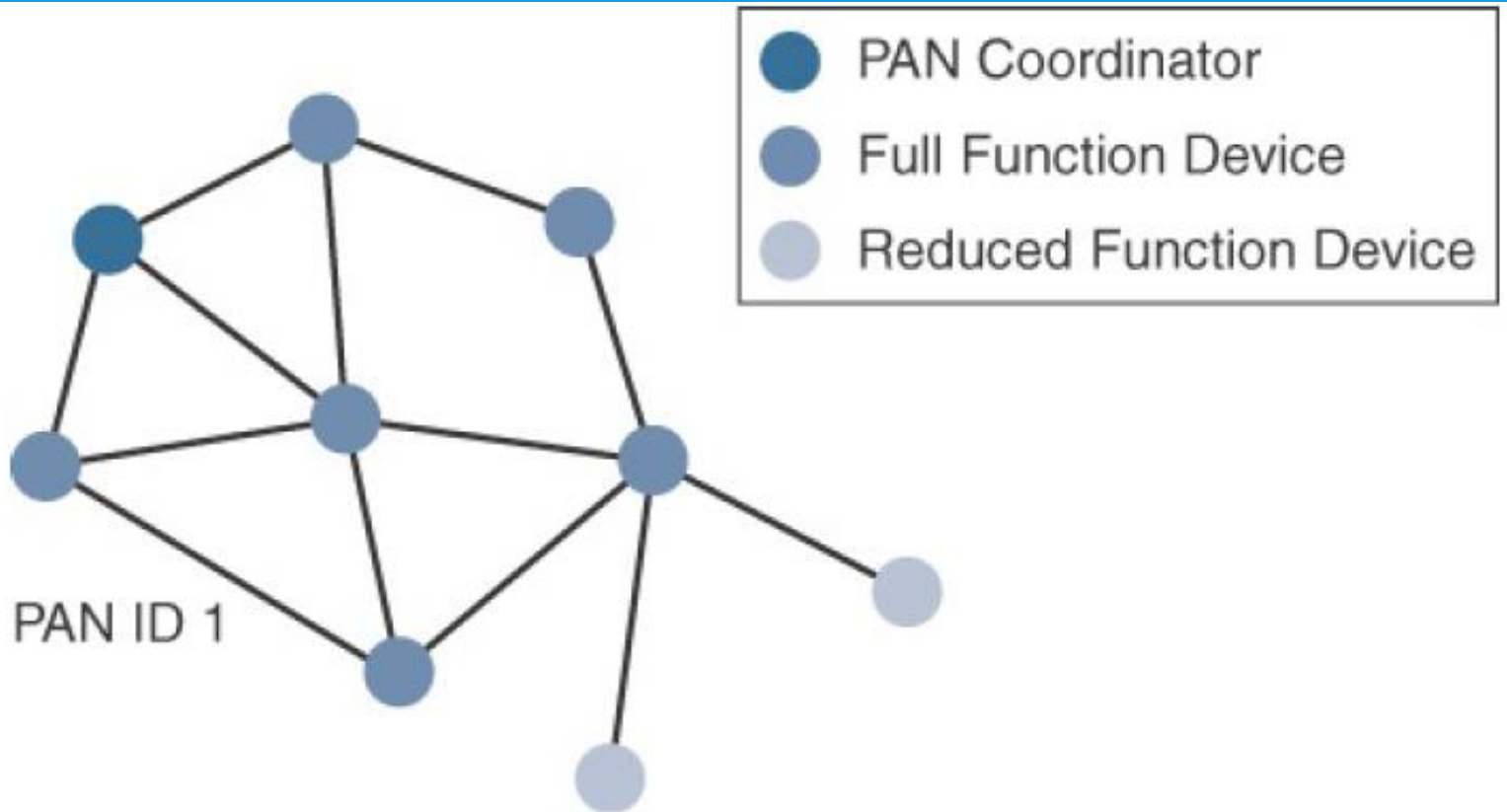
**Figure 4.6 : IEEE 802.15.4 MAC Format**

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



# Topology

- IEEE **802.15.4**–based networks can be built as **star, peer-to-peer, or mesh topologies**.
- Mesh networks tie together many nodes. This allows nodes that would be out of range if trying to communicate directly to leverage intermediary nodes to transfer communications.
- 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**.



**Figure 4.7** : 802.15.4 Sample Mesh Network Topology

- Figure 4.7 shows an example of an 802.15.4 mesh network with a PAN ID of 1.

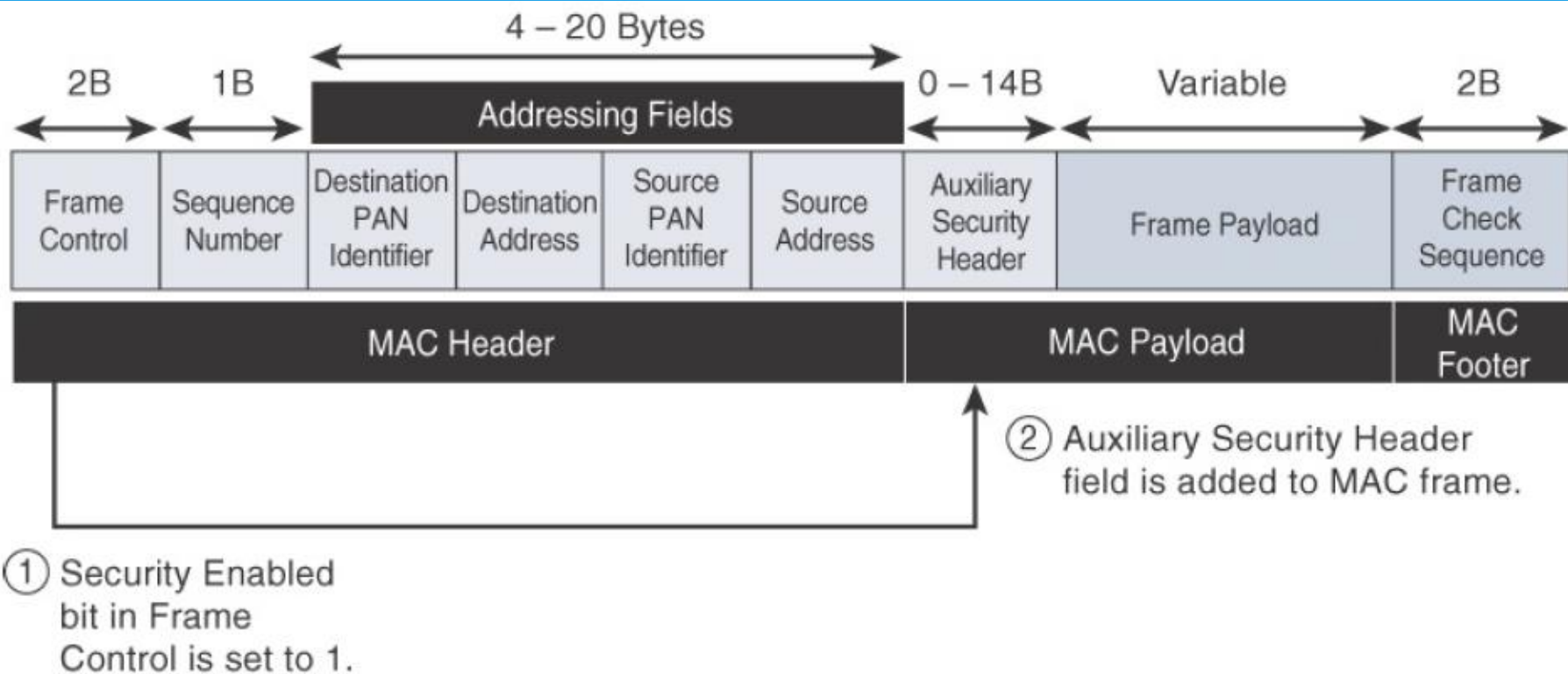
- A minimum of **one FFD** acting as a **PAN coordinator** is required to deliver services that allow other devices to associate and form a cell or PAN.
- In the Figure 4.7 a single PAN coordinator is identified for PAN ID 1. FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

- A path selection within the MAC layer for a mesh topology is done at Layer 2 and is known as **mesh-under**.
- Alternatively, the routing function can occur at Layer 3, using a routing protocol, such as the IPv6 **Routing Protocol for Low Power and Lossy Networks (RPL)**. This is referred to as **mesh-over**.

# 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 is a block cipher**, which means it operates on fixed-size blocks of data. In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent.
- Enabling these security features for 802.15.4 changes the frame format slightly and consumes some of the payload.

- Using the **Security Enabled** field in the **Frame Control** portion of the 802.15.4 header is the first step to enabling **AES encryption**. This field is a **single bit** that is set to **1 for security**.
- Once this bit is set, a field called the **Auxiliary Security Header** is created after the **Source Address** field, by stealing some bytes from the **Payload** field.
- Figure 4.8 shows the IEEE 802.15.4 frame format at a high level, with the **Security Enabled bit set** and the **Auxiliary Security Header field present**.



**Figure 4.8 :** Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions

# Competitive Technologies

- The IEEE 802.15.4 PHY and MAC layers are the foundations for several networking profiles that compete against each other in various IoT access environments.
- These various vendors and organizations build upper-layer protocol stacks on top of an 802.15.4 core.
- A competitive radio technology that is different in its PHY and MAC layers is **DASH7**.



- DASH7 was originally based on the ISO18000-7 standard and positioned for industrial communications, whereas IEEE 802.15.4 is more generic.
- **Commonly employed in active radio frequency identification (RFID) implementations, DASH7 was used by US military forces for many years, mainly for logistics purposes.**

- The current **DASH7** technology offers **low power consumption, a compact protocol stack, range up to 1 mile, and AES encryption.**
- Frequencies of 433MHz, 868 MHz, and 915 MHz have been defined, enabling data rates up to 166.667 kbps and a maximum payload of 256 bytes.

## IEEE 802.15.4 Conclusions

- The IEEE 802.15.4 wireless PHY and MAC layers are mature specifications that are the foundation for various industry standards and products.
- The PHY layer offers a maximum speed of up to 250 kbps, but this varies based on modulation and frequency.
- The MAC layer for 802.15.4 is robust and handles how data is transmitted and received over the PHY layer.
- Specifically, the MAC layer handles the association and disassociation of devices to/from a PAN, reliable communications between devices, security, and the formation of various topologies.

- The topologies used in 802.15.4 include star, peer-to-peer, and cluster trees that allow for the formation of mesh networks.
- From a security perspective, 802.15.4 utilizes AES encryption to allow secure communications and also provide data integrity.
- The main competitor to IEEE 802.15.4 is DASH7, another wireless technology that compares favorably.
- However, IEEE 802.15.4 has an edge in the marketplace through all the different vendors and organizations that utilize its PHY and MAC layers.
- As 802.15.4 continues to evolve, we will likely see broader adoption of the IPv6 standard at the network layer.

# IEEE 802.15.4g and 802.15.4e


- The IEEE frequently makes amendments to the core 802.15.4 specification, before integrating them into the next revision of the core specification.
- When these amendments are made, a lowercase letter is appended. Two such examples of this are **802.15.4e-2012** and **802.15.4g-2012**, both of which are especially relevant to the subject of IoT.

- \* The IEEE 802.15.4e amendment of 802.15.4-2011 expands the MAC layer feature set to remedy the disadvantages associated with 802.15.4, including
  - \* MAC reliability,
  - \* unbounded latency,
  - \* multipath fading.

- In addition to making general enhancements, **IEEE 802.15.4e** also made improvements to cope with certain application domains, such as factory and process automation and smart grid.
- IEEE 802.15.4e-2012 enhanced the **IEEE 802.15.4 MAC layer** capabilities in the areas of **frame format, security, determinism mechanism, and frequency hopping.**


- The focus of this specification is the smart grid or, more specifically, **smart utility network communication**.
- **802.15.4g** seeks to optimize large outdoor wireless mesh networks for **field area networks (FANs)**.
- This technology applies to IoT use cases such as the following:
  - **Distribution automation and industrial supervisory control and data acquisition (SCADA)** environments for remote monitoring and control.



- 
- Public lighting
  - Environmental wireless sensors in smart cities
  - Electrical vehicle charging stations
  - Smart parking meters
  - Microgrids
  - Renewable energy

# Standardization and Alliances

- The additional capabilities and options provided by 802.15.4g-2012 and 802.15.4e-2012 led to additional difficulty in achieving the interoperability between devices.
- To guarantee interoperability, the **Wi-SUN** Alliance was formed. (**SUN** stands for smart utility network.)
- **It defines communication profiles for smart utility and related networks.**

- 
- These **profiles** are based on open standards, such as **802.15.4g-2012, 802.15.4e-2012, IPv6, 6LoWPAN, and UDP for the FAN profile.**
  - In addition, **Wi-SUN** offers a **testing** and **certification** program to further ensure interoperability. The Wi-SUN Alliance performs the same function as the Wi-Fi Alliance and WiMAX Forum.

- Each of these organizations has an associated standards body as well as a commercial name, as shown in Table 4.3

<b>Commercial Name/Trademark</b>	<b>Industry Organization</b>	<b>Standards Body</b>
Wi-Fi	Wi-Fi Alliance	IEEE 802.11 Wireless LAN
WiMAX	WiMAX Forum	IEEE 802.16 Wireless MAN
Wi-SUN	Wi-SUN Alliance	IEEE 802.15.4g Wireless SUN

**Table 4.3 :** Industry Alliances for Some Common IEEE Standards

# Physical Layer

- In IEEE 802.15.4g-2012, the original IEEE 802.15.4 maximum **PSDU** or payload size of **127 bytes** was increased for the SUN PHY to 2047 bytes.
- This provides a better match for the **greater packet sizes** found in many upper-layer protocols.
- For example, the default IPv6 MTU setting is 1280 bytes.

- **Fragmentation** is no longer necessary at Layer 2 when IPv6 packets are transmitted over IEEE 802.15.4g **MAC frames**.
- The **error protection** was improved in IEEE 802.15.4g by evolving the CRC from 16 to **32 bits**.
- The SUN PHY, as described in IEEE 802.15.4g-2012, supports **multiple data rates** in bands ranging from **169 MHz to 2.4 GHz**.

- These bands are covered in the **unlicensed ISM frequency** spectrum and within these bands data must be **modulated** onto the frequency using at least one of the following PHY mechanisms to be IEEE 802.15.4g compliant:
  - **Multi-Rate and Multi-Regional Frequency Shift Keying (MR-FSK)**
  - **Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing (MR-OFDM)**
  - **Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying (MR-O-QPSK)**

➤ **MR-FSK:**

- Offers good transmit power efficiency due to the constant envelope of the transmit signal.

➤ **MR-OFDM :**

- Provides higher data rates but may be too complex for low-cost and low-power devices.
- Offers good transmit power efficiency due to the constant envelope of the transmit signal.

➤ **MR-O-QPSK :**

- Shares the same characteristics of the IEEE 802.15.4- 2006 O-QPSK PHY, making multi-mode systems more cost-effective and easier to design.



- For ex : for the 902–928 MHz ISM band that is used in the United States, MR-FSK provides 50, 150, or 200 kbps. MR-OFDM at this same frequency allows up to 800 kbps.
- Therefore, products and solutions must refer to the proper IEEE 802.15.4 specification, frequency band, modulation, and data rate when providing details about their PHY implementation.

# MAC Layer

- While the IEEE 802.15.4e-2012 amendment is not applicable to the PHY layer, it is pertinent to the MAC layer.
- The following are some of the main enhancements to the MAC layer proposed by IEEE 802.15.4e-2012:
  - **Time-Slotted Channel Hopping (TSCH)**
  - **Information elements**
  - **Enhanced beacons (EBs)**
  - **Enhanced beacon requests (EBRs)**
  - **Enhanced Acknowledgement**<sub>82</sub>

## ➤ **Time-Slotted Channel Hopping (TSCH):**

- TSCH is an IEEE 802.15.4e- 2012 **MAC operation mode** that works to guarantee media access and channel diversity.
- **Channel hopping**, also known as **frequency hopping**, utilizes different channels for transmission at different times.
- TSCH divides time into fixed time periods, or “**time slots**,” which offer guaranteed bandwidth and predictable latency.
  - In a time slot, **one packet** and its **acknowledgement** can be transmitted.

- \* A number of time slots are defined as a “**slot frame,**” which is regularly repeated to provide “**guaranteed access.**”
- \* The **transmitter** and **receiver** agree on the channels and the timing for switching between channels.
- \* TSCH adds **robustness** in noisy environments and smoother coexistence with other wireless technologies, especially for industrial use cases.

## ➤ **Information Elements**

- IEs allow for the **exchange** of information at the **MAC layer** in an extensible manner, either as header IEs (standardized) and/or payload IEs (private).
- Specified in a **tag, length, value** (TLV) format, the IE field allows frames to carry additional metadata to support MAC layer services.

➤ **Enhanced Beacons(EBs):**

- EBs extend the flexibility of IEEE 802.15.4 beacons to allow the construction of application-specific beacon content.
- This is accomplished by including relevant IEs in EB frames.

➤ **Enhanced beacon requests (EBRs):**

- Like enhanced beacons, an enhanced beacon request (EBRs) also leverages IEs.

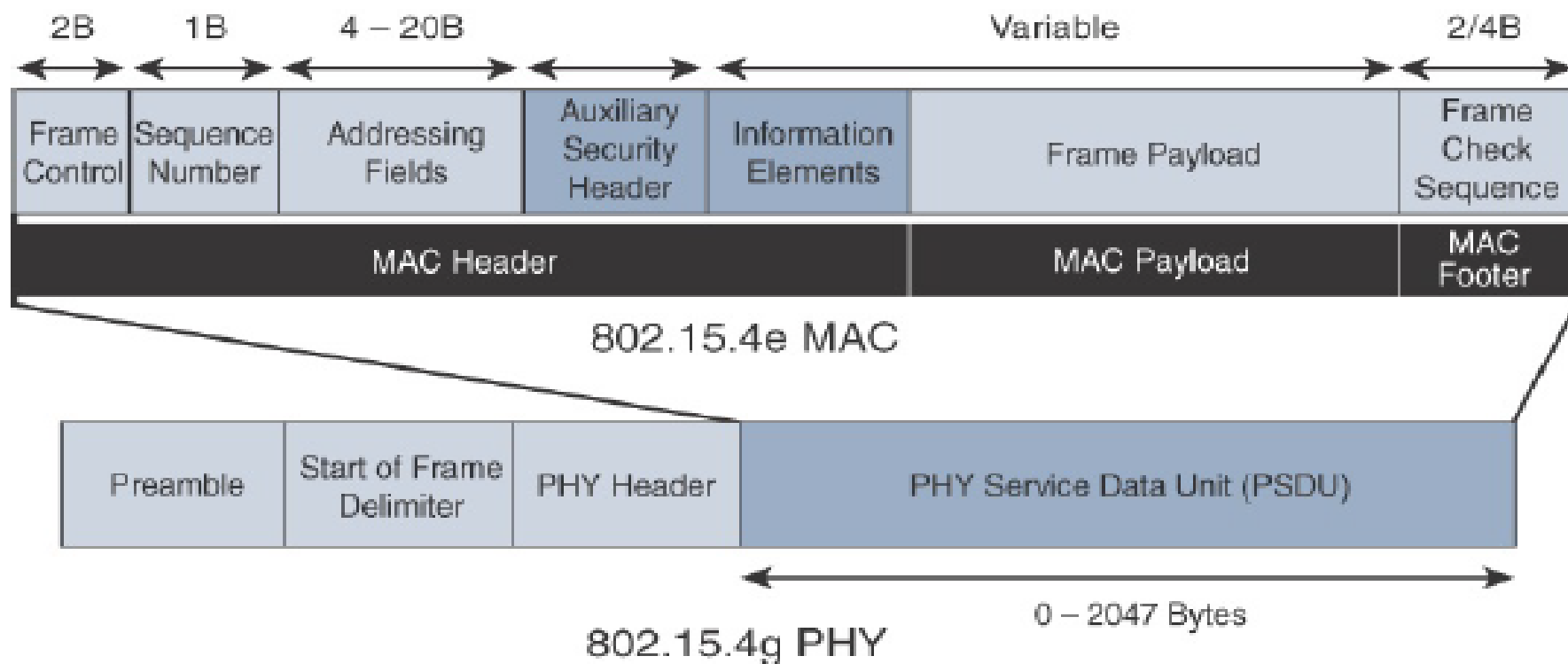
- The IEs in EBRs allow the sender to selectively specify the request of information. Beacon responses are then limited to what was requested in the EBR.
- For ex : a device can query for a PAN that is allowing new devices to join or a PAN that supports a certain set of MAC/PHY capabilities



## ➤ **Enhanced Acknowledgement**

- The **Enhanced Acknowledgement frame** allows for the **integration of a frame counter** for the frame being acknowledged.
- This feature helps protect against certain attacks that occur when Acknowledgement frames are spoofed.





**Figure 4-9 IEEE 802.15.4g/e MAC Frame Format**

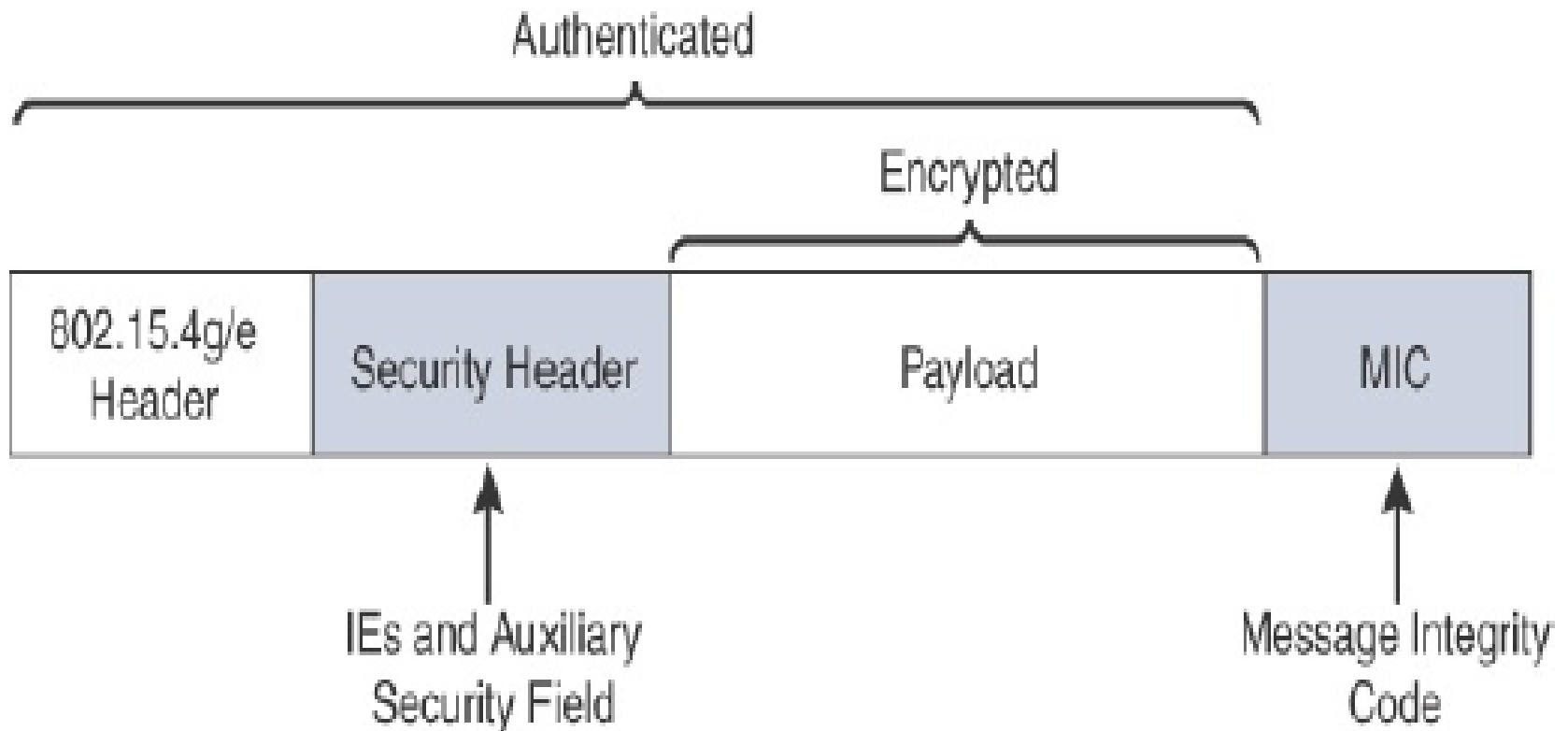
- The **802.15.4g-2012** PHY is similar to the **802.15.4** PHY. The main difference between the two is the **payload size**, with **802.15.4g** supporting up to **2047 bytes** and **802.15.4** supporting only **127 bytes**.
- The **802.15.4e** MAC is similar to the **802.15.4** MAC. The main difference is that in the IEEE 802.15.4e header has the presence of the **Auxiliary Security Header** and **Information Elements field**.
- The **Auxiliary Security header** provides for the **encryption** of the **data frame**. This field is optionally supported in IEEE 802.15.4.

# Topology


- Deployments of IEEE 802.15.4g-2012 are mostly based **on a mesh topology.**
- A mesh topology **allows deployments to be done in urban or rural areas, expanding the distance** between nodes that can relay the traffic of other nodes.

# Security

- \* Both IEEE **802.15.4g** and **802.15.4e** inherit their **security** attributes from the IEEE 802.15.4-2006 specification.
- \* Encryption is provided by AES, with a 128-bit key.
- \* In addition to the Auxiliary Security Header field initially defined in 802.15.4-2006, a **secure acknowledgement** and a **secure Enhanced Beacon field** complete the MAC layer security.



**Figure 4-10** *IEEE 802.15.4g/e MAC Layer Security*

- 
- The Security Header field denoted in Figure 4.10 is composed of the **Auxiliary Security field** and **one or more Information Elements fields**.
  - Integration of the **Information Elements fields** allows for the adoption of additional **security capabilities**, such as the IEEE 802.15.9 **Key Management Protocol (KMP) specification**.

# Competitive Technologies

- Competitive technologies to IEEE 802.15.4g and 802.15.4e parallel the technologies that also compete with IEEE 802.15.4, such as **DASH7**.
- In many ways, 802.15.4 and its various flavors of upper-layer protocols can be seen as competitors as well.

## IEEE 802.15.4g and 802.15.4e Conclusions

- It is important to remember that IEEE 802.15.4g and 802.15.4e are simply amendments to the IEEE 802.15.4 standard.
- They are mature specifications that are integrated into IEEE 802.15.4-2015. They have been successfully deployed in real-world scenarios, and already support millions of endpoints.
- IEEE 802.15.4g focuses mainly on improvements to the PHY layer, while IEEE 802.15.4e targets the MAC layer.



- These improvements overcome many of the disadvantages of IEEE 802.15.4, such as latency and vulnerability to multipath fading.
- The Wi-SUN Alliance is an important industry alliance that provides interoperability and certification for industry implementations.
- Utilizing 802.15.4g as a foundation, the alliance releases profiles, such as the FAN profile, to help promote the adoption of the technology while guaranteeing interoperability between vendors.

# IEEE 1901.2a

- IEEE 1901.2a-2013 is a wired technology that is an update to the original IEEE 1901.2 specification.
- This is a standard for Narrowband Power Line Communication (NB-PLC).
- NB-PLC leverages a narrowband spectrum for low power, long range, and resistance to interference over the same wires that carry electric power.

- NB-PLC is often found in use cases such as the following:
  - **Smart metering**
  - **Distributed Automation**
  - **Public lighting**
  - **Electric vehicle charging stations**
  - **Microgrids**
  - **Renewable energy**

## ➤ **Smart metering:**

- NB-PLC can be used to automate the reading of utility meters, such as electric, gas, and water meters.
- This is true particularly in Europe, where PLC is the preferred technology for utilities deploying smart meter solutions.

## ➤ **Distributed Automation**

- NB-PLC can be used for distribution automation, which involves monitoring and controlling all the devices in the power grid.



➤ **Public lighting**

- A common use for NB-PLC is with public lighting—the lights found in cities and along streets, highways, and public areas such as parks.

➤ **Electric vehicle charging stations**

- NB-PLC can be used for electric vehicle charging stations, where the batteries of electric vehicles can be recharged.



➤ **Microgrids**

- NB-PLC can be used for microgrids, local energy grids that can disconnect from the traditional grid and operate independently.

➤ **Renewable energy**

- NB-PLC can be used in renewable energy applications, such as solar, wind power, hydroelectric, and geothermal heat.

- All these **use cases require** a direct connection to the **power grid**.
- So it makes sense to transport IoT data across power grid connections that are already in place.
- **Multiple PLC standards exist**, but the formation of IEEE 1901.2a was driven by the absence of a **low-frequency PLC solution below 500 kHz**.

# Standardization and Alliances

- The first generations of NB-PLC implementations have generated a lot of interest from utilities in Europe but have often suffered from poor reliability, low throughput, lack of manageability, and poor interoperability.
- This has led several organizations (including standards bodies and alliance consortiums) to develop their own specifications for new generations of NB-PLC technologies.

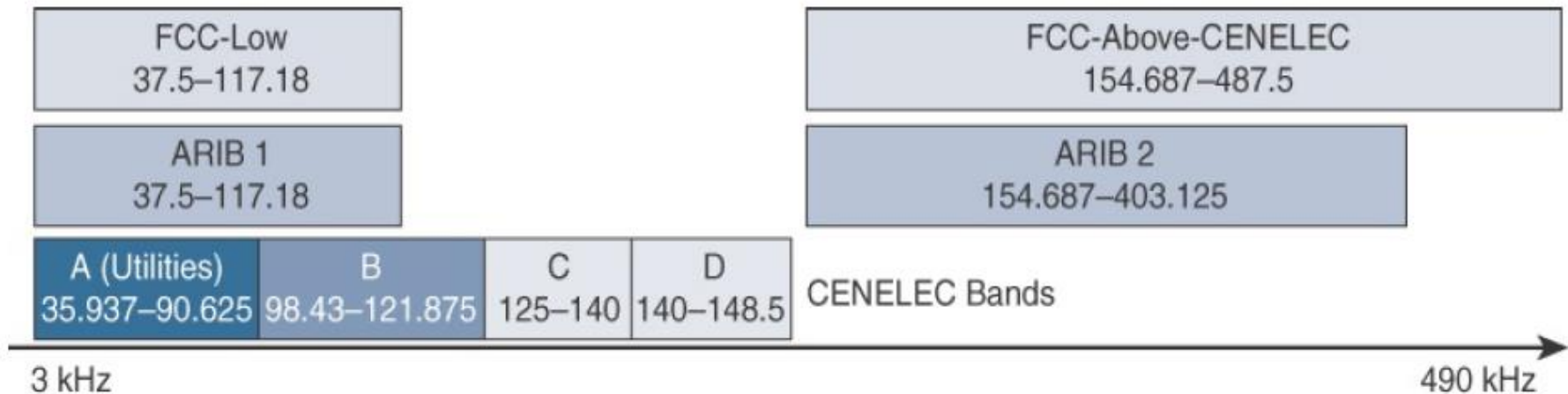


- Most recent NB-PLC standards are based on orthogonal frequency-division multiplexing (OFDM).
- The IEEE 1901.2 working group published the IEEE 1901.2a specification in November 2013.
- The IEEE 1901.2a standard does have some alignment with the latest developments done in other IEEE working groups.
- For example, using the 802.15.4e Information Element fields eases support for IEEE 802.15.9 key management.

# Physical Layer

- NB-PLC is defined for frequency bands from **3 to 500 kHz**.
- Much as with wireless sub-GHz frequency bands, regional regulations and definitions apply to NB-PLC.
- The IEEE 1901.2 working group has integrated support for all world regions in order to develop a worldwide standard.

- CENELEC is the European Committee for Electrotechnical Standardization. This organization is responsible for standardization in the area of electrical engineering for Europe
- Figure 4.11 shows the various frequency bands for NB-PLC.
- The most **well-known bands are regulated by CENELEC** and the FCC, but the Japan Association of Radio Industries and Businesses (ARIB) band is also present.
- The **two ARIB frequency bands are ARIB 1, 37.5–117.1875 kHz, and ARIB 2, 154.6875–403.125 kHz.**



**Figure 4.11:** NB-PLC Frequency Bands

- Based on **OFDM**, the IEEE 1901.2 specification leverages the best from other **NB-PLC OFDM** technologies that were developed previously.
- Therefore, **IEEE 1901.2a** supports the **largest set of coding** and enables **both robustness and throughput**.

- The standard includes tone maps and modulations such as
  - **robust modulation (ROBO)**
  - differential binary phase shift keying (DBPSK)
  - differential quadrature phase shift keying (DQPSK),
  - differential 8-point phase shift keying (D8PSK) for all bands
  - optionally 16 quadrature amplitude modulation (16QAM) for some bands.

- **ROBO** utilizes **QPSK modulation**, and its **throughput** depends on the degree to which coding is **repeated across streams**.
- With **IEEE 1901.2a**, the data throughput rate has the ability to **dynamically change**, depending on the **modulation type and tone map**.

- One major difference between IEEE 802.15.4g/e and IEEE 1901.2a is the full integration of different types of modulation and tone maps by a single PHY layer in the IEEE 1901.2a specification.
- The PHY payload size can change dynamically, based on channel conditions in IEEE 1901.2a.
- Therefore, MAC sublayer segmentation is implemented. If the size of the MAC payload is too large to fit within one PHY service data unit (PSDU), the MAC payload is partitioned into smaller segments.

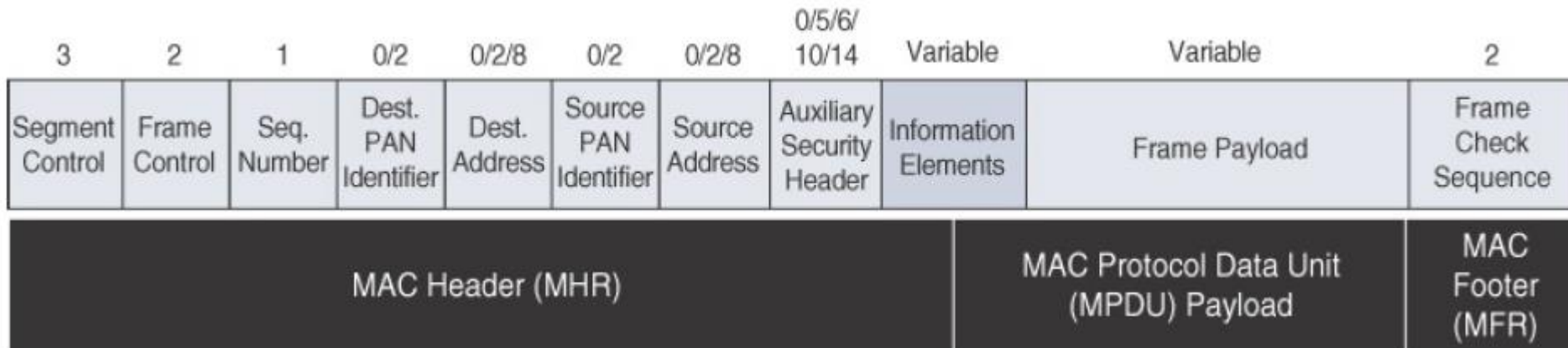
- **MAC payload segmentation** is done by dividing the **MAC payload into multiple smaller amounts of data (segments), based on PSDU size.**
- The segmentation may require the addition of padding bytes to the last payload segment so that the **final MPDU fills the PSDU.**



# MAC Layer

- The **MAC frame format of IEEE 1901.2a** is based on the IEEE 802.15.4 MAC frame but integrates the latest IEEE 802.15.4e-2012 amendment, which enables key features to be supported.
- One of the key components brought from 802.15.4e to IEEE 1901.2a is **information elements**.

- With IE support, additional capabilities, such as IEEE 802.15.9 Key Management Protocol and SSID, are supported.
- Figure 4.12 provides an overview of the general MAC frame format for IEEE 1901.2.




**Figure 4.12:** General MAC Frame Format for IEEE 1901.2

- IEEE 1901.2 has a **Segment Control field**. This is a new field that was not present in the MAC frame for 802.15.4 and 802.15.4e.
- This field handles the segmentation or fragmentation of upper-layer packets with sizes larger than what can be carried in the MAC protocol data unit (MPDU).

# Topology

- Use cases and deployment topologies for IEEE 1901.2a are tied to the physical power lines.
- As with wireless technologies, signal propagation is limited by factors such as noise, interference, distortion, and attenuation.
- NB-PLC deployments use some sort of **mesh topology**.
- **Mesh networks** offer the **advantage of devices** relaying the traffic of other devices **so longer distances can be segmented**.

- 
- Figure 4.13 highlights a network scenario in which a PLC mesh network is applied to a neighborhood.
  - The IEEE 1901.2a standard offers the flexibility to run any upper-layer protocol. So, implementations of IPv6 6LoWPAN and RPL IPv6 protocols are supported.
  - These protocols enable the use of network layer routing to create mesh networks over PLC.




# Security

- **IEEE 1901.2a** security offers **similar** features to **IEEE 802.15.4g**.
- **Encryption and authentication are performed using AES.** In addition, IEEE 1901.2a aligns with 802.15.4g in its ability to support the **IEEE 802.15.9 Key Management Protocol**.


- These differences are mostly tied to the PHY layer fragmentation capabilities of IEEE 1901.2a and include the following:
  - The Security Enabled bit in the Frame Control field should be set in all MAC frames carrying segments of an encrypted frame.
  - If data encryption is required, it should be done before packet segmentation. During packet encryption, the Segment Control field should not be included in the input to the encryption algorithm.




- 
- On the receiver side, the data decryption is done after packet reassembly.
  - When security is enabled, the MAC payload is composed of the ciphered payload and the message integrity code (MIC) authentication tag for non-segmented payloads.
  - If the payload is segmented, the MIC is part of the last packet (segment) only.

# Competitive Technologies

- In the domain of NB-PLC, **two technologies compete against IEEE 1901.2a: G3-PLC (now ITU G.9903) and PRIME (now ITU G.9904).**
- IEEE 1901.2a leverages portions of G3-PLC and PRIME, and it also competes with them. More specifically, G3-PLC is really close to IEEE 1901.2.

- 
- The main differences include the fact that G3-PLC mandates data link layer protocol options for bootstrapping and allocating device addresses, and it is incompatible with IEEE 802.15.4g/e and an end-to-end IPv6 model.
  - This means there is no information element support and no global IPv6 address support.

- 
- PRIME is more like an ATM approach, with a Layer 7 protocol that runs directly on top of Layer 2.
  - Following the IEEE 1901.2 working group efforts, new versions of G3-PLC and PRIME were published.

## IEEE 1901.2a Conclusions

- IEEE 1901.2a is an open PHY and MAC standard approach to enable the use of Narrowband Power Line Communication.
- The set of use cases for this standard depends on and also benefits from the physical power lines that interconnect the devices.
- The IEEE 1901.2a standard leverages the earlier standards G3-PLC (now ITU G.9903) and PRIME (now ITU G.9904).
- Supporting a wide range of frequencies at the PHY layer, IEEE 1901.2a also has a feature-rich MAC layer, based on 802.15.4.

- The HomePlug Alliance's Netricity program and the liaison agreement with the Wi-SUN Alliance provide industry support for IEEE 1901.2a by means of a profile definition and a certification program.
- IEEE 1901.2a faces competition from G3-PLC and PRIME as they are more established standards that continue to evolve.
- Most chipsets offer support for IEEE 1901.2a, G3-PLC, and PRIME because they are the three competitive OFDM-based PLC technologies.

# IEEE 802.11ah

- In unconstrained networks, IEEE 802.11 Wi-Fi is certainly the most successfully deployed wireless technology.
- This standard is a key IoT wireless access technology, either for connecting endpoints such as fog computing nodes, high datarate sensors, and audio or video analytics devices

**OR**

- For deploying Wi-Fi backhaul infrastructures, such as outdoor Wi-Fi mesh in smart cities, oil and mining, or other environments.
- However, Wi-Fi lacks sub-GHz support for better signal penetration, low power for battery-powered nodes, and the ability to support a large number of devices.
- For these reasons, the IEEE 802.11 working group launched a task group named IEEE 802.11ah to specify a sub-GHz version of Wi-Fi.



- Three main use cases are identified for IEEE 802.11ah:
  - **Sensors and meters covering a smart grid**
    - Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors.
  - **Backhaul aggregation of industrial sensors and meter data**
    - Potentially connecting IEEE 802.15.4g subnetworks.
  - **Extended range Wi-Fi**
    - For outdoor extended-range hotspot or cellular traffic offloading when distances already covered by IEEE 802.11a/b/g/n/ac are not good enough

# Standardization and Alliances

- In July 2010, the IEEE 802.11 working group decided to work on an “industrial Wi-Fi” and created the IEEE 802.11ah group.
- The 802.11ah specification operates in unlicensed sub-GHz frequency bands, similar to IEEE 802.15.4 and other LPWA technologies.
- The industry organization that promotes Wi-Fi certifications and interoperability for 2.4 GHz and 5 GHz products is the Wi-Fi Alliance.

- For the 802.11ah standard, the Wi-Fi Alliance defined a new brand called **Wi-Fi HaLow**.
- This marketing name is based on a play on words between “11ah” in reverse and “**low power**.”
- The **HaLow** brand exclusively covers IEEE 802.11ah for sub-GHz device certification.

# Physical Layer

- **IEEE 802.11ah** essentially provides an additional 802.11 physical layer operating in **unlicensed sub-GHz bands**.
- For example, various countries and regions use the following bands for IEEE 802.11ah-
  - 868–868.6 MHz for EMEAR, 902–928 MHz and associated subsets for North America and Asia-Pacific regions
  - 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779–787 MHz for China.

- Based on OFDM modulation, IEEE 802.11ah uses channels of 2, 4, 8, or 16 MHz (and also 1 MHz for low-bandwidth transmission).
- While 802.11ah does not approach this transmission speed of IEEE 802.11ac , it does provide an extended range for its lower speed data.

# MAC Layer

- The IEEE 802.11ah MAC layer is optimized to support the **new sub-GHz Wi-Fi PHY while providing low power consumption and the ability to support a larger number of endpoints.**
- Enhancements and features specified by IEEE 802.11ah for the MAC layer include the following:
  - **Number of devices**
    - Has been scaled up to 8192 per access point.
  - **MAC Header**
    - Has been shortened to allow more efficient communication.

## ➤ **Null data packet (NDP) support**

- Is extended to cover several control and management frames.
- Relevant information is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided.
- This change makes the control frame exchanges efficient and less power-consuming for the receiving stations.



## ➤ **Grouping and sectorization**

- Enables an AP to use sector antennas and also group stations (distributing a group ID).
- In combination with RAW and TWT, this mechanism reduces contention in large cells with many clients by restricting which group, in which sector, can contend during which time window.



## ➤ **Restricted access window (RAW)**

- Is a control algorithm that avoids simultaneous transmissions when many devices are present and provides fair access to the wireless network.
- By providing more efficient access to the medium, additional power savings for battery-powered devices can be achieved, and collisions are reduced.

## ➤ **Target Wake Time(TWT)**

- Reduces energy consumption by permitting an access point to define times when a device can access the network.
- This allows devices to enter a low-power state until their TWT time arrives. It also reduces the probability of collisions in large cells with many clients.



➤ **Speed Frame Exchange**

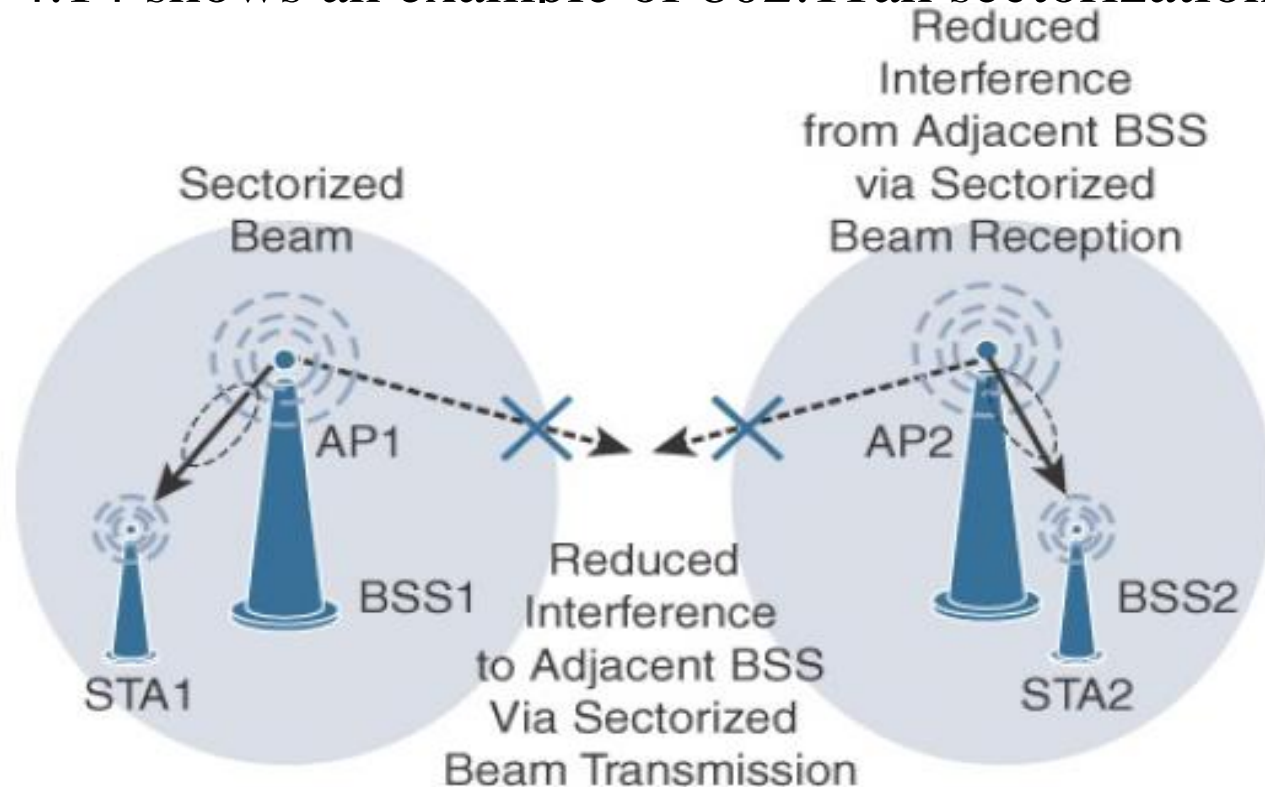
- Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP).
- This reduces contention on the medium, minimizes the number of frame exchanges to improve channel efficiency, and extends battery life by keeping awake times short.

# Topology

- While IEEE 802.11ah is deployed as a **star topology**, it includes a simple hops relay operation **to extend its range**. This relay option is not capped, but the IEEE 802.11ah task group worked on the assumption of two hops.
- It allows one 802.11ah device to act as an intermediary and relay data to another.
- In some ways, this is similar to a mesh, and it is important to note that the clients and not the access point handle the relay function.

- This relay operation can be combined with a higher transmission rate or **modulation and coding scheme (MCS)**.
- Sectorization is a technique that involves partitioning the coverage area into several sectors to get reduced contention within a certain sector.
- This technique is useful for limiting collisions in cells that have many clients. This technique is also often necessary when the coverage area of 802.11ah access points is large, and interference from neighboring access points is problematic.

- Sectorization uses an antenna array and beam-forming techniques to partition the cell coverage area.
- Figure 4.14 shows an example of 802.11ah sectorization.



# Security

- No additional security has been identified for **IEEE 802.11ah** compared to other **IEEE 802.11** specifications.
- These protocols include **IEEE 802.15.4**, **IEEE 802.15.4e**, and **IEEE 1901.2a**, and the security information for them is also applicable to **IEEE 802.11ah**.

# Competitive Technologies

- \* Competitive technologies to IEEE 802.11ah are
- \* IEEE 802.15.4,
- \* IEEE 802.15.4e
- \* 802.15.4g,
- \* DASH7 etc.



## Conclusions

- The IEEE 802.11ah access technology is an ongoing effort of the IEEE 802.11 working group to define an “**industrial Wi-Fi.**”
- Currently, this standard is just at the beginning of its evolution, and it is not clear how the market will react to this new Wi-Fi standard.
- This specification offers a longer range than traditional Wi-Fi technologies and provides good support for low-power devices that need to send smaller bursts of data at lower speeds.

- At the same time, it has the ability to scale to higher speeds as well.
- IEEE 802.11ah is quite different in terms of current products and the existing Wi-Fi technologies in the 2.4 GHz and 5 GHz frequency bands.
- To gain broad adoption and compete against similar technologies in this space, it will need an ecosystem of products and solutions that can be configured and deployed at a low cost.

# LoRaWAN

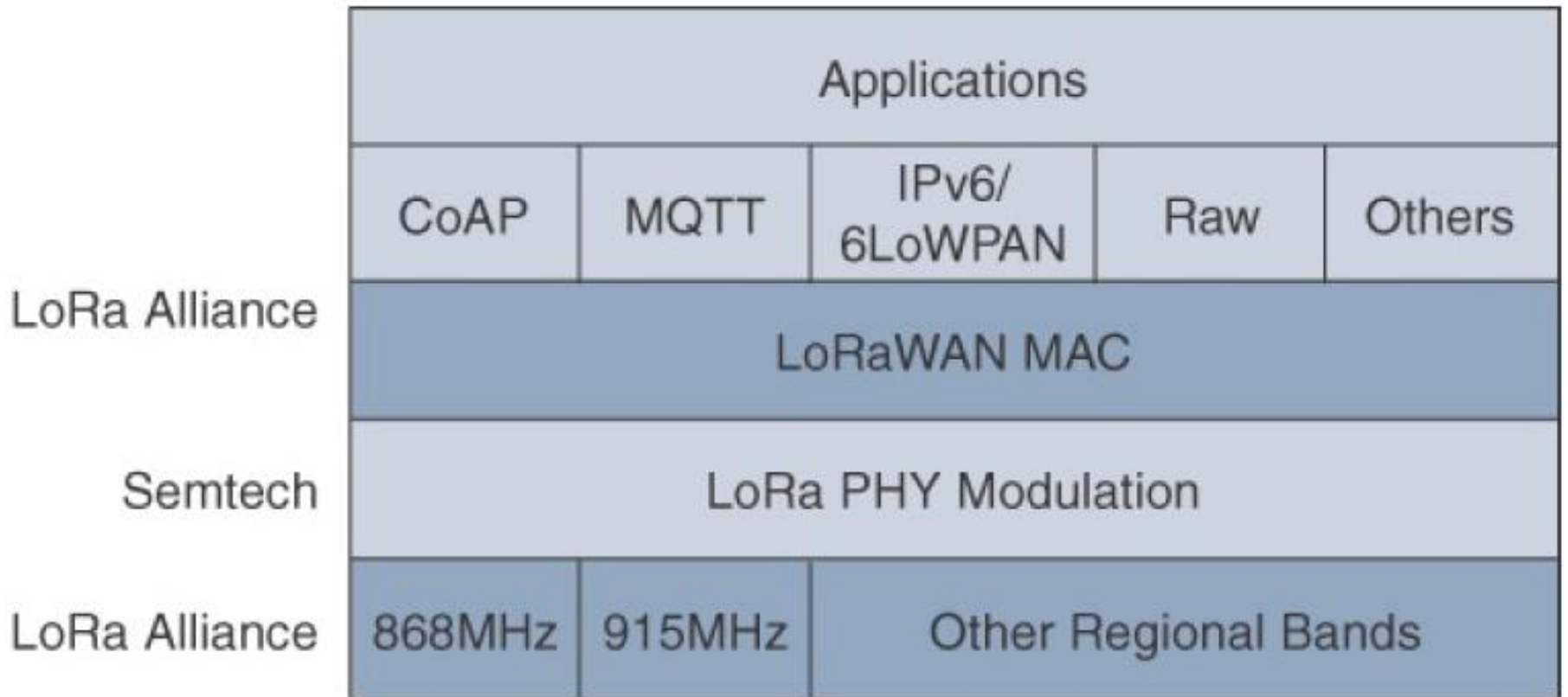
- In recent years, a new set of wireless technologies known as **Low-Power Wide-Area (LPWA)** has received a lot of attention from the industry and press.
- Particularly well adapted for long-range and battery-powered endpoints, LPWA technologies open new business opportunities to both services providers and enterprises considering IoT solutions.
- An example of an **unlicensed-band LPWA technology**, known as **LoRaWAN**

# Standard and Alliances

- Initially, LoRa was a physical layer, or Layer 1, modulation that was developed by a French company named **Cycleo**.
- Later, **Cycleo** was acquired by **Semtech**.
- Optimized for long-range, two-way communications and low power consumption, the technology evolved from Layer 1 to a broader scope through the creation of the **LoRa** Alliance.

- The LoRa Alliance quickly achieved industry support and currently has hundreds of members.
- Semtech LoRa as a Layer 1 PHY modulation technology is available through multiple chipset vendors.
- The LoRa Alliance uses the term LoRaWAN to refer to its architecture and its specifications that describe end-to-end LoRaWAN communications and protocols.

- Figure 4.15 provides a high-level overview of the LoRaWAN layers.
- In this figure, notice that Semtech is responsible for the PHY layer, while the LoRa Alliance handles the MAC layer and regional frequency bands.
- Overall, the LoRa Alliance owns and manages the roadmap and technical development of the LoRaWAN architecture and protocol.




**Figure 4.15:** LoRa WAN Layers

# Physical Layer

- Semtech LoRa modulation is based on **chirp spread spectrum** modulation
  - which trades a lower data rate for receiver sensitivity to significantly increase the communication distance.
- It allows **demodulation** below the noise floor, offers robustness to noise and interference, and manages a single channel occupation by different spreading factors.
- This enables LoRa devices to **receive on multiple channels in parallel.**



- 
- LoRaWAN 1.0.2 regional specifications describe the use of the **main unlicensed sub-GHz frequency** bands of 433 MHz, 779–787 MHz, 863–870 MHz, and 902–928 MHz, as well as regional profiles for a subset of the 902–928 MHz bandwidth.

- A **LoRa gateway** is deployed as the **center hub** of a **star network** architecture.
- It uses **multiple transceivers** and **channels** and can **demodulate multiple channels at once** or even **demodulate multiple signals on the same channel simultaneously**.
- The data rate in LoRaWAN varies depending on the frequency bands and **adaptive data rate (ADR)**.

- **ADR is an algorithm that manages the data rate and radio signal for each endpoint.**
- It ensures that packets are delivered at the best data rate possible and that network performance is both optimal and scalable.
- Endpoints close to the gateways with good signal values transmit with the highest data rate, which enables a shorter transmission time over the wireless network, and the lowest transmit power.
- An important feature of LoRa is its ability to handle various data rates via the spreading factor.

- Devices with a **low spreading factor (SF)** achieve less distance in their communications but transmit at faster speeds, resulting in less airtime.
- A higher SF provides slower transmission rates but achieves a higher reliability at longer distances.
- Table 4.4 illustrates how LoRaWAN data rates can vary depending on the associated spreading factor for the two main frequency bands, 863–870 MHz and 902–928 MHz.

<b>Configuration</b>	<b>863–870 MHz bps</b>	<b>902–928 MHz bps</b>
LoRa: SF12/125 kHz	250	N/A
LoRa: SF11/125 kHz	440	N/A
LoRa: SF10/125 kHz	980	980
LoRa: SF9/125 kHz	1760	1760
LoRa: SF8/125 kHz	3125	3125
LoRa: SF7/125 kHz	5470	5470
LoRa: SF7/250 kHz	11,000	N/A
FSK: 50 kbps	50,000	N/A
LoRa: SF12/500 kHz	N/A	980
LoRa: SF11/500 kHz	N/A	1760
LoRa: SF10/500 kHz	N/A	3900
LoRa: SF9/500 kHz	N/A	7000
LoRa: SF8/500 kHz	N/A	12,500
LoRa: SF7/500 kHz	N/A	21,900

**Table 4.4 :** LoRaWAN Data Rate Example

# MAC Layer

- The MAC layer is defined in the LoRaWAN specification.
- This layer takes advantage of the LoRa physical layer and classifies LoRaWAN endpoints to optimize their battery life and ensure downstream communications to the LoRaWAN endpoints

- The LoRaWAN specification documents three classes of LoRaWAN devices:

- **Class A**

- **Class B**

- **Class C**

## ➤ **Class A**

- This class is the default implementation.
- Optimized for battery powered nodes.
- it allows bidirectional communications, where a given node is able to receive downstream traffic after transmitting.
- Two receive windows are available after each transmission



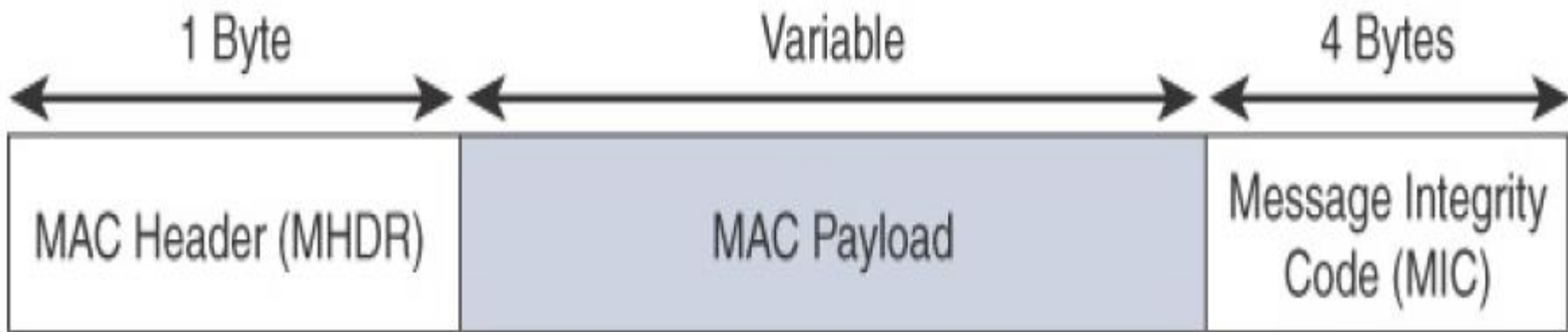
## ➤ **Class B**

- This class was designated “**experimental**” in LoRaWAN 1.0.1 until it can be better defined.
- A Class B node or endpoint should get additional receive windows compared to Class A, but gateways must be synchronized through a beaconing process.

## ➤ **Class C**

- This class is particularly adapted for powered nodes.
- This classification enables a node to be continuously listening by keeping its receive window open when not transmitting.

- LoRaWAN messages, either uplink or downlink, have a PHY payload composed of a 1-byte MAC header, a variable-byte MAC payload, and a MIC that is 4 bytes in length.
- The MAC payload size depends on the frequency band and the data rate, ranging from 59 to 230 bytes for the 863–870 MHz band and 19 to 250 bytes for the 902–928 MHz band.



**Figure 4.16:** High-Level LoRaWAN MAC Frame Format

- The other message types are unconfirmed data up/down and confirmed data up/down.
- A “**confirmed**” message is one that must be acknowledged, and “**unconfirmed**” signifies that the end device does not need to acknowledge.
- “**up/down**” is simply a directional notation identifying whether the message flows in the uplink or downlink path.

- Uplink messages are sent from endpoints to the network server and are relayed by one or more LoRaWAN gateways.
- Downlink messages flow from the network server to a single endpoint and are relayed by only a single gateway.
- Multicast over LoRaWAN is being considered for future versions.

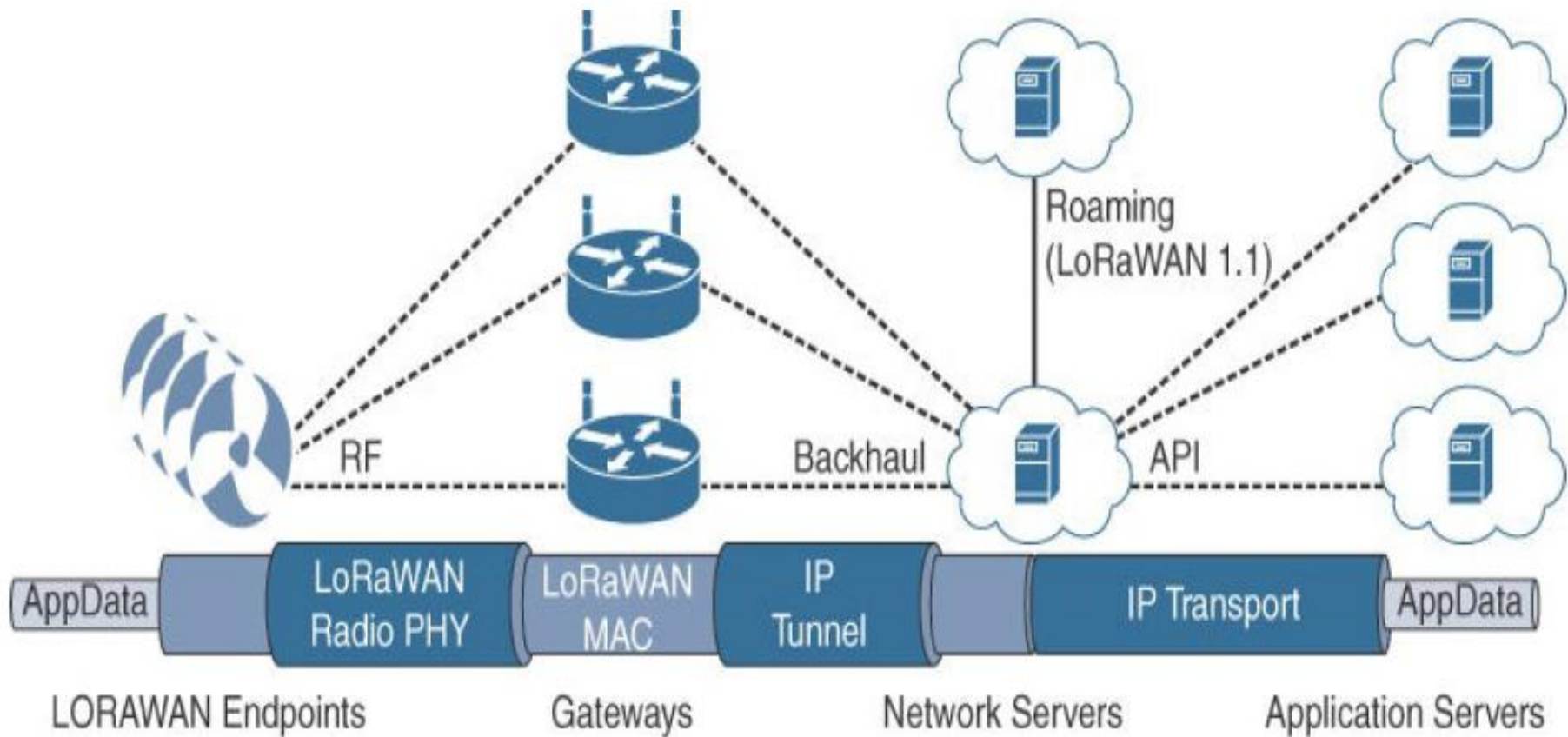
- LoRaWAN endpoints are uniquely addressable through a variety of methods, including the following:
  - An endpoint can have a global end device ID or DevEUI represented as an IEEE EUI-64 address.
  - An endpoint can have a global application ID or AppEUI represented as an IEEE EUI-64 address that uniquely identifies the application provider, such as the owner, of the end device.

- \* In a LoRaWAN network, endpoints are also known by their end device address, known as a DevAddr, a 32-bit address.
- \* The 7 most significant bits are the network identifier (NwkID), which identifies the LoRaWAN network.
- \* The 25 least significant bits are used as the network address (NwkAddr) to identify the endpoint in the network.



# Topology

- LoRaWAN topology is often described as a “**star of stars**” topology.
- Figure 4.17 shows the infrastructure consists of endpoints exchanging packets through gateways acting as bridges, with a central LoRaWAN network server.



**Figure 4.17:** LoRaWAN Architecture

- **Gateways** connect to the **backend network** using standard **IP connections**, and endpoints communicate directly with one or more gateways.
- LoRaWAN endpoints transport their selected **application data over the LoRaWAN MAC layer on top of one of the supported PHY layer frequency bands**.
- The application data is contained in upper protocol layers. These upper layers are not the responsibility of the LoRa Alliance, but best practices may be developed and recommended.


- These upper layers could just be raw data on top of the LoRaWAN MAC layer, or the data could be stacked in **multiple protocols**.
- For ex : We could have upper-layer protocols, such as ZigBee Control Layer (ZCL), Constrained Application Protocol (CoAP), or Message Queuing Telemetry Transport (MQTT), with or without an IPv6/6LoWPAN layer.
- **LoRaWAN gateways** act as bridges that relay between **endpoints and the network servers**.

- Multiple gateways can receive and transport the same packets. When duplicate packets are received, de-duplication is a function of the network server.
- The LoRaWAN network server manages the data rate and radio frequency (RF) of each endpoint through the adaptive data rate (ADR) algorithm.

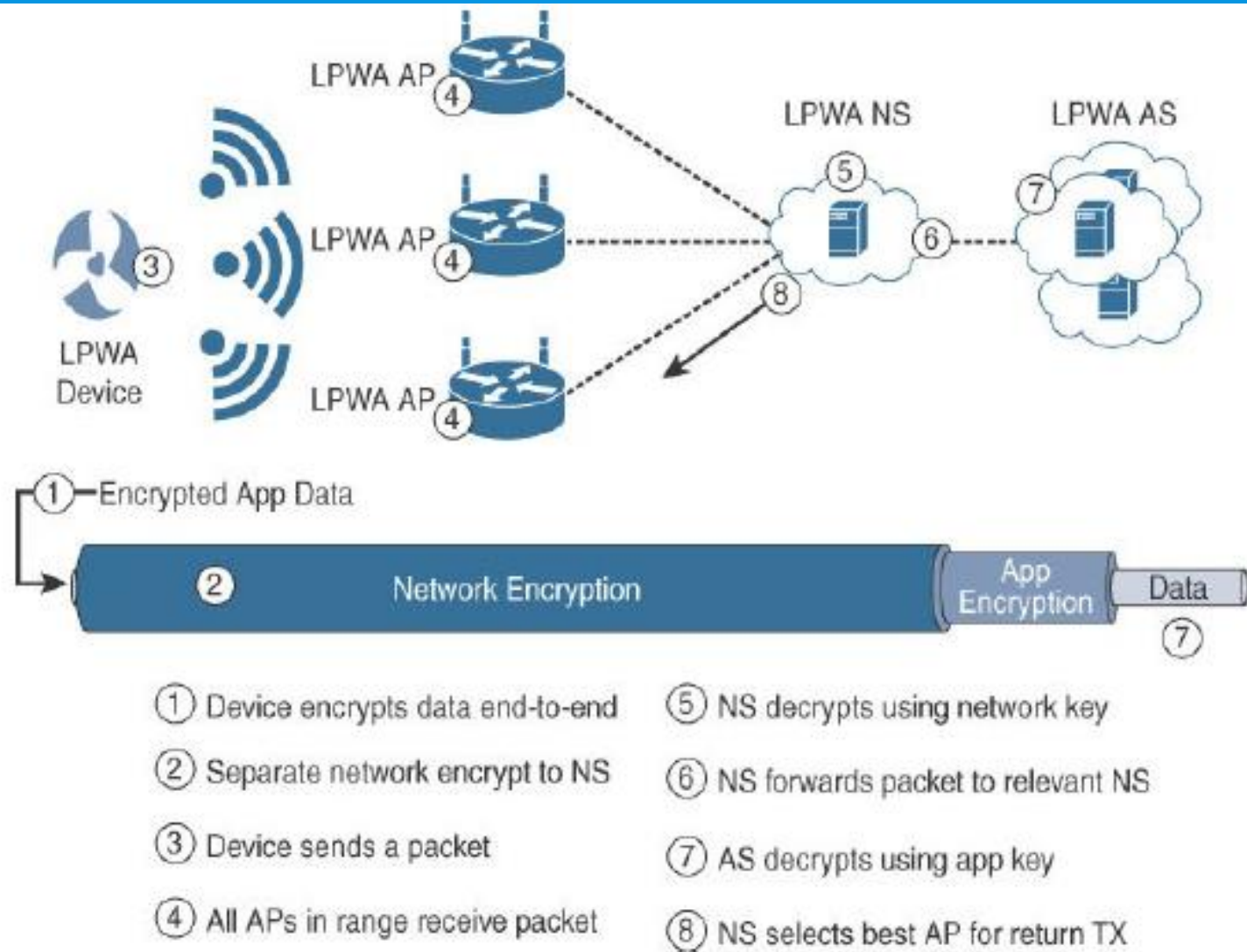
- ADR is a key component of the network scalability, performance, and battery life of the endpoints.
- In future versions of the LoRaWAN specification, roaming capabilities between LoRaWAN network servers will be added.
- These capabilities will enable mobile endpoints to connect and roam between different LoRaWAN network infrastructures.

# Security

- Security in a LoRaWAN deployment applies to different components of the architecture as shown in the Figure 4.18
- LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network

- 
- The first layer, called “**network security**” but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server. Also, it protects LoRaWAN packets by performing encryption based on AES.
  - Each endpoint implements a **network session key** (NwkSKey), used by both itself and the LoRaWAN network server





**Figure 4.18:** LoRaWAN Security

- The NwkSKey ensures data integrity through computing and checking the MIC of every data message as well as encrypting and decrypting MAC-only data message payloads.
- The second layer is an **application session key** (AppSKey), which performs encryption and decryption functions between the endpoint and its application server. Furthermore, it computes and checks the application-level MIC, if included.

- Endpoints receive their AES-128 application key (AppKey) from the application owner. This key is most likely derived from an application-specific root key exclusively known to and under the control of the application provider.
- LoRaWAN endpoints attached to a LoRaWAN network must get registered and authenticated. This can be achieved through one of the two join mechanisms:

## ➤ **Activation by Personalization(ABP)**

- Endpoints don't need to run a join procedure as their individual details, including DevAddr and the NwkSKey and AppSKey session keys, are preconfigured and stored in the end device.
- This same information is registered in the LoRaWAN network server.

## ➤ **Over-the-air activation(OTAA)**

- Endpoints are allowed to dynamically join a particular LoRaWAN network after successfully going through a join procedure.
- The join procedure must be done every time a session context is renewed.
- During the join process, which involves the sending and receiving of MAC layer join request and join accept messages, the node establishes its credentials with a LoRaWAN network server, exchanging its globally unique DevEUI, AppEUI, and AppKey.

# Competitive Technologies

- LPWA solutions and technologies are split between unlicensed and licensed bands.
- The licensed-band technologies are dedicated to mobile service providers that have acquired spectrum licenses.
- In addition, several technologies are targeting the unlicensed-band LPWA market to compete against LoRaWAN.
- Table 4.5 evaluates two of the best-established vendors known to provide LPWA options.

<b>Characteristic</b>	<b>LoRaWAN</b>	<b>Sigfox</b>	<b>Ingenu Onramp</b>
Frequency bands	433 MHz, 868 MHz, 902–928 MHz	433 MHz, 868 MHz, 902–928 MHz	2.4 GHz
Modulation	Chirp spread spectrum	Ultra-narrowband	DSSS
Topology	Star of stars	Star	Star; tree supported with an RPMA extender
Data rate	250 bps–50 kbps (868 MHz) 980 bps–21.9 kbps (915 MHz)	100 bps (868 MHz) 600 bps (915 MHz)	6 kbps
Adaptive data rate	Yes	No	No
Payload	59–230 bytes (868 MHz) 19–250 bytes (915 MHz)	12 bytes	6 bytes–10 KB
Two-way communications	Yes	Partial	Yes
Geolocation	Yes (LoRa GW version 2 reference design)	No	No
Roaming	Yes (LoRaWAN 1.1)	No	Yes
Specifications	LoRA Alliance	Proprietary	Proprietary

**Table 4.5** : Unlicensed LPWA Technology Comparison

## LoRaWAN Conclusions

- The LoRaWAN wireless technology was developed for LPWANs that are critical for implementing many new devices on IoT networks.
- The term LoRa refers to the PHY layer, and LoRaWAN focuses on the architecture, the MAC layer, and a unified, single standard for seamless interoperability.
- The PHY and MAC layers allow LoRaWAN to cover longer distances with a data rate that can change depending on various factors.
- The LoRaWAN architecture depends on gateways to bridge endpoints to network servers.



- From a security perspective, LoRaWAN offers AES authentication and encryption at two separate layers.
- Unlicensed LPWA technologies represent new opportunities for implementing IoT infrastructures, solutions, and use cases for private enterprise networks, broadcasters, and mobile and non-mobile service providers.
- The ecosystem of endpoints is rapidly growing and will certainly be the tie-breaker between the various LPWA technologies and solutions, including LoRaWAN.
- As private enterprises look at developing LPWA networks, they will benefit from roaming capabilities between private and public infrastructures.

# NB-IoT and other LTE Variations

- Existing **cellular technologies**, such as **GPRS, Edge, 3G, and 4G/LTE**, are not particularly well adapted to battery-powered devices and small objects specifically developed for the Internet of Things.
- While industry players have been developing unlicensed-band LPWA technologies, 3GPP and associated vendors have been working on evolving cellular technologies to better address IoT requirements.
- The effort started with the definition of new LTE device categories.

- The new LTE-M device category was not sufficiently close to LPWA capabilities, in 2015 3GPP approved a proposal to standardize a **new narrowband radio access technology called Narrowband IoT (NB-IoT)**.
- NB-IoT specifically addresses the requirements of **a massive number of low-throughput devices, low device power consumption, improved indoor coverage, and optimized network architecture.**

# Standardization and Alliances

- The 3GPP organization includes multiple working groups focused on many different aspects of telecommunications (for example, radio, core, terminal, and so on).
- Many **service providers** and vendors make up 3GPP, and the results of their collaborative work in these areas are the 3GPP specifications and studies.

- \* Then, depending on the access technology that is most closely aligned, such as 3G, LTE, or GSM, the IoT related contribution is handled by either 3GPP or the GSM EDGE Radio Access Networks (GERAN) group.
- \* Mobile vendors and service providers are not willing to lose leadership in this market of connecting IoT devices.
- \* Therefore, a couple intermediate steps have been pushed forward, leading to the final objectives set for NB-IoT and documented by 3GPP.

## LTE Cat 0

- The first enhancements to better support IoT devices in 3GPP occurred in LTE Release 12.
- A new user equipment (UE) category, Category 0, was added, with devices running at a maximum data rate of 1 Mbps.
- Generally, LTE enhancements target higher bandwidth improvements.
- Category 0 includes important characteristics to be supported by both the network and end devices.

- These Cat 0 characteristics include the following:
  - **Power Saving Mode(PSM)**
    - This new device status minimizes energy consumption. Energy consumption is expected to be lower with PSM than with existing idle mode.
    - PSM is defined as being similar to “powered off” mode, but the device stays registered with the network.
    - By staying registered, the device avoids having to reattach or reestablish its network connection.

- The device negotiates with the network the idle time after which it will wake up. When it wakes up, it initiates a **tracking area update** (TAU), after which it stays available for a configured time and then switches back to sleep mode or PSM.
- A TAU is a procedure that an LTE device uses to let the network know its current tracking area, or the group of towers in the network from which it can be reached.
- Basically, with PSM, a device can be practically powered off but not lose its place in the network.



## ➤ **Half-duplex mode**

- This mode reduces the cost and complexity of a device's implementation because a duplex filter is not needed.
- Most IoT endpoints are sensors that send low amounts of data that do not have a full duplex communication requirement

## LTE-M

- Following LTE Cat 0, the next step in making the licensed spectrum more supportive of IoT devices was the introduction of the LTE-M category for 3GPP LTE Release 13.
- These are the main characteristics of the LTE-M category in Release 13:
  - **Lower Receiver Bandwidth**
    - Bandwidth has been lowered to 1.4 MHz versus the usual 20 MHz. This further simplifies the LTE endpoint.



➤ **Lower data rate**

- Data is around 200 kbps for LTE-M, compared to 1 Mbps for Cat 0.

➤ **Half-duplex mode**


- Just as with Cat 0, LTE-M offers a half-duplex mode that decreases node complexity and cost.

## ➤ **Enhanced discontinuous reception(eDRX)**

- This capability increases from seconds to minutes the amount of time an endpoint can “sleep” between paging cycles.
- A paging cycle is a periodic check-in with the network. This extended “sleep” time between paging cycles extends the battery lifetime for an endpoint significantly.

# NB-IoT

- The work on NB-IoT started with multiple proposals pushed by the involved vendors, including the following:
  - Extended Coverage GSM (EC-GSM), Ericsson proposal
  - Narrowband GSM (N-GSM), Nokia proposal
  - Narrowband M2M (NB-M2M), Huawei/Neul proposal
  - Narrowband OFDMA (orthogonal frequency-division multiple access), Qualcomm proposal

- 
- Narrowband Cellular IoT (NB-CIoT), combined proposal of NB-M2M and NB-OFDMA
  - Narrowband LTE (NB-LTE), Alcatel-Lucent, Ericsson, and Nokia proposal
  - Cooperative Ultra Narrowband (C-UNB), Sigfox proposal

- Consolidation occurred with the agreement to specify a single NB-IoT version based on orthogonal frequency-division multiple access (OFDMA) in the downlink and a couple options for the uplink.
- Three modes of operation are applicable to NB-IoT:
  - **Standalone**
    - A GSM carrier is used as an NB-IoT carrier, enabling reuse of 900 MHz or 1800 MHz.

## ➤ **In-band**

- Part of an LTE carrier frequency band is allocated for use as an NB-IoT frequency.
- The service provider typically makes this allocation, and IoT devices are configured accordingly.
- We should be aware that if these devices must be deployed across different countries or regions using a different service provider, problems may occur unless there is some coordination between the service providers, and the NB-IoT frequency band allocations are the same.



## ➤ Guard-band

- An NB-IoT carrier is between the LTE or WCDMA bands. This requires coexistence between LTE and NB-IoT bands.
- NB-IoT is defined for a 200-kHz-wide channel in both uplink and downlink, allowing mobile service providers to optimize their spectrum, with a number of deployment options for GSM, WCDMA, and LTE spectrum, as shown in the Figure 4.19.
- In an LTE network, resource blocks are defined with an effective bandwidth of 180 kHz, while on NB-IoT, tone or subcarriers replace the LTE resource blocks.

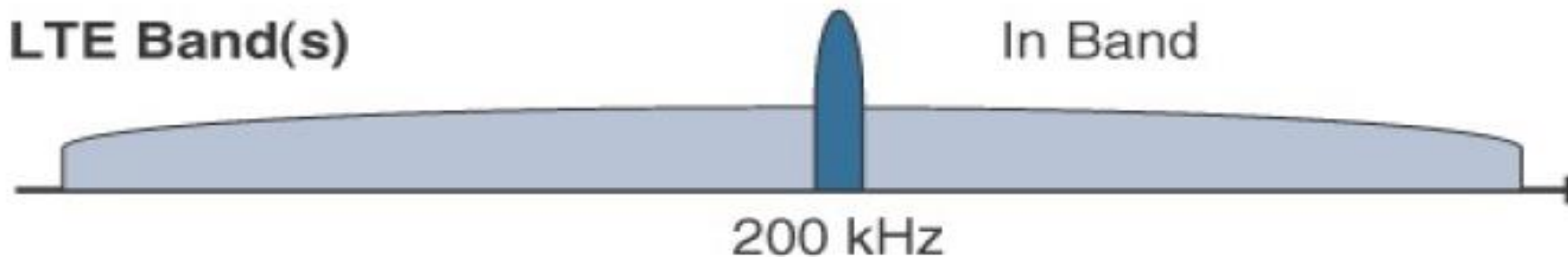
**GSM Band(s)**

Standalone



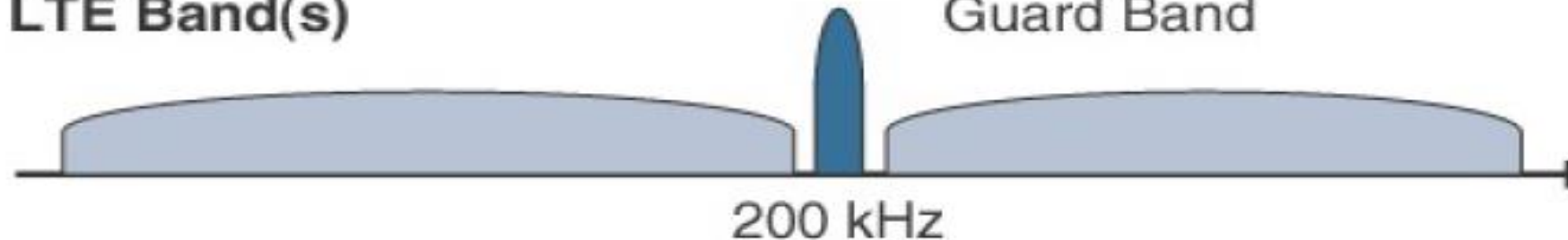
**LTE Band(s)**

In Band



**LTE Band(s)**

Guard Band



**Figure 4.19** : NB-IoT Deployment Options

- The uplink channel can be **15 kHz** or **3.75 kHz** or **multi-tone** ( **$n \times 15$  kHz**, **n up to 12**).
- At Layer 1, the maximum transport block size (TBS) for **downlink is 680 bits**, while **uplink is 1000 bits**.
- At Layer 2, the **maximum Packet Data Convergence Protocol (PDCP) service data unit (SDU) size is 1600 bytes**.
- NB-IoT operates in **half-duplex frequency-division duplexing (FDD)** mode with a **maximum data rate uplink of 60 kbps** and **downlink of 30 kbps**.

# Topology

- NB-IoT is defined with a link budget of 164 dB; compare this with the GPRS link budget of 144 dB, used by many machine-to-machine services.
- The additional 20 dB link budget increase should guarantee better signal penetration in buildings and basements while achieving battery life requirements.


# Competitive Technologies

- In licensed bands, it is expected that 3GPP NB-IoT will be the adopted LPWA technology when it is fully available.
- Competitive technologies are mostly the unlicensed-band LPWA technologies such as LoRaWAN.
- The main challenge faced by providers of the licensed bands is the opportunity for non-mobile service providers to grab market share by offering IoT infrastructure without buying expensive spectrum

# NB-IoT and Other LTE Variations

## Conclusions

- NB-IoT represents the future of LPWA technology for the mobile service providers who own licensed-band spectrum.
- IoT-related specifications must be completed and published by 3GPP to enable vendors, mobile service providers, and applications to successfully and widely endorse the technology

- 
- Evolution to eSIMs, which are still not widely supported, should be tied to NB-IoT as managing millions of SIM cards may not be an acceptable path for the market.
  - An eSIM card is compliant across multiple operators and also reconfigurable. This means that it is a permanent part of the device and is easily rewritten if the device is switched to a different provider.