Connecting Smart Objects

A common information set is provided about the IoT access technologies which are as listed below:

- 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

Technologies for connecting smart objects

- **IEEE 802.15.4:** an older but foundational wireless protocol for connecting smart objects.
- **IEEE 802.15.4g and IEEE 802.15.4e:** improvements to 802.15.4 that are targeted to utilities and smart cities deployments.
- **IEEE 1901.2a:** technology for connecting smart objects over power lines.
- **IEEE 802.11ah:** A technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
- **LoRaWAN: A** scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.
- **NB-IoT and Other LTE Variations:** That are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.

Communications Criteria

- **Range:** This section examines the importance of signal propagation and distance.
- **Frequency Bands:** This section describes licensed and unlicensed spectrum, including sub-GHz frequencies. Power Consumption: This section discusses the considerations required for devices connected to a stable power source compared to those that are battery powered.
- **Topology:** This section highlights the various layouts that may be supported for connecting multiple smart objects.
- **Constrained Devices:** This section details the limitations of certain smart objects from a connectivity perspective.
- **Constrained-Node Networks:** This section highlights the challenges that are often encountered with networks connecting smart objects.

IEEE 802.15.4

- Wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries
- Enables easy installation using a compact protocol stack
- Simple and flexible.
- Wide range of IoT use cases in both the consumer and business markets

IEEE 802.15.4 deployments:

- Home and building automation
- Automotive networks
- Industrial wireless sensor networks
- Interactive toys and remote controls

Disadvantages

- The negatives around reliability and latency often have to do with the Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithms.
- CSMA/CA is an access method in which a device “listens” to make sure no other devices are transmitting before starting its own transmission. If another device is transmitting, a wait time (which is usually random) occurs before “listening” occurs again.
- Interference and multipath fading occur with IEEE 802.15.4 because it lacks a frequency-hopping technique.
- Later variants of 802.15.4 from the IEEE start to address these issues.

most well-known protocol stacks based on 802.15.4

S.No	Protocol	Description
1.	ZigBee	Promoted through the 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
2.	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. RFCs document header compression and IPv6 enhancement to cope with the specific details of IEEE 802.15.4
3.	ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer , IPv6 network layer, RPL routing protocol. In addition, it offers improvement in IP security.
4.	ISA100.11a	This is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial automation: Process Control and Related Applications".It is based on IEEE 802.15.4-2006. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards
5.	Wireless HART	Wireless HART 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 2.4GHz frequency band.
6.	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.

ZIGBEE TECHNOLOGY

- Technological Standard Created for Control and Sensor Networks
- Based on the IEEE 802.15.4 Standard
- High level Communication
- Wireless Personal Area Networks (WPANs)
- Created by the ZigBee Alliance

History

- ZigBee-style networks began to be conceived in 1998 when many engineers realized that WiFi and Bluetooth would be unsuitable for many applications.

  In particular, many engineers saw a need for self-organizing ad-hoc digital radio networks.
- The IEEE 802.15.4 standard was completed in May 2003.
- The ZigBee specifications were ratified on 14 December 2004.
- The ZigBee Alliance announces the public availability of Specification 1.0 on 13 June 2005.

Layers of ZigBee network:

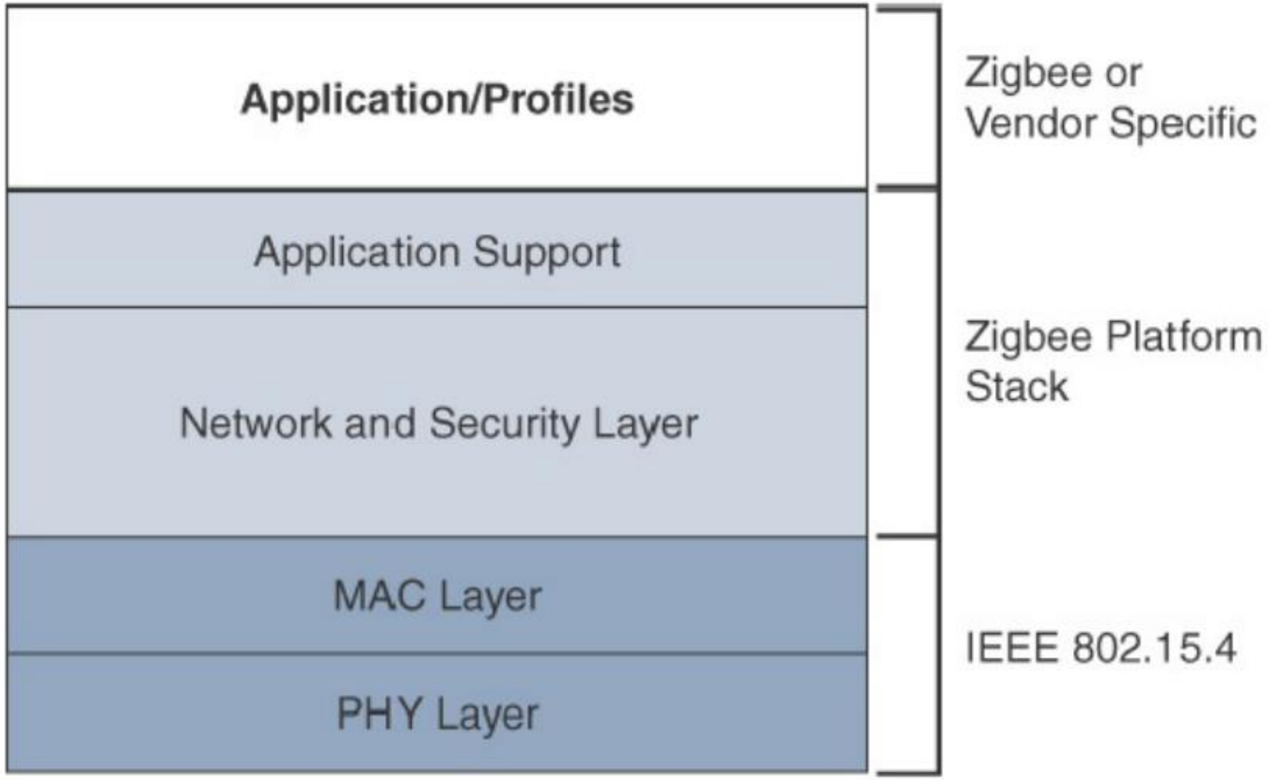
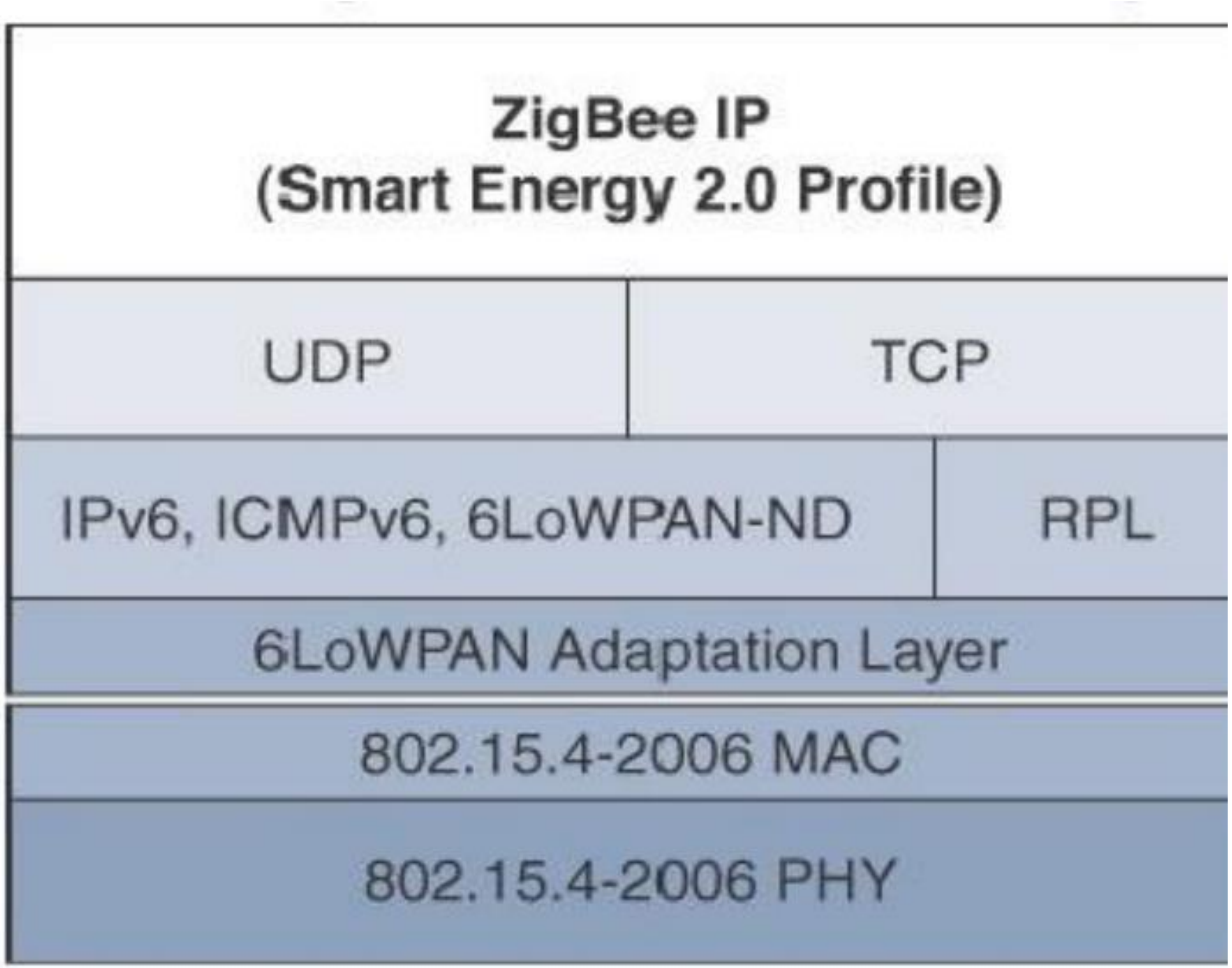


Figure 2.1 High Level ZigBee Protocol Stack

- 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 interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications.
- ZigBee predefines many application profiles for certain industries, and vendors can optionally create their own custom ones at this layer. 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.

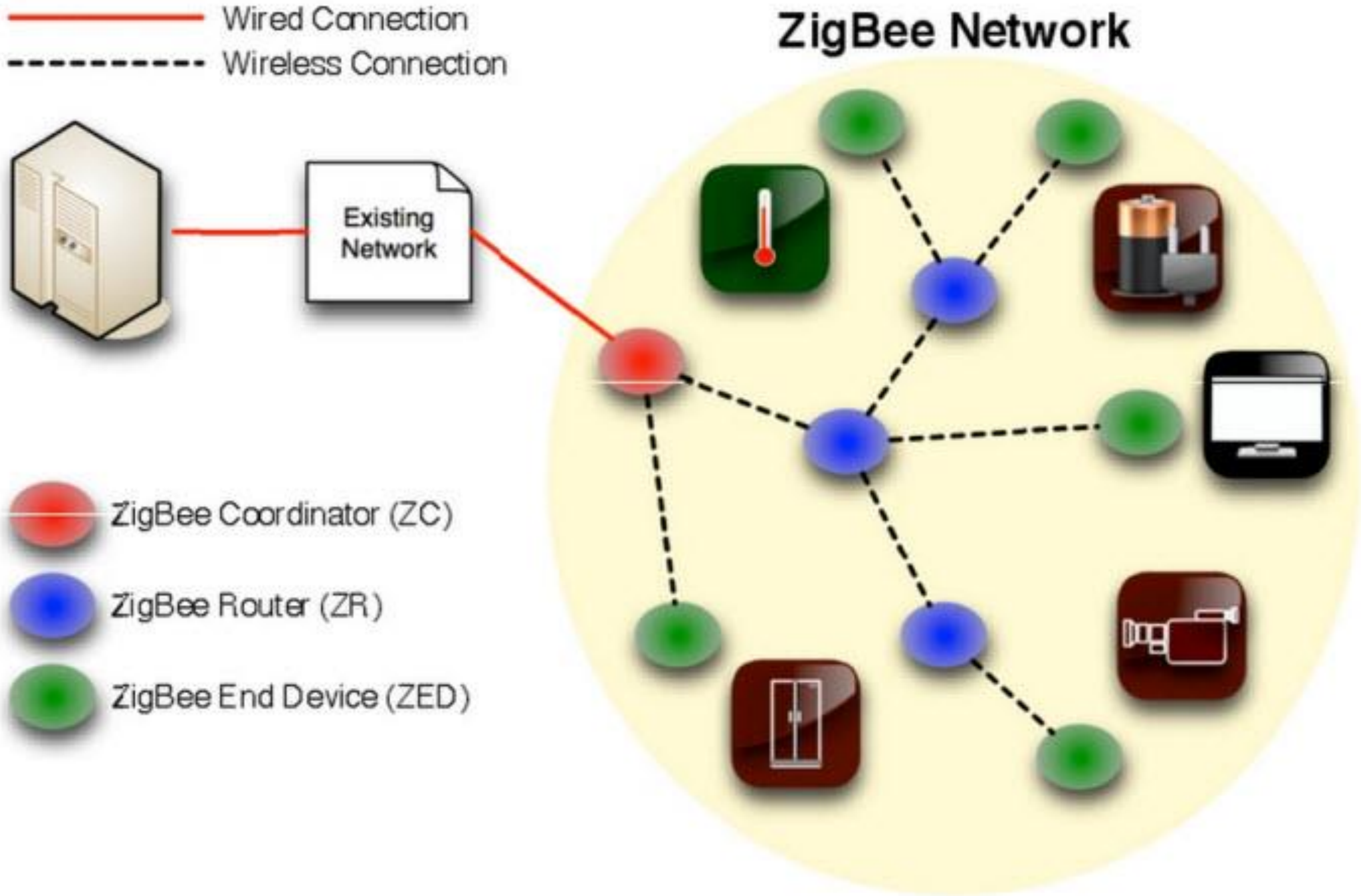


ZigBee IP protocol stack

ZigBee IP/SE 2.0

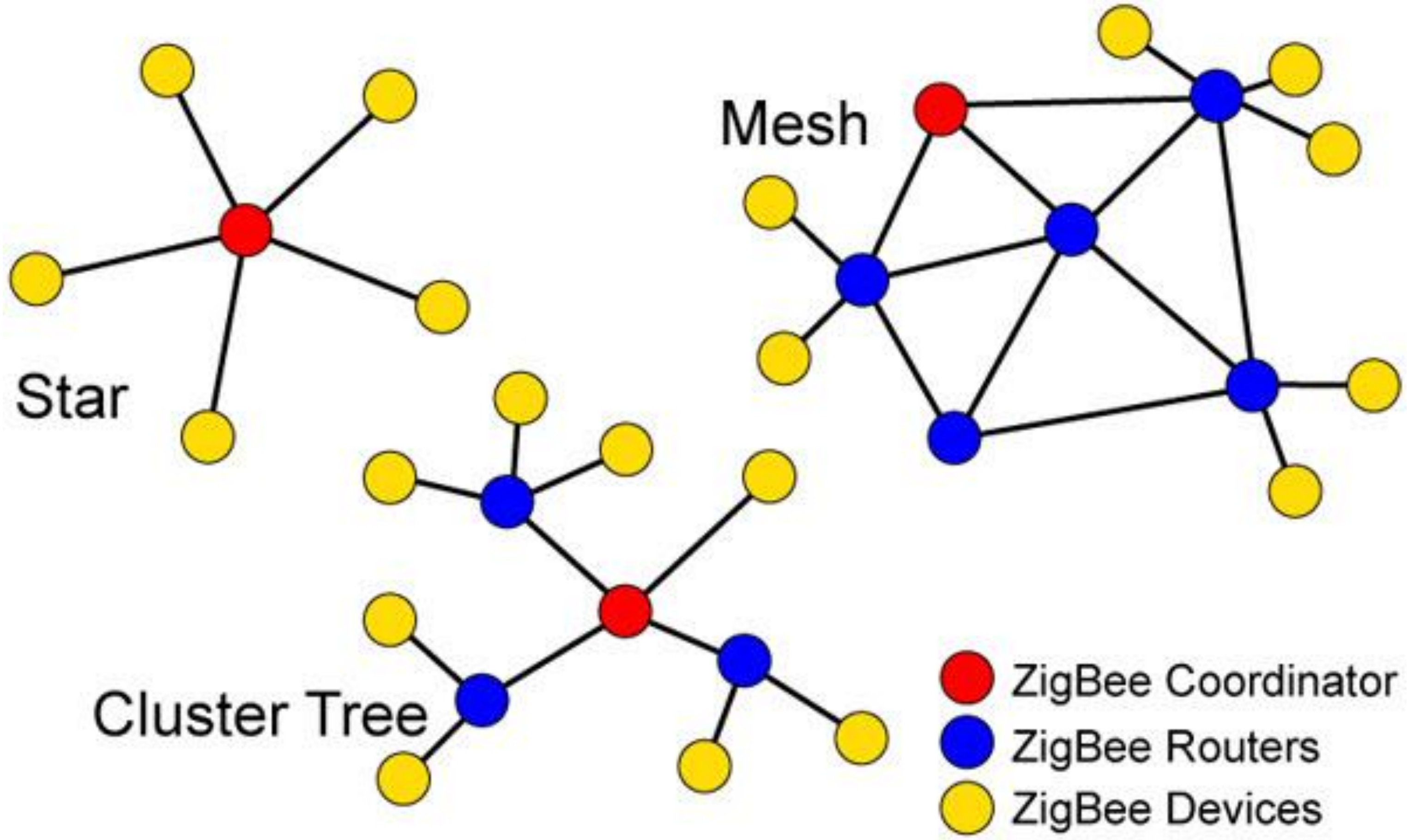
- Follows IEEE STD 802.15.4 STD protocol
- Zigbee endpoint devices form WPAN of embedded sensors, actuators, appliance controllers or medical data s/y's – IoT Applications
- Zigbee Neighborhood Area N/w (NAN) is the version for Smart Grid. Ex Smart Metering.
- Features of Zigbee IP
  - Used for Low Power Short range WPAN
  - Device can function in 6 modes – end point, ZigBee device router, N/W coordinator, IP coordinator, IP router and IP Host
  - Supports RFD – Reduced function device - goes to sleep mode once its work is done
  - Supports IPv6 with 6LoWPAN
  - Self configuring, healing , dynamic pairing
  - Range – 10 – 200m, Data rates : 250kbps, low power operation
  - AES-CCM-128

Zigbee

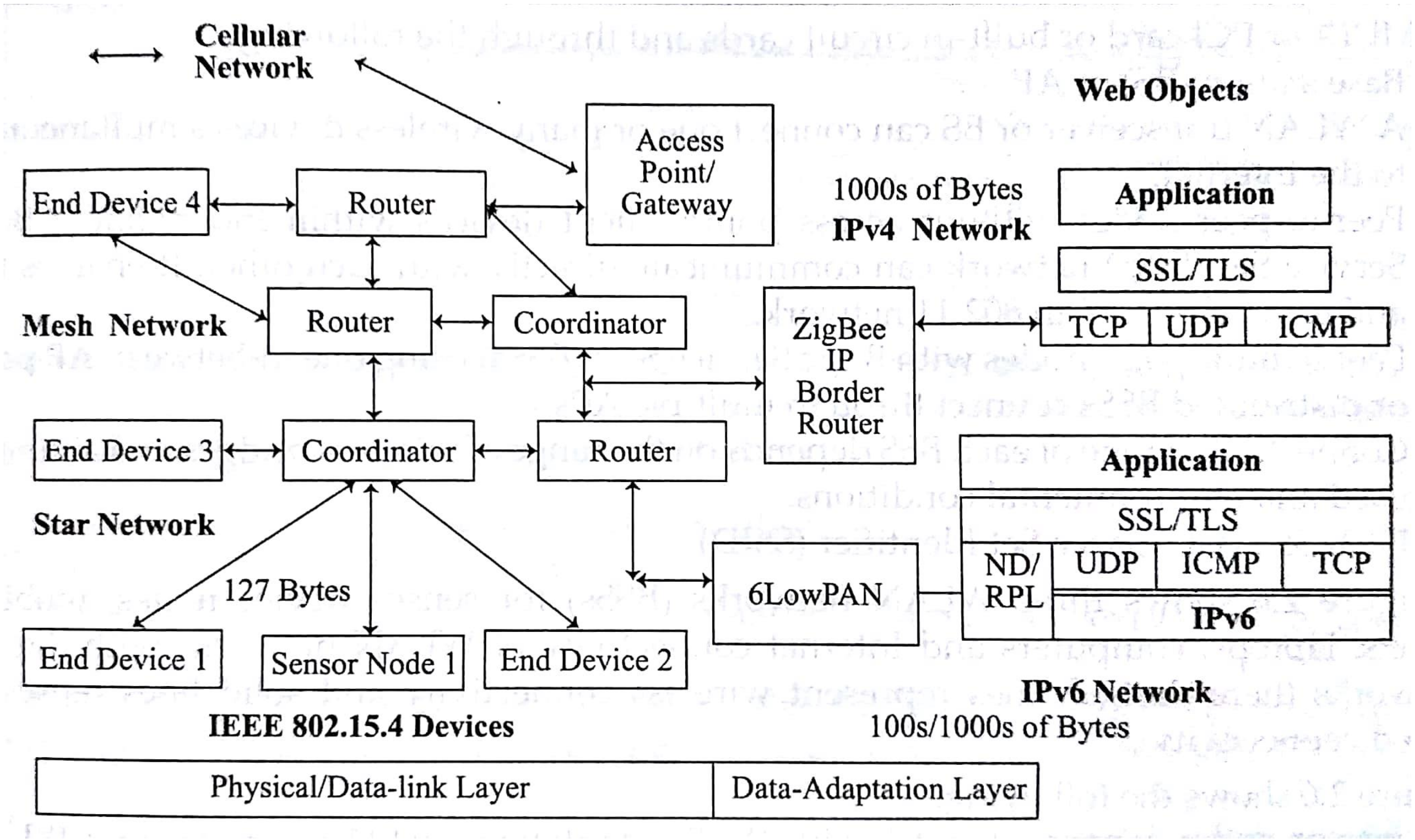


Wired Connection
Wireless Connection
ZigBee Network
Existing Network
ZigBee Coordinator (ZC)
ZigBee Router (ZR)
ZigBee End Device (ZED)

Zigbee Topologies



Zigbee - Modes



ZigBee IP/SE 2.0

- Features of Zigbee
- The router in star network connects to 6LoWPAN, which connects an IEEE 802.15.4 devices network to IPv6 n/w

Physical Layer

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

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

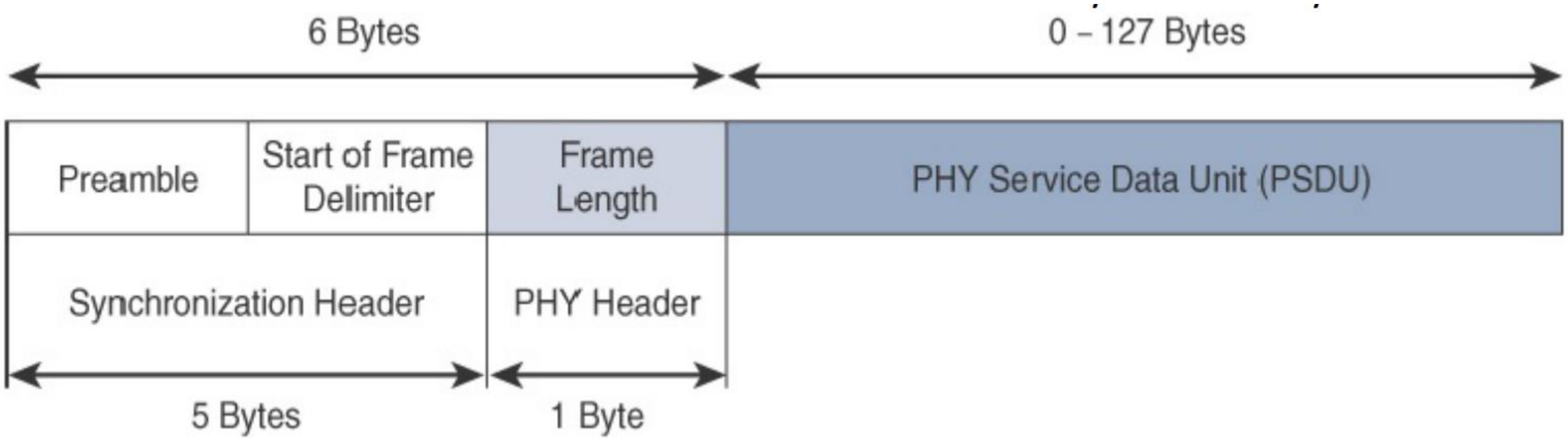


Figure 2.3 IEEE 802.15.4 PHY Format

MAC Layer

- 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

- 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

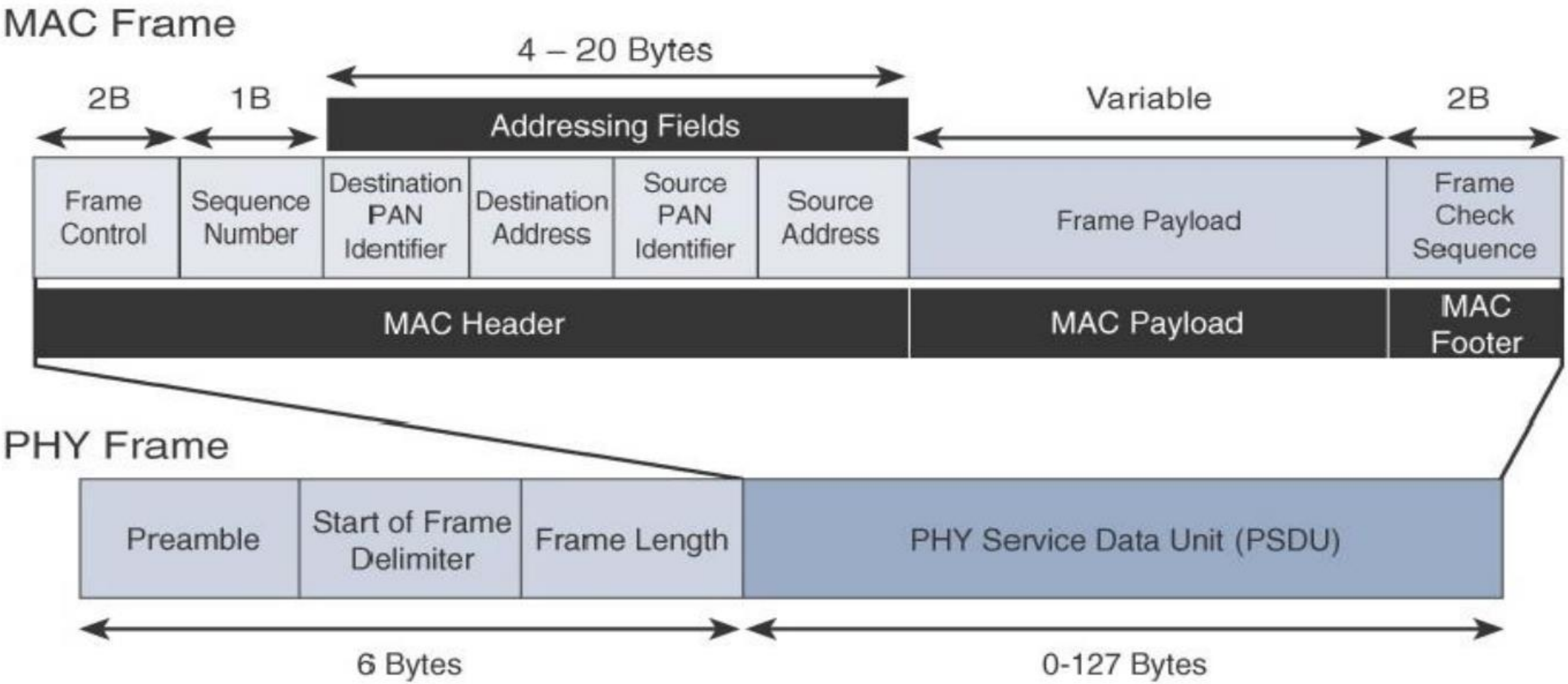


Figure 2.4 IEEE 802.15.4 MAC Format

IEEE 802.15.4g and 802.15.4e

- IEEE 802.15.4g-2012 is also an amendment to the IEEE 802.15.4-2011 standard
- New PHY definitions are introduced, as well as some MAC modifications needed to support their implementation

This technology applies to IoT use cases such as the following:

- Distribution automation and industrialsupervisory 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

Commercial Name/Trademark	Industry Organization	Standards Body
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*

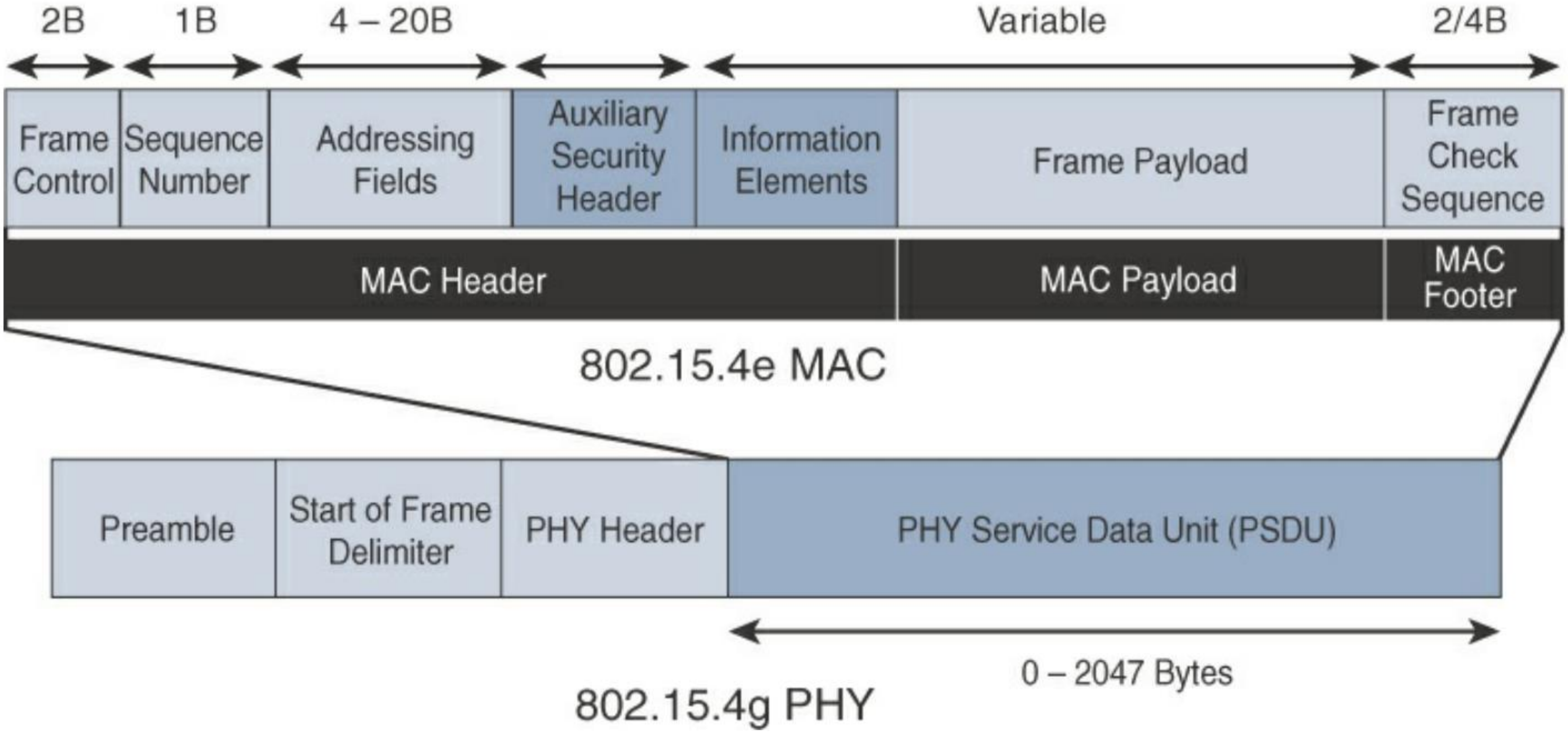
Physical Layer

- **Multi-Rate and Multi-Regional Frequency Shift Keying (MR-FSK):** Offers good transmit power efficiency due to the constant envelope of the transmit signal
- **Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing (MR-OFDM):** Provides higher data rates but may be too complex for low-cost and low-power devices
- **Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying (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

MAC Layer: enhancements to the MAC layer proposed by IEEE 802.15.4e-2012

- Time-Slotted Channel Hopping (TSCH)
- Information elements
  - 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. Some IEs that may be found in EBs include network metrics, frequency hopping broadcast schedule, and PAN information version.

- 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 example, 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.


2B
1B
4 – 20B
Variable
2/4B
Frame Control
Sequence Number
Addressing Fields
Auxiliary Security Header
Information Elements
Frame Payload
Frame Check Sequence
MAC Header
MAC Payload
MAC Footer
802.15.4e MAC
Preamble
Start of Frame Delimiter
PHY Header
PHY Service Data Unit (PSDU)
0 – 2047 Bytes
802.15.4g PHY

Topology

- Mesh
- 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. Considering the use cases addressed by this technology, powered nodes have been the primary targets of implementations. Support for batterypowered nodes with a long lifecycle requires optimized Layer 2 forwarding or Layer 3 routing protocol implementations. This provides an extra level of complexity but is necessary in order to cope with sleeping battery-powered nodes.

security

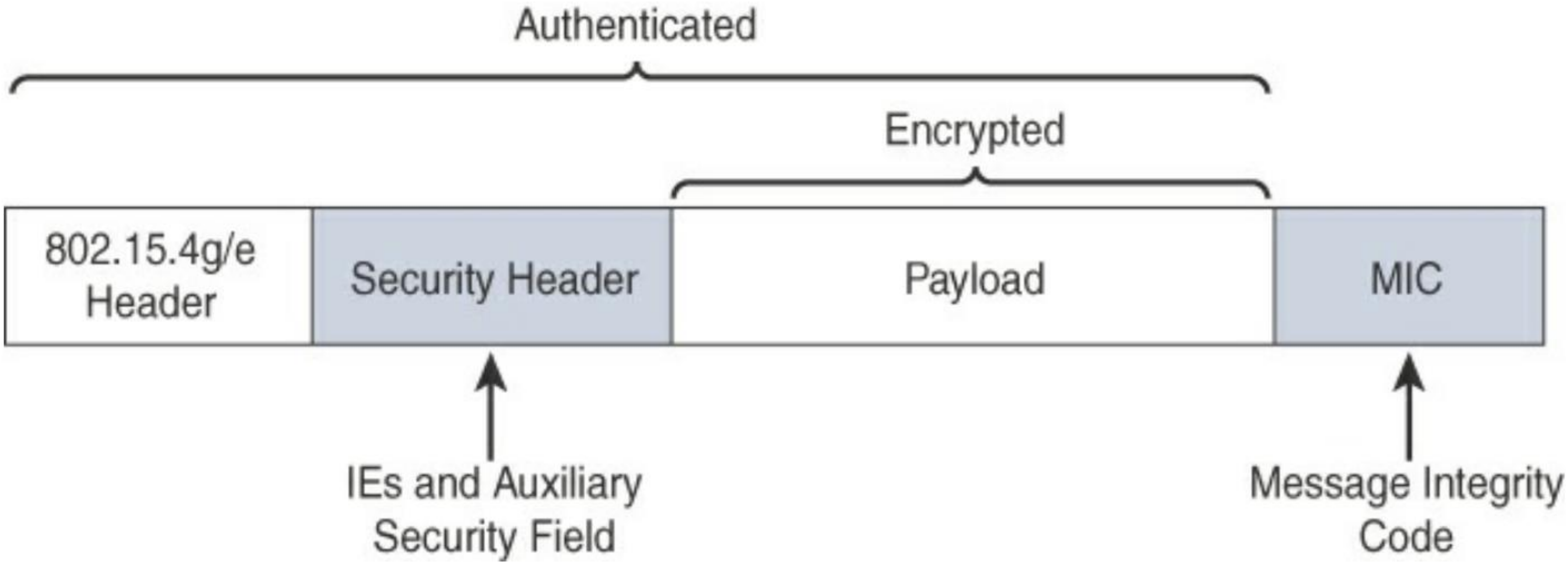


Figure 4-10 *IEEE 802.15.4g/e MAC Layer Security*

IEEE 1901.2a

- 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:** 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.
- **Distribution 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.