MODULE III

IoT Connectivity Technologies

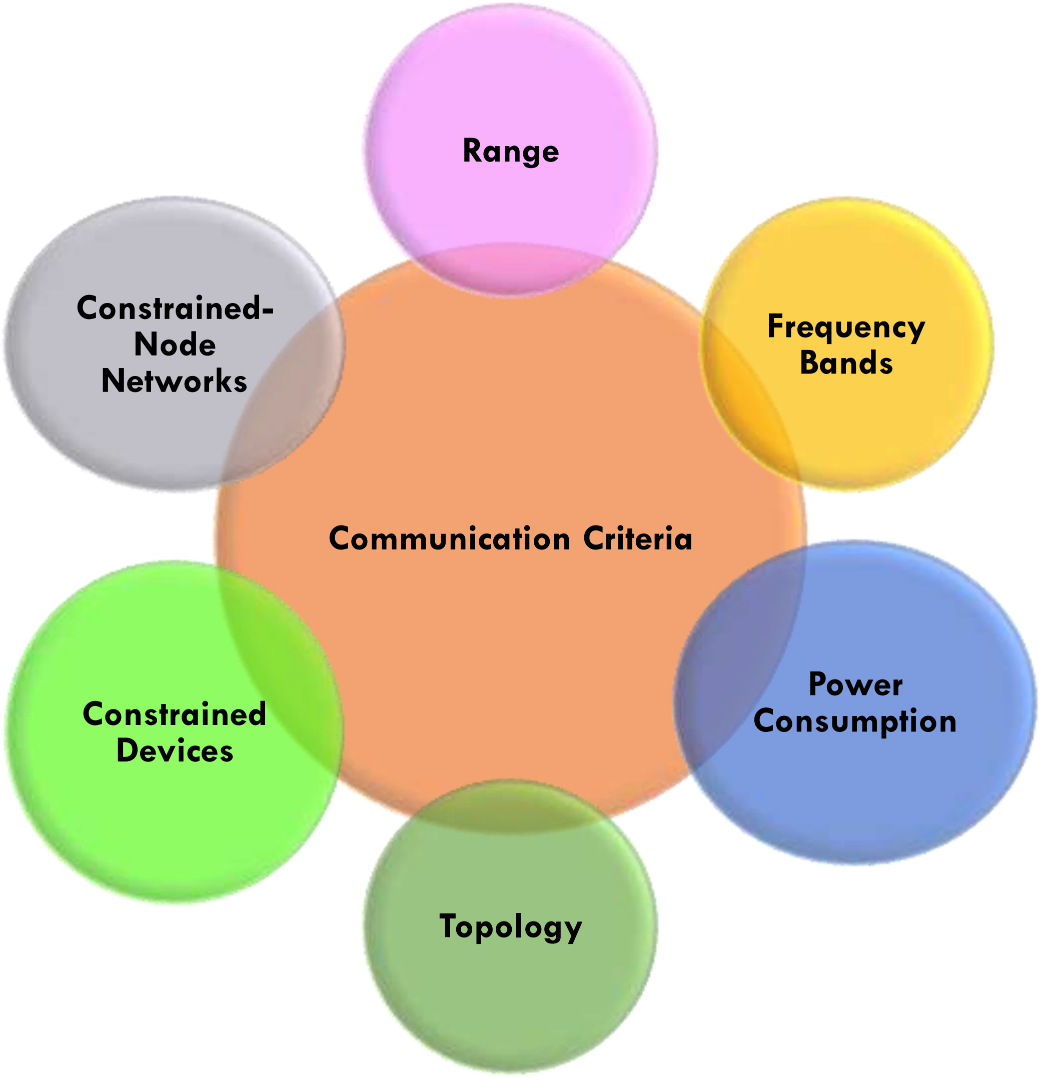
SYLLABUS

Connecting Smart Objects - IoT Access Technologies:

Physical and MAC layers, topology and Security of IEEE

802.15.4, 1901.2a, 802.11ah and LoRaWAN

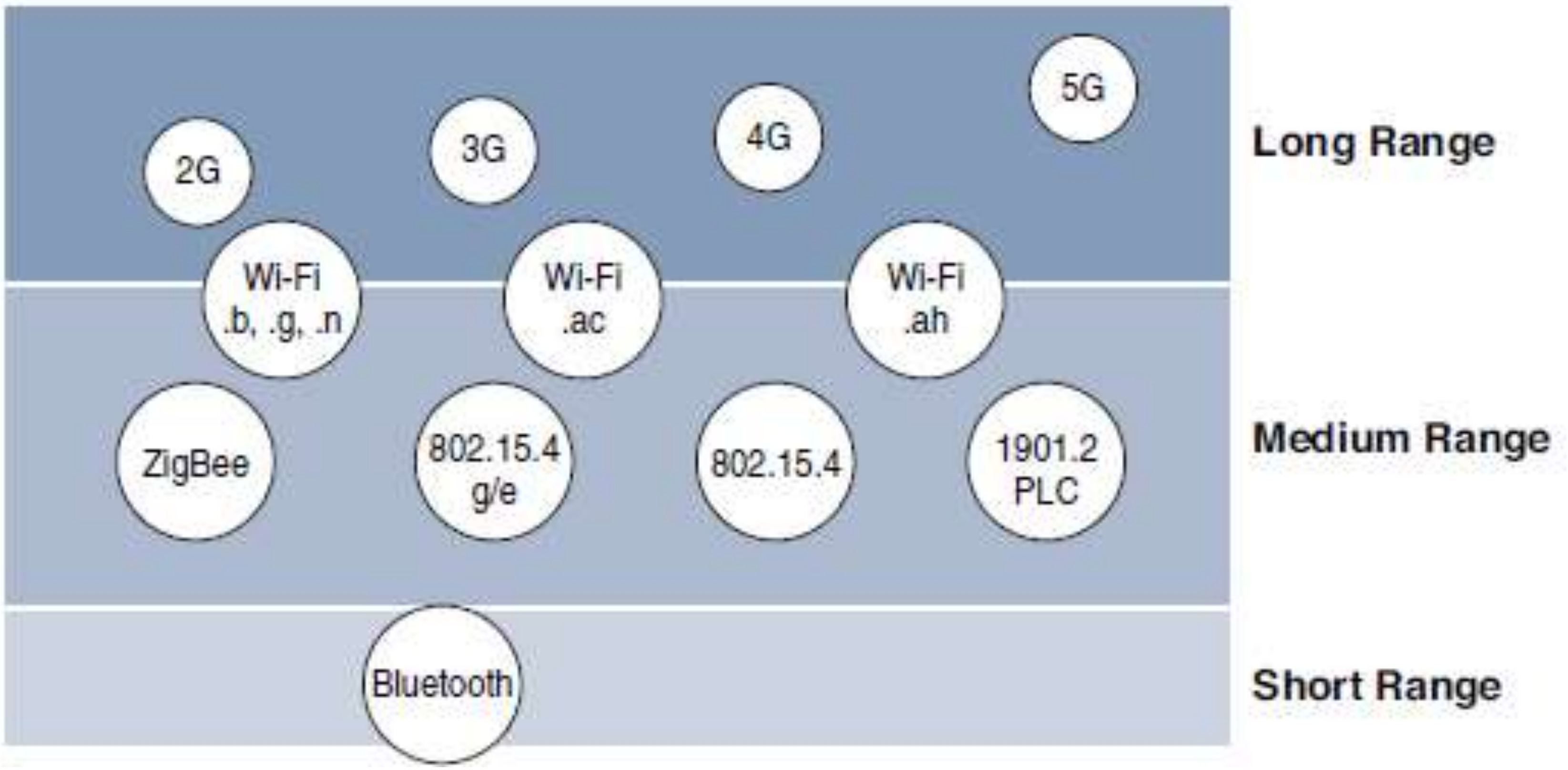
Connecting Smart Objects



IoT Access Technologies

- IEEE 802.15.4 - Smart Objects
- IEEE 802.15.4g - Smart Cities
- IEEE 1901.2a - Smart Objects over power lines
- IEEE 802.11ah – Wi-Fi standards for smart objects
- LoRaWAN
- NB-IoT and other LTE Variations

1. Communication Criteria



Communication Criteria

Short range	Medium range	Long range
Supports: tens of **meters** of maximum distance between two devices	**Supports**: tens to **hundreds** of meters (less than 1 mile between two devices)	**Supports**: Distances greater than 1 **mile** between two devices
Examples: Wireless technologies: • IEEE 802.15.1 (Bluetooth) • IEEE 802.15.7 Visible Light Communications (VLC) Wired technologies: • Serial cable	**Examples**: Wireless technologies: • IEEE 802.11 Wi-Fi, IEEE 802.15.4, 802.15.4g and WPAN Wired technologies: • IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC)	**Examples**: Wireless technologies: • cellular (2G, 3G, 4G), IEEE 802.11 Wi-Fi, Low-Power Wide-Area (LPWA) technologies ideal for IoT devices Wired technologies: • IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications

(b) Frequency Bands

- Radio spectrum is regulated by International Telecommunication Union (ITU) and the Federal Communications Commission (FCC)
- Spectrum – critical resource
- Wireless communication frequency bands - licensed and unlicensed bands
- ITU Licensed spectrum
  - Applicable to IoT long-range access technologies
  - Allocated to communications infrastructures deployed by service providers, public services, broadcasters and utilities
  - Examples: IoT devices access are cellular, WiMAX and Narrowband IoT (NB-IoT) technologies
  - Digital Enhance Cordless Telecommunication (DECT) – No royalty fees

- ITU Unlicensed spectrum
  - Industrial, Scientific and Medical (ISM) portions of radio bands
  - Short range devices (SRD)
  - No guarantee or protection

- Well-known ISM Bands:
    - 2.4 GHz band used by IEEE 802.11B/G/N Wi-Fi
    - IEEE 802.15.1 Bluetooth
    - IEEE 802,15.4 WPAN

- Sub-GHz bands are used by
  - IEEE 802.15.4, 802.15.4g, 802.11ah, LPWA (LoRa and Sigfox)
  - 169 MHz, 433MHz, 868 MHz, 915 MHz
  - CEPT
  - Effective Isotrophic Radiated Power (EIRP)
  - Duty Cycle

c) Power Consumption

- Powered Nodes vs Battery-powered
- LPWA

d) Topology

- Name the topologies learnt before.

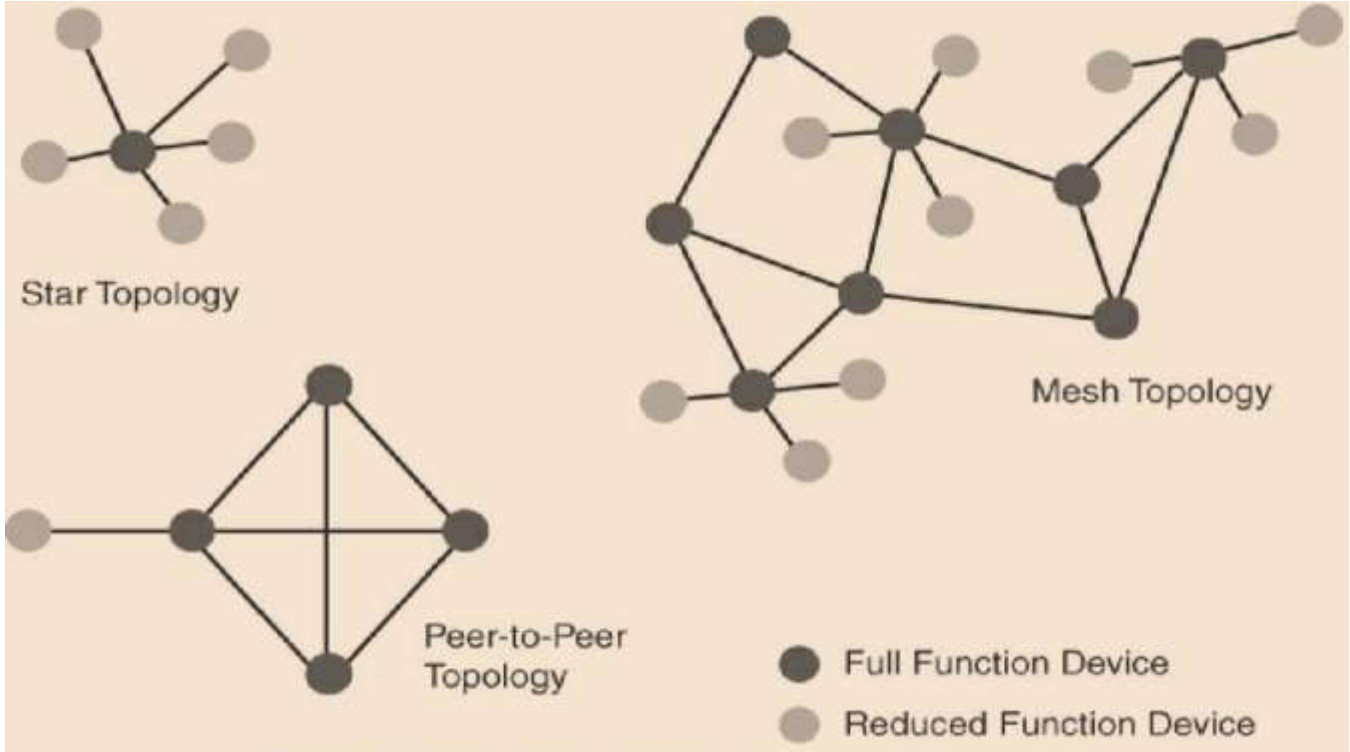


Figure 4-2 Star, Peer-to-Peer, and Mesh Topologies

d) Topology

Star Topology	Peer-to-peer Topology	Mesh topology
Single central base station or controller to allow communications with endpoints	Allow any device to communicate with any other device as long as they are in range of each other	• Helps to cope with low transmit power • Searching to reach a greater overall distance • Coverage by having intermediate nodes relaying traffic for other nodes
Long-range, medium-range and Short-range technologies	Medium-range technologies	Medium-range, Long-range technologies
Example: Cellular, LPWA, indoor Wi-Fi deployments and Bluetooth networks	Rely on multiple full-function devices	Example: outdoor Wi-Fi, IEEE 802.15.4 IEEE 802.15.4g and wired IEEE 1901.2a PLC

Mesh topology :

- Requires the implementation of a forwarding protocol - Layer 2 known as **mesh-under** or a Layer 3 referred to as **mesh-over** on each intermediate node
- Battery-powered nodes in mesh topology
- Sleep-mode
- Either act as **leaf nodes** (or reduced-function device RFD) or as a **“last resource path”** to relay traffic when used as intermediate nodes
- The topology type and the role of the node in the topology are significant factors for a successful implementation

e) Constrained Devices

S.No	Class	Definition
1.	Class 0	• Severely constrained with <10KB of memory, <100 KB of Flash processing and storage capability • Battery-powered • Eg:- Push button that sends 1 byte of information when changing its status • Well suited for new unlicensed LPWA wireless technology
2.	Class 1	• Processing and code space characteristics approximately 10 KB RAM and 100 KB Flash • Cannot easily communicate with nodes employing a full IP stack • Constrained Application Protocol (CoAP) • Provides support for the necessary security functions • Eg:- Environmental sensors
3.	Class 2	• Running full implementations of an IP stack on embedded devices • > 50 KB of memory and 250 KB of Flash • Fully integrated in IP networks • Eg:- Smart power meter

f) Constrained-Node Networks

- Constrained nodes have limited resources - networking feature set and capabilities
- The Internet Engineering Task Force (IETF) acknowledges in RFC (Request for Comments) 7228 that different categories of IoT devices are deployed
- Constrained-node networks are often referred to as Low-power and Lossy Networks (LLNs)
  - Low-power indicate **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
  - Data Rate and Throughput
  - Latency and Determinism
  - Overhead and Payload

f) Constrained-Node Networks

- LPWA networks
  - Designed with a certain number of messages per day or per endpoint

- LLN constrained nodes
  - Send only one message a day, real throughput is often very important for constrained devices implementing an IP stack
  - Throughput is a lower percentage of the data rate

- Two-way communication handling and variable data payload size - reduces the throughput
  - LLNs are able to transport IP such as
    - IEEE 802.15.4 payload size is 127 bytes
    - IPv6 payload size is 1280 bytes
    - IEEE 802.15.4g payload size is 2048 bytes
  - LPWA technologies offer small payload sizes
    - LoRaWAN technology payload size is 19 bytes

Introduction - IoT Access Technology

- Following topics are addressed:
  - **Standardization and alliances**: Standards bodies that maintain the protocols for a technology
  - **Physical layer**: 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

IEEE 802.15.4

- IEEE 802.15.4
  - **low-cost** and **low-data-rate** devices that are powered or run on batteries

- IEEE 802.15.4 commonly found in the following types of deployments:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls

- IEEE 802.15.4 uses Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm - degrades the reliability and cause unbounded latency
- Interference and multipath fading – due to lack of frequency-hopping technique

IEEE 802.15.4 Standardization and Alliances

- Low-data-rate PHY and MAC layer in wireless personal area networks (WPAN)
  - This standard have low-complexity wireless devices with low data rates with good battery life

- IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks
  - ZigBee
  - 6LoWPAN
  - ZigBeeIP
  - ISA100.11a
  - WirelessHART
  - Thread

IEEE 802.15.4 - ZigBee

- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth, interoperate and low power needs
- Sets of Commands and Message types called **clusters**
- ZigBee is the most well-known automation for commercial, retail, smart energy, and home applications

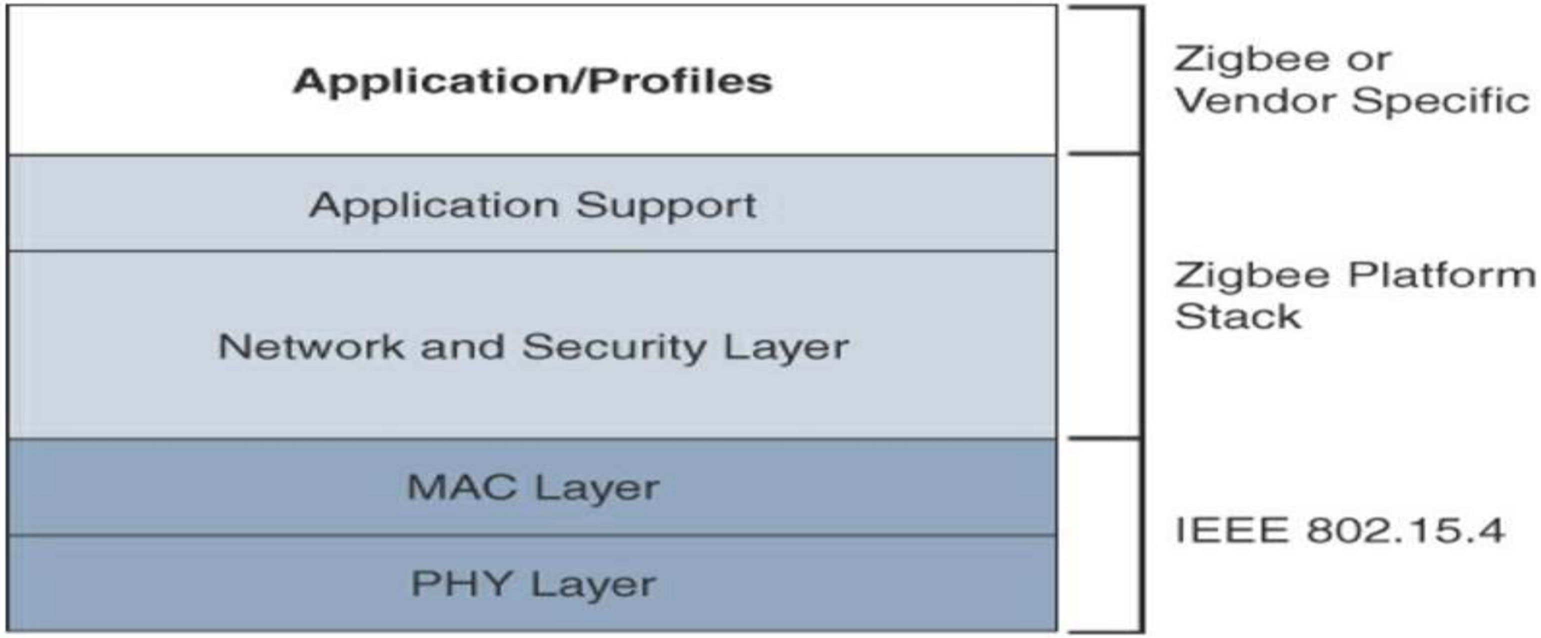


Figure 4-3 High-Level ZigBee Protocol Stack

IEEE 802.15.4 – ZigBee IP

- ZigBee IP
  - IEEE 802.15.4, IP and TCP/UDP protocols and various other open standards are supported at the **network and transport layers**
  - Suitable for low-bandwidth, low-power, and cost-effective communications when connecting smart objects

- ZigBee IP Applications
  - Smart Energy (SE) Profile 2.0
  - Smart metering and residential energy management systems

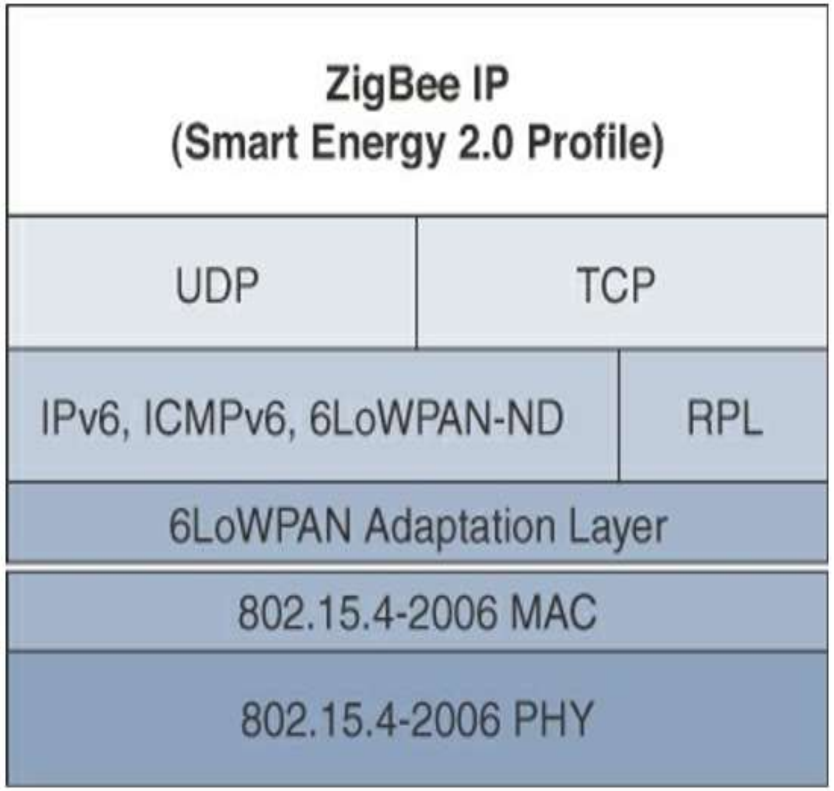


Figure 4-4 ZigBee IP Protocol Stack

IEEE 802.15.4 - Physical Layer

- 802.15.4: Supports an extensive number of PHY options that range from **2.4 GHz to sub-GHz** frequencies in ISM bands based on Direct Sequence Spread Spectrum (DSSS)
  - Modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth

- Original physical layer transmission options
  - <u>**2.4 GHz, 16 channels, with a data rate of 250 kbps**</u>
  - 915 MHz, 10 channels, with a data rate of **40** kbps
  - 868 MHz, 1 channel, with a data rate of **20** kbps

- **PHY communication options :** Offset Quadrature Phase-Shift Keying (OQPSK), Binary Phase-Shift Keying (BPSK) and Amplitude Shift Keying (ASK)

IEEE 802.15.4 - Physical Layer

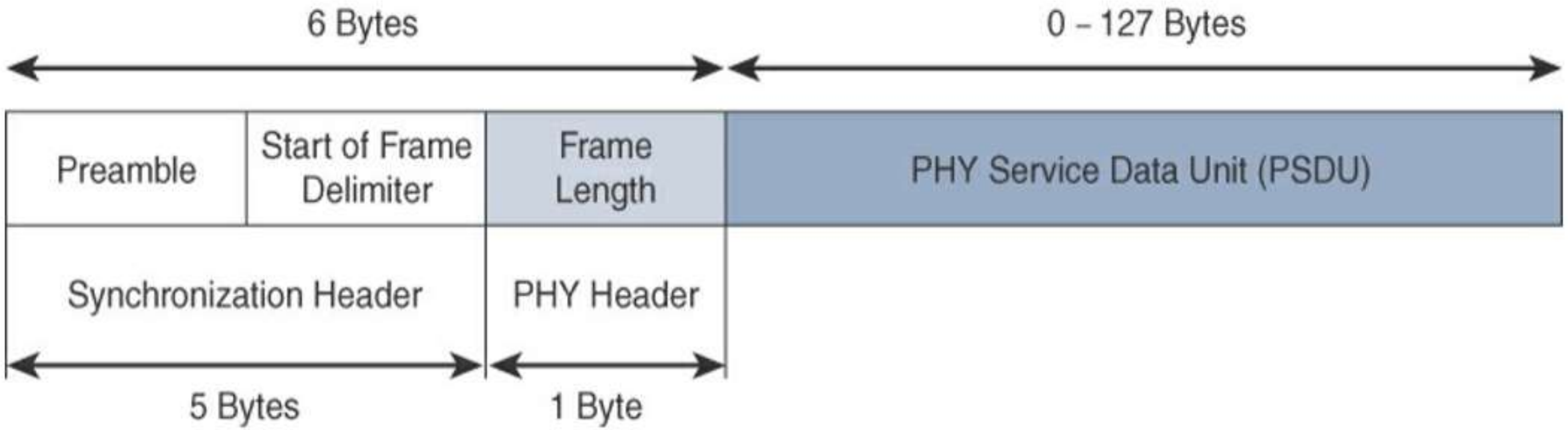


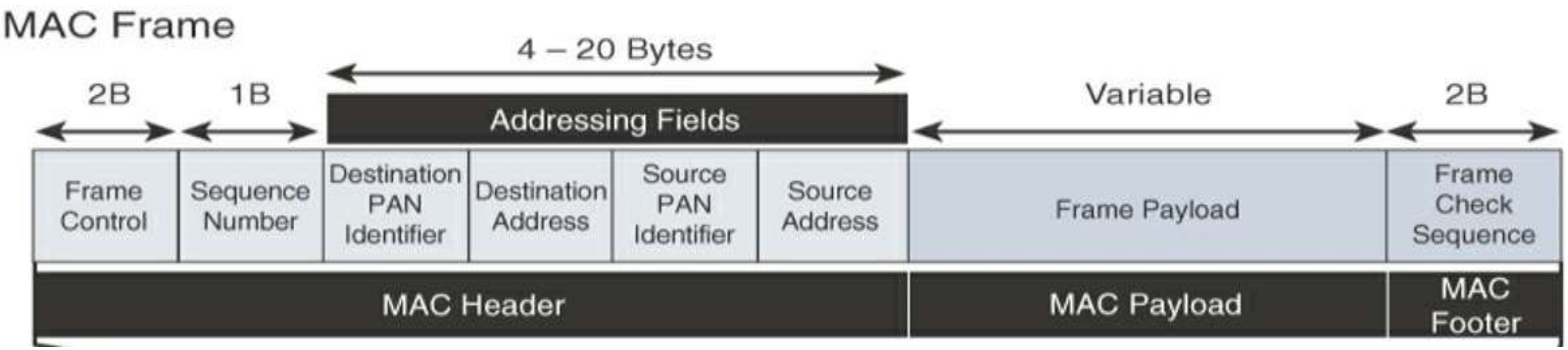
Figure 4-5 IEEE 802.15.4 PHY Format

- **Preamble: 32-bit** or **4-byte** pattern that identifies the start of the frame and is used to synchronize the data transmission
- **Start of Frame Delimiter fields:** Informs the receiver that frame contents start immediately after this byte
- **PSDU (PHY service data unit)** is the data field or payload
    - Maximum size of the PSDU is **127** bytes

IEEE 802.15.4 - MAC Layer

- MAC frames are specified in 802.15.4:
  - **Data frame**: Handles all transfers of data: maximum payload is **127** bytes
  - **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

- The 802.15.4 MAC frame broken down into



IEEE 802.15.4 - MAC Layer

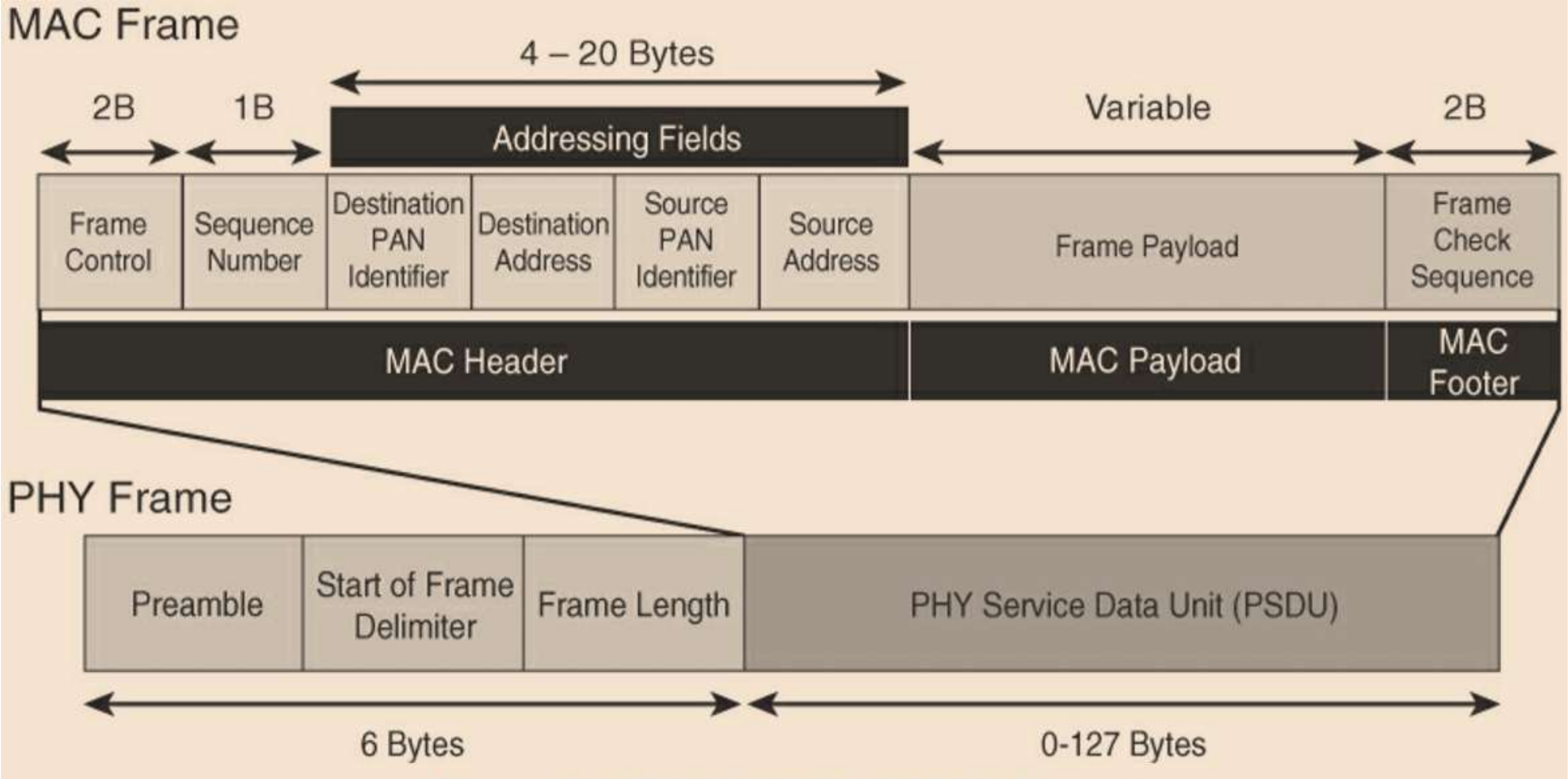


Figure 4-6 IEEE 802.15.4 MAC Format

IEEE 802.15.4 - Topology

- Star, peer-to-peer or mesh topologies
- A minimum of one **FFD** acting as a PAN coordinator, required to deliver services that allow other devices to associate and form a cell or PAN
- 802.15.4 PAN should be set up with a unique ID
  - FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices

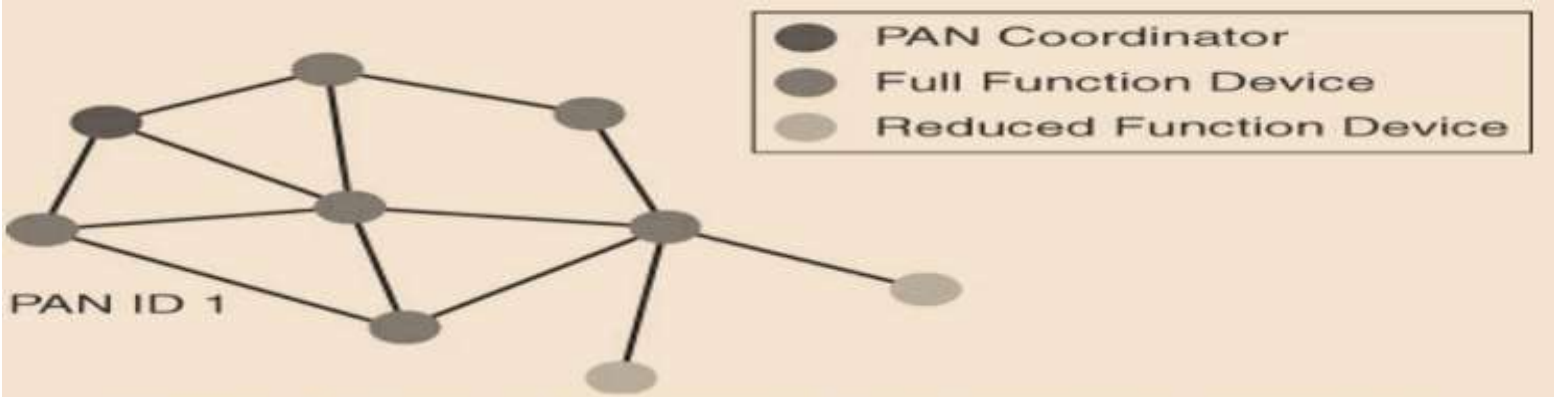


Figure 4-7 802.15.4 Sample Mesh Network Topology

IEEE 802.15.4 - Security

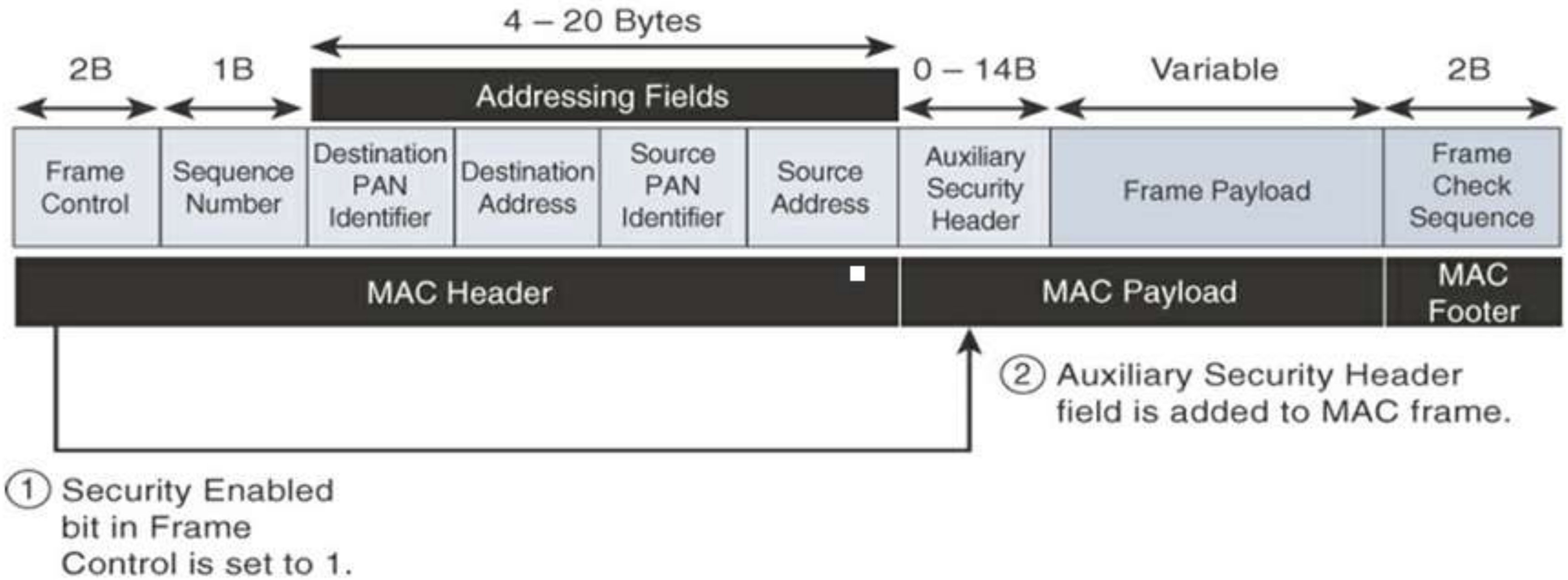


Figure 4-8 Frame Format with the Auxiliary Security Header Field for 802.15.4

- Uses **Advanced Encryption Standard (AES)** with a **128-bit** key length
- Frame Control portion of the header is the first step to enabling AES encryption
  - This field is a single bit that is set to **1** for security

IEEE 802.15.4 - Competitive Technologies

- 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
- Active RFID utilizes radio waves generated by a battery-powered tag on an object to enable continuous tracking
- The current DASH7 technology offers low power consumption, a compact protocol stack, range **up to 1 mile** and **AES** encryption

IEEE 802.15.4g and IEEE 802.15.4e

Optimization in IEEE 802.15.4g and IEEE 802.15.4e

- What are the drawbacks of IEEE 802.15.4?
- IEEE 802.15.4e:
  - ➢ Factory, Process Automation and Smart Grid
- IEEE 802.15.4g:
  - Outdoor wireless mesh networks for FAN

Applications:

1. SCADA
2. Public Lighting
3. Environmental wireless sensors in smart cities
4. Electrical Vehicle Charging Stations
5. Microgrids
6. Smart Parking meters
7. Renewable Energy

STANDARDISATION AND ALLIANCE

What can be the major issue when more amendments arises in standards?

INTEROPERABLILITY – Wi-SUN Alliance Smart Utility Network (SUN Alliance Formed)

Table 4-3 *Industry Alliances for Some Common IEEE Standards*

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

IEEE 802.15.4g - Physical Layer

- What is the maximum payload size of IEEE 802.15.4?
- **It is now increased to 2047 bytes**
- How many bits are used for CRC in IEEE 802.15.4?
- **It is now increased to 32 bits**

Modulation Techniques

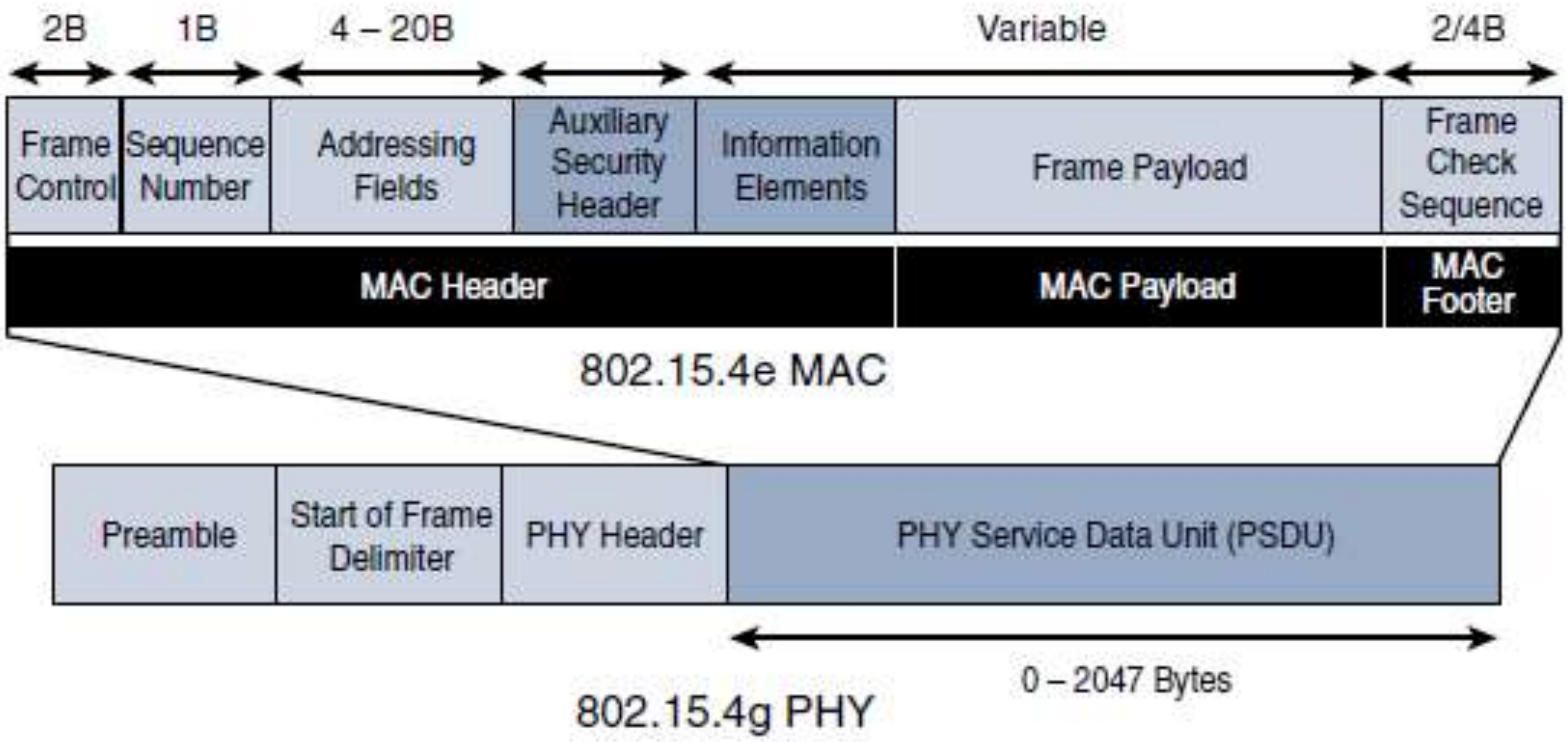
- Supported bandwidth – 169MHz to 2.4GHz
- Multi-Rate Multi-Regional FSK
- Multi-Rate Multi-Regional Orthogonal-FDM
- Multi-Rate Multi-Regional Offset-QPSK

IEEE 802.15.4e - MAC Layer

- Time-Slotted Channel Hopping(TSCH) –time slots
    - Number of time slots – Slot frame
- Industrial Elements

  IE can carry additional metadata to support MAC layer service
- Enhanced Beacons(EB)
    - Construction of application-specific beacon content.
    - Added IE in EB frames
- Enhanced Beacon Request
- Enhanced Acknowledgement

IEEE 802.15.4g/e MAC Frame Format

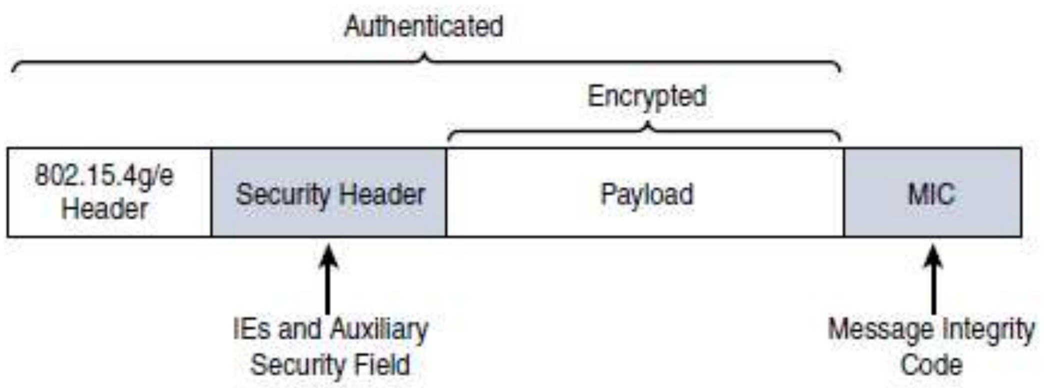


TOPOLOGY

- Mesh Topology is preferred
- Smart Cities, Industrial Applications
- Battery powered nodes needs optimized Layer 2 forwarding or Layer 3 routing protocol
- Necessary to cope up with sleeping-battery powered nodes

Security

- Encryption – AES
- IEEE 802.15.9 Key Management Protocol (KMP)
- Robust Datagram Security



IEEE 1901.2a

- Narrowband Power Line Communication (NB-PLC)
- Low Power, Low Range and Interference over same wires
- Applications
  - Smart metering
  - Distribution automation
  - Public Lighting
  - Electric Vehicle Charging Stations
  - Microgrids
  - Renewable Energy

Standardization and Alliances

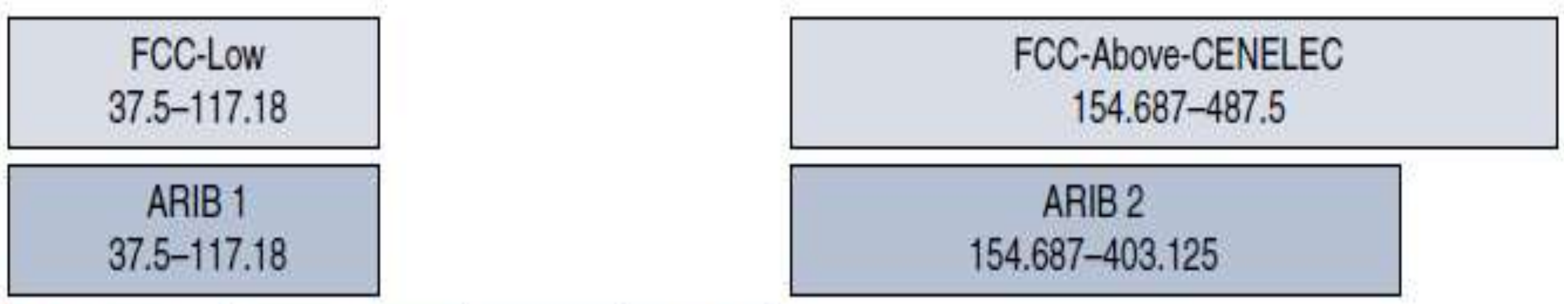
- NB-PLC - Lack of reliability, manageability, interoperability
- OFDM
- Different standards from various vendors compete with one another- fragmented market
- Encodes digital data on multiple carrier frequencies
- Several parallel streams that suffer less from high frequency attenuation in copper wire and narrowband interference

- Worked only for standardizing NB-PLC PHY and MAC layers independently
- Differs from G.9903 and G.9904 that are focused on single use case single metering
- HomePlug Alliance – Technical Specification publicly available

Physical Layer

- CENLEC – European Committee for Electrotechnical Standardisation
- CENLEC A and B bands, FCC-Low and FCC-above CENLEC, Japan ARIB bands.
- CENLEC A and B bands refer 9-95kHz and 95-125kHz
- Modulation:

  ROBO,DBPSK, DQPSK,D8PSK,16QAM
- Throughput depends on how much time coding is repeated
- PHY payload size change dynamically based on channel conditions in MAC Payload



M

3	2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/ 10/14	Variable	Variable	2
Segment Control	Frame Control	Seq. Number	Dest. PAN Identifier	Dest. Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Information Elements	Frame Payload	Frame Check Sequence
MAC Header (MHR)								MAC Protocol Data Unit (MPDU) Payload		MAC Footer (MFR)

- MAC Sublayer Segmentation supports for payload segmentation in PHY Layer
- IE – Key Management Protocol and SSID
- Segment Control – Controls segments of upper layers that are carried in MAC PDU

TOPOLOGY

- Wireless Technologies – noise, interference, distortion and attenuation

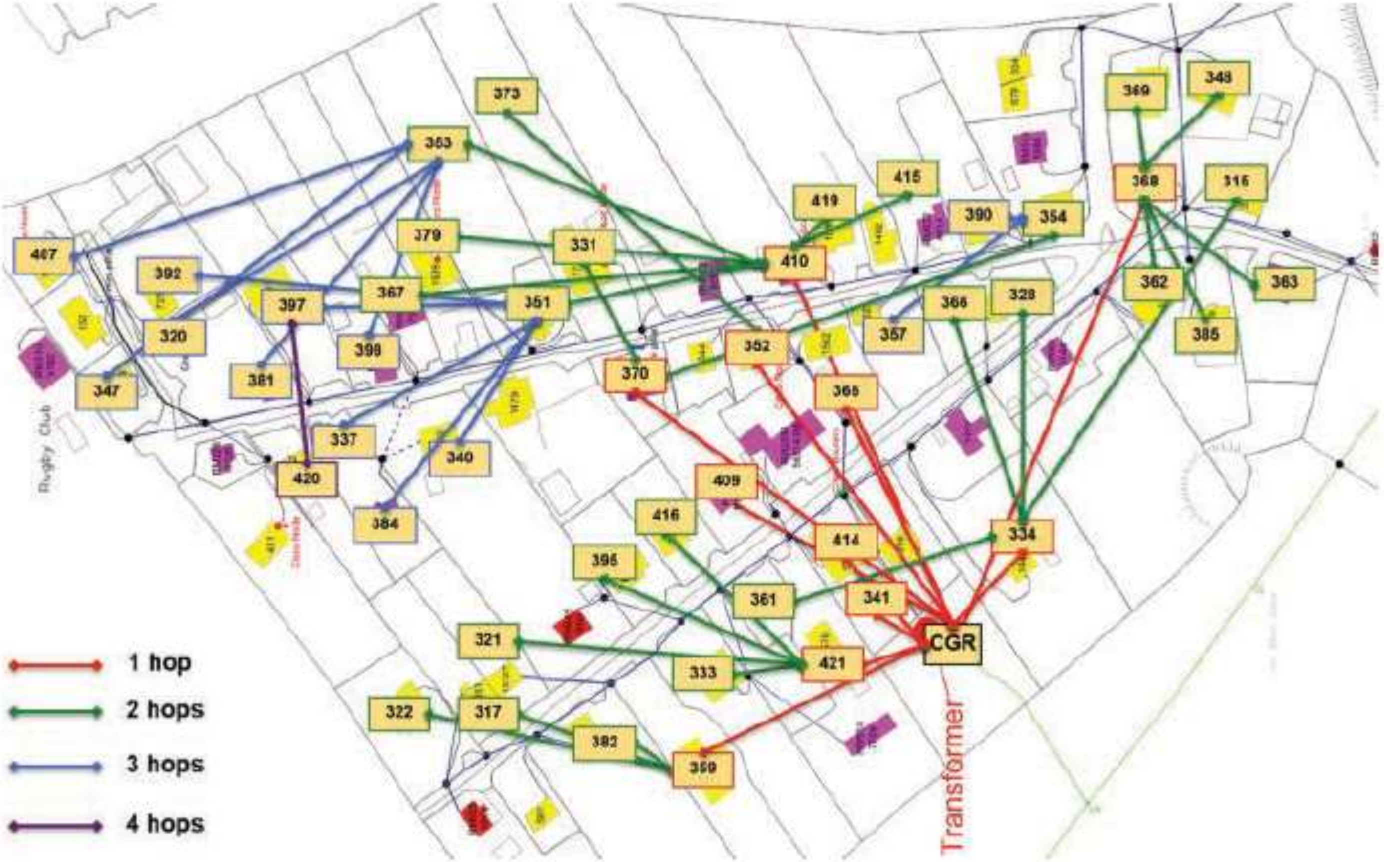


Figure 4-13 *IPv6 Mesh in NB-PLC*

SECURITY

- Security Enabled Bit
- Data Encryption – Packet Segmentation
- Message Integrity Code (MIC) – Non-segmented payload

IEEE 802.11ah

- Unconstrained Network – Wi-Fi (IEEE 802.11)
- Can be able to connect endpoints
- Three main use cases:
  - Sensors and meters covering a smart grid
  - Backhaul aggregation of industrial sensors and meter data
  - Extended Range Wi-Fi

Standardization and Alliances

- July 2010 – IEEE 802.11 decided to work on “Industrial-Wifi”
- Unlicensed sub-GHz
- Wi-Fi Alliance
- Wi-Fi HaLow – Low Power (Hello to Hay-Low)

Physical Layer

- IEEE 802.11 ah:
  - 868 MHz,928 MHz, 316 MHz
- OFDM modulation – IEEE 802.11ah uses channels of 2,4,8 or 16 MHz
- IEEE 802.11ah can cover upto 0.62 mile for outdoor transmission

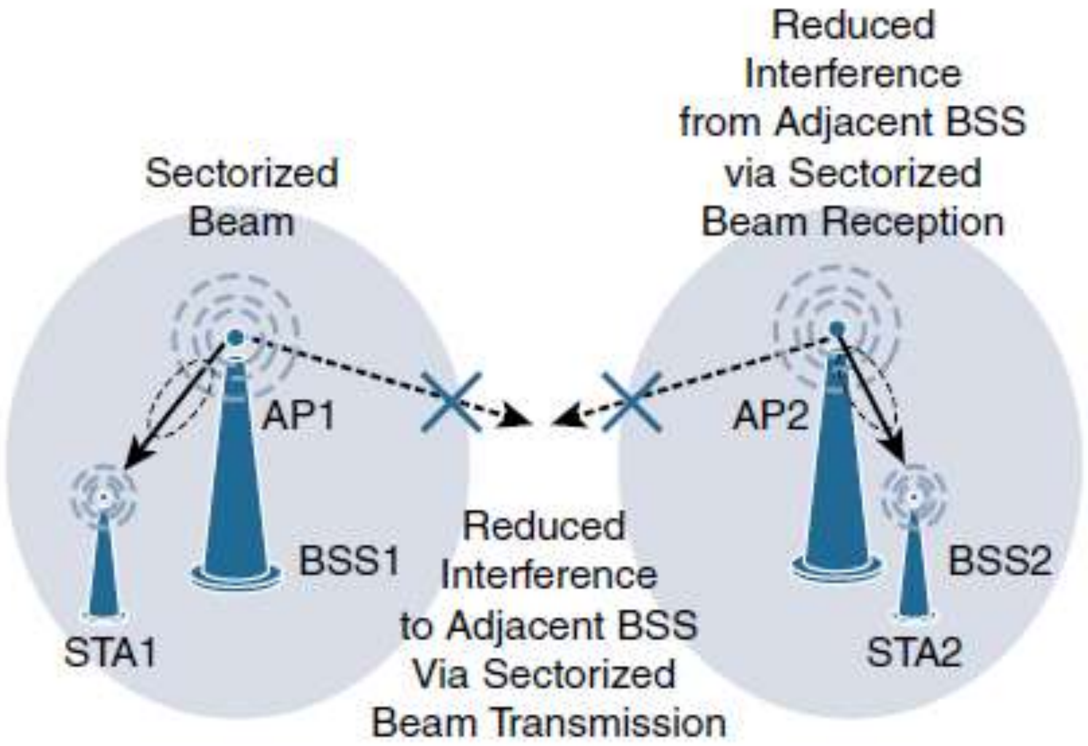
MAC Layer

- Ability to support large number of devices
- Enhanced Features are:
  - Number of Devices – 8192 per access point
  - MAC header – Shortened to allow more efficient communication
  - Null data packet (NDP)
  - Grouping and Sectorization
  - Restricted access window (RAW)
  - Target wake time (TWT)
  - Speed Frame Exchange – TXOP

Topology

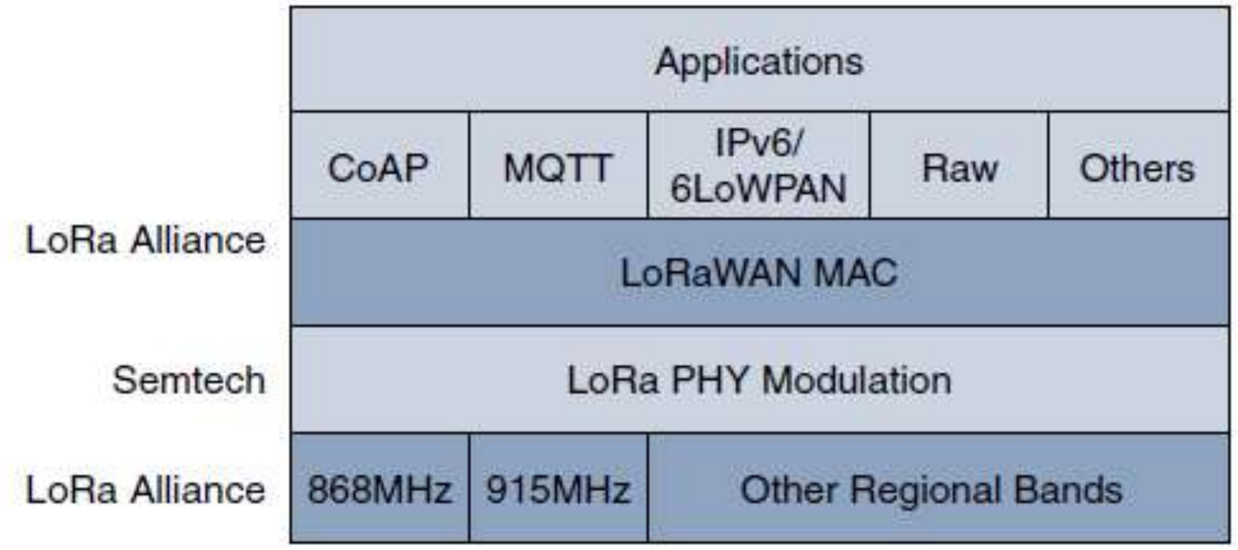
- Star Topology
- Works on two hops
- Relay Function
- Relay Operation – Higher Transmission Rate or Modulation Coding Scheme
- Sectorization – Partitioning the coverage area into several sectors

IEEE 802.11ah Sectorization



LoRaWAN

- LoRaWAN – Unlicensed band LPWA technology
- LoRa- PHY Layer (Layer 1) developed by French Company Cycleo acquired by SemTech
- Long-range and two-way communications - LoRa Alliance Specifications
- To differentiate from Layer 1 PHY modulation– named as LoRaWAN



Physical Layer

- Chirp Spread Spectrum Modulation
- Lower data rate – receiver sensitivity
- Demodulation below noise floor – Robust modulation
- Unlicensed sub-GHz – 433 MHz, 779-787 MHz, 863-870 MHz, 902-928 MHz
- LoRaWAN – LoRa Gateway act as central hub forming star network
- Multiple transceivers – demodulate multiple signals or multiple channels
- Adaptive Data Rate (ADR)
- Spreading Factor

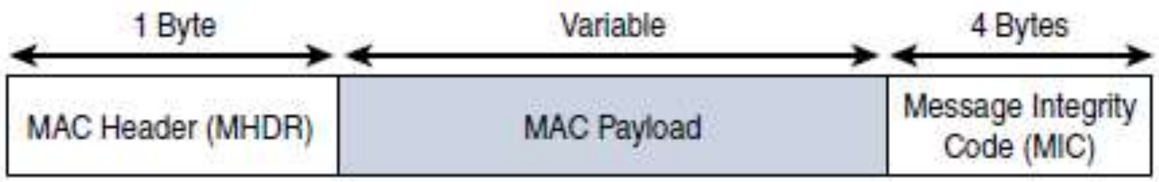
Data Rate vs Spreading Factor

Table 4-4 *LoRaWAN Data Rate Example*

Configuration	863–870 MHz bps	902–928 MHz bps
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

MAC Layer

- Class A – Bidirectional communication
- Class B – Experimental (additional receiver windows)
- Class C – Powered Nodes (continuously open and keep listening)
- Frequency band ranging from 50 to 230 bytes for 860-870 MHz and 19-250 bytes for 902-928 MHz

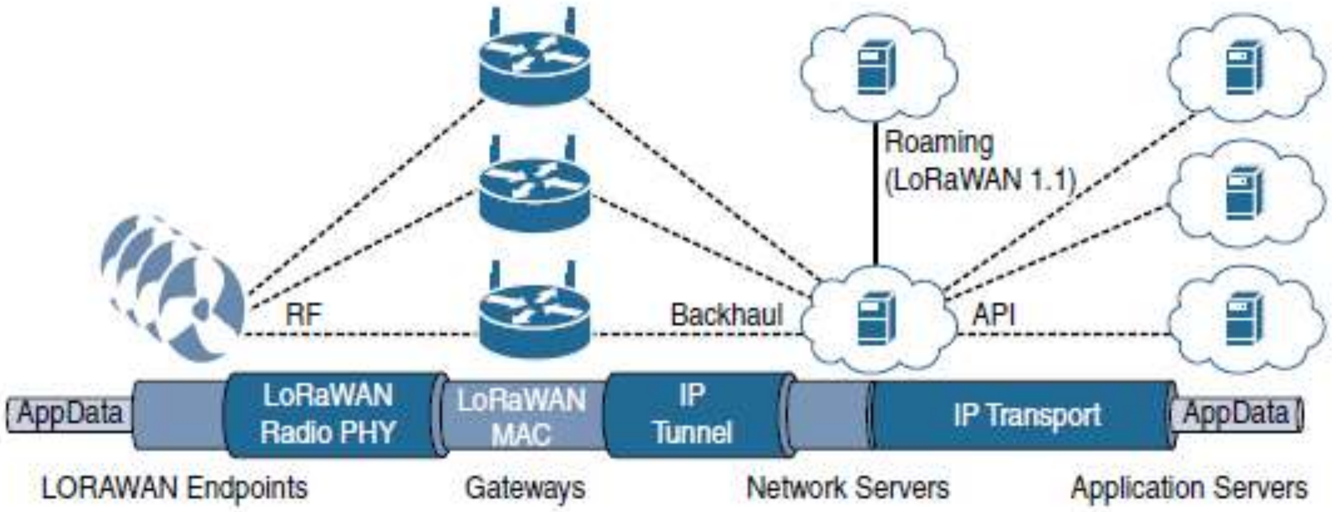


MAC Layer – 6 Type of Messages

- Join Request and Join Accept
- Confirmed and Unconfirmed
- Up and Down messages
- Endpoints – Global End Device ID, Global Application ID
- LoRaWAN – DevAddr, NwkID, NwkAddr

Topology

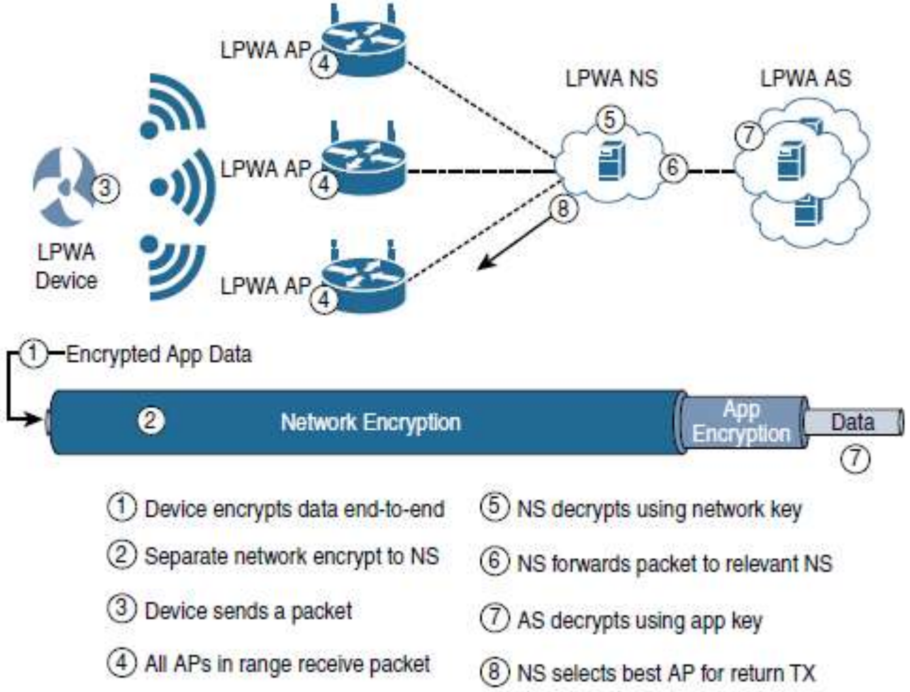
- Star-of-stars topology having gateways acting as bridges, LoRaWAN network server
- ADR – key component for scalability, performance and battery life



Security

- Network Security (NwkSKey) – guarantee the authentication in endpoints, data integrity
- Application session key (AppSKey) – encryption and decryption between endpoints and its application server
- Endpoints – AES Application Key(AppKey)

Security



- Activation by Personalization (ABP)
- Over-the-Air Activation (OTAA)

Competitive Technologies

Table 4-5 *Unlicensed LPWA Technology Comparison*

Characteristic	LoRaWAN	Sigfox	Ingenu Onramp
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