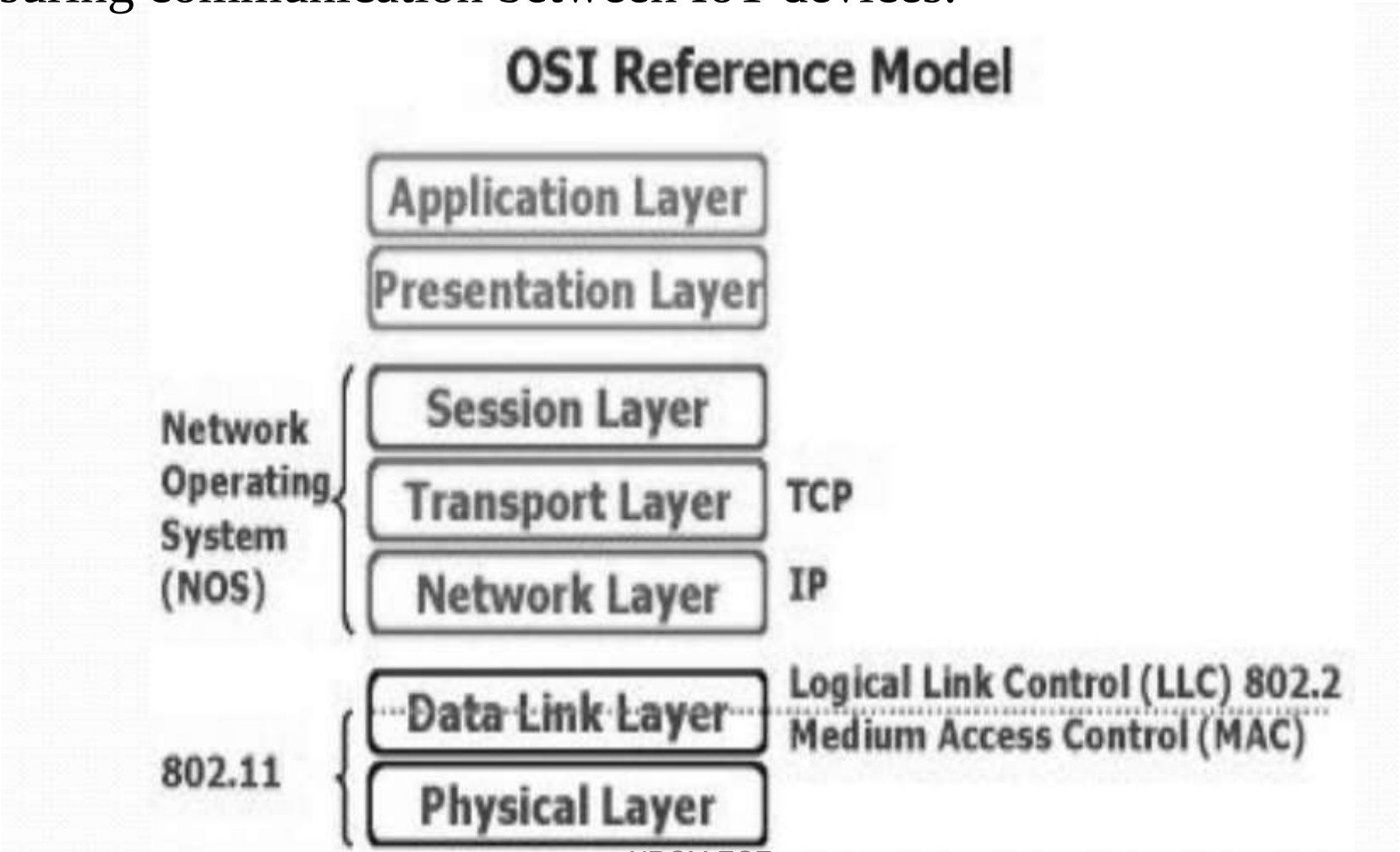
UNIT – III- IOT Data link layer and Network layer protocols:

IoT Data link layer and Network layer protocols: PHY/MAC Layer (3GPP MTC, IEEE 802.11, IEEE 802.15), Wireless HART, Z Wave, Bluetooth Low Energy, Zigbee Smart Energy, DASH7

Network Layer-IPv4, IPv6, 6LoWPAN, 6TiSCH, ND, DHCP, ICMP, RPL, CORPL, CARP

PHY (Physical) and MAC (Medium Access Control)

- In IoT (Internet of Things), the PHY (Physical) and MAC (Medium Access Control) layers are part of the OSI model's Data Link Layer (Layer 2), and they play crucial roles in ensuring communication between IoT devices.



1-Physical Layer (PHY) :

- 1. The **PHY layer** is responsible for the **transmission and reception of raw data** over a physical medium (such as wireless radio waves, cables, or optical fibers).
- It defines the hardware requirements and handles the following:
- • **Modulation and demodulation** of signals
- • **Data encoding** (converting digital data into signals)
- • **Frequency selection** and **channel allocation**
- • **Signal strength** and **power control**
- • **Data rate** and **transmission speeds**

Different PHY layer standards:

For IoT, different PHY layer standards may be used depending on the type of network, such as:

- Wi-Fi (IEEE 802.11 series)
- Bluetooth (IEEE 802.15.1)
- Zigbee (IEEE 802.15.4)
- LoRa (Low Power Wide Area Network)
- NB-IoT (Narrowband IoT, a cellular technology)
- LTE/5G (for mobile communication)

2-Medium Access Control Layer (MAC) :

- The MAC layer manages how devices access the network and use the communication medium. It controls data transfer between devices and ensures efficient, collision-free communication.
- The key responsibilities of the MAC layer include:
- **Framing:** Encapsulating data into frames and addressing the information for proper delivery
- **Addressing:** Assigning unique MAC addresses to devices for communication
- **Error detection and retransmission:** Detecting errors and ensuring reliable communication
- **Medium access control:** Determining when a device can transmit data (avoiding collisions in shared media)

- **QoS (Quality of Service):** Prioritizing data traffic if necessary (e.g., ensuring real-time communication for critical IoT tasks)
- **Energy management:** For low-power IoT devices, MAC protocols often manage sleep cycles and energy-efficient transmission strategies
- IoT uses a variety of MAC protocols optimized for different types of communication. These include:
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): Used in Wi-Fi, Zigbee, and others to avoid data collisions.
- TDMA (Time Division Multiple Access): Used in low-power networks, splitting the communication into time slots.
- ALOHA-based protocols: For simple, low-overhead communication in some LPWANs (Low Power Wide Area Networks).

3GPP MTC:

- 3GPP MTC (Machine-Type Communications) refers to a set of standards and technologies developed by the 3rd Generation Partnership Project (3GPP) to support machine-to-machine (M2M) communication, which is a key component of the Internet of Things (IoT).
- These technologies are designed to enable low-power, cost effective communication for a large number of connected devices, such as sensors, meters, and other IoT devices.

Here are some key aspects of 3GPP MTC in IoT:

- **Low-Power and Low-Complexity Devices:** 3GPP MTC focuses on enabling communication for low-power and low-complexity IoT devices. These devices typically have limited processing capabilities, memory, and power supply, requiring communication technologies that are optimized for efficiency and resource conservation.
- **Coverage Enhancement:** 3GPP MTC technologies, such as LTE-M (LTE for MTC), eMTC (enhanced Machine Type Communication), and NB-IoT (Narrowband IoT), offer coverage enhancements to ensure reliable connectivity in challenging environments. These technologies provide extended coverage range, improved signal penetration through buildings and underground areas, and better performance in remote or rural areas.

Here are some key aspects of 3GPP MTC in IoT:

- **Quality of Service (QoS):** 3GPP MTC supports differentiated QoS for different types of IoT applications. It provides mechanisms to prioritize critical data traffic and ensure reliable transmission for mission-critical applications. QoS parameters can be adjusted to meet the specific requirements of diverse IoT use cases.
- **Security and Authentication:** 3GPP MTC includes robust security mechanisms to protect IoT device communications. It utilizes encryption, authentication, and access control measures to ensure the confidentiality and integrity of data transmitted over the cellular network.
- **Integration with IoT Platforms:** 3GPP MTC technologies are designed to seamlessly integrate with IoT platforms and cloud services. They provide standardized protocols and interfaces for data exchange, device management, and integration with higher-level IoT systems.

Here are some key aspects of 3GPP MTC in IoT:

- **Power Efficiency:** Power consumption is a critical concern for IoT devices, many of which operate on battery power. 3GPP MTC introduces power-saving features such as extended discontinuous reception (eDRX) and power saving mode (PSM) to minimize energy consumption. These mechanisms allow IoT devices to enter sleep modes for extended periods while still maintaining network connectivity.
- **Optimized Data Rates:** 3GPP MTC technologies provide optimized data rates suitable for IoT applications. While they may not offer the high data throughput of traditional cellular networks, they provide sufficient bandwidth for transmitting small amounts of data, periodic sensor readings, and control messages required by IoT devices.

Key Technologies in 3GPP MTC

1.eMTC (Enhanced Machine-Type Communication)

1. eMTC, also known as LTE Cat-M1, is a 3GPP standard developed as part of the LTE-Advanced Pro to meet the specific needs of IoT devices.
2. It supports low power consumption, extended coverage, and reduced complexity for devices, while operating on existing LTE networks.

Key Technologies in 3GPP MTC

1.eMTC (Enhanced Machine-Type Communication)

3. Key features of eMTC:

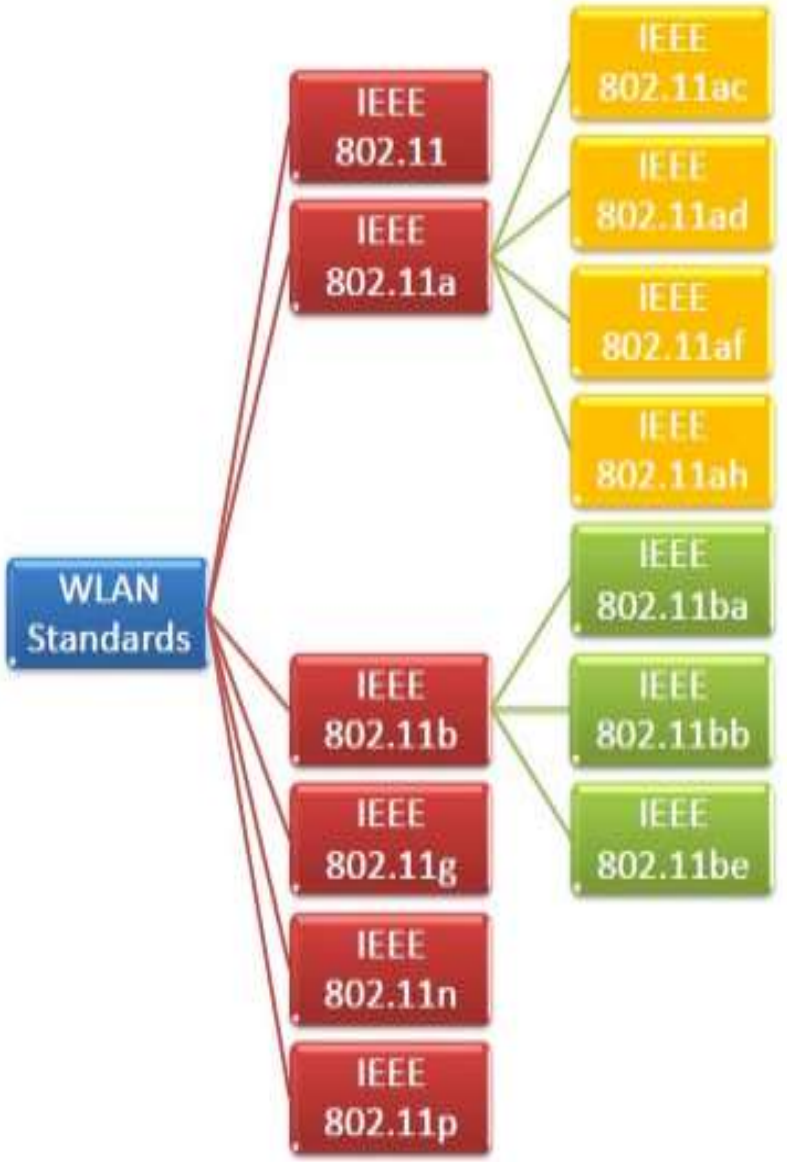
1. **Low-power consumption:** Optimized for battery-operated devices with features like Power Saving Mode (PSM) and Extended Discontinuous Reception (eDRX).
2. **Low data rates:** eMTC supports data rates of up to 1 Mbps, suitable for many IoT applications like wearables and sensors.
3. **Extended coverage:** eMTC is designed for reliable operation in difficult environments, such as deep indoor locations, with coverage extension techniques.
4. **Mobility support:** Unlike NB-IoT, eMTC supports full mobility, making it suitable for applications such as asset tracking or wearable devices.

- 1. **NB-IoT (Narrowband IoT)**
  1. NB-IoT is another 3GPP technology specifically designed for low-power, wide-area (LPWA) IoT applications.
  2. It operates in a narrowband spectrum (180 kHz) and offers excellent coverage and energy efficiency, making it suitable for applications like smart metering, environmental monitoring, and industrial IoT.
- **2. Power Saving Mode (PSM) and eDRX (Extended Discontinuous Reception)**
  1. Both eMTC and NB-IoT support these power-saving mechanisms to extend battery life, which is crucial for IoT devices that need to operate for years without human intervention.
     1. **Power Saving Mode (PSM):** Allows devices to sleep for long periods without needing to re-establish the network connection after waking up.
     2. **Extended Discontinuous Reception (eDRX):** Allows devices to remain in a low-power state between communications, checking in with the network only at scheduled intervals.

- **3. LTE Cat-0 and LTE Cat-1**

  1. These are earlier 3GPP categories designed for IoT, with LTE Cat-1 offering modest power and complexity reductions compared to traditional LTE. LTE Cat-0 was introduced to simplify device design further but is less widely adopted than eMTC and NB-IoT.

- **IEEE 802.11 STANDARDS:**
  - IEEE 802.11 standard, popularly known as Wi-Fi, lays down the architecture and specifications of wireless LANs (WLANs). Wi-Fi or WLAN uses high frequency radio waves for connecting the nodes.
  - There are several standards of IEEE 802.11 WLANs. The prominent among them are 802.11, 802.11a, 802.11b, 802.11g, 802.11n and 802.11p.
  - All the standards use carrier-sense multiple access with collision avoidance (CSMA/CA). Also, they have support for both centralized base station based as well as ad hoc networks.



- **IEEE 802.11**
- IEEE 802.11 was the original version released in 1997. It provided 2 Mbps data rate in the 2.4 GHz band and used either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS). It is obsolete now.
- **IEEE 802.11a**
- 802.11a was published in 1999 as a modification to 802.11, with orthogonal frequency division multiplexing (OFDM) based air interface in physical layer instead of FHSS or DSSS of 802.11. It provides a maximum data rate of 54 Mbps operating in the 5 GHz band. Besides it provides error correcting code. As 2.4 GHz band is crowded, relatively sparsely used 5 GHz imparts additional advantage to 802.11a.
- Further amendments to 802.11a are 802.11ac, 802.11ad, 802.11af, 802.11ah, 802.11ai, 802.11aj etc.

- **IEEE 802.11b**
- 802.11b is a direct extension of the original 802.11 standard that appeared in early 2000. It uses the same modulation technique as 802.11, i.e. DSSS and operates in the 2.4 GHz band. It has a higher data rate of 11 Mbps as compared to 2 Mbps of 802.11, due to which it was rapidly adopted in wireless LANs. However, since 2.4 GHz band is pretty crowded, 802.11b devices faces interference from other devices.
- Further amendments to 802.11b are 802.11ba, 802.11bb, 802.11bc, 802.11bd and 802.11be.
- **IEEE 802.11g**
- 802.11g was indorsed in 2003. It operates in the 2.4 GHz band (as in 802.11b) and provides a average throughput of 22 Mbps. It uses OFDM technique (as in 802.11a). It is fully backward compatible with 802.11b. 802.11g devices also faces interference from other devices operating in 2.4 GHz band

- **IEEE 802.11n**
- 802.11n was approved and published in 2009 that operates on both the 2.4 GHz and the 5 GHz bands. It has variable data rate ranging from 54 Mbps to 600 Mbps. It provides a marked improvement over previous standards 802.11 by incorporating multiple-input multiple-output antennas (MIMO antennas).
- **IEEE 802.11p**
- 802.11 is an amendment for including wireless access in vehicular environments (WAVE) to support Intelligent Transportation Systems (ITS). They include network communications between vehicles moving at high speed and the environment. They have a data rate of 27 Mbps and operate in 5.9 GHz band.

- **IEEE 802.11 protocol architecture:**

1) **Stations (STA)** − Stations comprise all devices and equipment that are connected to the wireless LAN. A station can be of two types:

   Wireless Access Points (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.

   Client. − Clients are workstations, computers, laptops, printers, smart phones, etc. Each station has a wireless network interface controller.

2) **Basic Service Set (BSS)** −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:

   Infrastructure BSS − Here, the devices communicate with other devices through access points.

   Independent BSS − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.

3) **Extended Service Set (ESS)** − It is a set of all connected BSS.

4) **Distribution System (DS)** − It connects access points in ESS.

• IEEE 802.11 protocol architecture:

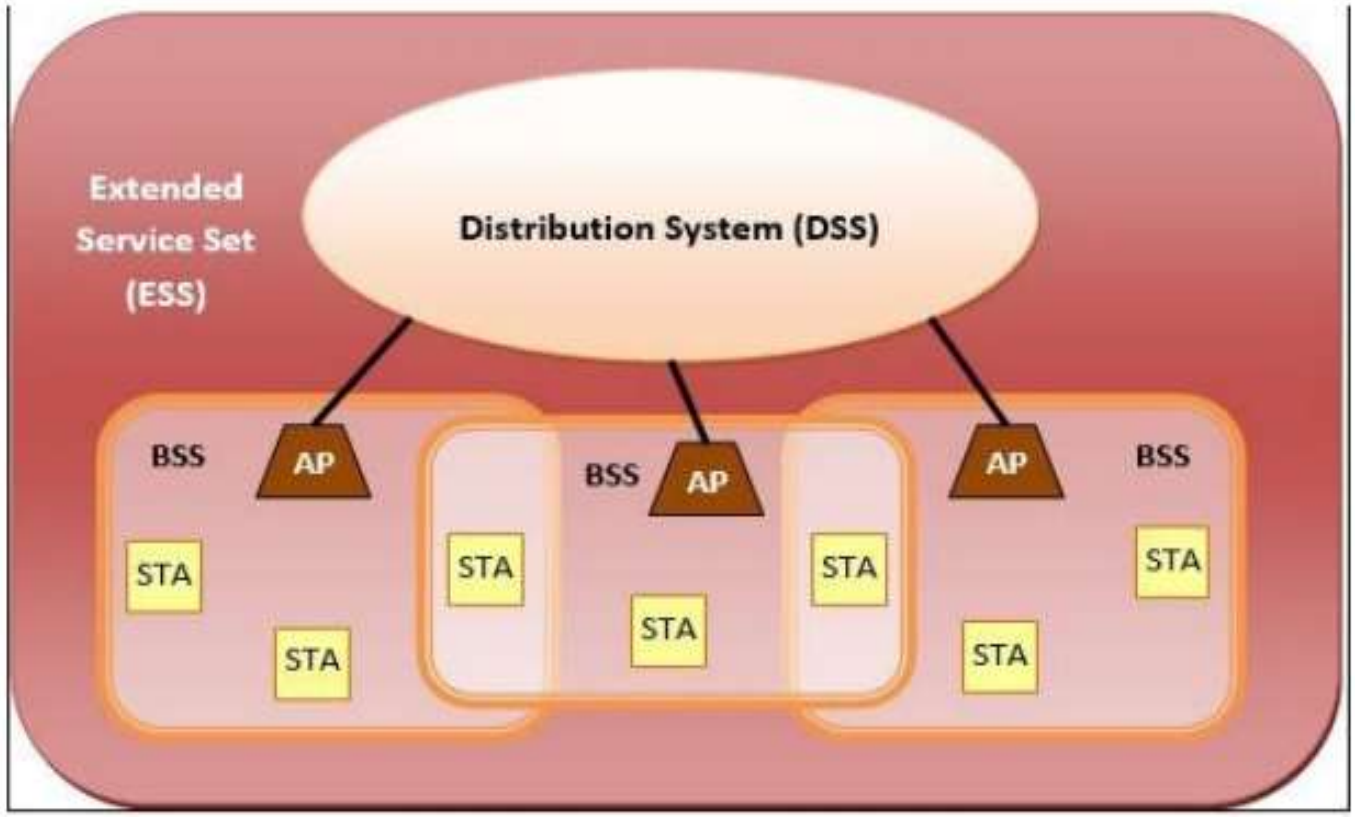
The technique used for this purpose is known as scanning, which involves the following steps:

• A station sends a probe frame.

• All APs within reach reply with a probe response frame.

• The station selects one of the access points, and sends the AP an Association Request frame.

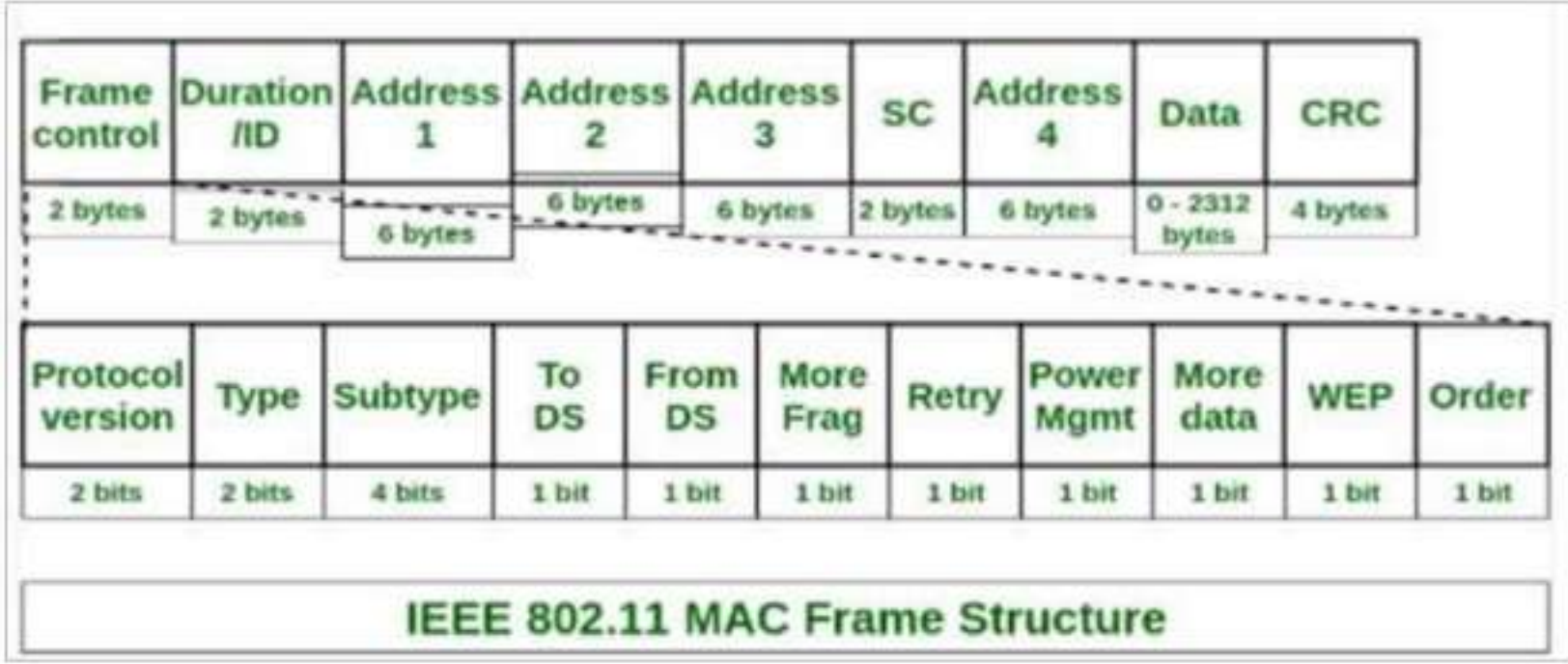
• The AP replies with an Association Response frame.



- Frame Format of IEEE 802.11:

- The main fields of a frame of wireless LANs as laid down by IEEE 802.11 are
- **Frame Control** − It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.
- **Duration** − It is a 2-byte field that specifies the time period for which the frame and its acknowledgment occupy the channel.
- **Address fields** − There are four 6-byte address fields containing addresses of source, immediate destination, and final endpoint respectively.
- **Sequence** − It a 2 bytes field that stores the frame numbers.
- **Data** − This is a variable-sized field that carries the data from the upper layers. The maximum size of the data field is 2312 bytes.
- **Check Sequence** − It is a 4-byte field containing error detection information.

- Frame Format of IEEE 802.11:



- **Frame Control(FC)** – It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:
- 1. **Version:** It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
- 2. **Type:** It is a 2 bit long field which determines the function of frame i.e management (00), control (01) or data (10). The value 11 is reserved.

- Frame Format of IEEE 802.11:

- 3. **Subtype:** It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
- 4. **To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
- 5. **From DS:** It is a 1 bit long field which when set indicates frame coming from DS.
- 6. **More frag (More fragments):** It is 1 bit long field which when set to 1 means frame is followed by other fragments.
- 7. **Retry:** It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
- 8. **Power Mgmt (Power management):** It is 1-bit long field that indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.

- Frame Format of IEEE 802.11**:**

- 9. **More data:** It is 1-bit long field that is used to indicate receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
- 10. **WEP (Wired Equivalent Privacy):** It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
- 11. **Order:** It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

- **IEEE 802.15 Standards :**

- IEEE 802.15 is a standard for wireless personal area networks (WPANs) developed by the Institute of Electrical and Electronics Engineers (IEEE). It defines the physical layer (PHY) and medium access control (MAC) layer specifications for short-range wireless communication.

- **IEEE 802.15.1 (Bluetooth):** This task group defines the specifications for Bluetooth wireless technology, which enables **short-range communication** between devices such as mobile phones, laptops, and peripherals.

- **IEEE 802.15.4:** This task group specifies the PHY and MAC layers for **low-rate wireless personal area networks (LR-WPANs)**. It is commonly used in applications like **home automation, industrial control, and wireless sensor networks**. The most well-known standard built on IEEE 802.15.4 is **Zigbee**.

- IEEE 802.15 Standards: **:**

- IEEE 802.15.3: This task group focuses on **high-rate wireless personal area networks (HR-WPANs).** It defines the PHY and MAC layers for applications that require higher data rates, such as **streaming multimedia**.

- IEEE 802.15.6: This task group concentrates on **wireless body area networks (WBANs).** It addresses the specific requirements of medical, healthcare, and fitness applications by defining the PHY and MAC layers suitable for wearable and implantable devices.

- IEEE 802.15.7: This task group defines the PHY and MAC layers for **visible light communication (VLC).** It enables communication using **light-emitting diodes (LEDs)** and is often used for indoor positioning, smart lighting, and other applications.

- **IEEE 802.15.4** (ZigBee)**:**

- IEEE 802.15.4 is a **subgroup** of features that refers to physical and medium access control layers that can support **ZigBee and 6LoWPAN**.
- IEEE 802.15.4 focuses on **physical and data link layer specification**.
- Defines PHY and MAC layers for personal area networks that demand **low rate and low cost applications**.
- This is also called a **LR-WPAN** (Low Rate Wireless Personal Area Network) Protocols.
- It has Following advantages:
  - -Simple and Flexible Protocol stack.
  - -Low cost
  - -Low energy consumption
  - -Short range operation
  - -reliable data transfer
  - -ease of operation

- **IEEE 802.15.4 :**

- These features are more important when operating in the personal operating space (POS) also defined as Personal Area Network (PAN) that involves the human body.

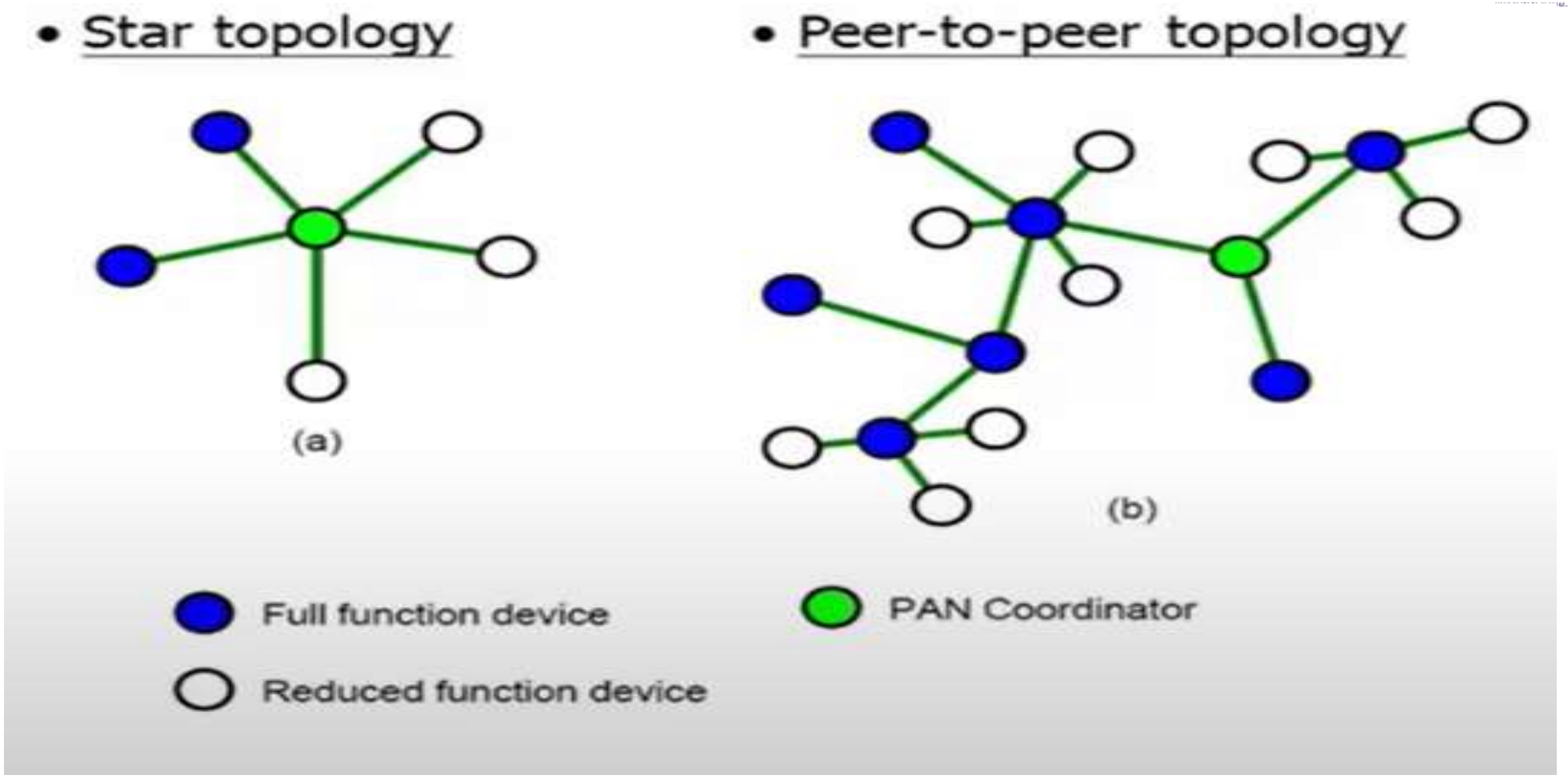
- An IEEE 802.15.4 device **address** can be a short **16-bit or 64-bit address**.

- In addition , IEEE802.15.4 uses a **Direct Sequence Spread Spectrum(DSSS)** access method and operates on **2450 MHZ**, **915 MHZ**, and **868 MHZ** ISM bands working with **16 channels, 10 channels, and one channel** respectively

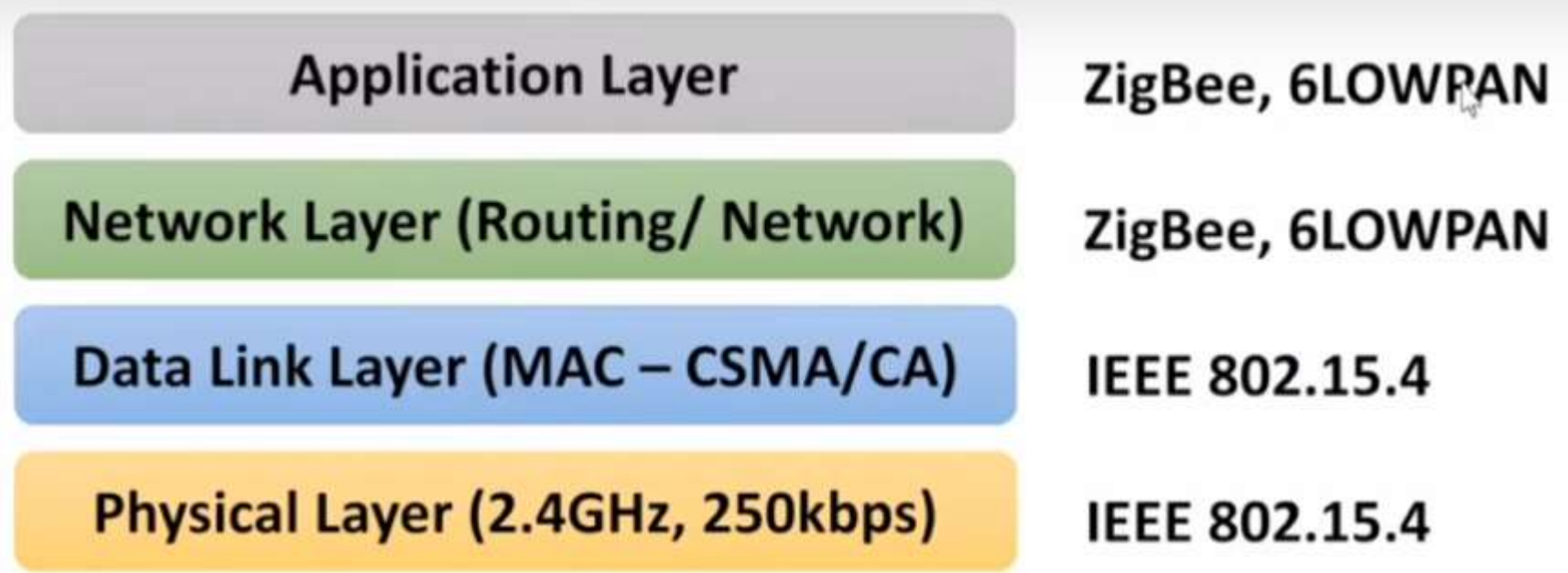
IEEE 802.15.4 - Topology

- 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.
- 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

- IEEE 802.15.4 :

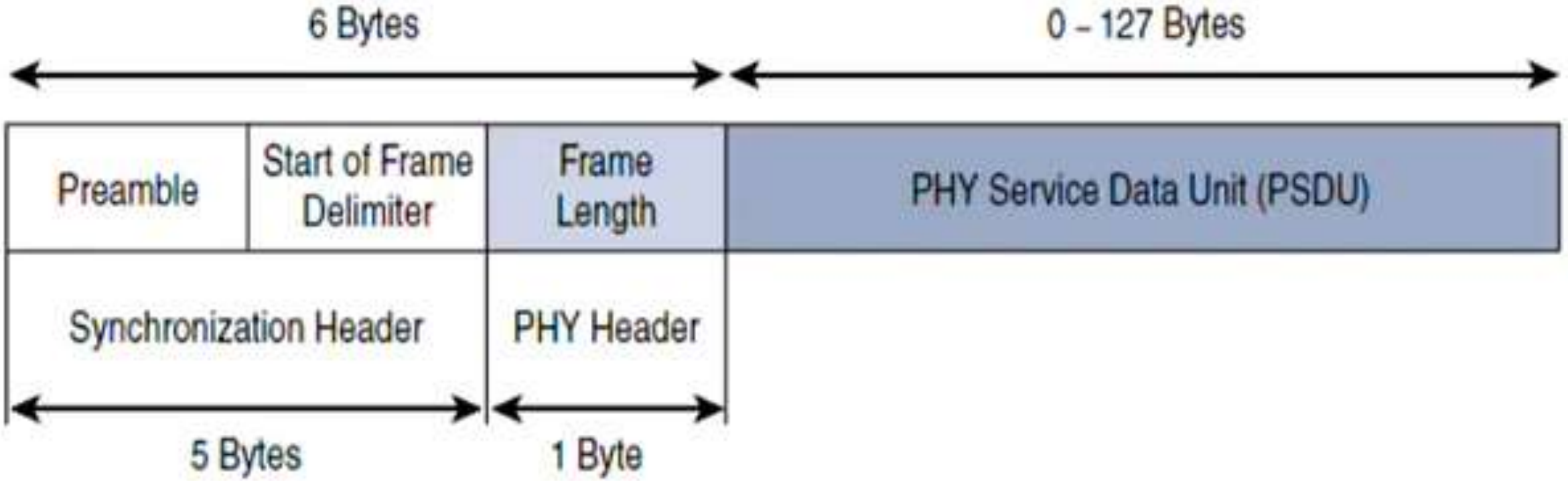

Star topology
(a)
Peer-to-peer topology
(b)
Full function device
Reduced function device
PAN Coordinator

- IEEE 802.15.4 Protocol Stack :



- MAC is done by **CSMA/CA**
- MAC defines **medium access** and **flow control** mechanism
- The physical layer defines **operational frequency ,transmission power and modulation schemes**.
- IEEE 802.15.4 utilizes a **Direct Sequence Spread Spectrum** coding Schemes to **transmit information**.

- IEEE 802.15.4 Physical Layer:



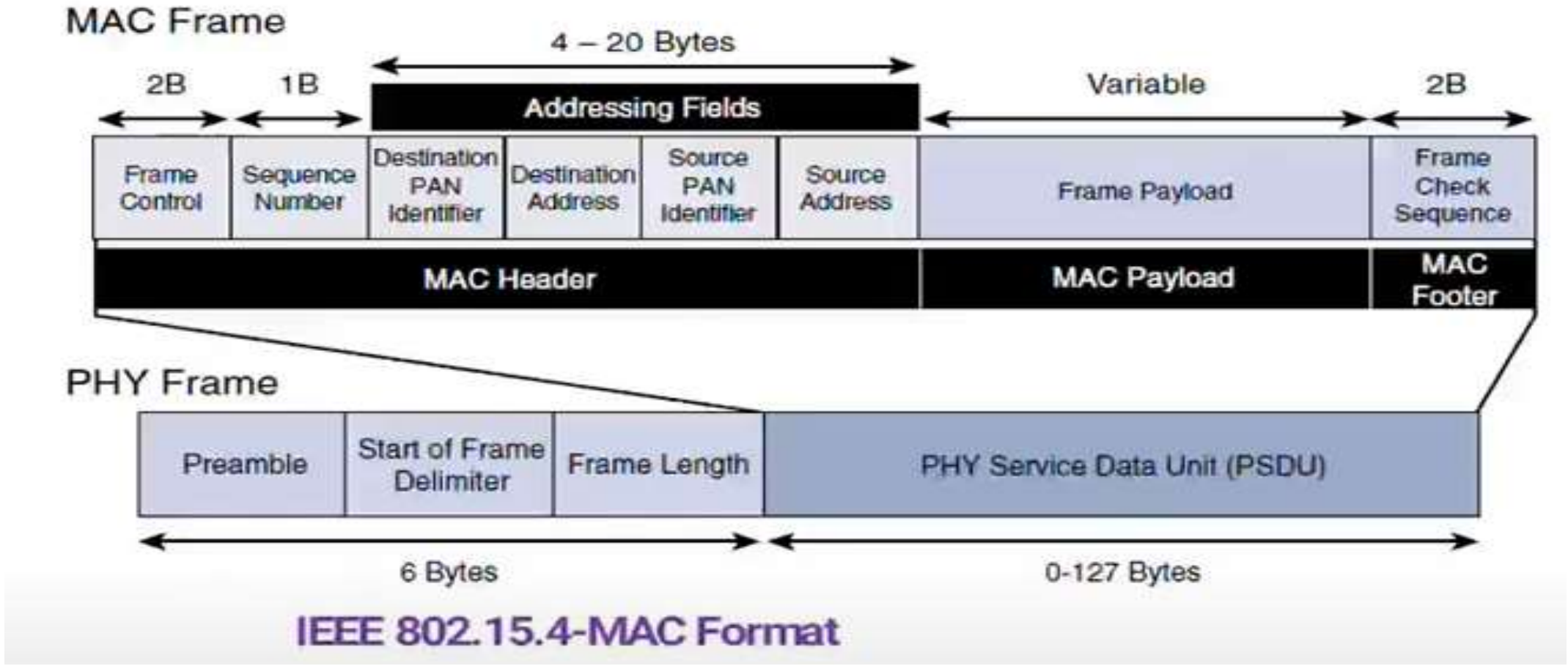
IEEE 802.15.4-PHY Format

IEEE 802.15.4 - Physical Layer

- **The synchronization header**
  - **Preamble:** is a 32-bit or 4-byte (for parallel construction) 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.
- **The PHY Header**
  - **Frame length value:** It lets the receiver know how much total data to expect in the PSDU.
- **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 layer performs the following tasks:
  - Manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated.
  - The scheduling and routing of data frames are coordinated
  - 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



IEEE 802.15.4-MAC Format

IEEE 802.15.4 - MAC Layer

- 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
- The 802.15.4 MAC frame broken down into the
  - MAC Header,
  - MAC Payload,
  - MAC Footer fields.

IEEE 802.15.4 - MAC Layer

- The MAC Header field
  - Frame Control : defines attributes such as frame type, addressing modes, and other control flags
  - Sequence Number : indicates the sequence identifier for the frame
  - Addressing fields : specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields.
- The MAC Payload field varies by individual frame type. maximum payload is 127 bytes, and also defines how a 16-bit " short address" is assigned to devices)
- The MAC Footer
  - A frame check sequence (FCS) is a calculation based on the data in the frame that is used by the receiving side to confirm the integrity of the

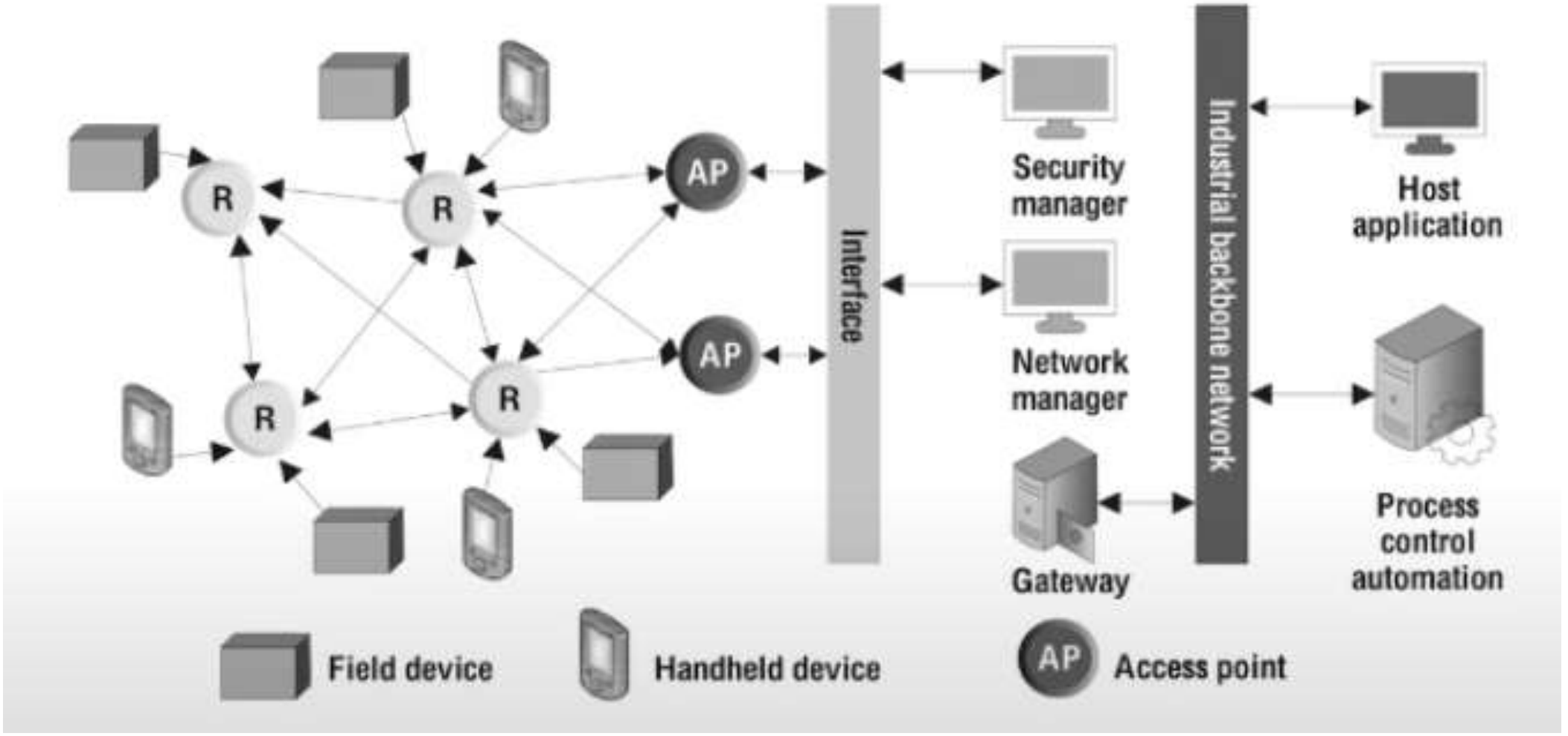
- **Wireless HART :**

- Wireless HART is a Wireless Sensor Network Technology based on the Highway Addressable Remote Transducer (HART).
- Developed as a multi-Vendor , interoperable wireless Standard.
- Wireless HART was defined for the requirements of process field device networks.
- The Protocol utilizes a time synchronized, self-organizing, and self-healing mesh architecture.
- The Protocol supports operation in the 2.4GHz ISM band using IEEE 802.15.4 Standard radios.

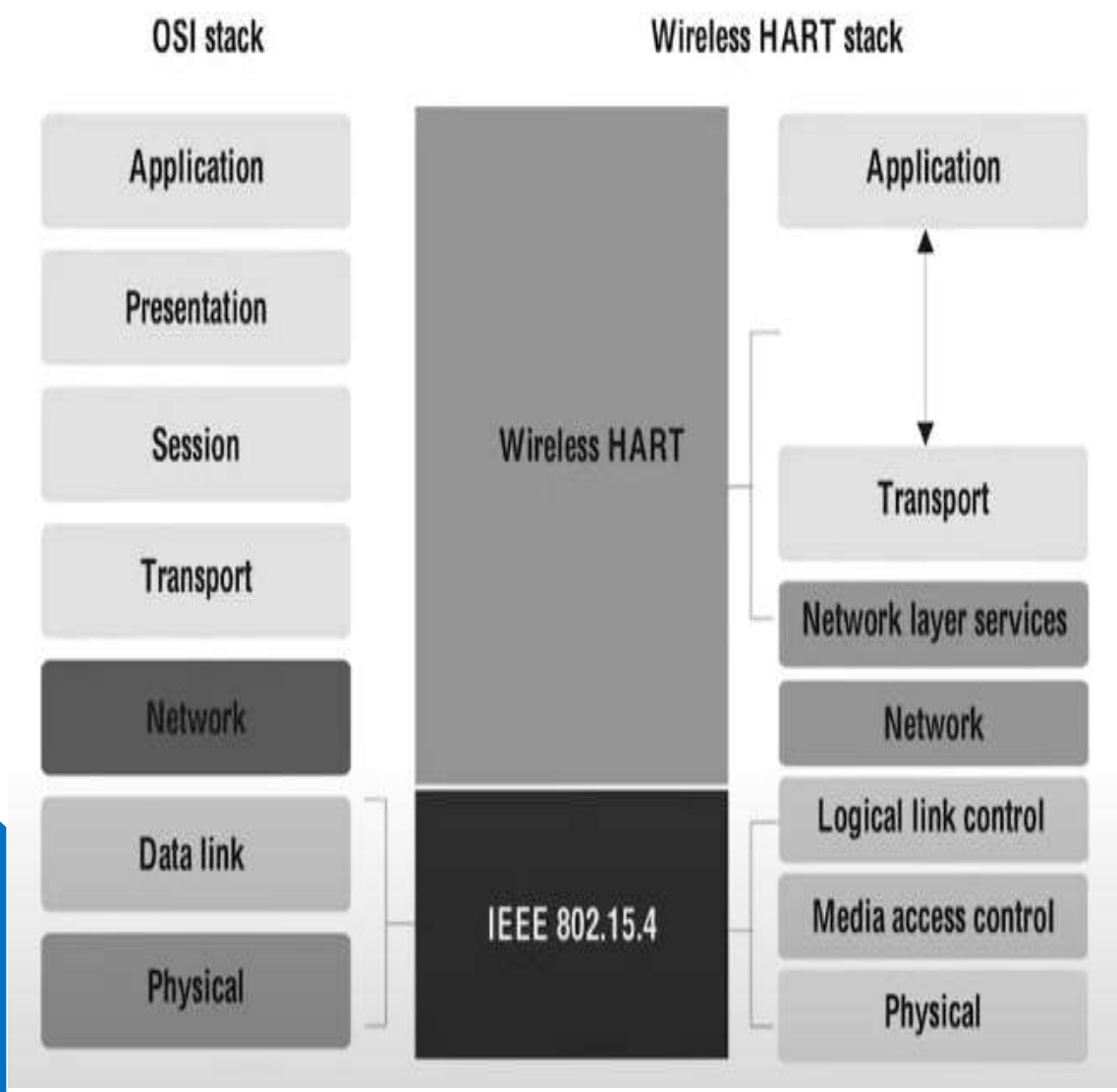
- **Example Wireless HART Network :**

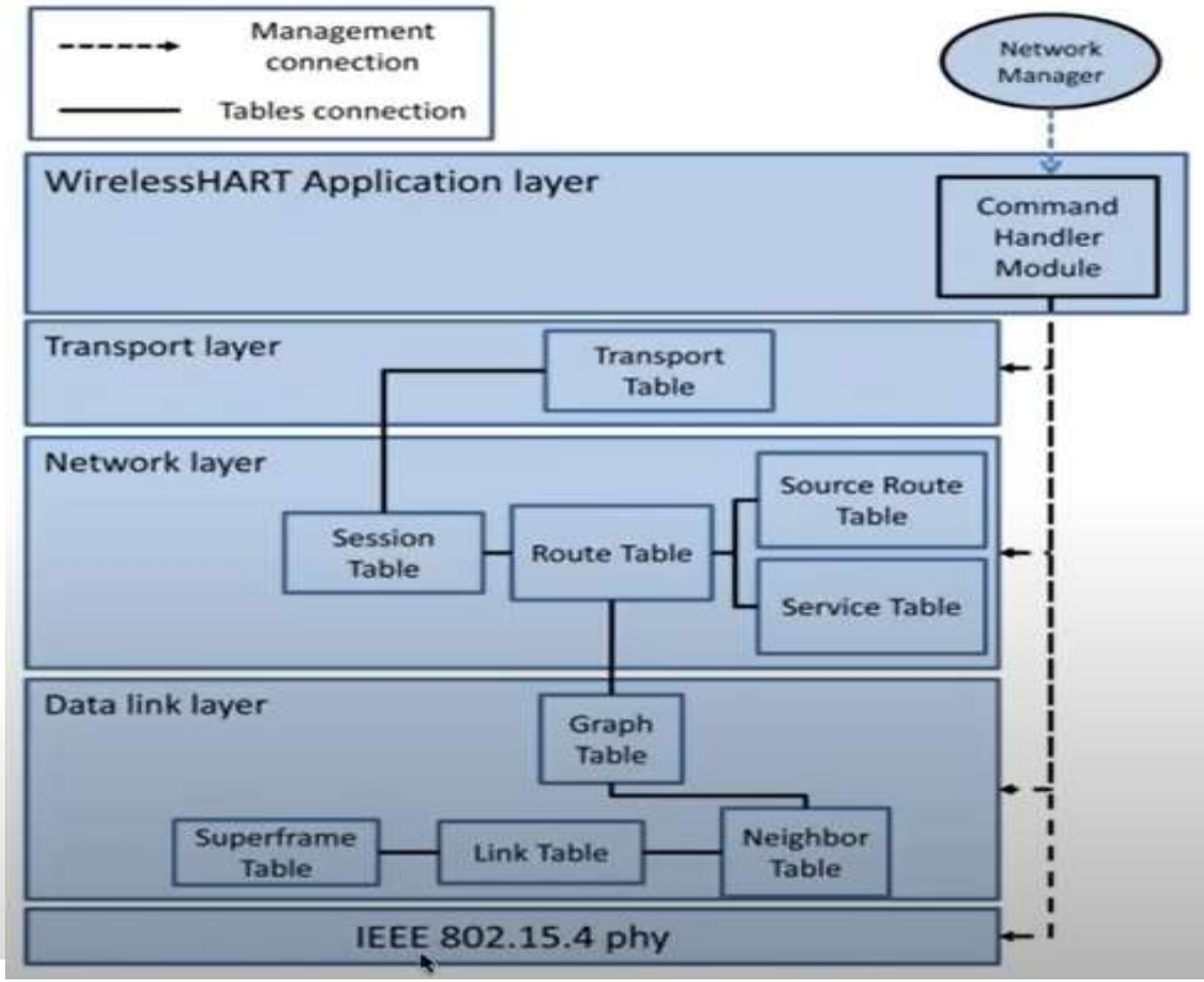
- Each Wireless HART network includes four main elements:
- **Field Devices:** They include wireless HART process transmitter and wireless adapters.
- **Gateway:** Gateway bridges the wireless HART network with wired infrastructures.
- **Network Manger (only one) :** It is responsible for network configuration , communication among devices, management of routing messages and monitor network conditions.
- **Security manager:** Security Manager deals with security and encryption, setting up session keys and their periodic change.

- **Example WirelessHART Network :**



- **Wireless HART Protocol Stack :**





- **Wireless HART Protocol Stack vs OSI Stack :**

- **Physical Layer:** Operates on 2.4GHz frequency band with 15 channels for reliability . It incorporates channel hopping & Channel backing to avoid interference.

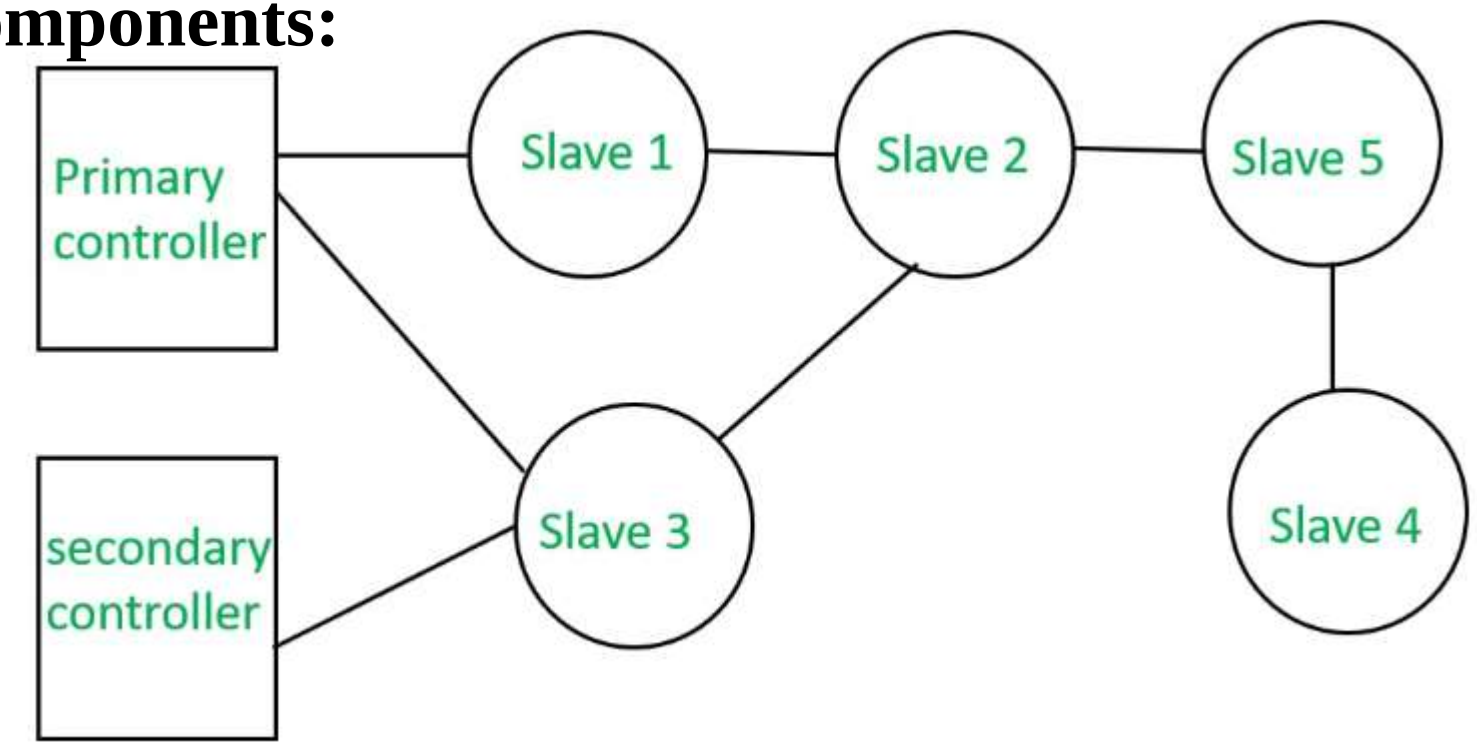
- **Datalink Layer :** It implements TDMA for deterministic communication uses super frames scooped into timeslots to synchronize transmissions.

- **Network Layers:** Handles routing , traffic manages , Security & Session control. It maintains a network graph for routing paths. Supports mesh type topology based open with all nodes capable of forwarding data.

- **Application Layer:** Provides seamless interfacing with legacy HART devices. Manages communication via commands & reponses between devices and gateways.

- **Z-Wave:**
    - In Smart home network using a Z-Wave wireless communication Protocol.
    - Wireless means connecting multiple devices in wireless manner to communicate.
    - Z-Wave operates under source crowdedness architecture.
    - It is invented in 1999 by ZENSYS.
    - Z-Wave consists of a primary controller, IoT devices so these also known as smart home hub.

- **Z-Wave Components:**



- **Controllers:** A controller is a unit that has the ability to compile a **routing table** of the network and can calculate routes to the different nodes. There are two types of controllers -
- **Primary controller:** Primary controller is the device that contains the **Device management, Device inclusion/Exclusion, ID allocation, Network topology**.

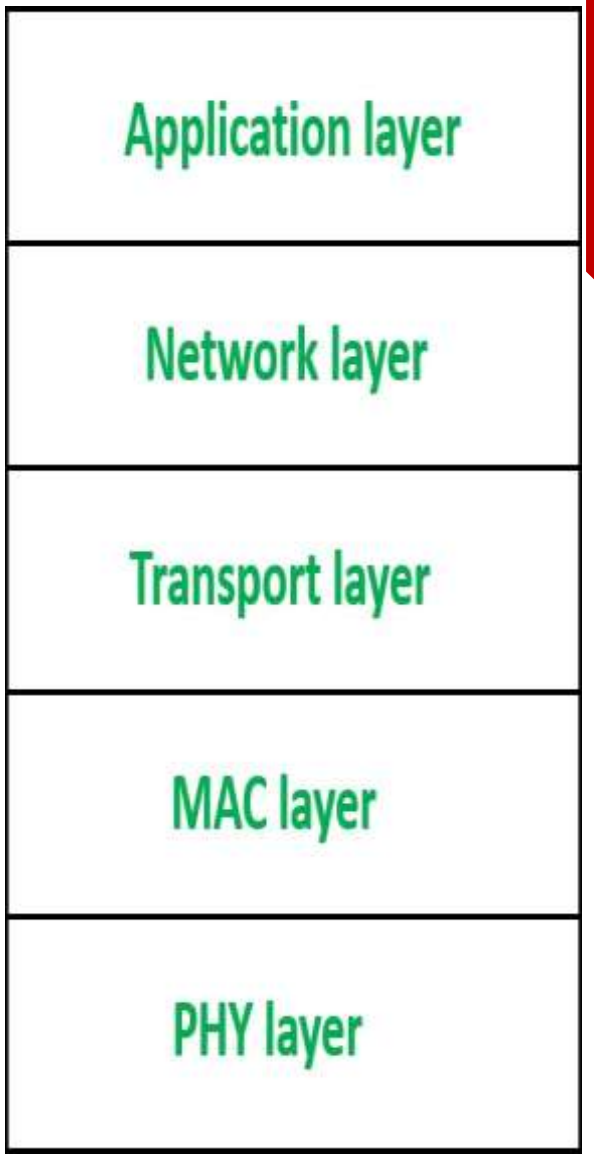
- **Z-Wave Components:**

- **Secondary controller:** It also has a Network ID and it remains constant to maintain routing tables.
- **Slave nodes:** Slave nodes are the nodes that do not contain routing tables but may contain a network map. slave nodes have the ability to receive frames and respond to them if necessary.
- **Home ID:** The ID used by z-Wave for the separation of the network from each other is called Home ID. It is created by the primary controller and is 32-bit in size.
- **Node ID:** The identification number or an address that is given to every device during the process of inclusion is called Node ID.
- **Routing table:** It is used by controllers for calculating routes.

- **Z-Wave Protocol Stack:**

- **PHY layer:** This layer has many functions but the important one is **modulation and coding**. In this layer, data is transferred in 8-bit blocks and the most significant bit is sent first.

- **MAC layer:** MAC layer as the name suggests takes care of medium access control among slave nodes based on **collision avoidance and backoff algorithms**. also, it takes care of network operations based on Home ID, Node ID, and other parameters in the z-wave frame.

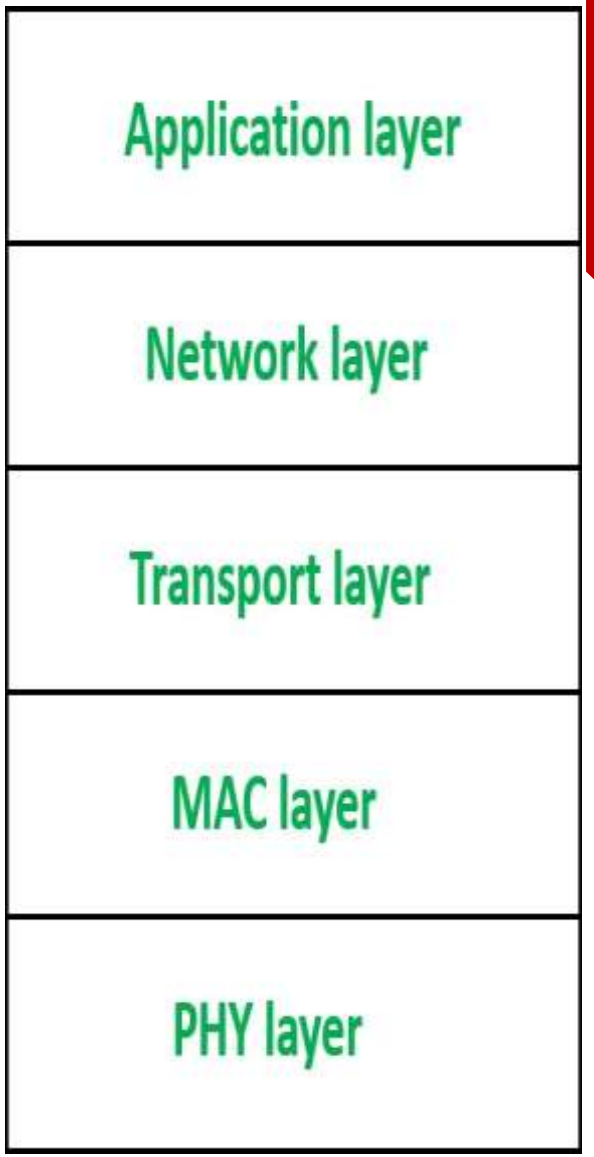


- **Z-Wave Protocol Stack:**

- **Transport layer:** Z-Wave transport layer is mainly responsible for retransmission, packet acknowledgement, and packet origin authentication. the z-wave layer consists of four basic frame types:
  1) Single cast frame : one device to specific destination frame
  2) Multicast frame :which are sent to a selected group.
  3) Broadcast frame : one to all message sent by controller
  4) ACK frame: simple msg sent by receiver in single cast frame

- **Network layer:** Z-Wave network layer controls the frame routing from one node to another node.

- **Application layer:** This layer is responsible for decoding and execution of commands in the z-wave network.



- **Z-Wave :**

- **Characteristics of Z-Wave :**
- Uses RF for signaling and control
- Frequency : 900 MHz (ISM)
- Range : 30 meter
- Data rates : upto 100 kbps
- FSK Modulation

- **Applications of Z-Wave :**
- Home automation
- Water management using flood sensors
- Fingerprint scanner

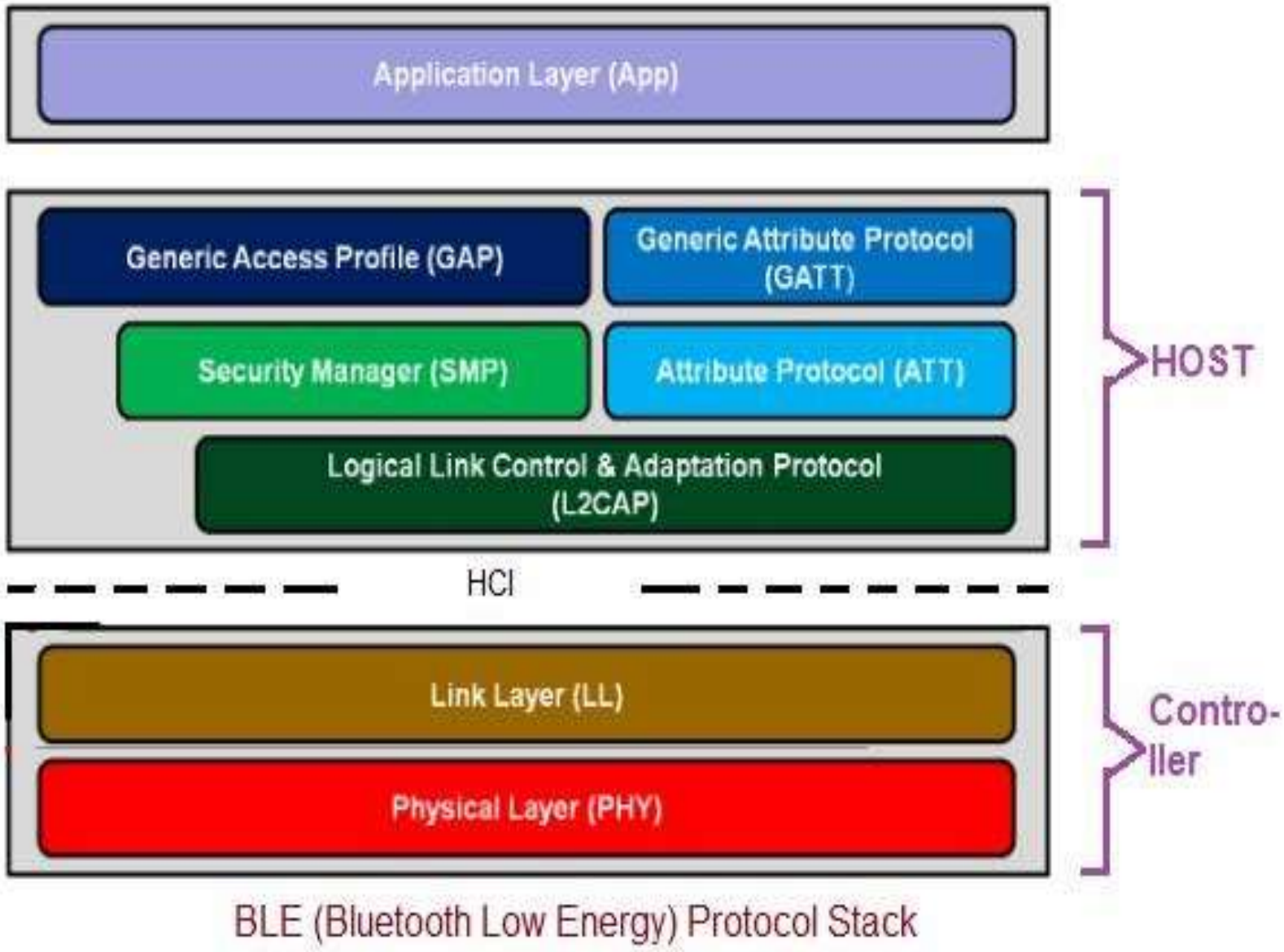
- **Bluetooth Low Energy :**

- BLE stands for Bluetooth Low Energy.
- It is a Low Power, Short-range radio communication technology.
- BLE is also called Bluetooth Smart
- BLE is designed by Bluetooth Special Interest Group (SIG).
- It works similar to traditional Bluetooth and is used in Personal Area Network (PANs)
- BLE is considered an advanced version of classic Bluetooth.
- It is widely used in IoT devices, fitness bands, smart watches, healthcare devices and smart home gadgets.

- **Key Features of BLE :**

- BLE is License-free and has no extra cost to use.
- It allows any manufacturer to use it without restriction.
- BLE modules are cheap and easy to afford.
- BLE modules are very small, so they fit easily in any device.
- BLE uses very little power, making it perfect for IoT applications.
- BLE has a better range compared to classic Bluetooth.

- **BLE Architecture:**



BLE (Bluetooth Low Energy) Protocol Stack

- **BLE Architecture components:**

- From the architecture perspective ,BLE is divided into three main components.
- BLE architecture is divided into three main blocks.
  - Application Block
  - Host Block
  - Controller Block

Application Block (Top Layer):

- This is where the user's application runs (like a health tracker, fitness band app etc.).
- It interacts with the Bluetooth stack to send or receive data.
- It is responsible for user interface, logic, and data handling.

Host Block (Middle layer)

- This is the main software layer and contain the following components.
- GAP (Generic Access Profile) : Handle device discovery connection setup and security

- **BLE Architecture components:**

Host Block (Middle layer) (cntd…..)

GATT (Generic Attribute Profile) :

- Manages Data exchange like reading and writing sensor data.

ATT (Attribute Protocol):

- Defines how device's structure, store, and access data through a client-server model.

SMP (Security Management Protocol) :

- Manages paring , encryption and authentication for secure communication.

L2CAP (Logical Link Control and Adaption Protocol) :

- Breaks and joins data packets.
- Handles multiple data channels over the same BLE connection.

HCI (Host Controller Interface):

- Ensures communication between Host and controller made by different manufactures.

- **BLE Architecture components:**

- Controller Block (Bottom Layer)
- This is the hardware-related part that connects with physical signals. It includes
  - **Link Layer (LL)** :
  - Defines the structure of data packets and handles device roles (master/slave).
  - **Physical Layer (PHY):**
  - Takes care of signal transmission and reception, modulation and digital conversion.

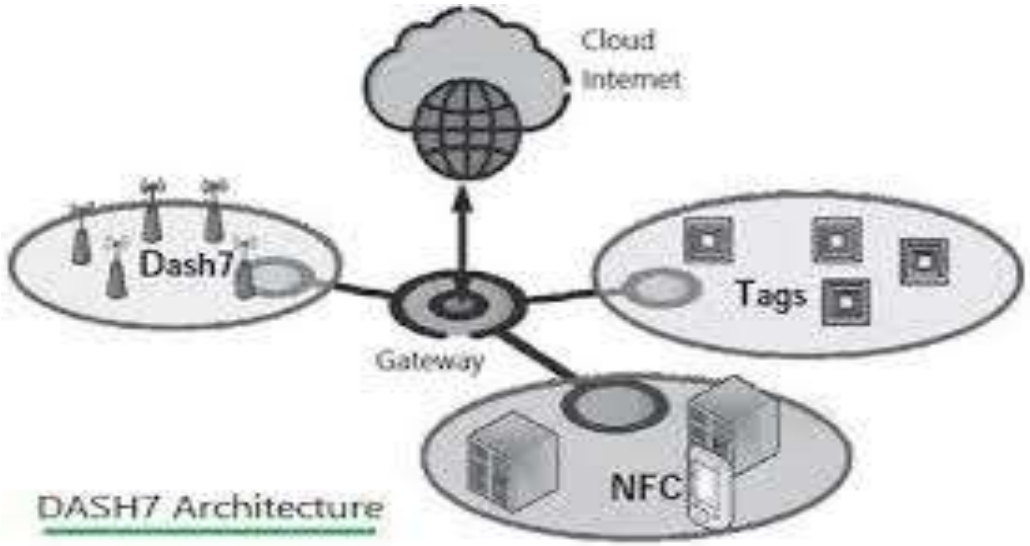
- **DASH7:**

- DASH7 is a wireless communication Protocol derived from active RFID Standards.
- It operates on 433MHz frequency band and is widely adopted in diverse application including agriculture , vehicle ,consumer, electronics & mobile devices .
- Dash7 is unique for its support for NFC compatibility and its adaptability to IOT communication systems.

- **DASH7 Key Features:**

- **Frequency:** It operates on a specific radio frequency at 433.92 MHz using method called Frequency shift keying(FSK) modulation for reliable msg transmission.
- **File system :** It has a built-in file system , which makes it a good choice for simple, low-cost devices.
- **Power and Memory :** It is designed to work with very little power and memory and it allows devices to communicate directly with each other. This is useful for creating large network for many small devices.
- **Range :** It can communicate over a distance of 1 to 10Km.
- **Speed :** It takes between 1 to 10 Seconds to get a response to query.

- **DASH7 Architecture:**



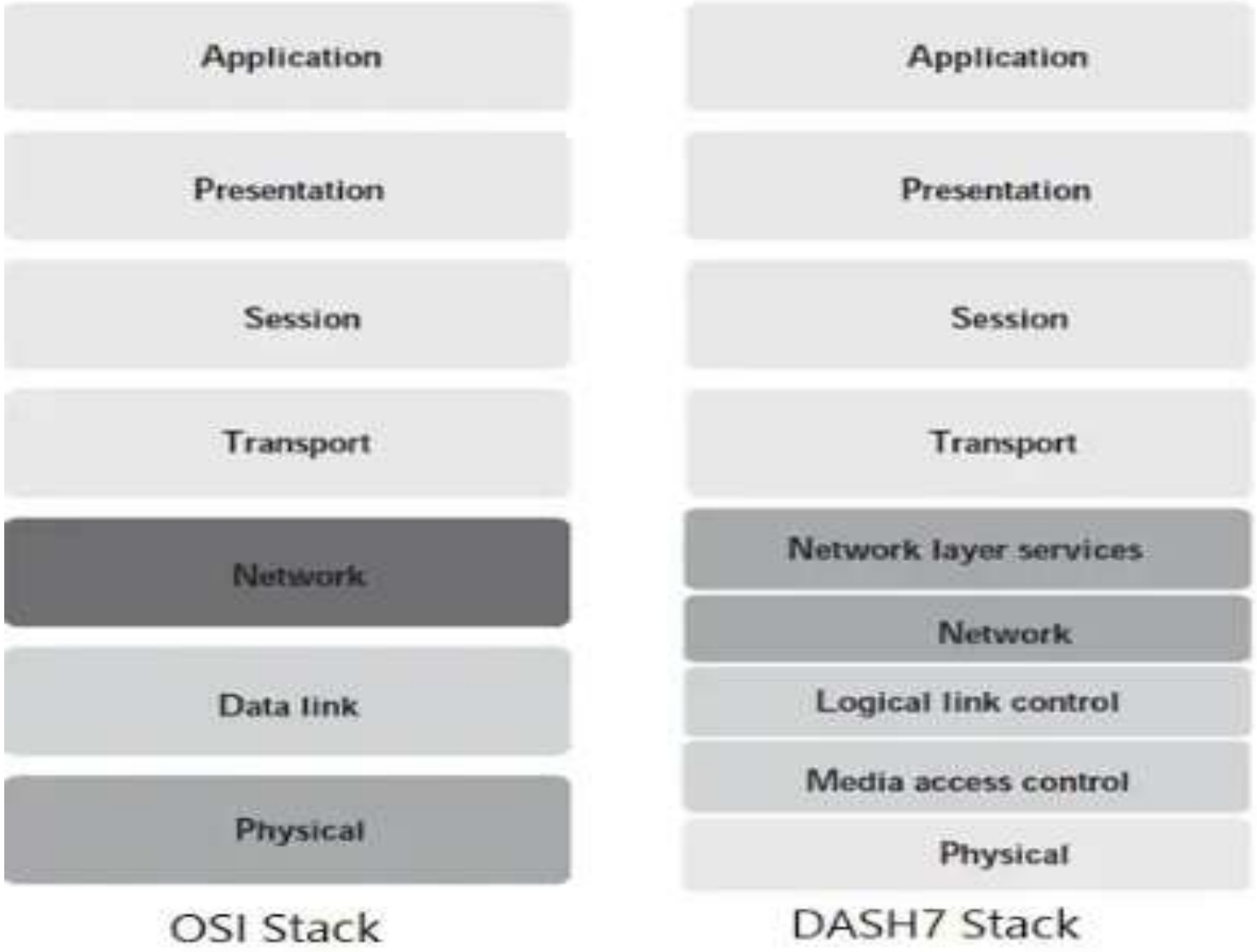
- Smart Devices
- Tags
- NFC Devices
- Gateways
- Internet

- It uses gateways and devices to communicate.
- It can also interact with NFC (Near field communication) devices.
- Gateways can actively check for near by devices without having to wait for specific time slots.
- This technology acts as a link b/w NFC and other IoT systems
- It allows devices to communicate directly with each other without needing central base station

DASH7 Applications:

- Agriculture
- Consumer Electronics
- Vehicle
- IoT systems.

- **DASH7 Protocol stack:**

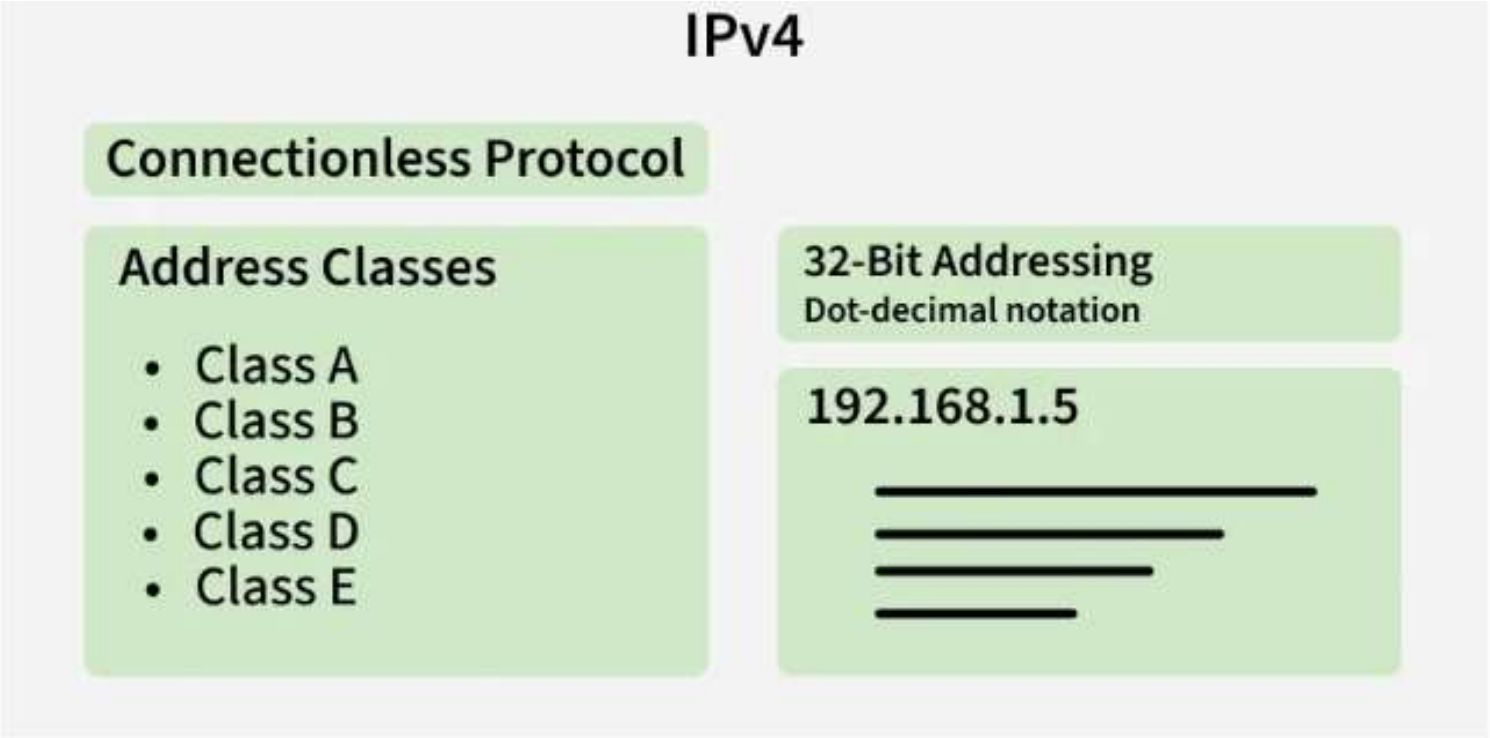


- **DASH7 Protocol stack:**

- Application Layer : manages user applications and services querying and data processing.
- Presentation and session layer : enables data formatting & session management for secure and reliable communication.
- Network layer services : manages routing, device addressing & protocol adaptation to technologies like Sigfox and LoRa.
- Data link layer : provides LLC &MAC ensuring collision free data transmission.
- Physical Layer- utilizes 433MHz FSK modulation for data transmission over wireless channels.

- **IPv4 :**

- IP stands for Internet Protocol version v4 stands for Version Four (IPv4), is the most widely used system for identifying devices on a network.
- It uses a set of four numbers, separated by periods (like 192.168.0.1), to give each device a unique address.
- This address helps data find its way from one device to another over the internet.



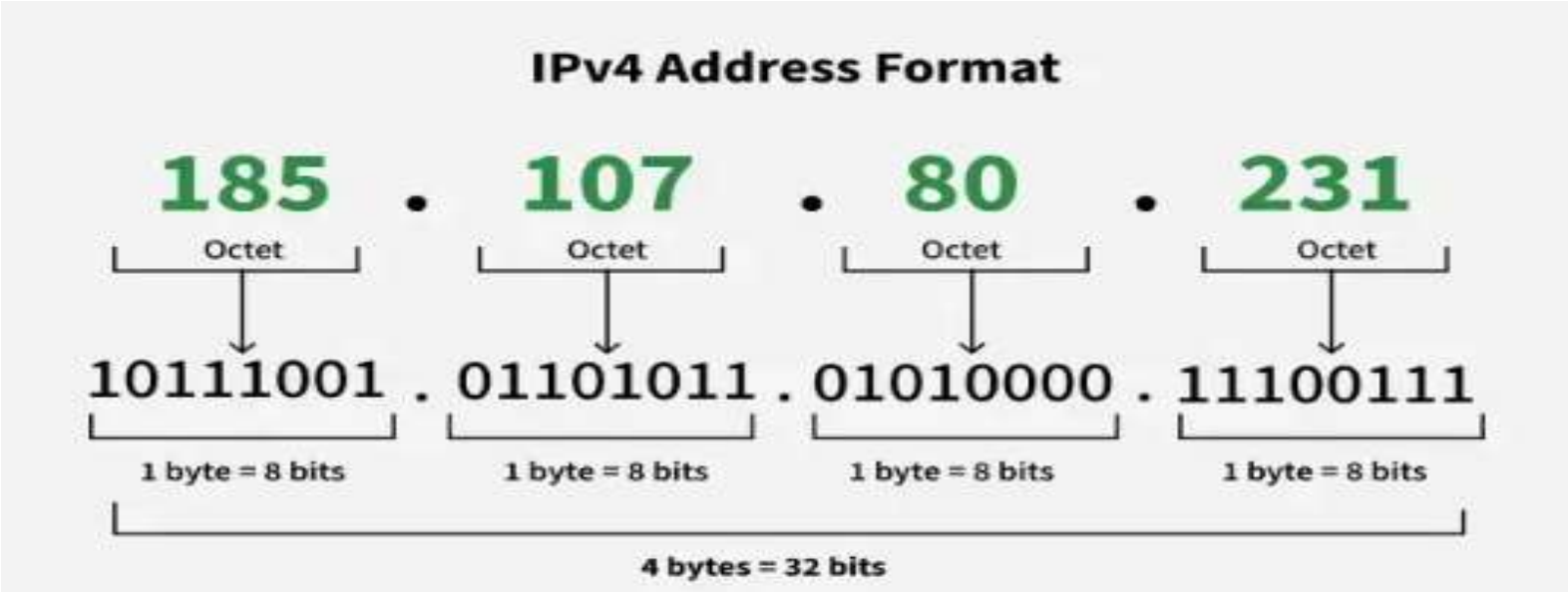
- **IPv4 :**

- An IPv4 address consists of series of four eight-bit binary numbers which are separated by decimal point.
- Although any numbering system can be used to represent a unique 32- bit number, most commonly you see IP address expressed in dot decimal notation.
- Some of the examples are:

Site	Dot-decimal	Binary
Twitter.com	104.244.42.129	01101000.11110100.00101010.10000001
Reddit.com	151.101.65.140	10010111.01100101.01000001.10001100
Linkedin.com	108.174.10.10	01101100.10101110.00001010.00001010

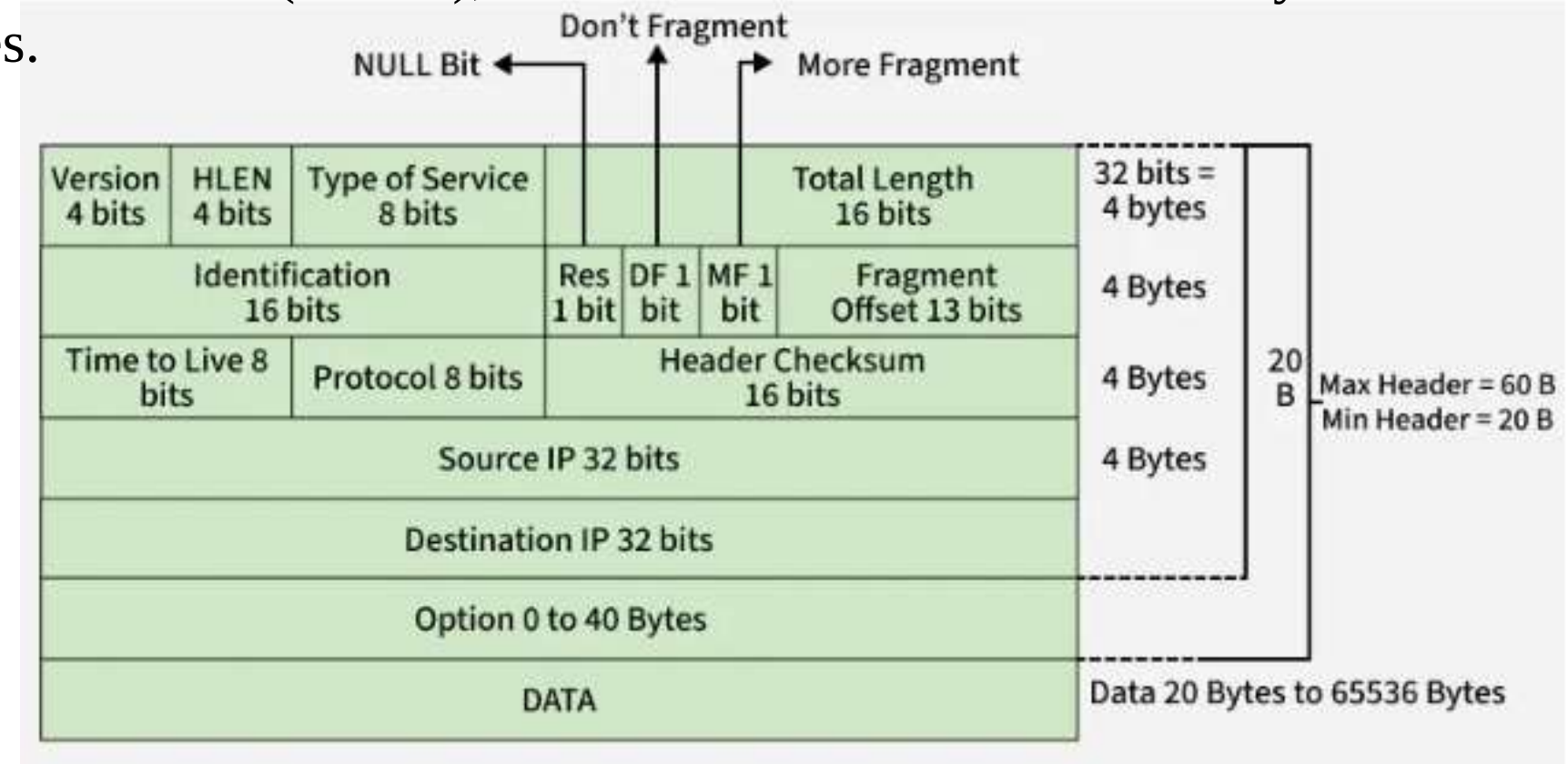
- **IPv4 address format :**

- An IPv4 address consists of 32 bit (binary digit), grouped into four section of known as octets or bytes.
- Each octet has 8 bits and this bits can be represented only in 0 or 1 form, and when they grouped together, they form a binary number.
- Since each octet has 8 bits, it can represent 256 numbers ranging from o to 255.
- These four octets are represented as decimal numbers, separated by periods known as dotted decimal notation.
- For example IPv4 address 185.107.80.231 consists of four octets.



• IPv4 Datagram Header :

VERSION: Version of the IP protocol (4 bits), which is 4 for IPv4
HLEN: IP header length (4 bits), which is the number of 32 bit words in the header. The minimum value for this field is 5 and the maximum is 15.
Type of service: Low Delay, High Throughput, Reliability (8 bits)
Total Length: Length of header + Data (16 bits), which has a minimum value 20 bytes and the maximum is 65,535 bytes.



• IPv4 Datagram Header :

Identification: Unique Packet Id for identifying the group of fragments of a single IP datagram (16 bits)

Flags: 3 flags of 1 bit each : reserved bit (must be zero), do not fragment flag, more fragments flag (same order)

Fragment Offset: Represents the number of Data Bytes ahead of the particular fragment in the particular Datagram. Specified in terms of number of 8 bytes, which has the maximum value of 65,528 bytes.

Time to live: Datagram's lifetime (8 bits), It prevents the datagram to loop through the network by restricting the number of Hops taken by a Packet before delivering to the Destination.

Protocol: Name of the protocol to which the data is to be passed (8 bits)

Header Checksum: 16 bits header Checksum for checking errors in the datagram header

Source IP address: 32 bits IP address of the sender

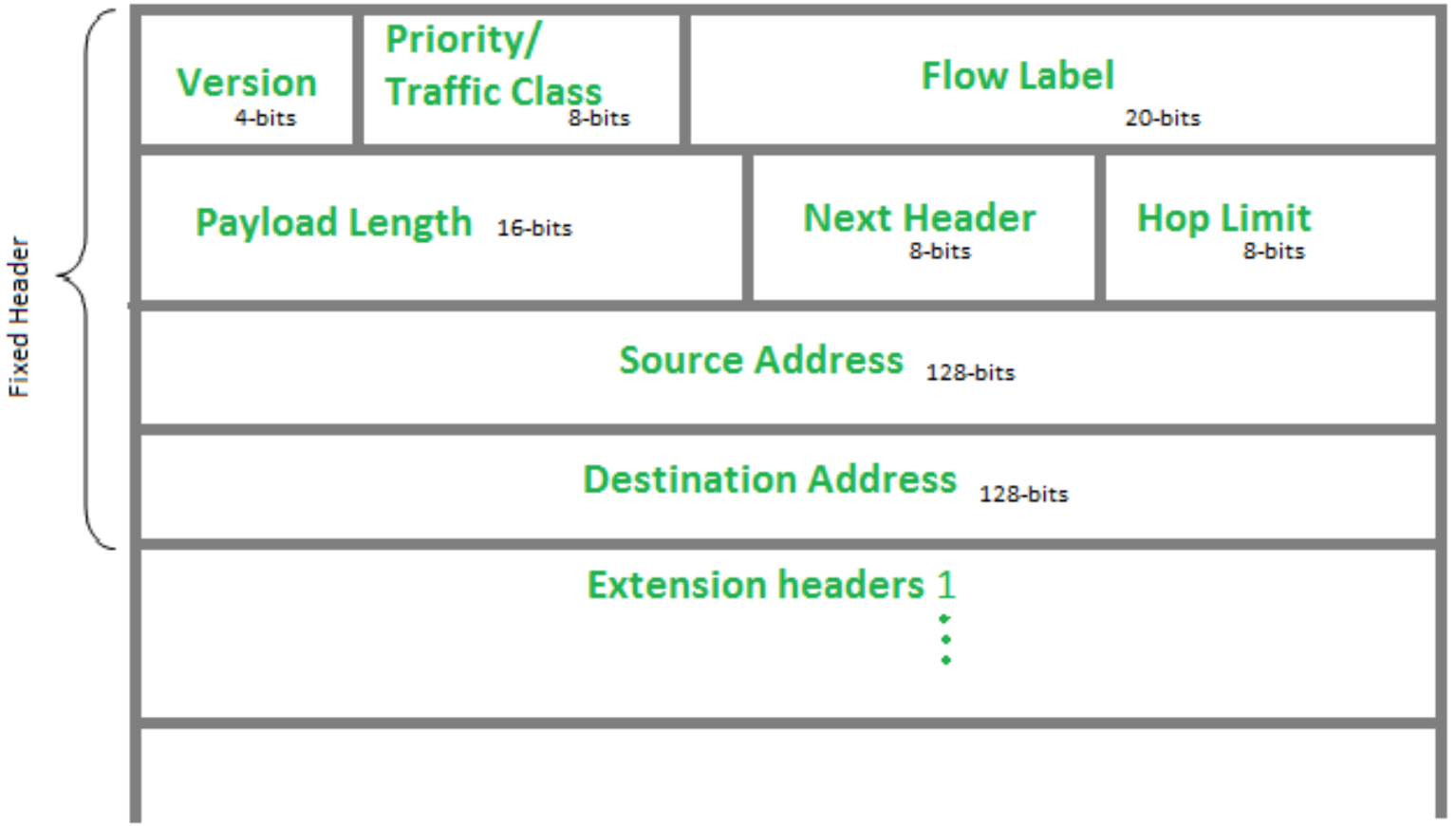
Destination IP address: 32 bits IP address of the receiver

Option: Optional information such as source route, record route. Used by the Network administrator to check whether a path is working or not.

- **IPv6 :**

- IP v6 was developed by Internet Engineering Task Force (IETF).
- IP v6 is a 128-bits address having an address space of 2^128.
- In IPv6 we use Colon-Hexa representation.
- There are 8 groups and each group represents 2 Bytes.
- In IPv6 representation, have three addressing methods:
  - 1) Unicast
  - 2) Multicast
  - 3) Anycast
- 1. **Unicast Address** – Unicast Address identifies a single network interface. A packet sent to a unicast address is delivered to the interface identified by that address.
- 2. **Multicast Address** – Multicast Address is used by multiple hosts, called as Group, acquires a multicast destination address. These hosts need not be geographically together. If any packet is sent to this multicast address, it will be distributed to all interfaces corresponding to that multicast address.
- 3. **Anycast Address** – Anycast Address is assigned to a group of interfaces. Any packet sent to an anycast address will be delivered to only one member interface (mostly nearest host possible).

- **IPv6 :**
  - **Version (4-bits):** Indicates version of Internet Protocol which contains bit sequence 0110.
  - **Traffic Class (8-bits):** The Traffic Class field indicates class or priority of IPv6 packet which is similar to Service Field in IPv4 packet. It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded. As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.



- **IPv6 :**

- Service Field in IPv4 packet : It helps routers to handle the traffic based on the priority of the packet. If congestion occurs on the router then packets with the least priority will be discarded. As of now, only 4-bits are being used (and the remaining bits are under research), in which 0 to 7 are assigned to Congestion controlled traffic and 8 to 15 are assigned to Uncontrolled traffic.
- **Priority assignment of Congestion controlled traffic:** Uncontrolled data traffic is mainly used for Audio/Video data. So we give higher priority to uncontrolled data traffic. The source node is allowed to set the priorities but on the way, routers can change it. Therefore, the destination should not expect the same priority which was set by the source node.

Priority	Meaning
0	No Specific traffic
1	Background data
2	Unattended data traffic
3	Reserved
4	Attended bulk data traffic
5	Reserved
6	Interactive traffic
7	Control traffic

- **IPv6 :**

- **Flow Label (20-bits):** Flow Label field is used by a source to label the packets belonging to the same flow in order to request special handling by intermediate IPv6 routers, such as non-default quality of service or real-time service. In order to distinguish the flow, an intermediate router can use the source address, a destination address, and flow label of the packets. Between a source and destination, multiple flows may exist because many processes might be running at the same time. Routers or Host that does not support the functionality of flow label field and for default router handling, flow label field is set to 0. While setting up the flow label, the source is also supposed to specify the lifetime of the flow.
- **Payload Length (16-bits):** It is a 16-bit (unsigned integer) field, indicates the total size of the payload which tells routers about the amount of information a particular packet contains in its payload. The payload Length field includes extension headers (if any) and an upper-layer packet. In case the length of the payload is greater than 65,535 bytes (payload up to 65,535 bytes can be indicated with 16-bits), then the payload length field will be set to 0 and the jumbo payload option is used in the Hop-by-Hop options extension header.

- **IPv6 :**

- **Next Header (8-bits):** Next Header indicates the type of extension header(if present) immediately following the IPv6 header. Whereas In some cases it indicates the protocols contained within upper layer packets, such as TCP, UDP.
- **Hop Limit (8-bits):** Hop Limit field is the same as TTL in IPv4 packets. It indicates the maximum number of intermediate nodes IPv6 packet is allowed to travel. Its value gets decremented by one, by each node that forwards the packet and the packet is discarded if the value decrements to 0. This is used to discard the packets that are stuck in an infinite loop because of some routing error.
- **Source Address (128-bits):** Source Address is the 128-bit IPv6 address of the original source of the packet.
- **Destination Address (128-bits):** The destination Address field indicates the IPv6 address of the final destination (in most cases). All the intermediate nodes can use this information in order to correctly route the packet.
- **Extension Headers:** The extension header mechanism is a very important part of the IPv6 architecture. The next Header field of IPv6 fixed header points to the first Extension Header and this first extension header points to the second extension header and so on.

- **IPV4 vs IPV6**

Feature	IPv4	IPv6
Address Length	32-bit address	128-bit address
Address Format	Decimal format (e.g., 192.168.0.1)	Hexadecimal format (e.g., 2001:0db8::1)
Configuration	Manual and DHCP configuration	Auto-configuration and renumbering supported
Connection Integrity	End-to-end integrity is unachievable	End-to-end integrity is achievable

- **IPV4 vs IPV6**

Security	No built-in security; external tools like IPSec needed	IPSec is built-in for encryption and authentication
Fragmentation	Performed by routers	Performed only by the sender
Flow Identification	Not available	Uses Flow Label field in header for packet flow identification
Checksum Field	Present	Not present
Transmission Scheme	Supports broadcast	Uses multicast and anycast; no broadcast
Header Size	Variable: 20–60 bytes	Fixed: 40 bytes

- **IPV4 vs IPV6**

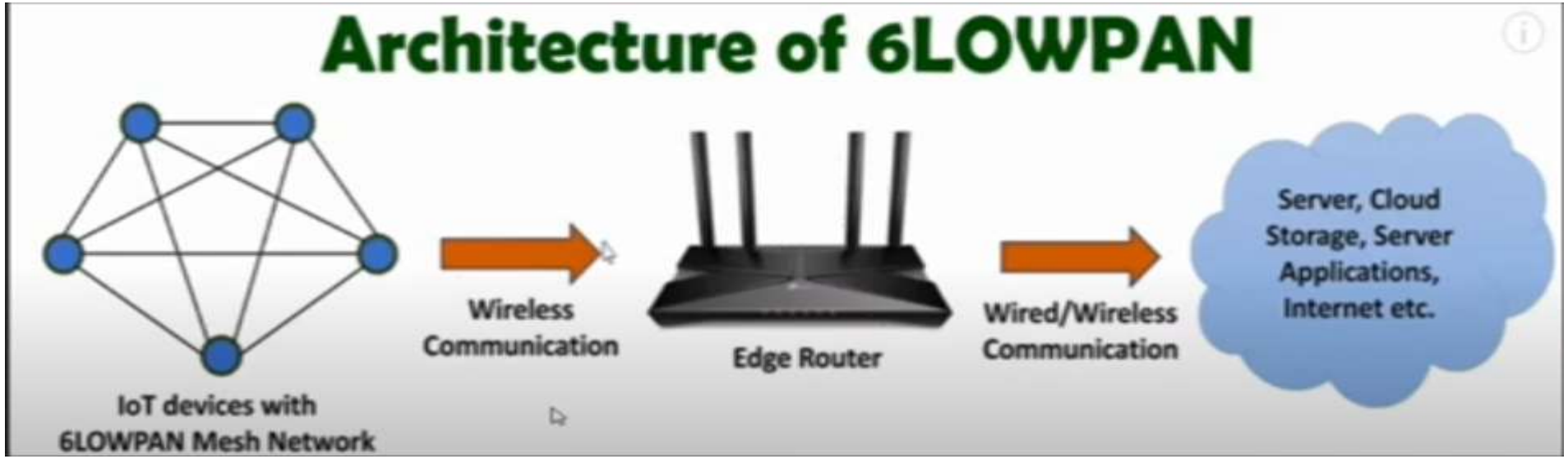
Conversion	Can be converted to IPv6	Not all IPv6 addresses can be converted to IPv4
Field Structure	4 fields separated by dots (.)	8 fields separated by colons (:)
Address Classes	Has address classes (A, B, C, D, E)	No concept of address classes
VLSM Support	Supports Variable Length Subnet Mask (VLSM)	Does not support VLSM
Example	66.94.29.13	2001:0000:3238:DFE1:0063:0000:0000:FEFB

- **6LoWPAN :**

- 6LOWPAN- IPV6 Over Low Power Wireless personal Area Network.
- It combines the latest internet protocol IPV6 and Low Power wireless Personal Area Networks.
- So,6LOWPAN allows the smallest device with limited processing ability to transmit information wirelessly on the internet using IPV6.
- 6LOWPAN is low-cost , short range, Low memory usage, low bit-rate and comprises of edge router and sensor nodes.
- Using 6LOWPAN, the smallest of the IoT devices can be part of the Network and communicate with the outside world (Ex: LED Streetlights).

- **6LoWPAN :**

- 6LOWPAN Technology makes individual nodes IP-enabled.
- Edge Router is the core of the 6LoWPAN network which connects the 6LoWPAN network with internet.
- 6LOWPAN can communicate with Zigbee devices (IEEE802.15.4)and Wi-Fi devices (IEEE 802.11).
- 6LowPAN uses AES -128 (Advanced Encryption Standard) Link layer security , which is defined in IEEE 802.15.4 and it provides link authentication and encryption.



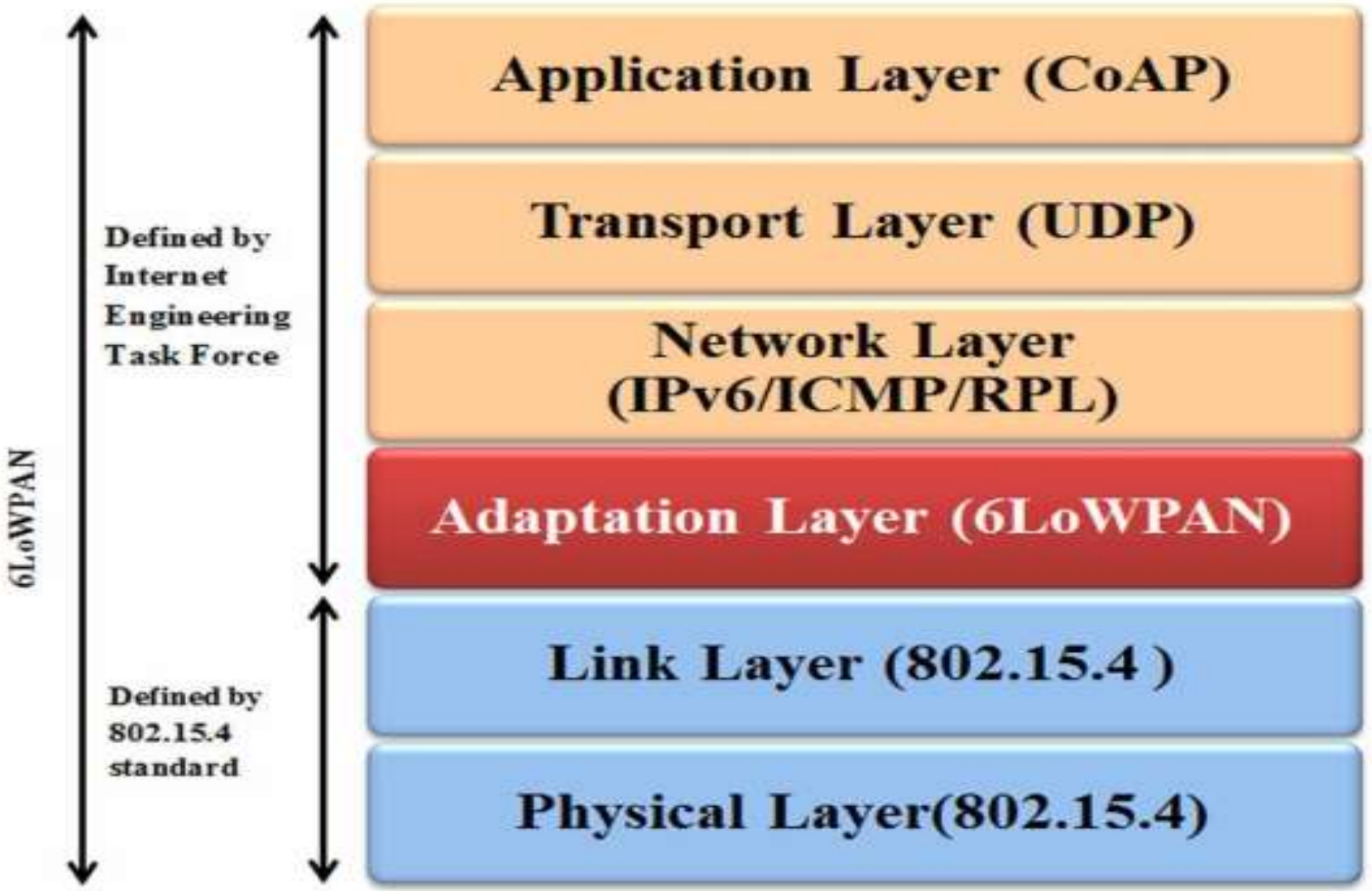
- **Requirements of 6LoWPAN :**

- The Devices must have sleep mode to support battery savings.
- Minimal Memory requirements (16KB RAM and 128KB ROM).
- Routing Overhead Should be Lower.
- Low computational are required with 6LOWPAN.

- **Features of 6LoWPAN :**

  - It is used with IEEE 802.15.4 (Zigbee) in 2.4GHz (ISM Band).
  - Outdoor range is up to 200m at Max.
  - Maximum data rate is 200 Kbps.
  - Maximum 100 nodes can be connected in 6LOWPAN.

- **Protocol Stack of 6LoWPAN :**



- **6LoWPAN layers :**
- **Physical Layer :** Uses wireless communication standards like 802.15.4, often in the 2.4 GHz band.
- **Data Link Layer :** Also based on IEEE 802.15.4 , it uses CSMA/CA for media access control and error correction.
- **Adaptation Layer :** This is the defining layer for 6LoWPAN.
- **IPv6 Header Compression:** Reduces the size of IPv6 and UDP headers to fit with in the small frame sizes of low-power networks.
- **Fragmentation and Reassembly :** Splits large IPv6 datagrams into smaller fragments for transmission over the link layer and reassembles them at the destination.
- **Fragment Forwarding :** Handles the forwarding of fragments across multi-hop networks.

- **6LoWPAN layers :**
- **Network Layer :** Uses the IPv6 protocol for addressing and RPL (Routing Protocol for Low-Power and Lossy Networks) for routing in resource-constrained environments.
- **Transport Layer :** Supports protocols like UDP and TCP for connection and data flow.
- **Application layer :** the top most layer , where application like HTTP, CoAP other run to Provide specific device functions.

- **Advantages of 6LoWPAN :**

- It is a Mesh network that is robust , scalable
- It offers one to many and many to one routing
- It ‘s directly routed to cloud platforms..

- **Disadvantages of 6LoWPAN :**

  - It is comparatively less secure than Zigbee.
  - Without the mesh topology , it supports a short range.

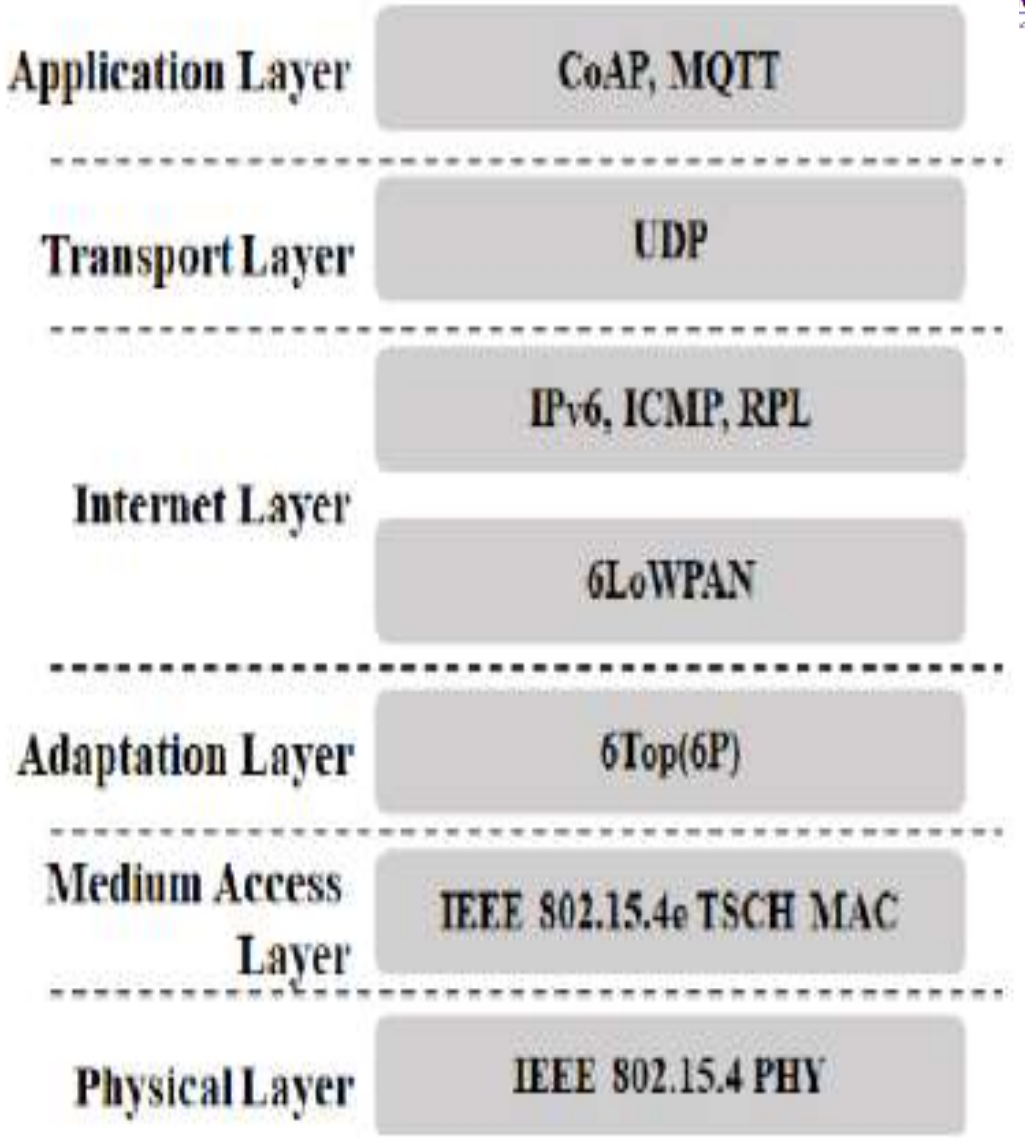
- **6TiSCH (Time Slotted Channel Hopping) :**

- 6TiSCH stands for IPv6 over the Time-Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e and is a set of protocols for building reliable, low-power wireless networks for the Internet of Things (IoT).
- It uses the TSCH MAC layer, which synchronizes network nodes to communicate at scheduled times on different radio channels, reducing collisions and power consumption.
- The technology integrates IPv6 connectivity with low-power wireless networks using protocols like 6LoWPAN and RPL.

- **6TiSCH (Time Slotted Channel Hopping) Key components :**
- **Reliable and deterministic communication:** 6TiSCH leverages the IEEE 802.15.4e TSCH link layer to provide reliable and deterministic communication essential for industrial control applications.
- **Low-power consumption:** By synchronizing nodes and using a time-slotted schedule, 6TiSCH minimizes radio-on time, resulting in ultra-low power consumption.
- **IPv6 integration:** It allows 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) to seamlessly integrate with the internet, offering full IPv6 connectivity.
- **Scheduled communication:** A key feature is the communication schedule, which dictates when nodes should activate their radios and on which frequency to communicate, making network traffic predictable.
- **Standardized architecture:** The IETF 6TiSCH working group has standardized a minimal architecture and 6top protocol, promoting interoperability.

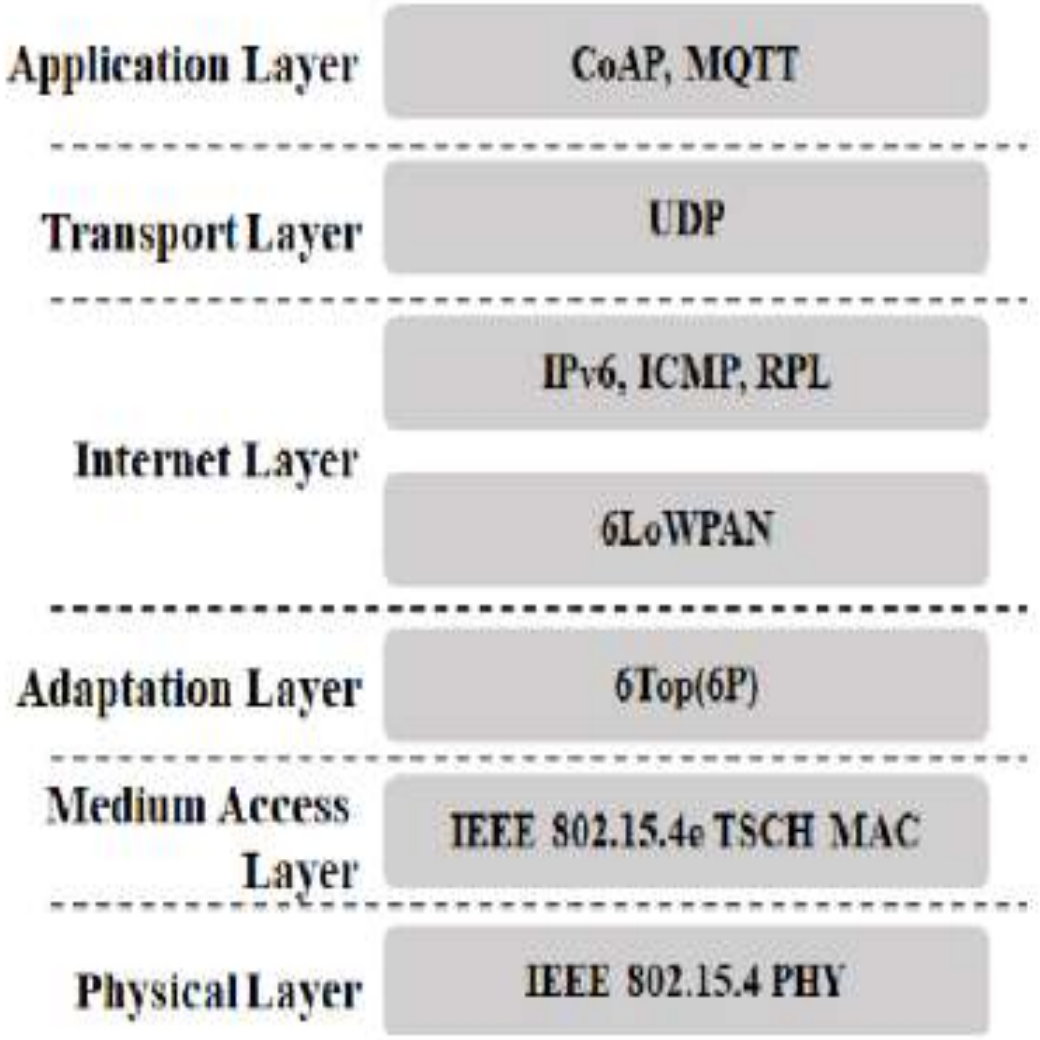
- **6TiSCH (Time Slotted Channel Hopping) Protocol Stack :**

- **Link Layer:** IEEE 802.15.4e TSCH (Time Slotted Channel Hopping) manages physical channel changes to avoid interference and operates on a synchronized slot frame.
- **Network Layer:** IPv6 provides the addressing and routing foundation. RPL (Routing Protocol for Low-power and Lossy Networks) is used to build a tree-shaped routing structure called a DODAG (Destination-Oriented Directed Acyclic Graph).



- **6TiSCH (Time Slotted Channel Hopping) Protocol Stack :**

- **Transport/Application Layer:** UDP is used for transport, with the Constrained Application Protocol (CoAP) for application and management interactions, which is lighter than HTTP.
- **6top:** This is the 6TiSCH operation sub-layer that builds and maintains the communication schedule, managing the TSCH link layer with upper layers.



- **6TiSCH (Time Slotted Channel Hopping) works :**

- The TSCH network is divided into time slots, and a schedule dictates which node communicates on which physical channel in each slot.
- The channel hopping aspect of TSCH increases reliability by using different channels, which helps avoid interference and fading.
- The architecture can include a backbone network with backbone routers that connect the low-power networks to the wider internet.

Applications

- 6TiSCH is designed for industrial-grade applications where reliability and low power are critical, such as in the industrial IoT.
- Examples include systems for smart grids, industrial automation, and monitoring in large environments like marinas.

- **6TiSCH (Time Slotted Channel Hopping) :**

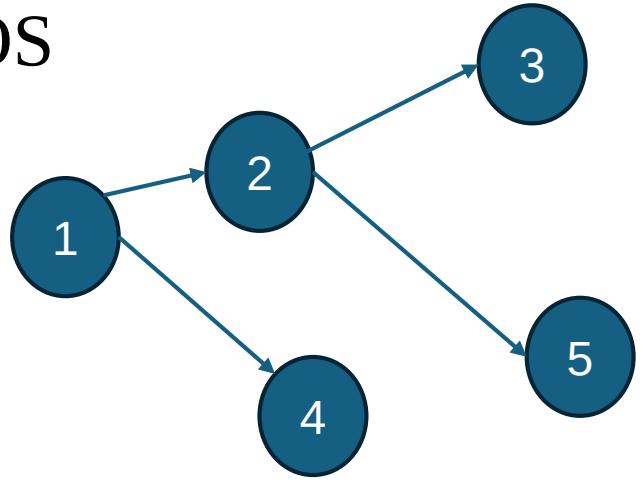
- Schedules in 6TisCH are broken down into cells.
- A cell is simply a single element in the TSCH schedule that can be allocated for unidirectional or bidirectional communication between specific nodes.
- Nodes only transmit when the schedule dictates that their cell is open for communication.
- The 6TiSCH architecture defines four schedule management mechanism
- Stack scheduling
- Neighbor to neighbor scheduling
- Remote monitoring and scheduling management
- Hop-by- Hop scheduling

- **RPL :**

- RPL stands for Routing protocol for Low Power and Lossy Networks.
- It’s a wireless Networks routing protocol.
- In present interconnected world, Low-power Lossy Networks play a crucial role.
- It enabling efficient communication for devices in resource constrained environments.
- RPL allows devices inside an LLN to communicate with one another.
- By using LLN, it difficult for traditional routing protocols to operate effectively RPL solve this issue.
- RPL is a distance vector routing protocol. It create Destination oriented Directed Acyclic Graph (DODAG).

- **Modes of RPL :**
- It defines two modes :
- 1. Storing mode.
- 2.Non-storing mode.
- RPL protocol implemented using the contaki OS
- It’s majorly focus on IoT devices.
- **Benefits :**
- 1.Scalability
- 2.Adaptive
- 3.Multipoint- to- point traffic
- Energy efficiency
- Security.

- **Directed Acyclic Graph :**



ND :

- The "ND protocol in IoT" refers to the Neighbor Discovery (ND) protocol, a core component of the IPv6 suite, and its specific applications and optimizations for Internet of Things (IoT) devices.
- ND is used to find neighboring devices, resolve their addresses, and handle automatic configurations, making it critical for the operation of modern, IPv6-based IoT networks.
- ND replaces several IPv4 protocols, including Address Resolution Protocol (ARP), ICMP Router Discovery, and ICMP Redirect. It uses a series of Internet Control Message Protocol for IPv6 (ICMPv6) messages to provide the following functions for local network communications:

ND :

- **Address Resolution:** Maps a neighbor's IPv6 address to its hardware (MAC) address. This is done through Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.
- **Router Discovery:** Allows devices to locate routers on an attached network link. Hosts send Router Solicitation (RS) messages, and routers respond with Router Advertisements (RA).
- **Stateless Address Autoconfiguration (SLAAC):** Enables a device to automatically configure its own IPv6 address using information from Router Advertisement messages, without needing a DHCP server.
- **Neighbor Unreachability Detection (NUD):** Determines when a neighbor is no longer reachable, improving the robustness of packet delivery.
- **Duplicate Address Detection (DAD):** Verifies that a newly assigned IPv6 address is unique on the link before it is used.
- **Redirect Function:** Informs hosts of a better next-hop router for a specific destination, optimizing network paths.

ND adaptations for IoT (6LoWPAN-NDP):

- Standard ND is too chatty and power-intensive for many low-power IoT devices. The Internet Engineering Task Force (IETF) has adapted ND for use in constrained environments, such as those that use the IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) standard. This optimized protocol, 6LoWPAN-NDP, features:
- **Reduced Multicast Flooding:** Minimizes the use of multicast messages to conserve network bandwidth and device battery life. It avoids periodic Router Advertisements in favor of on-demand discovery.
- **Role-Based Behavior:** Defines a client-server relationship where a sensor node acts as a client requesting an address from an IoT middleware or gateway that acts as a router.
- **Sleep Mode Support:** Allows low-power devices to sleep and only participate in the ND process when necessary, reducing energy consumption.

Advantages in NDP

- **Simplified Network Configuration:** They also noted that SLAAC enables devices to set themselves spontaneously while not requiring a user or a DHCP server.
- **Scalability:** However, they are suitable for large-scale network environments especially if frequent maintenance is not feasible.
- **Enhanced Security:** SEND is a SPD that can be used to protect neighbor discovery processes included in NDP.
- **Seamless Mobility:** It conveniences means that Devices can have portable connectivity from one network to another by using the dynamic address configuration.

DHCP:

- DHCP is a crucial protocol in IoT because it automates the process of assigning IP addresses and other network settings to a vast number of devices, making it easy for them to connect to a network without manual configuration.
- It provides scalability and seamless connectivity for devices like sensors, smart appliances, and industrial controllers by dynamically managing IP address allocation and preventing conflicts.
- However, standard DHCP in IoT can be vulnerable to security threats like rogue servers and DHCP starvation attacks, leading to the development of more robust security solutions for IoT environments. .

How DHCP works in IoT

- Automatic configuration: DHCP servers automatically provide devices with an IP address and other configuration parameters, such as a subnet mask and default gateway. This eliminates the need for manual setup on each device.
- Scalability: The ability to automatically assign addresses is vital for the large scale of IoT deployments, where thousands or millions of devices may need to connect to the network.
- Device mobility: As devices move within a network, DHCP ensures they can maintain consistent network settings without manual reconfiguration.
- Dynamic address assignment: DHCP manages a pool of available IP addresses, leasing them to devices as they connect and reclaiming them when they disconnect, which is essential for efficiency.

Security concerns in IoT

- Vulnerability to attacks: The lack of strong authentication in standard DHCP makes IoT networks susceptible to attacks where a malicious server can provide false configuration details.
- Rogue DHCP servers: Malicious actors can set up rogue DHCP servers to intercept traffic or redirect devices to malicious sites.
- DHCP starvation: An attacker can flood the network with bogus requests to exhaust the DHCP server's address pool, preventing legitimate devices from joining the network.

Modern solutions for secure DHCP in IoT

- To address these security vulnerabilities, new security protocols are being developed that incorporate methods like blockchain technology and advanced encryption to authenticate both clients and servers.
- For example, some advanced models use blockchain technology to create a secure and decentralized registry of valid IoT devices, helping to combat internal and external threats to the DHCP protocol.
- The Internet Engineering Task Force (IETF) is also developing new protocols, such as DHCP for IoT, which is designed to meet the unique needs of resource-constrained IoT devices.