UNIT – III:

WLAN and WAN Protocols: Low power wide area networking technologies, IEEE 802.11: IEEE 802.11 suite of protocols and comparison, architecture, spectrum allocation, modulation and encoding techniques, MIMO, packet structure, operation, security Long-range Communication Systems and Protocols: Cellular Connectivity-LTE, LoRa and LoRaWAN, Sigfox

IEEE 802.11 suite of protocols and comparison

The IEEE 802.11 is a suite of protocols with a rich history and different use cases.

802.11 is the specification defining the Media Access Controller (MAC) and physical layer (PHY) of a networking stack.

IEEE 802.11 standard, popularly known as Wi-Fi (Wireless Fidelity), lays down the architecture and specifications of wireless LANs (WLANs).

Wi-Fi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN.

Users connected by WLANs can move around within the area of network coverage.

The success of IEEE802.11 can be attributed to the layered stack approach of the OSI model.

Simply replacing the MAC and PHY layers with IEEE802.11 layers allowed existing TCP/IP infrastructure to seamless be used. Today, nearly every mobile device, notebook, tablet, embedded system, toy, and video game incorporate an IEEE802.11 radio of some kind.

The IEEE LAN/MAN Standards Committee maintains and governs the IEEE 802 specification(s). The original 802.11 goal was to provide a link layer protocol for wireless networking. This evolved from the 802.11 base specification to 802.11ac in 2013. Since then, the working group has focused on other areas.

Specific 802.11 variants have been examined for use cases and segments such as low power/low bandwidth IoT interconnect (802.11ah), vehicle-to-vehicle communication (802.11p), reuse of television analog RF space (802.11af), extreme bandwidth near meter communication for audio/video (802.11ad).

The new variants are designed for different areas of the RF spectrum or to reduce latency and improve safety for vehicular emergencies.

IEEE 802.11 Protocol	Features/ Use Case
802.11	First 802.11 design
802.11a	Release simultaneously with 802.11b Less prone to interference than 802.11b
802.11b	Release simultaneously with 802.11a Significant speed increase over 802.11a at improved range
802.11g	Speed increase over 802.11b
802.11n	Multiple antenna technology for improved speed and range
802.11ac	Better performance and cover over 802.11n. Wider channel and improved modulation
802.11ah	“Wi-Fi HaLow” Designed for IoT and Sensor networks Very low power and wider range
802.11p	“Wireless Access in Vehicular Environments” “Intelligent Transport Systems” Dedicated Short Range Communication Transport Use cases:

	Toll collection, Safety and collision emergencies, vehicular networking
802.11af	"White Wi-Fi" or "Super Wi-Fi" Deploy unused spectrum in TV bands to provide connectivity
802.11ad	WiGig Alliance 60 GHz Wireless for HD video and projectors Audio and video transport and cable replacement
802.11ax	"High Efficiency Wireless (HEW)" Next gen 802.11 4x increase in capacity over 802.11ac Backwards compatible to 802.11a/b/g/n/ac Dense deployment scenarios

Understanding:

1. Explain IEEE 802.11?

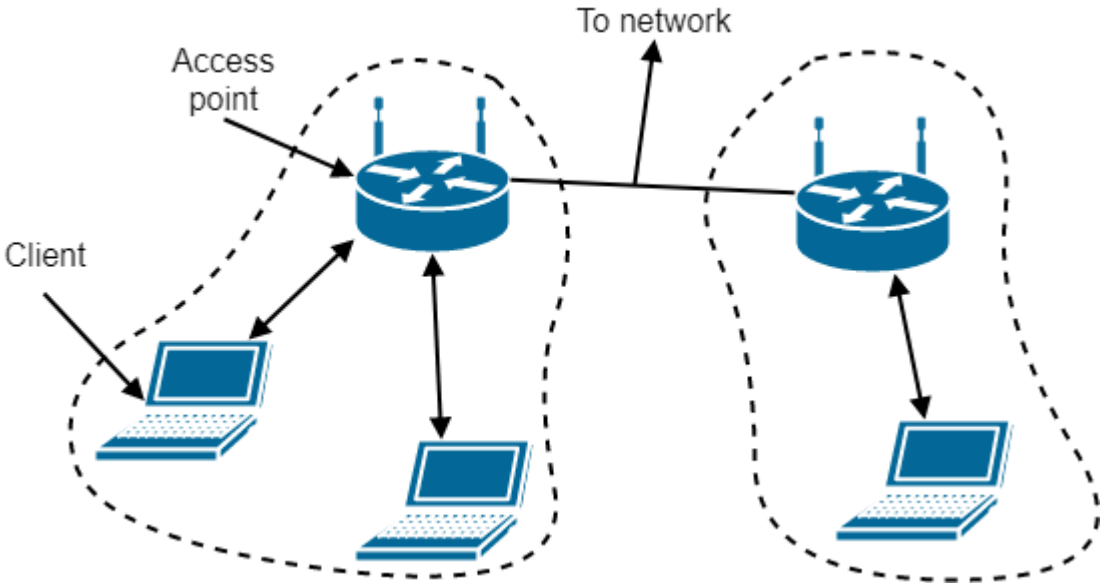
2. Compare IEEE 802.11 suite of protocols?

IEEE 802.11 Architecture

802.11 networks can be used in two modes: infrastructure mode and ad-hoc mode

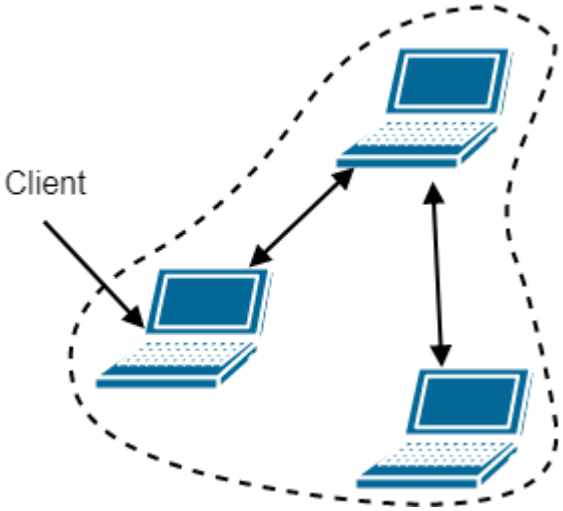
Infrastructure mode uses an AP (Access Point) that is connected to the network. Clients send and receive packets via the AP. Several APs can be connected to form an extended network

802.11 architecture in infrastructure mode

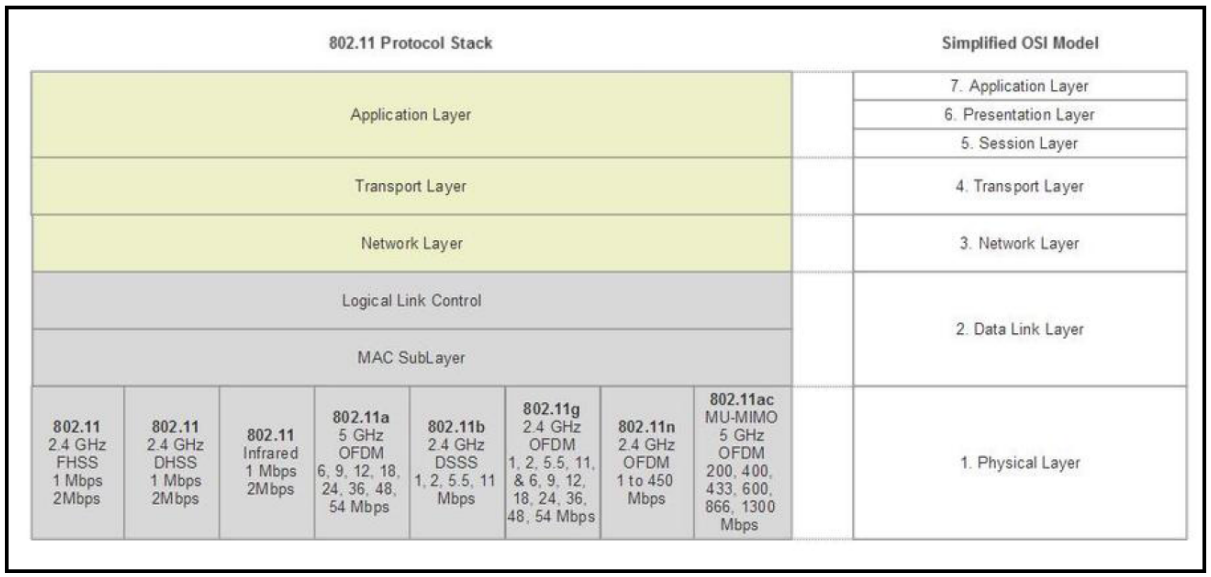


Ad-hoc mode is a collection of computers connected to each other so that they can send frames to each other. There's no AP

802.11 architecture in ad-hoc mode



From a stack perspective, the 802.11 protocols reside in the link layer (one and two) of the OSI model, as shown in the following figure:



The 802.11 physical layer corresponds to the OSI physical layer, but the data link layer is split into multiple sublayers. The stack includes various PHYs from older 802.11 specifications such as the 802.11 original PHYs (including infrared), a, b, g, and n. This is to ensure backward compatibility across networks.

In 802.11 the MAC sublayer determines which channel gets to transmit next. The sublayer above, the LLC (Logical Link Layer), hides the differences between the varying 802.11 versions for the network layer.

The functions of MAC layer include:

- Channel allocation
- Protocol data unit (PDU) addressing
- Frame formatting
- Error checking
- Fragmentation
- Reassembly

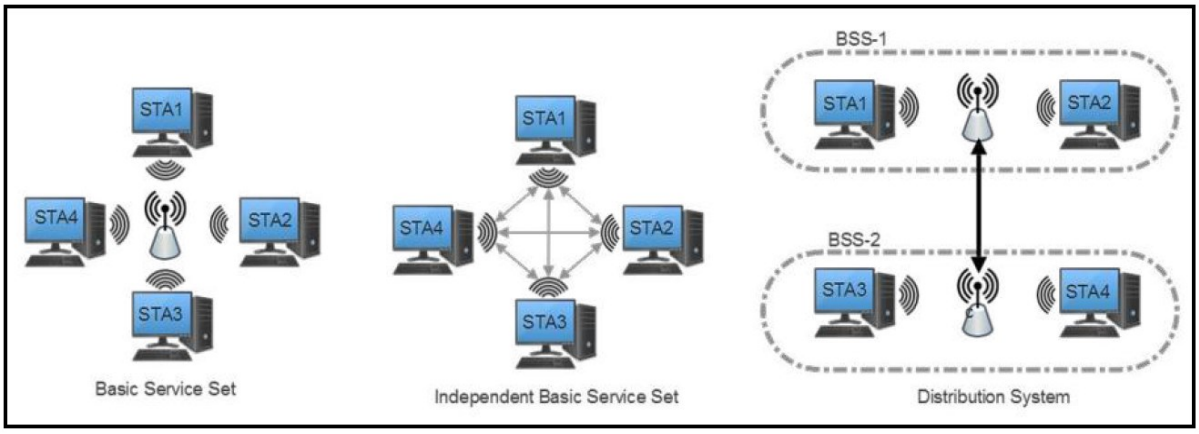
The LLC sublayer acts as an interface between the media access control (MAC) sublayer and the network layer.

The LLC sublayer is primarily concerned with:

- Multiplexing protocols transmitted over the MAC layer (when transmitting) and decoding them (when receiving).
- Providing node-to-node flow and error control

802.11 systems support three basic topologies

Below are examples of the three basic topologies of an IEEE 802.11 architecture:



1. Infrastructure: In this form, a Station (STA) refers to an 802.11 endpoint device (like a Smartphone) that communicates with a central access point (AP). An AP can be a gateway to other networks (WAN), a router, or a true access point in a larger network. This is also known as Infrastructure Basic Set Service (BSS). This topology is a star topology.

2. Ad hoc: 802.11 nodes can form what is called an Independent Basic Set Service (IBSS) where each station communicates and manages the interface to other stations. No access point or a star topology is used in this configuration. This is a peer-to-peer type of topology.

3. Distribution system (DS): The DS combines two or more independent BSS networks through access point interconnects.

In total, the 802.11 protocol allows for up to 2007 STAs to be associated with a single access point.

Understanding:

1. Explain the architecture of IEEE 802.11?

-Modes

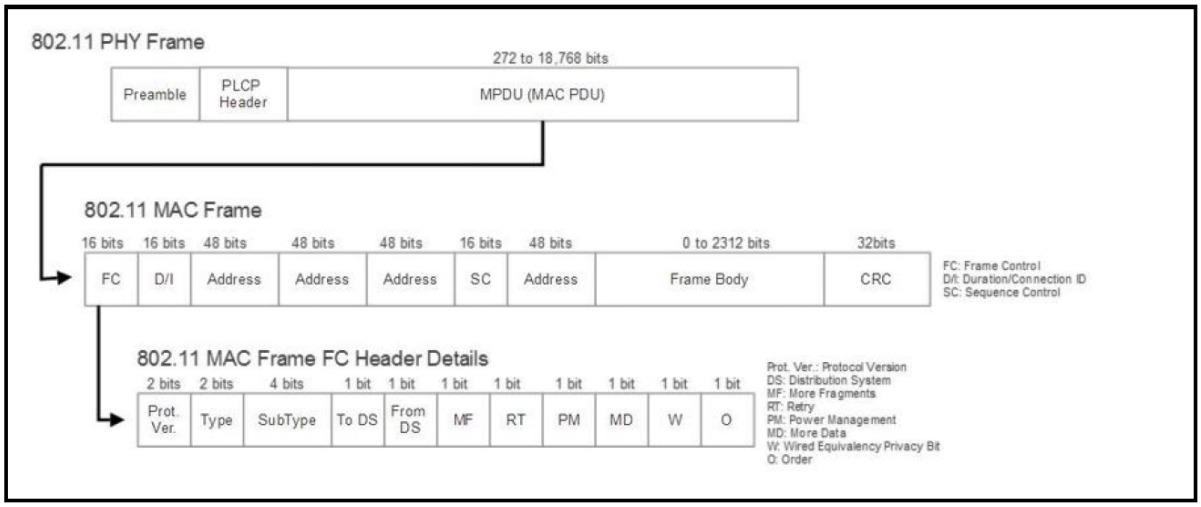
-Protocol Stack

-Topologies

IEEE 802.11 packet structure

802.11 uses the typical packet structure with headers, payload data, frame identifiers, and so on. Starting with the PHY frame organization, we have three fields: a preamble, which assists in the synchronization phase, a Physical Layer Convergence Protocol (PLCP) header, which describes the packet configuration and characteristics such as data rates, and the MPDU (MAC Protocol Data Unit).

The following illustration is the 802.11 PHY and link layer packet frame structure:



Preamble includes a short training field (two symbols) and a long training field (two symbols). These are used by the subcarriers for timing sync and frequency estimation. Additionally, the preamble includes a signal field that describes the data rate, length, and parity. The signal determines how much data is being transmitted in that particular frame.

The PLCP Header: contains information needed on both PHY and MAC layers.

The MAC frame contains the plurality of representative fields.

The frame control (FC field) subfields are detailed as follows:

Protocol version: Indicates version of the protocol used.

Type: WLAN frame as control, data, or management frame type.

Subtype: Further delineation of frame type.

ToDS and FromDS: Data frames will set one of these bits to 1 to indicate if the frame is headed to a distribution system.

More fragments: If a packet is divided into many frames, then every frame except the last will have this bit-set.

Retry: Indicates a frame was resent and assists in resolving duplicate frames being transmitted.

Power management: Indicates the power state of the sender. APs cannot set this bit.

More data: An AP will use this bit to assist when STAs are in a power save mode. This bit is used to buffer frames in a distribution system.

Wired equivalent privacy: Set to a 1 when a frame is decrypted.

Order: If a strict order mode is used in the network this bit will be set. Frames may not be sent in-order and strict order mode forces in-order transmission.

Moving up the MAC frame from the frame control field, we first examine the duration/connection ID bit:

Duration/connection ID: Indicates duration, contention-free period, and association ID. The association ID is registered during Wi-Fi initial handshaking.

Address fields: 802.11 can manage four MAC addresses in the following order:

Address 1: Receiver

Address 2: Transmitter

Address 3: Used for filtering

SC: Sequence control is a 16-bit field for message order

UNIT-II

Protocols for IoT Eco System: Layered Architecture for IoT, Protocol Architecture of IoT, Categorization of IoT protocols
WPAN Standards: 802.15 standards: Bluetooth, IEEE 802.15.4, Zigbee, Z-wave, Internet Protocol and Transmission Control Protocol, 6LoWPAN, Thread

Layered Architecture for IoT

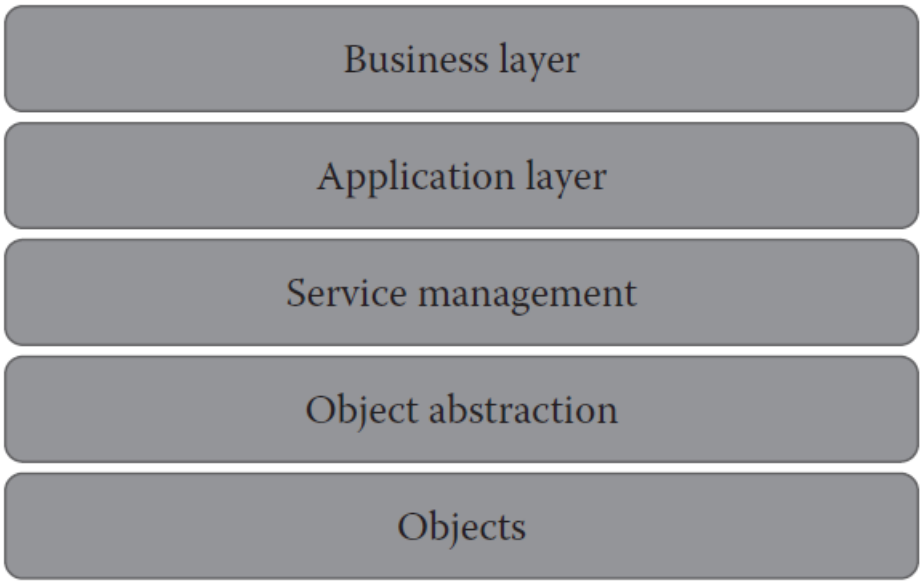
IoT Architecture enables the users to see an IoT system as a whole and what are the different components in the system.

IoT should have the capability to connect and transfer data among billions and trillions of devices.

For this to happen seamlessly, it is critical to have a layered architecture in place.

The architecture should be highly scalable and flexible to accommodate the wide gamut of components and technologies that form a part of the IoT ecosystem.

Layered architecture for IoT



The IoT architecture can be described using five layers. Each layer has its own function.

The different layers are as follows:

1. Objects layer
2. Object abstraction layer
3. Service management layer
4. Application layer
5. Business layer

1. Objects Layer

Objects layer, also known as devices layer, comprises the physical devices that are used to collect and process information from the IoT ecosystem.

Physical devices include different types of sensors such as those that are typically based on micro-electromechanical systems (MEMS) technology.

Sensors could be optical sensors, light sensors, gesture and proximity sensors, touch and fingerprint sensors, pressure sensors, and more.

Standardized plug and play mechanisms should be used by the objects layer in order to integrate and configure the heterogeneous types of sensors that belong to the IoT device ecosystem.

The device data that are collected at this layer are transferred to the object abstraction layer using secure channels.

2. Objects Abstraction Layer

This layer transfers data that are collected from objects to service management layer using secure transmission channels.

Data transmission can happen using any of the following technologies:

- ✓ RFID
- ✓ 3G
- ✓ GSM
- ✓ Wi-Fi
- ✓ Bluetooth low energy
- ✓ Infrared
- ✓ ZigBee

Specialized processes for handling functions such as cloud computing and data management are also present in this layer.

3. Service Management Layer

This layer acts as middleware for the IoT ecosystem.

This layer pairs specific services to its requester based on addresses and names.

This layer provides flexibility to the IoT programmers to work on different types of heterogeneous objects irrespective of their platforms.

This layer also processes the data that are received from the object abstraction layer.

After data processing, necessary decisions are taken about the delivery of required services, which are then done over network wire protocols.

4. Application Layer

This layer provides the diverse kinds of services requested by the customer.

The type of service requested by the customer depends on the specific use case that is adopted by the customer.

For example, if smart home is the use case under consideration, then the customer may request for specific parameters such as heating, ventilation, and air conditioning (HVAC) measurements or temperature and humidity values.

This layer provides the various types of smart services, which are offered by various IoT verticals.

Some of the prominent IoT verticals are as follows:

- ✓ Smart cities
- ✓ Smart energy
- ✓ Smart health care
- ✓ Smart buildings or homes
- ✓ Smart living
- ✓ Smart transportation
- ✓ Smart industry

5. Business Layer

This layer performs the overall management of all IoT activities and services.

This layer uses the data that are received from the network layer to build various components such as business models, graphs, and flowcharts.

This layer also has the responsibility to design, analyse, implement, evaluate, and monitor the requirements of the IoT system.

This layer has the capability to use big data analysis to support decision-making activities.

This layer also performs a comparison of obtained versus expected outputs to enhance the quality of services.

Summary of Layered Architecture of IoT

Business Layer	Manages the whole IoT System including applications, business models etc.,
Application Layer	Responsible for delivering application services to the users via user interfaces
Service Management	Stores, Analyses and Process data coming from the transport layer
Objects Abstraction	Transfers data from objects layer to service management layer
Objects	It is a Physical Layer which contains sensors to gather data

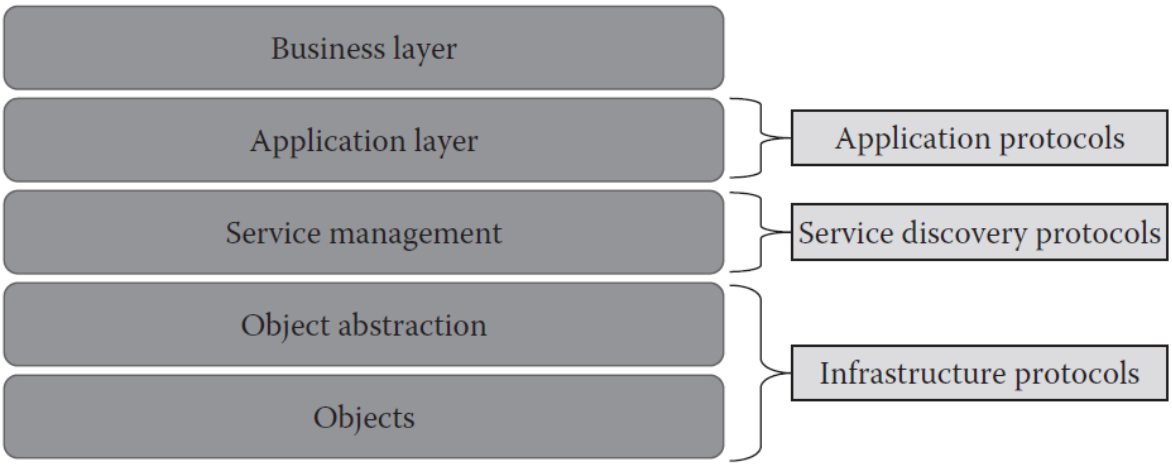
Protocol Architecture of IoT

A Protocol is a set of rules that governs the communication between two or more devices

The Protocol defines the rules, syntax, semantics and synchronization of communication and possible error recovery methods

The various protocols used for communication in the various layers of the IoT ecosystem are categorized as shown:

Protocol architecture of IoT



The protocols that are used in these five layers are divided into three categories:

1. Infrastructure Protocols

2. Service Discovery Protocols

3. Application Protocols

1. Infrastructure Protocols:

All the protocols involved in objects layer and object abstraction layer are called infrastructure protocols because they are actually related to infrastructure for building IoT

These protocols provide device to device communication and device to network communication

2. Service discovery Protocols

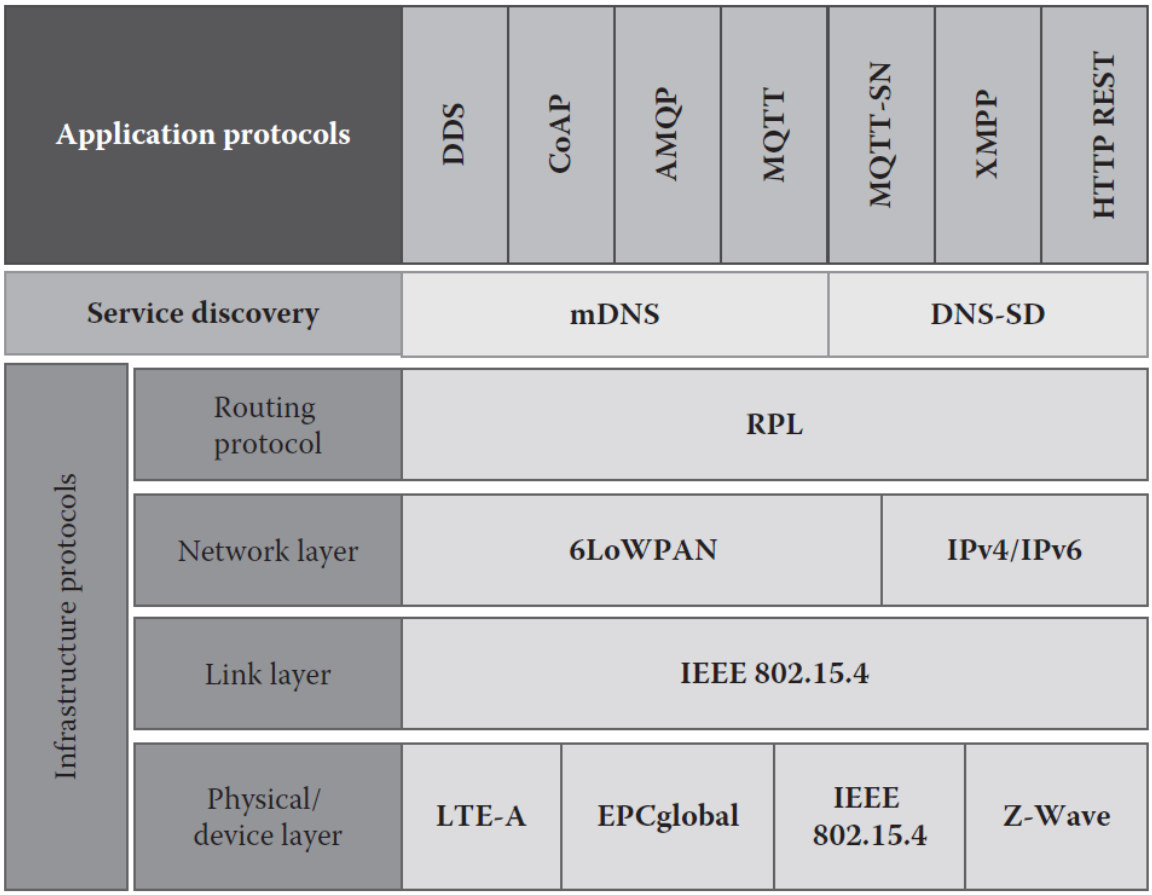
Protocols involved in Service Management layer are called Service Discovery Protocols since they provide some kind of service.

Service discovery is very important for an IoT eco system as it is important for IoT devices to advertise and use the services of other devices that are present in the IoT network

3. Application Protocols

Protocols that help in building different IoT applications

Categorization of IoT Protocols



Physical/ device layer

Deals with transfer of data bits

Examples:

1. LTE-A – Long Term Evolution Advanced

2. EPC Global – RFID Standard

Link Layer

Ensure data is transmitted properly without errors

Examples:

IEEE 802.15.4

Network Layer

This layer is responsible for sending IP (Internet Protocol) datagrams from source network to destination network. The datagrams contain source address and destination address. It performs addressing of communicating devices.

Examples:

IPv4/IPv6, 6LoWPAN

Routing Protocols

It performs routing of data packets

Example:

RPL-RIPPLE

-Routing data from gateway to cloud

-Routing data from one device to another device

Service Discovery Protocols

Protocols involved in Service Management layer are called Service Discovery Protocols since they provide some kind of service.

Service discovery is very important for an IoT eco system as it is important for IoT devices to advertise and use the services of other devices that are present in the IoT network

Example:

mDNS- Multicast Domain Name Service

DNS-SD- DNS Service Discovery

Application Protocols

Protocols that help in building different IoT applications

Example:

DDS- Data Distribution Service

CoAP- Constrained Application Protocol

AMQP- Advanced Message Queuing Protocol

MQTT- Message Queuing Telemetry Transport

MQTT-SN- MQTT for Sensor Networks

XMPP- Extensible Messaging and Presence Protocol

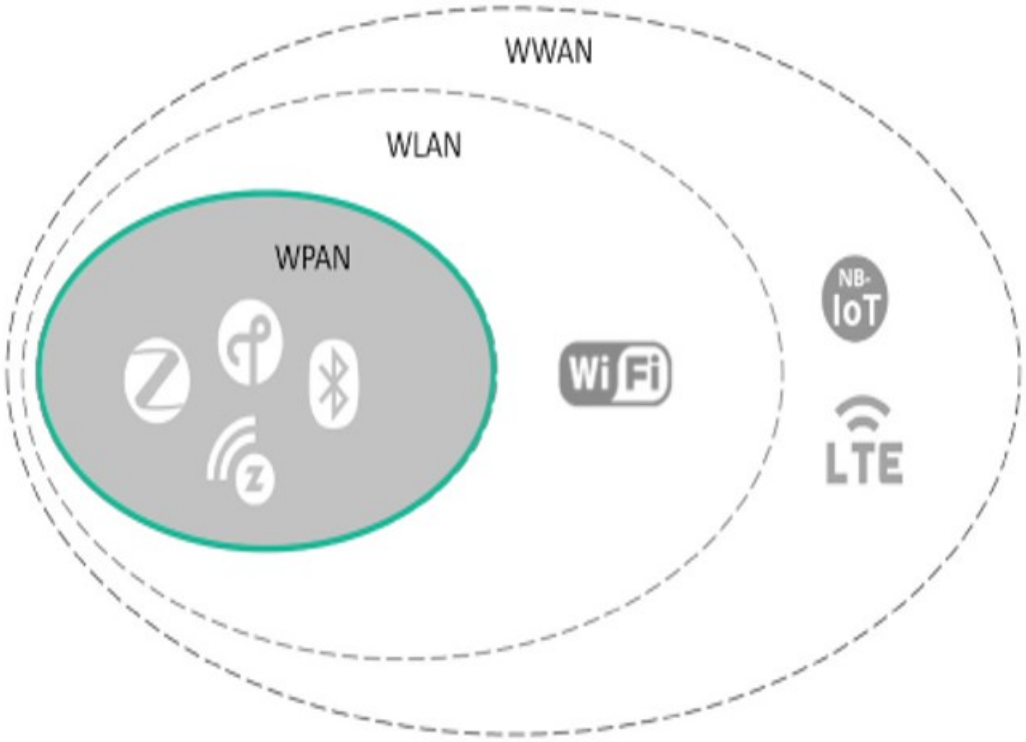
HTTP REST- Hyper Text Transfer Protocol Representational State Transfer

Understanding:

1. Explain the layered architecture of IoT?

2. Explain the Protocol architecture of IoT and categorize the IoT Protocols?

Classification of IoT Wireless Networks based on the size and location of the communication model



Wireless Personal Area Network (WPAN)

A Wireless Personal Area Network (WPAN) is meant to span a small area such as a private home or an individual workspace.

It is used to communicate over a relatively short distance. **ZigBee** and **Bluetooth** fall under this category.

Wireless local area networks (WLAN)

WLAN- Wireless local area networks are meant to span a relatively small area, e.g., a house, a building or a college campus.

Wi-Fi falls under this category.

Wireless wide area network (WWAN)

Wireless wide area network spans a large area, such as a city, state, or country.

It makes use of telephone lines and satellite dishes as well as radio waves to transfer data.

Non-IP Based WPAN

Introduction:

Sensors, and other things connected to the internet, need a method of transmitting and receiving information. This is the topic of **personal area network** (**PAN**) and near-range communication.
In an IoT ecosphere, communication to a sensor or actuator can be a copper wire or a **Wireless Personal Area Networks** (**WPANs**).
WPAN is the prevalent method for industrial, commercial, and consumer connections to the things of the internet.
Wire-based connectivity is still used, but primarily in legacy industries and areas that are not radio-frequency friendly.
There is a wide variety of different communication channels between the endpoint and the internet;

-some may be built on a **traditional IP stack** (Example: 6LoWPAN) and
-others use **non-IP (internet protocol)** communication to maximize energy savings (Example: BLE).

Non-IP communication systems are optimized for cost and energy usage, whereas IP-based solutions usually have fewer constraints (for example, 802.111 Wi-Fi).

Non-IP standards of communication operate in the near meter to about 200-meter range (although some can reach much further).

Understanding

Why we use non-IP based WPAN protocols in IoT?

Ans) To maximize energy saving
Example: BLE (Bluetooth Low Energy)

Explain the difference between non-IP based communication solutions and IP based Communication solutions for IoT?
Ans) Non-IP communication systems are optimized for cost and energy usage (for example Zigbee, BLE), whereas IP-based solutions usually have fewer constraints (for example, 802.111 Wi-Fi).

Explain the two important features of non-IP based communication standards?
Ans) 1. Optimized for cost and energy usage
2. Operate in the near meter to about 200-meter range

There are number of non-IP based WPAN protocols used in IoT. Each communication protocol has been adopted for certain reasons and use cases;

The following non-IP based WPAN protocols are investigated:

- Bluetooth,
- IEEE 802.15.4,
- Zigbee,
- Z-wave

All these non-IP based WPAN protocols are based upon IEEE 802.15 standards.

802.15 standards

The 802.15 group was initially formed to focus on wearable devices (coining the phrase personal area network).

Their work has expanded significantly and now focuses on higher data rate protocols, meter to kilometre ranges, and specialty communications.

Over one million devices are shipped each day using some form of 802.15.x protocol.

The following is a list of the various protocols, standards, and specifications that the IEEE maintains and governs:

- 802.15: Wireless personal area network definitions
- 802.15.1: Original foundation of the Bluetooth PAN
- 802.15.2: Coexistence specifications for WPAN and WLAN for Bluetooth
- 802.15.3: High data rate (55 Mbps+) on WPAN for multimedia
- 802.15.4: Low data rate, simple, simple design, multi-year battery life specifications (Zigbee)
- 802.15.5: Mesh networking
- 802.15.6: Body area networking for medical and entertainment
- 802.15.7: Visible light communications using structured lighting
- 802.15.8: Peer Aware Communications (PAC) infrastructure-less peer to peer at 10 Kbps to 55 Mbps
- 802.15.9: Key Management Protocol (KMP), management standard for key security
- 802.15.10: Layer 2 mesh routing, recommend mesh routing for 802.15.4, multi-PAN
- 802.15.12: Upper layer interface, attempts to make 802.15.4 easier to use 802.11 or 802.3

Understanding:

Explain the features of IEEE 802.15 standards?

Bluetooth

Bluetooth is a low-power wireless connectivity technology

WPAN IEEE 802.15.1 also called a Bluetooth Basic Rate (BR) is a global 2.4GHz specification working with short range wireless networking.

Bluetooth has been used extensively in IoT deployments for some time, being the principal device when used in low energy mode (LE) for beacons, wireless sensors, asset tracking systems, remote controls, health monitors, and alarm systems.

Versions of Bluetooth

Version	Features
Bluetooth 1.0 and 1.0B	Basic rate Bluetooth (1 Mbps) Initial version released.
Bluetooth 1.1	IEEE 802.15.1 standardized Received Signal Strength Indicator (RSSI)
Bluetooth 1.2	Adaptive Frequency hopping
Bluetooth 2.0	Enhanced Data Rate Mode (EDR): 3 Mbps
Bluetooth 2.1 (+EDR optional)	Improved resistance to radio frequency interference Low Power Consumption mechanisms Fast Transmission Speed
Bluetooth 3.0	Enhanced power control
Bluetooth 4.0 (BLE)	Bluetooth Low Energy Introduced Low Energy mode (LE) Introduced ATT and GATT protocols and profiles **Dual mode:** BR/EDR (Basic rate/Enhanced Data Rate) and LE mode Security manager with AES encryption
Bluetooth 4.1	Better alignments in Piconets timing when the transmission suffers interference
Bluetooth 4.2	Low energy is reinforced with the adoption of longer packet transmissions
Bluetooth 5.0	Improvements in transmission and receiving

Bluetooth 5 communication process and topologies

Bluetooth wireless is comprised of two wireless technology systems:
Basic Rate (BR) and
Low Energy (LE or BLE).

Nodes can either be advertisers or scanners by this definition:

Advertiser: Devices transmitting advertiser packets
Scanner: Devices receiving advertiser packets without the intention to connect
Initiator: Devices attempting to form a connection

There are several Bluetooth events that transpire in a Bluetooth WPAN:

1. Advertising: Initiated by a device to broadcast to scanning devices to alert them of the presence of a device wishing to either pair or simply relay a message in the advertisement packet.

2. Connecting: This event is the process of pairing a device and a host.

3. Periodic advertising: (for Bluetooth 5) allows an advertising device to periodically advertise over the 37 non-primary channels by channel hopping at an interval of 7.5ms to 81.91875s.

4. Extended advertising: (for Bluetooth 5) allows for extended Protocol Data Units (PDUs) to support advertisement chaining and large PDU payloads, possibly as well as new use cases involving audio or other multimedia

In LE mode, a device may complete an entire communication by simply using the advertising channel.

Alternatively, communication may require pair-wise bi-directional communication and force the devices to formally connect.
Devices that must form this type of connection will start the process by listening to advertising packets.
The listener is called an initiator in this case.
If the advertiser issues a connectable advertising event, the initiator can make a connection request using the same PHY channel it received the connectable advertising packet on.
The advertiser can then determine if it wishes to form a connection.
If a connection is formed, the advertising event ends and the initiator is now called the master and the advertiser is called the slave.

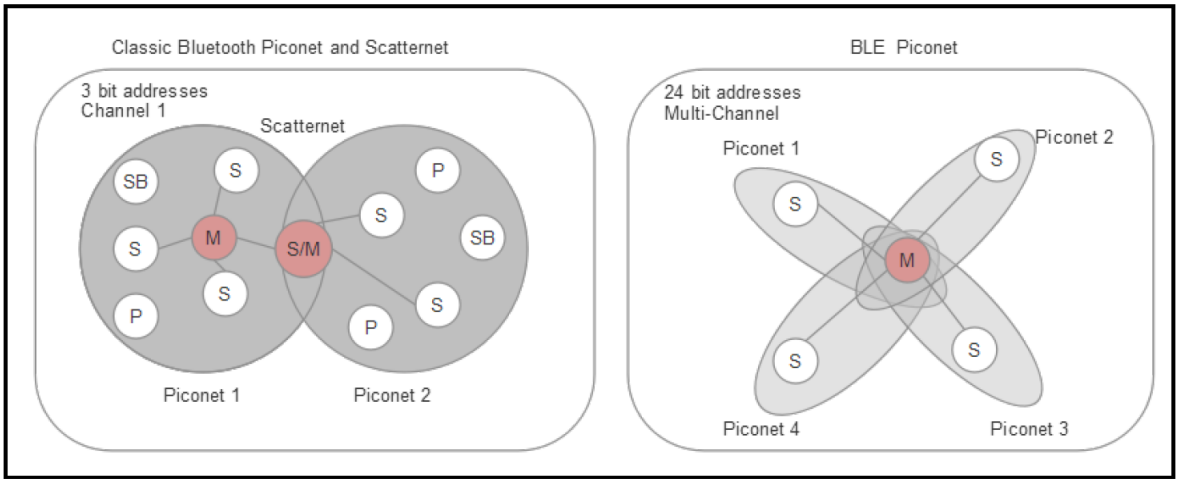
This connection is termed a piconet in Bluetooth jargon and connection events transpire.
The connection events all take place on the same starting channel between the master and slave.
After data has been exchanged and the connection event ends, a new channel can be chosen for the pair using frequency hopping.

Piconets form in two different fashions depending on BR/EDR mode or BLE mode.

In BR/EDR, the piconet uses **three-bit addressing** and can only reference seven slaves on **one piconet.**
Multiple piconets can form a union and then be called a scatternet, but there must be a second master to connect to and manage the secondary network.
The slave/master node takes on the responsibility of bridging two piconets together.
In BR/EDR mode, the network uses the same frequency hopping schedule and all the nodes will be guaranteed to be on the same channel at a given time.

In BLE mode, that system uses **24-bit addressing** so the number of slaves associated with a master is in the millions. Each master-slave relationship is itself a piconet and can be on a unique channel.

A piconet topology is illustrated in the following diagram:



In a piconet, nodes may be a master (M), slaves (S), standby (SB), or parked (P). Standby mode is the default state for a device. In this state, it has the option to be in a low-power mode. Up to 255 other devices can be in an SB or P mode on a single piconet.

Understanding:

Explain the difference between classic (BR/EDR) Bluetooth and BLE piconets?

Ans) In BR/EDR mode up to seven slaves can be associated on a single piconet due to 3-bit addressing. They all share a common channel between the seven slaves. Other piconets can join the network and form a scatternet only if an associated master on the secondary network is present.
In BLE mode millions of slaves can join in multiple piconets with a single master due to 24-bit addressing. Each piconet can be on a different channel but only one slave can associate with the master in each piconet. Practically speaking, BLE piconets tend to be much smaller.

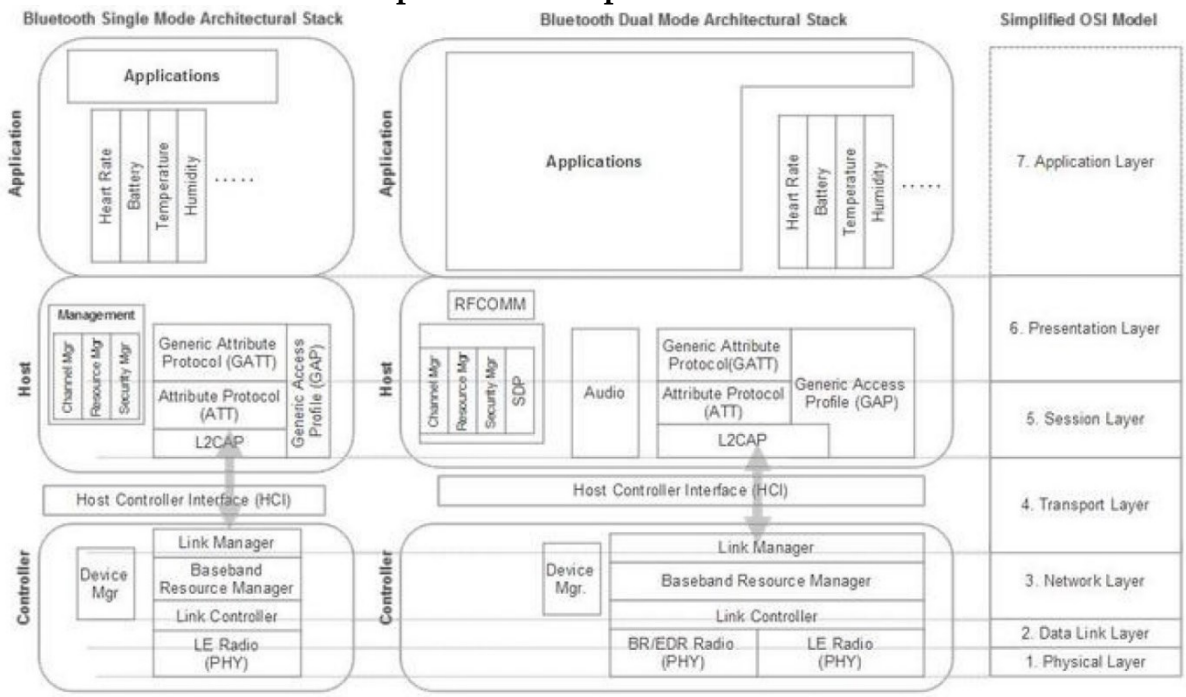
Bluetooth 5 stack

Bluetooth devices come in single and dual-mode versions, which means they either support only the BLE stack or they support classic mode and BLE simultaneously.

In the following figure, one can see the separation between the controller and host at the Host Controller Interface (HCI) level.

Bluetooth allows for one or more controllers to be associated with a single host.

Bluetooth Single Mode (BLE only) and Dual Mode (Classic and BLE) versus a comparison to simplified OSI stack



The stack consists of layers, or protocols and profiles:
Protocols: Horizontal tiers and layers representing functional blocks. The following diagram represents a stack of protocols.
Profiles: Represent vertical functions that use protocols.
There are essentially two Bluetooth modes of operation shown in the preceding figure (Each requiring a different PHY):
1. Low Energy (LE) mode:
This uses the 2.4 GHz ISM band and employs FHSS for interference protection.
The PHY differs from BR/EDR and AMP radios by modulation, coding, and data rates.
LE operates at 1 Msym/s at a bit rate of 1 Mbps.
Msym/s – Mega Symbols Per Seconds
Mbps – Mega Bits Per Second

Bluetooth 5 allows for multiple configurable data rates of 125 Kbps, 500 Kbps, 1 Mbps, and 2 Mbps

2. Basic Rate/Enhanced Data Rate mode (BR/EDR):

This uses a different radio than LE but operates in the ISM 2.4 GHz band.
Basic radio operation is rated at 1 Msym/s and supports a bit rate of 1 Mbps.
EDR sustains a data rate of 2 or 3 Mbps.
This radio uses FHSS for interference protection.

We will now detail the function of each element of the stack. We will start with the physical layer and move up the stack towards the application layer.

Core architectural blocks:

Controller level:

BR/EDR PHY (controller block): Responsible for transmitting and receiving packets through a physical channel on 79 channels.

LE PHY: Low energy physical interface responsible for managing 40 channels and frequency hopping.

Link controller: Encodes and decodes Bluetooth packets from the data payload.

Baseband resource manager: Responsible for all access to the radio from any source. Manages the scheduling of physical channels and negotiates access contracts with all entities to ensure Quality of Services (QoS) parameters are met.

Link manager: Creates, modifies, and releases logical links and updates parameters related to physical links between devices. It is reused for BR/EDR and LE modes using different protocols.

Device manager: Block in the controller baseband level that controls the general behaviour of Bluetooth. Responsible for all operations not related to data transmission, including making devices discoverable or connectable, connecting to devices, and scanning for devices.

Host Controller Interface (HCI): This is a separation between the host and the silicon controller in layer four of the network stack. It exposes interfaces to allow a host to add, remove, manage, and discover devices on the piconet

Host level:

L2CAP: This is the **logical link control and adaptation protocol**. It is used to multiplex logical connections between two different devices using higher level protocols than the physical layer. It can segment and reassemble packets.

Channel manager: Responsible for creating, managing, and closing L2CAP channels. A master will use the L2CAP protocol to communicate to a slave channel manager.

Resource manager: Responsible for managing the ordering of submission of fragments to the baseband level. Helps ensure the quality-of-service conformance.

Security Manager Protocol (SMP): Also known as security manager protocol. This block is responsible for generating keys, qualifying keys, and storing keys.

Service Discovery Protocol (SDP): Discovers services offered on other devices by UUID.

Audio: An optional efficient streaming audio playback profile.

RFCOMM: This block is responsible for RS-232 emulation and interfacing and is used for supporting telephony functionality.

Attribute protocol (ATT): When two devices are connected under a server and client association architecture, the server needs to maintain a set of attributes.
The ATT Protocol handles the attributes of this connection like the definition of data structure used to store the information managed by GATT that works on top of ATT. A wire application protocol used mainly in BLE (but can apply to BR/EDR). Optimized to run on BLE low power battery-based hardware. ATT is tightly coupled to GATT.

Generic Attribute Profile (GATT): This block represents the functionality of the attribute server and, optionally, the attribute client. The profile describes the services used in the attribute server. Every BLE device must have a GATT profile.

Generic Access Profile (GAP): Controls connections and advertising states. Allows a device to be visible to the outside world and forms the basis of all other profiles.

Understanding Bluetooth:

1. Versions of Bluetooth
2. Bluetooth Modes
    -BR/EDR Mode
    -LE Mode
3. Bluetooth 5 Communication Process and Topologies
4. Bluetooth 5 Protocol Stack (Role of each layer)

IEEE 802.15.4

The IEEE 802.15.4 is a standard wireless personal area network defined by the IEEE 802.15 working group.
IEEE 802.15.4 forms the basis of many other protocols including Thread, Zigbee, Wireless HART, and others.
802.15.4 only defines the bottom portion (PHY and data link layer) of the stack and not the upper layers. It is up to other consortiums and working groups to build a full network solution.
The goal of 802.15.4 and the protocols that sit on it are low-cost WPAN with low power consumption.

Understanding:
1. List the goal of IEEE 802.15.4
2. Give the example of any two protocols that uses IEEE 802.15.4 for defining Physical layer and MAC layer?

IEEE 802.15.4 architecture

The IEEE 802.15.4 protocol operates in the unlicensed spectrum in three different radio frequency bands: 868 MHz, 915 MHz, and 2.4 GHz.

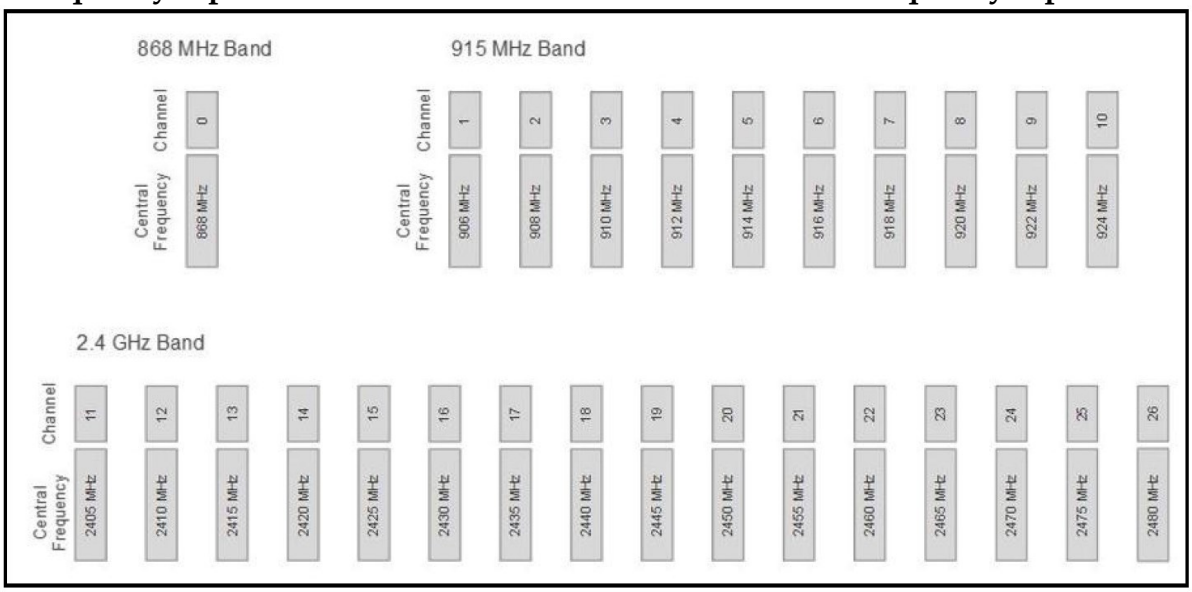
The intent is to have as wide a geographical footprint as possible, which implies three different bands and multiple modulation techniques.

While the lower frequencies allow 802.15 to have fewer issues with RF interference or range, the 2.4 GHz band is by far the most often used 802.15.4 band worldwide. **The higher frequency band has gained its popularity because the higher speed allows for shorter duty cycles on transmitting and receiving, thus conserving power**.

The typical range of an 802.15.4-based protocol is roughly 200 meters in an open-air, line-of sight test. Indoors, the typical range is roughly 30 m. Higher power transceivers (15 dBm) or mesh networking can be used to extend the range.

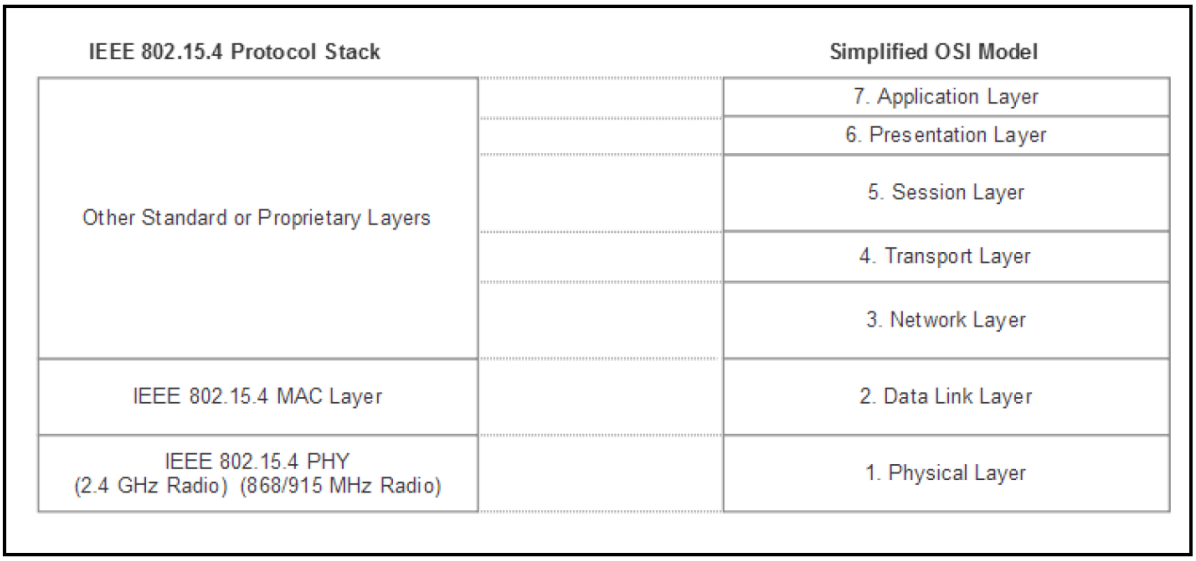
The following figure shows the three bands used by 802.15.4 and the frequency distribution.

IEEE 802.15.4 bands and frequency allocations. 915 MHz band uses a 2MHz frequency separation and the 2.4GHz band uses a 5 MHz frequency separation



To manage a shared frequency space, 802.15.4 and most other wireless protocols use some form of **Carrier Sense Multiple Access Collision Avoidance (CSMA/CA).**
Since it is impossible to listen to a channel while transmitting on the same channel, collision detection schemes don't work; therefore, we use collision avoidance. CSMA/CA simply listens to a specific channel for a predetermined amount of time. If the channel is sensed "idle", then it transmits by first sending a signal telling all other transmitters the channel is busy. If the channel is busy, then the transmission is deferred for a random period of time.
The data rate as state peaks at 250 kbps, as stated using the offset quadrature phase shift key.

IEEE 802.15.4 protocol stack as a comparison to the OSI model



In IEEE 802.15.4 Protocol Stack only PHY and MAC layers are defined, other standards and organizations are free to incorporate layers 3 to 7 above the PHY and MAC.
The protocol stack only consists of the bottom two layers of the OSI model (PHY and MAC).

Role of PHY Layer:
The PHY is responsible for symbol encoding, bit modulation, bit demodulation, and packet synchronization.
It also performs transmit-receiving mode switching and intra-packet timing/acknowledgment delay control.

Role of MAC Layer:
On top of the physical layer is the data link layer responsible for detecting and correcting errors on the physical link. This layer also controls the media access layer (MAC) to handle collision avoidance using protocols such as CSMA/CA. The MAC layer is typically implemented in software

The interface from the MAC to the upper layers of the stack are provided through two interfaces called the Service Access Points (SAP):
MAC-SAP: For data management
MLME-SAP: For control and monitoring (MAC layer management entity)

Understanding:

1. Explain the channel access scheme used in IEEE 802.15.4? (CSMA/CA)
2. What are the three frequency bands used by IEEE 802.15.4?
3. Why 2.4 GHz frequency band is preferred by IEEE 802.15.4?
4. Explain Protocol Stack of IEEE 802.15.4? (Diagram, role of PHY and MAC)
5. Name two interfaces used by IEEE 802.15.4 for interfacing form the MAC layer to upper layers of the stack?

Communication Process in IEEE 802.15.4

There are two types of communication in IEEE 802.15.4: **beacon and beaconless communication.**

Beacon Communication:

For a beacon-based network, the MAC layer can generate beacons that allow a device to enter a PAN as well as provide timing events for a device to enter a channel to communicate.

The beacon is also used for battery-based devices that are normally sleeping.

The device wakes on a periodic timer and listens for a beacon from its neighbours.

If a beacon is heard, it begins a phase called a Super Frame Interval where time slots are pre-allocated to guarantee bandwidth to devices, and devices can call for a neighbour node attention.

The Super Frame Interval (SO) and Beacon Interval (BO) are fully controllable by the PAN coordinator.

The Super Frame is divided into sixteen equally sized time slots with one dedicated as the beacon of that Super Frame.

Slotted CSMA/CA channel access is used in beacon-based networks.

The guaranteed time slots (GTS) can be assigned to specific devices preventing any form of contention.

Up to seven GTS domains are allowed.

The GTS slots are allocated by the PAN coordinator and announced in the beacon it broadcasts.

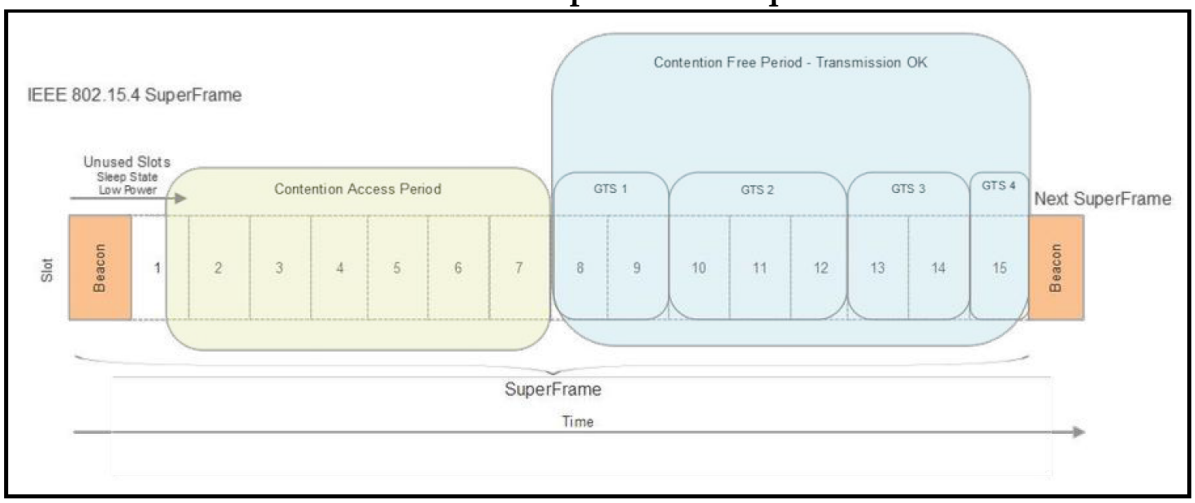
The PAN coordinator can change the GTS allocations on the fly dynamically based on system load, requirements, and capacity.

The GTS direction (transmit or receive) is predetermined before the GTS starts.

A device may request one transmit and/or one receive GTS.

The following figure illustrates a Super Frame consisting of 16 equal time slots bounded by beacon signals (one of which must be a beacon).

IEEE 802.15.4 Super Frame Sequence



The Super Frame has contention access periods (CAP) where there is crosstalk on the channel and contention free periods (CFP) where the frame can be used for transmission and GTS.
Contention Free Period will be further divided into Guaranteed Time Slots (GTS) and one or more GTSW may be allocated to a particular device. No other device may use that channel during a GTS.

Beaconless Communication:

In addition to beacon-based networking, IEEE 802.15.4 allows for beacon-less networking.
This is a much simpler scheme where no beacon frame is transmitted by the PAN coordinator.
It implies, however, that all nodes are in a receiving mode all the time.
This provides full-time contention access through the use of unslotted CSMA/CA.
A transmitting node will perform a clear channel assessment (CCA) in which it listens to the channel to detect if it's used and then transmit if clear.
CCA is part of a CSMA/CA algorithm and is used to "sense" if a channel is used.
A device can receive access to a channel if it is clear of other traffic from other devices (including non-802.15.4 devices).
In the event a channel is busy, the algorithm enters a "back-off" algorithm and waits a random amount of time to retry the CCA.
This mode will consume much more power than beacon-based communication.

Understanding:

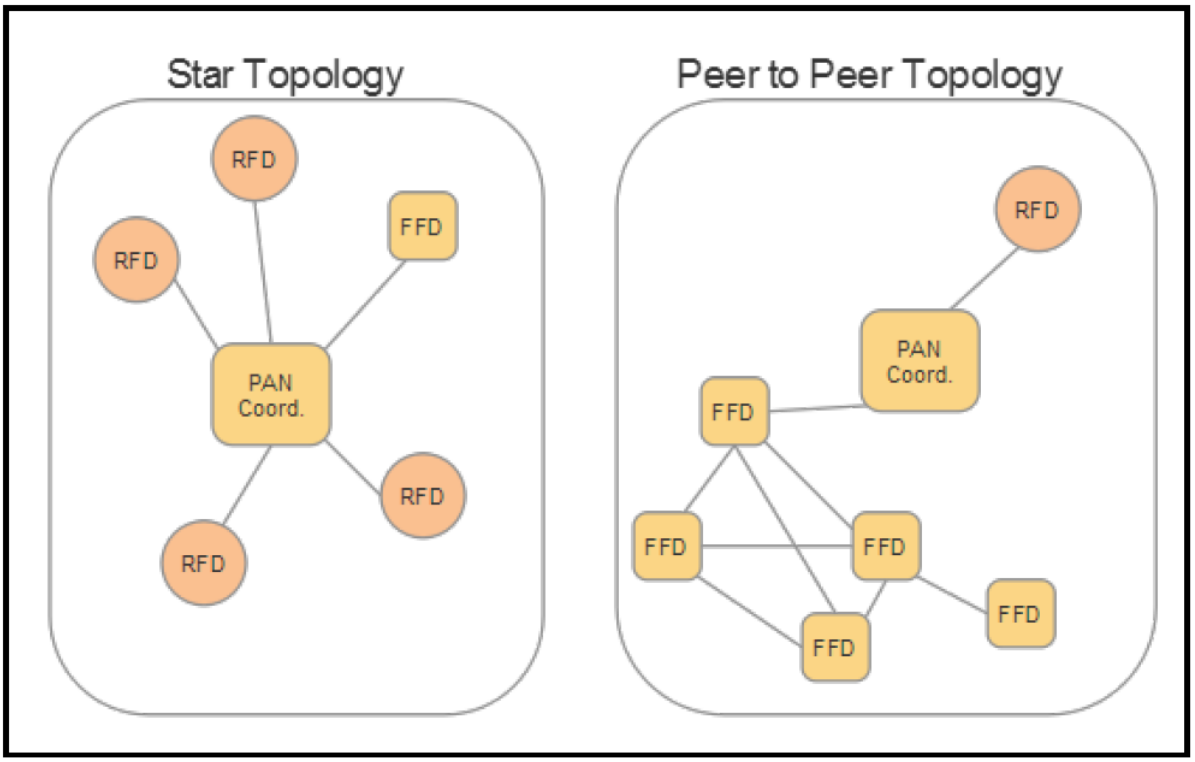
1. Explain Beacon and Beaconless Communication modes of IEEE 802.15.4?
2. Draw the format of IEEE 802.15.4 Super Frame Sequence?

IEEE 802.15.4 topology

There are two fundamental device types in IEEE 802.15.4:

Full function device (FFD): Supports any network topology, can be a network (PAN) coordinator and can communicate to any device PAN coordinator
Reduced function device (RFD): Limited to only a star topology, cannot perform as a network coordinator, can only communicate with a network coordinator

Diagram of a star versus peer-to-peer topology



The star topology is the simplest but requires all messages between peer nodes to travel through the PAN coordinator for routing. A peer-to-peer topology is a typical mesh and can communicate directly with neighbour nodes.

The PAN coordinator has a unique role that is to set up and manage the PAN. It also has the duty of transmitting network beacons and storing node information. Unlike sensors that may use battery or energy harvesting power sources, the PAN coordinator is constantly receiving transmissions and is usually on a dedicated power line (wall power). The PAN coordinator is always an FFD.
The RFD or even low power FFDs can be battery based. Their role is to search for available networks and transfer data as necessary. These devices can be put into a sleep state for very long periods of time.

IEEE 802.15.4 start-up sequence

IEEE 802.15.4 maintains a process for start-up, network configuration, and joining of existing networks.
The process is as follows:
1. Device initializes its stack (PHY and MAC layers).
2. PAN coordinator is created. Each network has only one PAN coordinator. The PAN coordinator must be assigned at this phase before proceeding.
3. The PAN coordinator will listen to other networks it has access to and derives a PAN ID (16-bit) that is unique to the PAN it will administer. It can do this over multiple frequency channels.
4. The PAN coordinator will choose a specific radio frequency to use for the network. It will do this using an energy detection scan where it scans the frequencies the PHY can support and listens to find a quiescent channel.
5. The network will be started by configuring the PAN coordinator and then starting the device in coordinator mode. At this point, the PAN coordinator can accept requests.
6. Nodes can join the network by finding the PAN coordinator using an active channel scan where it broadcasts a beacon request across all its frequency channels. When the PAN coordinator detects the beacon, it will respond back to the requesting device. Alternatively, in a beacon-based network, the PAN coordinator will routinely send out a beacon and the device can perform a passive channel scan and listen for the beacon. The device will then send an association request.
7. The PAN coordinator will determine if the device should or can join the network. This could be based on access control rules, or even if the PAN coordinator has enough resources to manage another device. If accepted, the PAN coordinator will assign a 16-bit short address to the device.

Understanding:

1. Explain the topology of IEEE 802.15.4 and illustrate the role of each device?

2. Distinguish between FFD and RFD in IEEE 802.15.4?

3. List the start-up sequence of IEEE 802.15.4?

Zigbee

Zigbee is a **WPAN protocol based on the IEEE 802.15.4 foundation** targeted for commercial and residential IoT networking that is **constrained by cost, power, and space.**

The Zigbee Alliance maintains and publishes standards for the protocol, organizes working groups, and manages the list of application profiles. The IEEE 802.15.4 defines the PHY and MAC layers, but nothing above.

ZigBee is a standards-based network protocol supported solely by the ZigBee Alliance that uses the transport services of the IEEE 802.15.4 network specification.

The IEEE 802.15.4 is a set of standards that

define power management,
addressing,
error correction,
message formats, and
other point-to-point

specifics necessary for proper communication to take place from one Radio to another.

Important Features of Zigbee

1. Zigbee is Highly reliable
2. Zigbee is cost effective
3. Zigbee is highly secure
4. Zigbee is low power
5. Zigbee is an open global standard

Understanding:

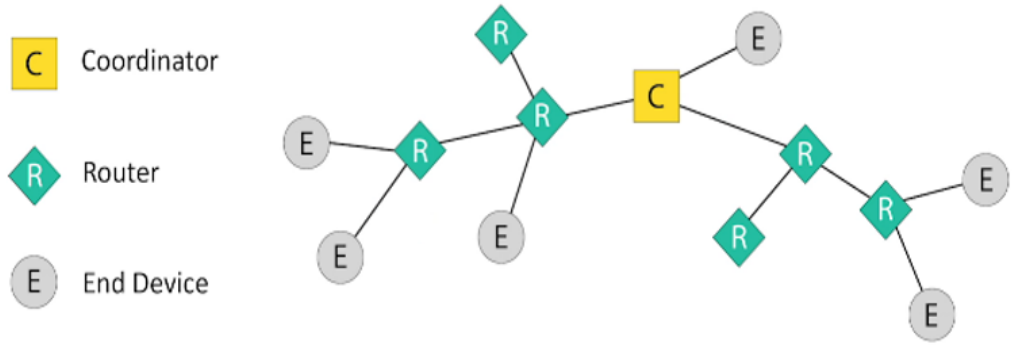
1. Define Zigbee?

2. What is the role of IEEE 802.15.4 in Zigbee?

3. List the important features of Zigbee?

Device roles in Zigbee

Zigbee can form networks, discover devices, provide security, and manage the network.
Zigbee is essentially a mesh network, it is self-healing and ad hoc in form.



There are three principal components in a Zigbee network.

1. Zigbee controller (ZC): Highly capable device on a Zigbee network that is used to form and initiate network functions. Each Zigbee network will have a single ZC that fulfils the role of an 802.15.4 2003 PAN coordinator (FFD). After the network is formed, the ZC can behave as a ZR (Zigbee router). It can assign logical network addresses and permit nodes to join or leave the mesh.

2. Zigbee router (ZR): This component is optional but handles some of a load of mesh network hopping and routing coordination. It too can fulfil the role of an FFD and has an association with the ZC. A ZR participates in multi-hop routing of messages and can assign logical network addresses and permit nodes to join or leave the mesh.

3. Zigbee end device (ZED): This is usually a simple endpoint device such as a light switch or thermostat. It contains enough functionality to communicate with the coordinator. It has no routing logic; therefore, any messages arriving at a ZED that are not targeted to that end device are simply relayed.

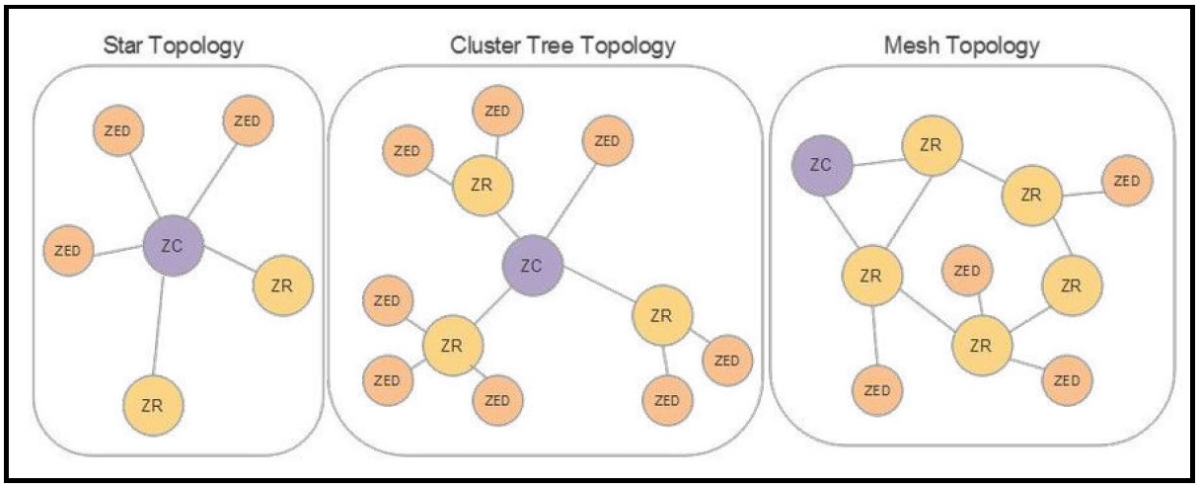
Zigbee targets three different types of data traffic.

1. Periodic data is delivered or transmitted at a rate defined by the applications (for example, sensors periodically transmitting).
2. Intermittent data occurs when an application or external stimulus occurs at a random rate. A good example of intermittent data suitable for Zigbee is a light switch.
3. The final traffic type Zigbee serves is repetitive low latency data. Zigbee allocates time slots for transmission and can have very low latency, which is suitable for a computer mouse or keyboard.

Understanding:

1. Mention the Principal Components of Zigbee Network and role of each component?
2. Explain the types of data traffic supported by Zigbee?

Zigbee topologies



Zigbee supports three basic topologies:

Star network: A single ZC with one or more ZEDs. Only extends two hops and is therefore, limited in node distance. It also requires a reliable link with a single point of failure at the ZC.
Cluster tree: A multi-hop network that employs beaconing and extends the network coverage and range over a star network. ZC and ZR nodes can have children, but ZEDs remain true endpoints. Child nodes only communicate with their parent (like a small star network). Parents can communicate downstream to its children or upstream to its parent. The problem still exists with a single point of failure at the centre.
Mesh network: Dynamic path formation. Routing can occur from any source device to any destination device. Uses tree and table-driven routing algorithms. ZC and ZR radios must be powered at all times to perform routing duties, consuming battery life. The main advantage is the network can grow beyond the line of sight and has multiple redundant paths.

Understanding:

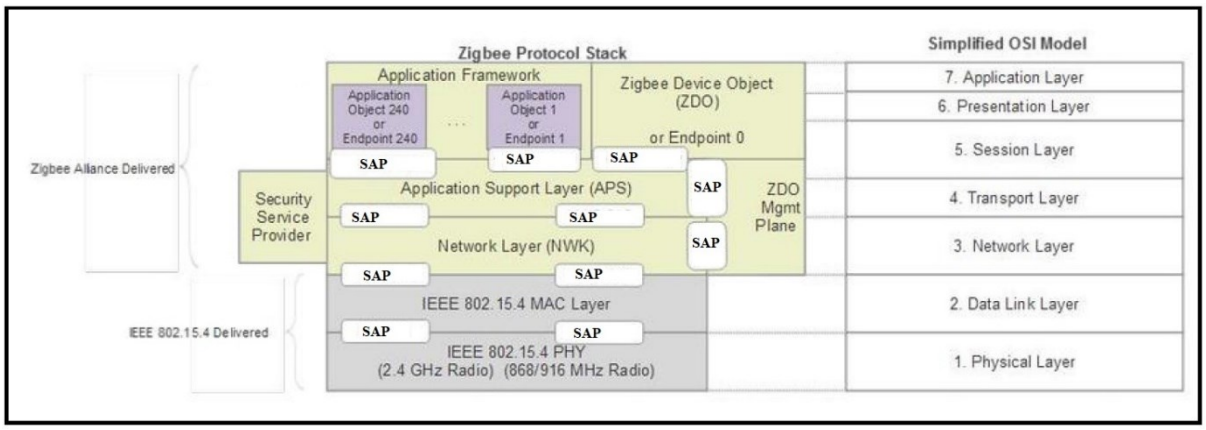
1. Explain the topologies supported by Zigbee Network?

2. Mention the limitation of Star and Cluster tree Topologies of Zigbee Network?

3. Mention the advantage of Mesh Network topology of Zigbee Network?

Zigbee protocol stack

The Zigbee protocol stack includes a network layer (NWK) and an application layer (APS). Additional components include a security service provider, a ZDO management plane, and a Zigbee device object (ZDO). The IEEE 802.15.4 defines the PHY and MAC layers.



SAP- Service Access Point

Each layer performs a specific set of services for the layer above it.
Each service is provided a way to interface to the upper layer through a service access point.
SAPs provide an API to isolate the inner workings of a layer from the layers above and below while allowing interfacing between layers.

Physical Layer

- Defining receiver sensitivity
- Handling channel rejection
- Optimizing output power
- Managing channels
- Defining transmission rate specifications
- Modulation of transmitted signal
- Demodulation of received signal

MAC Layer

- Responsible for reliable communication between the nodes
- Manages collision of signals
- Improve efficiency of communication
- Responsible for decomposing data packets and frames
- Responsible for assembling data packets and frames
- Responsible for managing data transactions between neighboring nodes only
- Handles network discovery, identification and packet synchronization
- Handles acknowledgement and implements collision avoidance techniques

Network Layer

- Responsible for mesh networking, broadcasting, routing and reliable data transmission
- Handles authentication, secure joining and graceful disconnection
- Handles payload encryption for the network frame

Application Support Sublayer (APS)

- Responsible for providing data services and device profiles
- Filters out duplicate messages sent by the network layer
- Keeps and updates a local binding table which keeps track of nodes the current node wishes to speak to (Facilitates intelligent routing)

Zigbee Device Object (ZDO)

- Defines device roles with in a network
- Handles the local and over the air network management
- Provides the services for network discovery

Application Framework

- Provides a framework for building and running applications
- Defines the description to build a Zigbee profile
- Provides different end points for different applications

Security Services

Defines methods for implementing security services such as

- Cryptographic key establishment
- Key transport
- Frame protection
- Device management

Understanding:

1. Explain the layered protocol stack of Zigbee and mention the role of each layer?

Z-Wave

Z-Wave is a WPAN protocol used for consumer and home automation primarily

Z-Wave is another mesh technology.

Important Features of Z-Wave

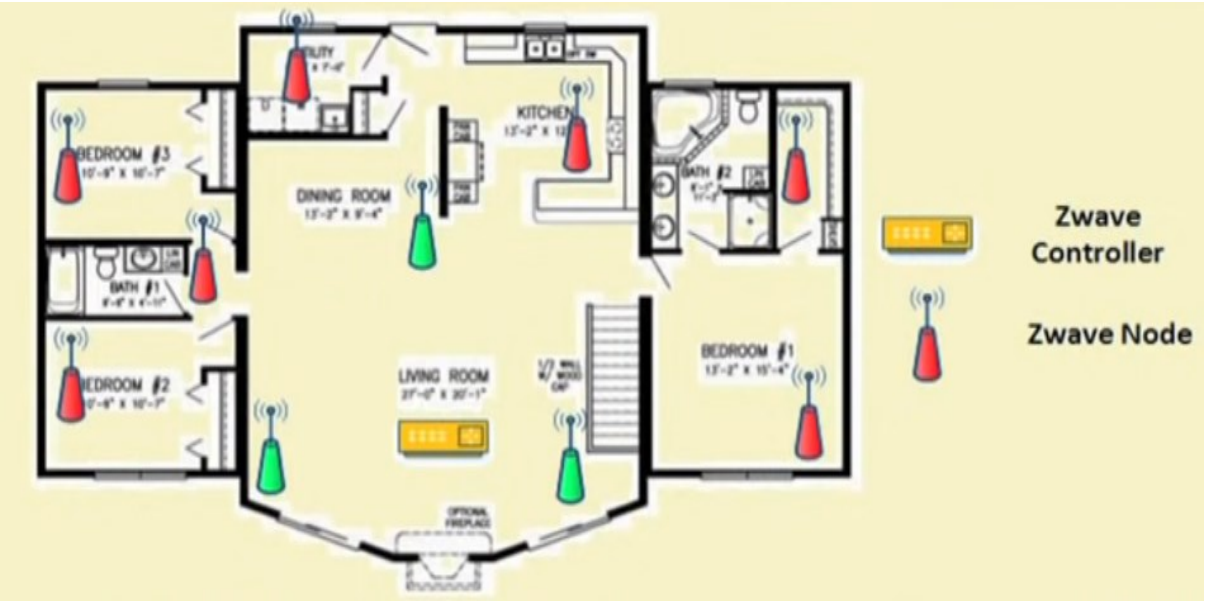
- **Modulation:** Gaussian Frequency Shift Keying (GFSK)
- **Channel Contention:** CSMA/CA

  "Nodes start in receive mode and wait a period of time before transmitting data if there is data being broadcast."
- **Topology:** Mesh Network Topology is the main mode of operation and can support 232 nodes in a network
- **Operating Frequency**
  - India- 865.2 MHz

Types of devices in a Z-Wave Network

There are primarily two kinds of devices in a Z-Wave Network

1. Controller device
   - Primary controller
   - Secondary controller
2. Slave device/node



Role of Controller

- This top-level device provides the routing table for the mesh network and is the host/master of the mesh under it.
- Z-Wave uses source routed network mesh topology using one primary controller

Primary Controller

- The primary controller is the master, and only a single master can exist in a network.
- It has the ability to maintain the network topology and hierarchy.
- It can also include or exclude nodes from the topology.
- It also has the duty of allocating node IDs.

Secondary Controller

- These nodes assist a primary controller with routing.

Slave device/node

- These devices perform actions based on commands they receive
- These devices cannot communicate with neighbor slave nodes unless instructed to do so via a command.
- Slaves can store routing information but do not compute or update routing tables.
- Typically, they will act as a repeater in a mesh.

Controller may be Portable and Static

- A portable controller is designed to move like a remote control.
- Once it has changed position, it will recalculate the fastest routes in the network.
- A static controller is intended to be fixed, such as a gateway plugged into a wall outlet.
- The static controller can always be "on" and receiving slave status messages.

Attributes of Controller

Controllers can also have different attributes within the network

- Status update controller (SUC)
- SUC ID server (SIS)
- Bridge controller
- Installer controller

Status update controller (SUC) and SUC ID server (SIS)

- The static controller also has the advantage of taking the role of status update controller.
    - In this case, it will receive notifications from a primary controller regarding topology changes.
- It can also assist in the routing of slaves.
- An SUC can also assist in including and excluding slaves for the primary.

Bridge controller

- This essentially is a static controller that has the ability to act as a gateway between the Z-Wave mesh and other network systems (for example, WAN or Wi-Fi).
- The bridge is allowed to control up to 128 virtual slave nodes.

Installer controller

- This is a portable controller that can assist in network management and quality-of-service analysis.

Attributes of Slave

Slaves also support different attributes

- Routing slave
- Enhanced slave

Routing slave

- Fundamentally a slave node but with the ability to send unsolicited messages to other nodes in the mesh.
- Typically, slaves are not allowed to send a message to another node without the command of a primary controller.
- The node stores a set of static routes that it uses when a message is sent.

Enhanced slave

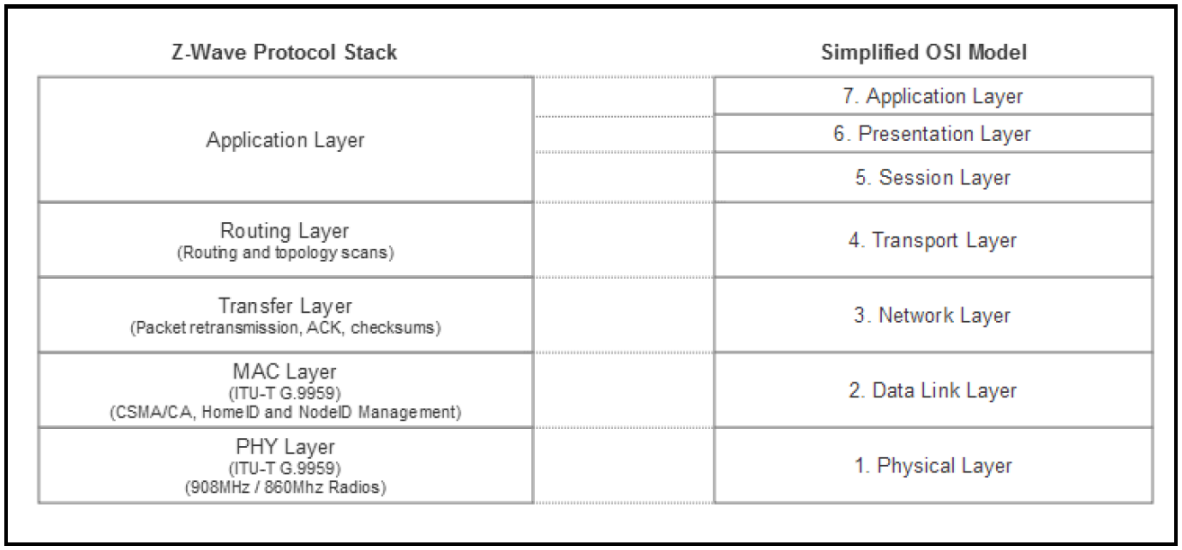
- These have the same abilities as a routing slave with the addition of a real-time clock and persistent storage for application data.
- An example might be a gas meter.

Understanding:

1. Define Z-Wave?
2. Important features of Z-Wave?
3. Role of different devices in Z-Wave Network?
4. Explain the attributes of controller and slave in a Z-wave network?

Z-Wave protocol stack

Because Z-Wave is a very low bandwidth protocol that is intended to have a sparse network topology, the protocol stack attempts to communicate in as few bytes per message as possible. The stack consists of five layers, as shown in the following figure:



PHY layer

- Defined by the ITU-T G.9959 Specification.
- This layer manages the signal modulation, channel assignment, and preamble binding at the transmitter and preamble synchronization at the receiver.

MAC layer

- This layer manages the HomeID and NodeID fields
- The MAC layer also uses a collision avoidance algorithm and backoff strategy to alleviate congestion and contention on the channel.

Transfer layer

- Manages the communication of Z-Wave frames.
- This layer is also responsible for the retransmission of frames as needed.
- Additional tasks include acknowledgment of transmissions and checksum binding.

Routing layer

- This provides routing services.
- Additionally, the network layer will perform a topology scan and update of the routing tables.

Application layer

- Provides the user interface to applications and data.

Understanding:

1. Explain the Z-Wave Protocol stack with role of each layer in the stack?

Z-Wave addressing

There are two fundamental addressing identifiers that need definition before proceeding:

- **Home ID:** This is a **32-bit** unique identifier that is preprogrammed in controller devices to assist with identifying Z-Wave networks from each other. During network start, all Z-Wave slaves have a home ID of zero and the controller will systematically populate the slave nodes with the correct home ID.
- **Node ID:** This is an **8-bit** value that is assigned to each slave by the controller and provides addressing of slaves in the Z-Wave network.

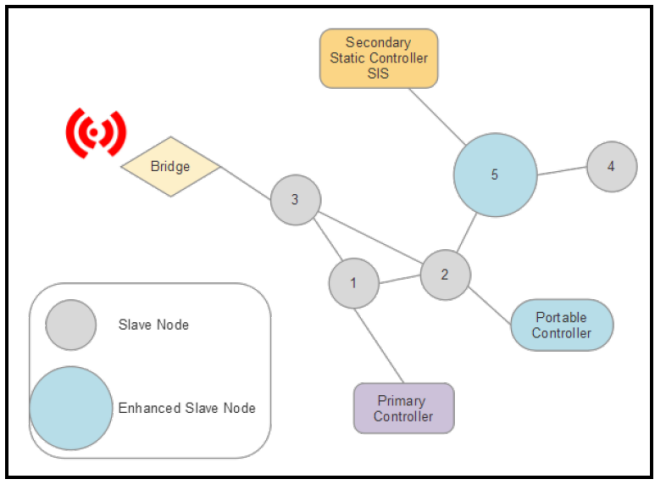
Pairing Process

- For a new Z-Wave device to be used on the mesh, it must undergo a pairing and adding process.
- The pairing process involves the primary controller assigning a home ID to the new node.

Z-Wave topology and routing

The bridge controller acts as a gateway to a WiFi network.
A Portable Controller and Secondary Controller also sits on the mesh for assistance to the Primary Controller.

Z-Wave topology including the single Primary Controller and four slaves and one enhanced slave



Routing Table

	Slave 1	Slave 2	Slave 3	Slave 4	Enhanced Slave 5	Primary Controller	Secondary SIS	Bridge	Portable Controller
Slave 1	0	1	1	0	0	1	0	0	0
Slave 2	1	0	1	0	1	0	0	0	1
Slave 3	1	1	0	0	0	0	0	1	0
Slave 4	0	0	0	0	1	0	0	0	0
Enhanced Slave 5	0	1	0	1	0	0	1	0	0
Primary Controller	0	0	0	0	0	0	0	0	0
Secondary SIS	0	0	0	0	1	0	0	0	0
Bridge	1	0	1	0	0	0	0	0	0
Portable Controller	0	1	0	0	0	0	0	0	0

Summary:

- **Objective:** Delivering IoT data from devices to the internet
    - **Step-1: Role of WPAN-** Connecting billions of devices is using the correct communication medium to reach sensors, objects, and actuators to cause some action
    - **Non-IP based WPAN (Don't communicate over TCP/IP)**
        - Bluetooth and BLE
        - IEEE 802.15.4
        - Zigbee
        - Z-Wave

Outcome:

- How as an architect we will measure the performance and behavior of a WPAN
- An architect should have an understanding of how these architectures compare and contrast

IP-Based WPAN

Internet protocol and transmission control protocol

Supporting an IP layer in a protocol stack does **consume resources**

- However, there are key benefits in **building an IoT system that allows devices to communicate over TCP/IP** (transmission control protocol/internet protocol).
- **Role of the architect:**
  - Balance the cost of these services and features against the impact on a system.

IP role in IoT

From an ecosystem point of view, regardless of the protocol used at a sensor level, the sensor data will ultimately be fed into a public, private, or hybrid cloud for analysis, control, or monitoring. Outside of the WPAN, the world is TCP/IP-based.

IP is the standard form of global communication for various reasons:

- **Ubiquity:** IP stacks are provided by nearly every operating system and every medium. IP communication protocols are capable of running on various WPAN systems, cellular, copper wire, fibre-optic, PCI Express, and satellite systems. IP specifies the exact format for all data communications and the rules used to communicate, acknowledge, and manage connectivity.
- **Longevity:** TCP was established in 1974, and the IPv4 standard still in use today was designed in 1978. It has withstood the test of time for 40 years. Longevity is paramount for many industrial and field IoT solutions that must support devices and systems for decades. Various other proprietary protocols have been designed by various manufacturers in those 40 years, such as AppleTalk, SNA, DECnet, and Novell IPX, but none have gained the market traction as well as IP.
- **Standards-based:** TCP/IP is governed by the Internet Engineering Task Force (IETF). The IETF maintains a set of open standards focused on the internet protocol.
- **Scalability:** IP has demonstrated scale and adoption. IP networks have demonstrated massive scaling to billions of users and many more devices. IPv6 could provide a unique IP address to every atom comprising Earth and still support 100 more worlds.
- **Reliability:** IP at its heart is a reliable protocol for data transmission. It accomplishes this through a packet delivery system based on a connectionless network. The service is considered unreliable from conception, meaning the data is not guaranteed to be delivered. IP is connectionless because each packet

is treated independently from one another. The IP is also referred to as best-effort delivery because all attempts will be made to transmit a packet through various routes. The strength of this model allows an architect to replace the delivery mechanism with another—essentially replacing layers one and two of the stack with something else (for example, Wi-Fi with cellular).

- **Manageability:** Various tools exist to manage IP networks and devices on an IP network. Modelling tools, network sniffers, diagnostic tools, and various appliances exist to assist in building, scaling, and maintaining networks.

The transport layer is also worth considering. While IP addresses the need for a well supported and robust network layer, TCP and Universal Datagram Protocol (UDP) are needed for the transport layer. The transport layer is responsible for end-to-end communication. The logical communication between different hosts and various network components is governed at this level. TCP is used for connection-oriented transmissions, whereas UDP is used for connectionless transmissions. UDP is naturally much simpler to implement than TCP, but not as resilient. Both services provide segment reordering as packets are not guaranteed to be delivered in order using an IP protocol. TCP also provides the layer of reliability to an unreliable IP network layer through the use of acknowledgment messages and retransmissions of lost messages. Additionally, TCP provides flow control using sliding windows and congestion avoidance algorithms. UDP provides a lightweight, high-speed method to broadcast data to various devices that may or may not be present or reliable.

From an IoT perspective, bringing IP close to the source of data bridges two worlds of data management. The Information Technology (IT) role manages the infrastructure, security, and provisioning of networks and things on the network. The Operational Technology (OT) role manages the health and throughput of the system that functions to produce something. These two roles have traditionally been separated, as things such as sensors, meters, and programmable controllers have not been connected, at least directly. Proprietary standards have governed the OT systems, at least from an industrial IoT perspective.

Understanding:

1. Explain the role of IP in IoT?

2. Distinguish between UDP and TCP Protocols?

3. Define the role of Information Technology (IT) and Operational Technology (OT) in the context of IoT data management?

6LoWPAN

- IPV6 over low power WPANs

Purpose of 6LoWPAN

- The intent is for IP networking over low-power RF communication systems for devices that are power and space constrained and do not need high bandwidth networking services.
- The principal advantage of 6LoWPAN is that the simplest of sensors can have IP addressability

Important Features of 6LoWPAN

- Low-Power wireless Personal Area Network over Ipv6.
- Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet Protocol
- Allows low-power devices to connect to internet
- Allows IEEE 802.15.4 radios to carry 128-bit addresses of Internet Protocol version 6 (IPv6)
- Header compression and address translation techniques allow the IEEE 802.15.4 radios to access the internet
- IPv6 packets compressed and reformatted to fit the IEEE 802.15.4 packet format

Understanding:

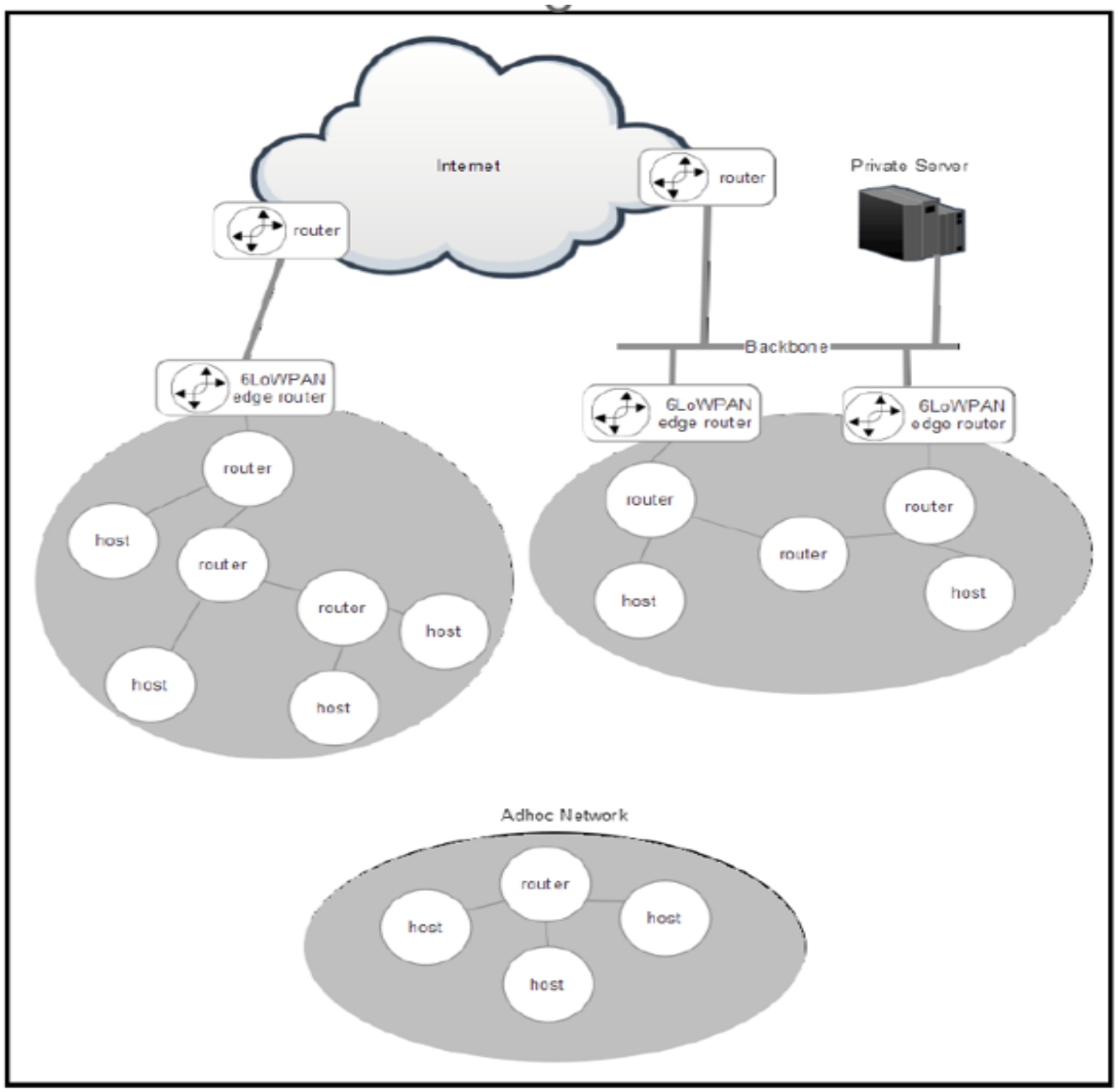
1. Explain the purpose of 6LowPAN Protocol?

2. Mention the important features of 6LowPAN?

6LoWPAN topology

6LoWPAN networks are mesh networks residing on the periphery of larger networks. The topologies are flexible, allowing for ad hoc and disjointed networks without any binding to the internet or other systems, or they can be connected to the backbone or the internet using edge routers. 6LoWPAN networks can be conjoined with multiple edge routers; this is called **multi-homing.** Additionally, **ad-hoc networks can form without requiring an Internet connectivity** of an edge router.

These topologies are shown below:



There are three types of nodes within the 6LoWPAN mesh:

1. Router nodes: These nodes marshal data from one 6LoWPAN mesh node to another. Routers can also communicate outward to the WAN and internet.

2. Host nodes: Hosts in the mesh network cannot route data in the mesh and are simply endpoints consuming or producing data. Hosts are allowed to be in sleep states, occasionally waking to produce data or receive data cached by their parent routers.

3. Edge routers: As stated, these are the gateways and mesh controllers usually at a WAN edge. A 6LoWPAN mesh would be administered under the edge router.

An edge router (also known as border router) is necessary for a 6LoWPAN architecture as it has four functions:

- Handles the communication to the 6LoWPAN devices and relays data to the internet.
- Performs compression of IPv6 headers by reducing a 40-byte IPv6 header and 8- byte UDP headers for efficiency in a sensor network. A typical 40-byte IPv6 header can compress to two to 20-bytes depending on usage.
- Initiates the 6LoWPAN network.
- Exchanges data between devices on the 6LoWPAN network.

Edge routers form 6LoWPAN mesh networks on larger traditional network perimeters.
They can also broker exchanges between IPV6 and IPV4 if necessary.
All nodes within a 6LoWPAN network share the same IPv6 prefix that the edge router establishes. Nodes will register with the edge routers as part of the **Network Discovery (ND) phase.**
ND controls how hosts and routers in the local 6LoWPAN mesh will interact with each other.
Multi-homing allows for multiple 6LoWPAN edge routers to manage a network.

Nodes are free to move and reorganize/reassemble in a mesh. For that matter, a node can move and associate with a different edge router in a multi-home scenario or even move between different 6LoWPAN meshes. These changes to the topology can be caused for various reasons, such as changes in signal strength or physical movement of nodes. When a topology change occurs, the IPv6 address of the associated nodes will also naturally change.

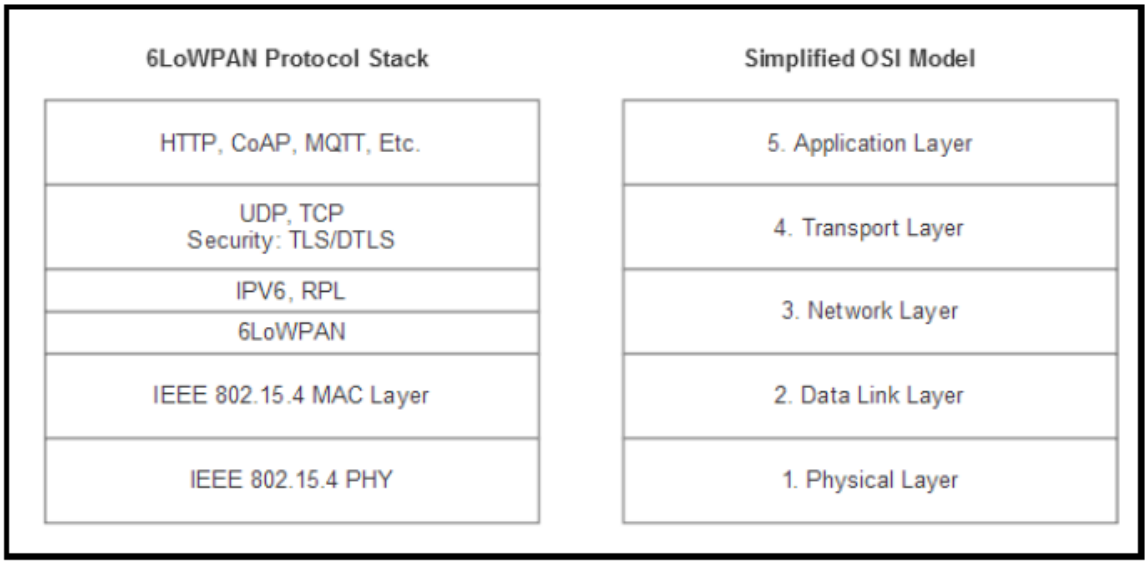
Understanding:

1. Explain the topology of 6LoWPAN with role of different nodes?

6LoWPAN protocol stack

To enable 6LoWPAN on a form of communication media such as 802.15.4 there is a set of recommended features necessary to support an IP protocol. These features include **framing, unicast transmission, and addressing.** 6LoWPAN resides on top of other protocols like 802.15.4 or Bluetooth to provide the physical and MAC address.

6LoWPAN Protocol Stack Comparison to the simplified OSI model.



The physical layer is responsible for receiving and converting data bits over the air.

On top of the physical layer is the data link layer, responsible for detecting and correcting errors on the physical link.

The 6LoWPAN layer is called adaptation layer which provides adaptation from IPV6 to IEEE 802.15.4

The network layer (RPL-Ripple) addresses and routes data through the network if needed over several hops

The IP (Internet Protocol) is the networking protocol used to provide all devices with an IP address to transport packets from one device to another

The transport layer generates communication sessions between applications running on end devices

Finally, the application layer is responsible for data formatting

Mesh addressing and routing

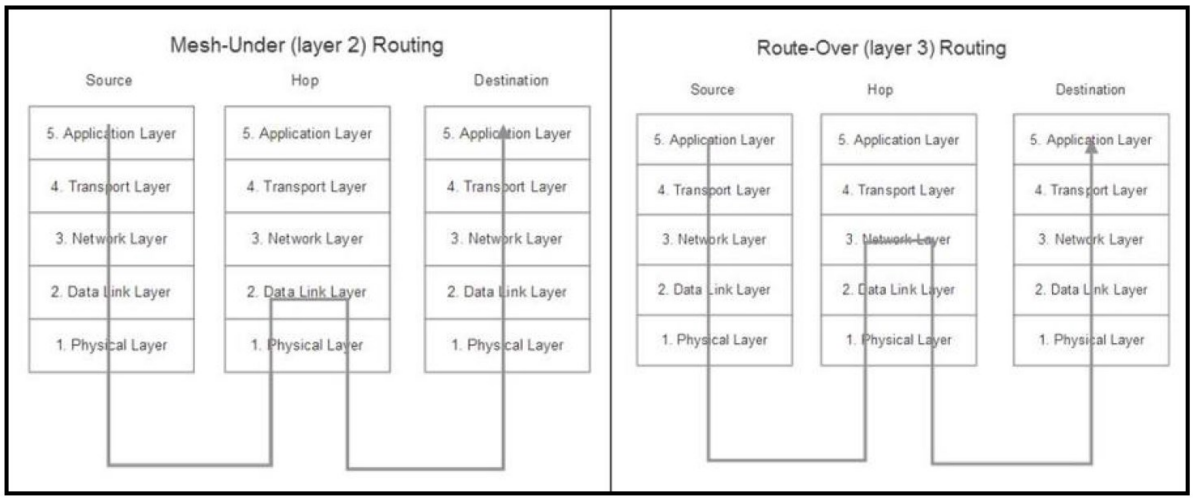
Mesh routing operates in the physical and data link layers to allow packets to flow through a dynamic mesh using multiple hops.

6LoWPAN mesh networks utilize two schemes for routing:

1. Mesh-under network: In a mesh-under topology, routing is transparent and assumes a single IP subnet representing the entirety of the mesh. A message is broadcast in a single domain and is sent to all devices in the mesh. As previously mentioned, this generates considerable traffic. Mesh-under routing will move from hop to hop in the mesh but only forward packets up to layer two (data link layer) of the stack. 802.15.4 handles all the routing for each hop in layer two.

2. Route-over network: In a route-over topology, networks will incur the charge of forwarding packets up to layer three (network layer) of the stack. Route-over schemes manage routes at an IP level. Each hop represents one IP router.

The difference between mesh-under and route-over networking. The intermediary hops reveal how far up each stack the packet is delivered before moving to the next node in the mesh.



Understanding:

1. Explain the 6LoWPAN protocol stack?
2. Explain the role of adaptation layer in 6LoWPAN?
3. Routing schemes in 6LoWPAN?

Thread

Thread is a relatively new networking protocol for IoT and is based on IPV6 (6LoWPAN).
Its principal target is home connectivity and home automation.
Based on the IEEE 802.15.4 protocol and 6LoWPAN, it has commonality with Zigbee and other 802.15.4 variants, but with a significant difference being Thread is IP addressable.
This IP protocol builds on the data and physical layers provided by 802.15.4 and the features such as security and routing from 6LoWPAN.
Thread is also mesh-based, making it attractive for home lighting systems with up to 250 devices in a single mesh.

The philosophy with Thread is that by enabling IP addressability in the smallest of sensors and home automation systems, one can reduce power because it doesn't need to persist application state since the protocol uses datagrams at the network layer. This also implies that the edge router hosting a Thread mesh network doesn't need to process application layer protocols and can lower its power and processing needs.

Finally, being IPV6 compliant, it is inherently is secure with all communications being encrypted using the Advanced Encryption Standard (AES). Up to 250 nodes can exist on a Thread mesh all with fully encrypted transport and authentication.

A software upgrade allows a pre-existing 802.15.4 device to be Thread compatible.

Understanding:

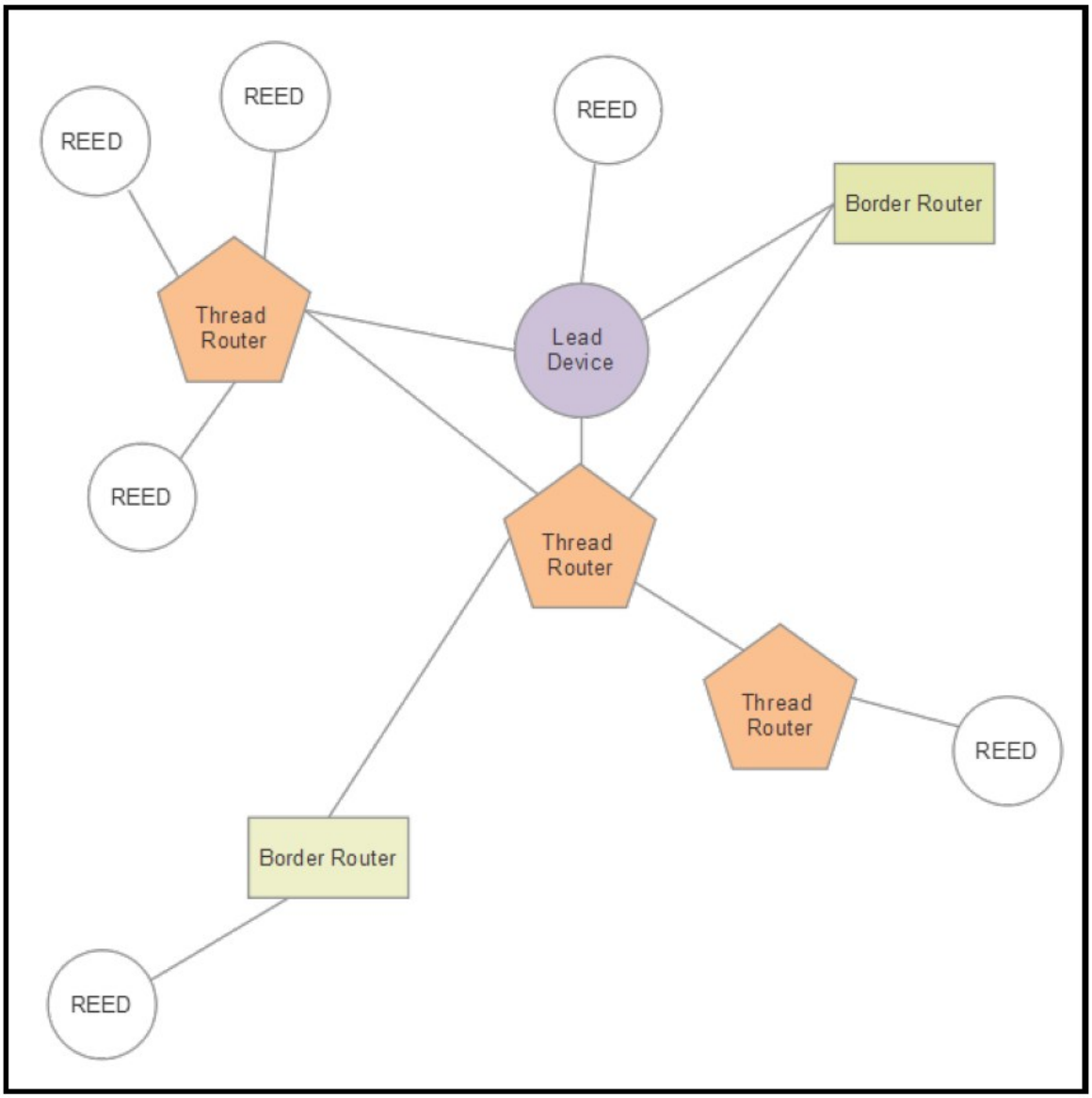
1. Explain the Philosophy of Thread?
2. Difference between Zigbee and Thread?

Thread architecture and topology

Based on the IEEE 802.15.4 standard, Thread uses the specification to define the Medium Access Controller (MAC) and physical (PHY) layers. It operates at 250 Kbps in the 2.4 GHz band.

From a topology point of view, Thread establishes communications with other devices through a border router (usually a Wi-Fi signal in a household). The rest of the communication is based on 802.15.4 and forms a self-healing mesh.

An example of such a topology is shown as follows:



The following are the roles of various devices in a Thread architecture.

Border router: A border router is essentially a gateway. In the home network, this would be a communications crossover from Wi-Fi to Thread and forms the entry point to the internet from a Thread mesh running underneath a border router. Multiple border routers are allowable under the Thread specification.

Lead device: The lead device manages a registry of assigned router IDs. The lead also controls the requests for **Router-eligible End Devices** (**REED**) to be promoted to routers. A leader can also act as a router and have device-end children. The protocol for assignment of router addresses is the **Constrained**
Application Protocol (**CoAP**). The state information a lead device manages can also be stored in the other thread routers. This allows for self-healing and failover in case the leader loses connectivity.

Thread routers: Thread routers manage the routing services of the mesh. Thread routers never enter a sleep state but are allowed by the specification to downgrade themselves to become a REED.

REEDs: A host device that is a REED can become routers or a leader. REEDs are not responsible for routing in the mesh unless they are promoted to a router or leader. REEDs also cannot relay messages or join devices to the mesh. REEDs essentially are endpoints or leaf nodes in the network.

End devices: Some endpoints cannot become routers. These types of REEDs have two other categories that they can subscribe to: **full end devices** (**FEDs**) and **minimal end devices** (**MEDs**).

Sleepy end devices: Host devices that have entered a sleep state communicate only with their associated thread router and cannot relay messages.

Understanding:

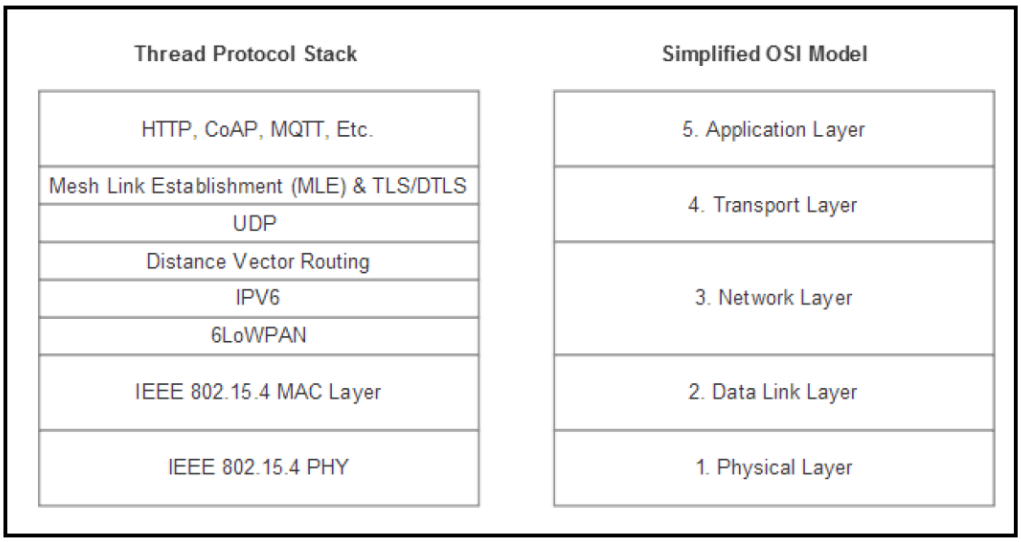
1. Explain the architecture and topology of Thread?

Thread protocol stack

Thread will make use of the full benefits of 6LoWPAN and enjoy the benefits of header compression, IPv6 addressing, and security. Thread also uses the fragmentation scheme of 6LoWPAN, but adds two additional stack components:

Distance vector routing
Mesh link establishment

Thread Protocol Stack



The physical layer is responsible for receiving and converting data bits over the air.

On top of the physical layer is the data link layer, responsible for detecting and correcting errors on the physical link.

The 6LoWPAN layer is called adaptation layer which provides adaptation from IPV6 to IEEE 802.15.4
The network layer (Distance Vector routing) addresses and routes data through the network if needed over several hops
The IP (Internet Protocol) is the networking protocol used to provide all devices with an IP address to transport packets from one device to another
The transport layer generates communication sessions between applications running on end devices
Mesh link establishment (MLE) is a method to update path traversal costs from one router to another in a network. Additionally, MLE provides a way to identify and configure neighbouring nodes in the mesh and secure them.
Finally, the application layer is responsible for data formatting

Understanding:

Explain the thread Protocol Stack?