MODULE 1

1. In which OSI layer the Wi-Fi standard/protocol fits?

   Wi-Fi (IEEE 802.11) fits within the Data Link Layer (Layer 2) and the Physical Layer (Layer 1) of the OSI model.

   Physical layer
   Handles the transmission of raw data bits over the wireless medium, including modulation, frequency selection, and signal strength.

   Data Link layer
   The Data Link Layer (Layer 2) of the OSI model is responsible for node-to-node communication over a physical medium. It ensures reliable data transfer by handling framing, error detection, and flow control.
   Key Functions:
   1. Framing – Encapsulates raw bits into structured frames for transmission.

   2. MAC Addressing – Uses unique addresses (like MAC addresses in Ethernet/Wi-Fi) to identify devices.

   3. Error Detection & Correction – Detects transmission errors using CRC (Cyclic Redundancy Check).

   4. Flow Control – Manages data transmission rates to prevent congestion.

   5. Media Access Control (MAC) – Regulates how multiple devices share the same communication medium (e.g., CSMA/CA in Wi-Fi, CSMA/CD in Ethernet).

2. Can you share the Wi-Fi devices that you are using day to day life, share that device's wireless capability/properties after connecting to network. Match your device to corresponding Wi-Fi Generations based on properties.

   Wi Fi devices:
   1. PC
   2. Laptop
   3. Android phone
   4. Smart Devices like Smart TV
   5. Routers

Generation	IEEE std.	Max speed	Frequency bands
Wi-Fi 4	802.11n	600 Mbps	2.4/5 GHz
Wi-Fi 5	802.11ac	6.9 Gbps	5 GHz

3. What is BSS and ESS?

Basic Service Set(BSS):
A BSS is the fundamental building block of a Wi-Fi network.
It consists of a single Access Point (AP) and the devices (stations) connected to it.
Communication happens only within this small area, and the devices rely on a single AP for connectivity.
Example:If you connect your phone to a single Wi-Fi router at home, it forms a BSS.

Extended Service Set(ESS):
An ESS is a collection of multiple BSSs that are interconnected.
Multiple APs are connected via a wired distribution system (like Ethernet) to extend coverage.
Devices can roam between APs without losing connection.
Example:A Wi-Fi network in an office, airport, or university where multiple APs provide seamless connectivity, forming an ESS.

4. What are the basic functionalities of Wi-Fi Accesspoint?

A Wi-Fi Access Point (AP) is a networking device that allows wireless devices to connect to a wired network. Its key functions include:
Wireless Connectivity – Enables wireless devices (laptops, smartphones, IoT devices) to connect to the network.
Signal Transmission & Reception – Sends and receives data using radio frequencies (2.4 GHz, 5 GHz, or 6 GHz).
Bridging Wired and Wireless Networks – Connects to a wired network (LAN) and extends it wirelessly.
Multiple Access Support – Allows multiple users to connect simultaneously using Wi-Fi protocols.
Security & Authentication – Implements encryption (WPA2, WPA3) and authentication mechanisms to protect network access.
Roaming Support – In an Extended Service Set (ESS), facilitates seamless transition between multiple APs.
Traffic Management – Manages data flow, reduces congestion, and prioritizes network traffic (QoS - Quality of Service).
Interference Management – Adjusts frequency channels and power levels to minimize interference with other networks.

5. Difference between Bridge mode and Repeater mode.

Bridge Mode
Function: Connects two separate networks to allow communication between them.
Working: Forwards traffic between different networks (wired or wireless).
Uses: Used to connect two physically separated networks (e.g., different buildings, wired and wireless networks).
Network Type: Connects different subnets (Layer 2 or Layer 3).
Performance: Maintains full bandwidth; does not halve the speed.
IP Address: Devices on both sides of the bridge can have different IP address ranges.

Repeater Mode
Function: Extends the coverage of an existing Wi-Fi network without creating a new network
Working: Receives Wi-Fi signals and rebroadcasts them to extend range.
Uses: Used to improve Wi-Fi signal strength in large areas with weak coverage.
Network type: Works within the same network (Layer 2).
Performance: Usually reduces bandwidth by half due to retransmission.
IP Address: Devices connected to the repeater share the same IP range.

6. What are the differences between 802.11a and 802.11b?

802.11 a
Introduced in 1999 alongside 802.11b but was less popular.
Operates in the 5 GHz frequency band, which is less crowded and has less interference from other wireless devices (like Bluetooth and microwaves).
Uses OFDM (Orthogonal Frequency Division Multiplexing) for better efficiency, achieving speeds up to 54 Mbps.
The higher frequency means a shorter range (approx. 30 meters indoors) and weaker signal penetration through walls and obstacles.
Mostly used in business and enterprise environments rather than homes.
Key point: Faster, but Shorter Range & Higher Frequency

802.11 b
Also introduced in 1999, but became more widely adopted.
Works in the 2.4 GHz frequency band, which is more crowded but provides better range (approx. 35-38 meters indoors).
Uses DSSS (Direct Sequence Spread Spectrum) for data transmission, reaching speeds up to 11 Mbps.
More susceptible to interference from devices like microwaves, Bluetooth, and cordless phones.
Became popular for home and small business Wi-Fi networks due to its lower cost and wider availability.
Key point: Slower, but Better Range & Cheaper

7. Configure your modem/hotspot to operate only in 2.4 Ghz and connect your laptop/Wi-Fi device, and capture the capability/properties in your Wi-Fi device. Repeat the same in 5 Ghz and tabulate all the differences your observed during this.

General Observations

Speed: The 5GHz band offers faster data transfer speeds compared to the 2.4GHz band, making it ideal for high-bandwidth applications like streaming and gaming.
Range: The 2.4GHz band has a longer range than 5GHz because its lower frequency waves can travel farther and penetrate walls more effectively.
Interference: The 2.4GHz band is more prone to interference from household devices like microwaves, Bluetooth devices, and cordless phones, whereas the 5GHz band has less interference.

Latency: The 5GHz band generally provides lower latency, making it a better choice for real-time applications like video conferencing and online gaming.
Bandwidth: The 5GHz band supports wider channel bandwidths (up to 160MHz), allowing more data to be transmitted at once, while the 2.4GHz band is limited to narrower channels (20-40MHz).
Device Compatibility: Older Wi-Fi devices primarily support 2.4GHz, while most modern devices support both 2.4GHz and 5GHz bands for better performance.
Use Cases: The 2.4GHz band is better suited for long-range, low-power IoT devices and basic web browsing, while the 5GHz band is ideal for high-speed internet activities in shorter ranges.

8. What is the difference between IEEE and WFA?

   IEEE (Institute of Electrical and Electronics Engineers) develops and maintains Wi-Fi standards, such as IEEE 802.11, while the Wi-Fi Alliance (WFA) ensures these standards are implemented correctly in devices.
   IEEE focuses on the technical standardization of networking technologies, whereas WFA works on certifying and branding Wi-Fi products to ensure interoperability.
   IEEE defines the core Wi-Fi protocols like 802.11a, 802.11b, and 802.11ax, but WFA verifies that devices follow these protocols and certifies them as "Wi-Fi CERTIFIED™."
   IEEE is an organization made up of engineers, researchers, and professionals contributing to technology advancements, while WFA consists of companies like Intel, Cisco, and Apple that develop and market Wi-Fi products.
   IEEE creates standards not just for Wi-Fi but also for Ethernet (IEEE 802.3) and Bluetooth (IEEE 802.15), whereas WFA is entirely focused on Wi-Fi certification and promotion.
   IEEE provides the foundational rules and specifications for wireless communication, while WFA ensures that certified products from different manufacturers work seamlessly together.
   A device can support IEEE 802.11 standards but may not be Wi-Fi Alliance certified if it hasn't passed interoperability testing.

9. List down the type of Wi-Fi internet connectivity backhaul, share your home/college's wireless internet connectivity backhaul name and its properties.

   WiFi Backhaul
   A Wi-Fi backhaul is the connection between the Wi-Fi access points (APs) and the main internet source (e.g., ISP router, fiber, or another AP). There are different types of backhaul:

   ->Wired Backhaul (Ethernet, Fiber, or DSL)
   Uses Ethernet cables or fiber optics to connect APs to the network.
   Offers higher speed, lower latency, and better reliability.
   Common in offices, homes with mesh systems, and enterprise networks.

   ->Wireless Backhaul (Wi-Fi, Microwave, or Satellite)
   Uses wireless signals to connect APs or networks.
   Good for remote areas where running cables is difficult.
   May introduce higher latency and bandwidth limitations.

->Cellular Backhaul (4G/5G, LTE)
Uses mobile networks to connect to the internet.
Useful for temporary setups, mobile offices, or disaster recovery.
Speed depends on network congestion and coverage.

Wired Backhaul (More Stable & High Speed)

Type	Speed	Latency
Fiber Optic (FTTH)	1 Gbps – 10 Gbps	Very Low (1–5 ms)
Ethernet (Wired LAN)	100 Mbps – 10 Gbps	Very Low (1–2 ms)
Cable Broadband (Coaxial DOCSIS)	100 Mbps – 1 Gbps	Low (10–30 ms)
DSL (Phone Line – ADSL/VDSL)	10–100 Mbps	Medium (20–50 ms)
Powerline (PLC)	50–500 Mbps	High (50+ ms)

Wireless Backhaul (More Flexible, Less Stable)

Type	Speed	Latency
Wi-Fi Backhaul (Wireless Mesh)	300 Mbps – 1 Gbps	Medium (10–50 ms)
4G LTE / 5G Cellular	10 Mbps – 1 Gbps	Medium-High (20–100 ms)
Satellite Internet (Starlink, VSAT)	50–250 Mbps	High (30–100 ms)
Microwave Point-to-Point	100 Mbps – 1 Gbps	Low-Medium (10–30 ms)

10. List down the Wi-Fi topologies and use cases of each one.

WiFi Topologies

->Infrastructure Mode (BSS & ESS)
Basic Service Set (BSS): A single access point (AP) connects multiple clients to the network.
Extended Service Set (ESS): Multiple APs are interconnected to extend coverage.
Use Case: Home networks, office environments, and public Wi-Fi hotspots.

->Repeater Mode
An AP in repeater mode extends the range of an existing network by relaying signals.
Use Case: Large homes or areas where a single AP cannot provide full coverage.

->Bridge Mode
Connects two different wired networks wirelessly using APs in bridge mode.
Use Case: Connecting buildings in a campus or enterprise setup without running cables.

->Ad-Hoc Mode (IBSS - Independent Basic Service Set)
Devices communicate directly with each other without an AP.
Use Case: Temporary connections for file sharing, IoT device communication.

->Mobile Hotspot Mode
A device (laptop or phone) shares its internet connection as a Wi-Fi hotspot.
Use Case: On-the-go internet access using cellular networks.

->Mesh Mode
Multiple mesh routers form a self-healing, adaptive network where devices switch to the best available node.
Use Case: Smart homes, large corporate campuses, outdoor city Wi-Fi networks.

->Work Group Bridge Mode
Bridges wired clients (like PCs, printers) to a Wi-Fi network through a Work Group Bridge (WGB).
Use Case: Industrial or enterprise environments needing wireless connectivity for wired devices.

->IoT Gateway Mode
Connects IoT devices to the internet using various protocols like MQTT, CoAP, and XMPP.
Use Case: Smart homes, industrial IoT applications, and smart city networks.