**1. In which OSL layer the Wi-Fi standard/protocol fits.**

Wi-Fi (IEEE 802.11) primarily operates in the **Data Link Layer (Layer 2)** of the OSI model, specifically within the **MAC (Media Access Control) sublayer**. It also interacts with the **Physical Layer (Layer 1)**.

**Breakdown of Wi-Fi in OSI Layers:**

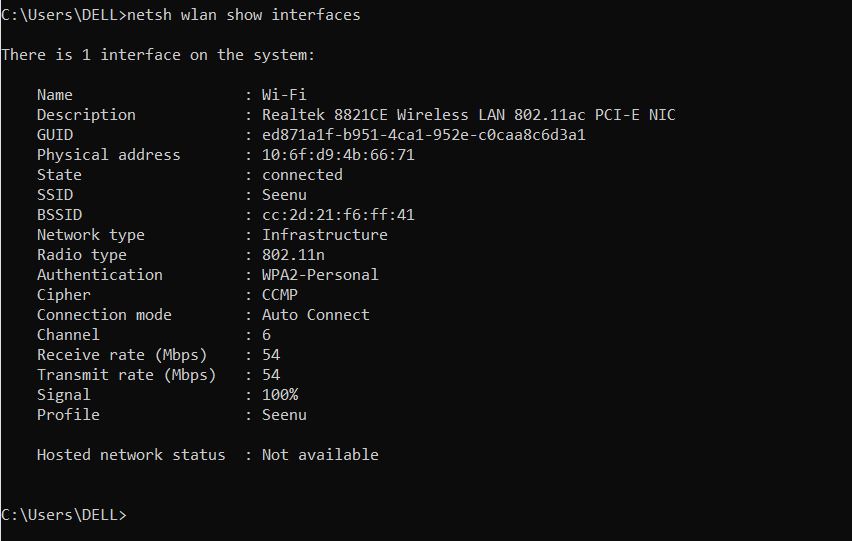
**Physical Layer (Layer 1)**

* + Defines radio frequencies, modulation schemes, and signal encoding.
  + Wi-Fi standards like **802.11a/b/g/n/ac/ax** define how data is transmitted over radio waves.

**Data Link Layer (Layer 2) - MAC Sublayer**

* + Handles MAC addressing, frame control, and media access using CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
  + Ensures reliable data transmission between Wi-Fi devices.
  + Manages authentication, association, and encryption (WPA, WPA2, WPA3).

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



**1**. Wi-Fi Standard & Generation

* Radio Type: 802.11ac
* Wi-Fi Generation: Wi-Fi 5
* Max Theoretical Speed: Up to 6.9 Gbps (depends on MIMO configuration).

2. Frequency Band & Channel

* Band: 5 GHz
* Channel: 36 (This is a low-band 5 GHz channel, commonly used in Wi-Fi 5).

3. Security & Encryption

* Authentication: WPA2-Personal
* Cipher: CCMP (AES-based encryption, secure for home networks).

4. Network Performance

* Receive Rate: 325 Mbps
* Transmit Rate: 325 Mbps
* Signal Strength: 54% (Moderate signal strength; might experience some drops)

**3. what is BSS and ESS?**

1. Basic Service Set (BSS)

* Definition: A single access point (AP) and the devices (stations) connected to it form a BSS.
* Components:
  + One Access Point (AP)
  + Multiple connected devices (stations)
  + A unique BSSID (Basic Service Set Identifier) (usually the MAC address of the AP)
* Example: Your home Wi-Fi router and all connected devices form a BSS.

🛠 Types of BSS:

1. Infrastructure BSS → Devices communicate via an AP. (Common in homes, offices, etc.)
2. Independent BSS (IBSS) → Devices communicate directly in ad-hoc mode (no AP).

2. Extended Service Set (ESS)

* Definition: Multiple BSS units connected together to form a larger network is called an ESS.
* Components:
  + Multiple access points (APs)
  + Common SSID (Wi-Fi network name)
  + Seamless roaming for devices between APs
* Example: A university campus Wi-Fi network where you can move across buildings while staying connected.

**4. what are the basic functionalities of Wi-Fi Accesspoint**

1. Wireless Connectivity

* Provides a wireless signal (SSID) for devices to connect.
* Supports different Wi-Fi standards (802.11a/b/g/n/ac/ax).

2. Network Bridging

* Connects wired Ethernet networks to wireless devices.
* Acts as a bridge between Wi-Fi devices and routers/switches.

3. Data Transmission & Reception

* Handles packet transmission and reception over Wi-Fi.
* Uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to manage wireless access.

4. Security & Authentication

* Implements WPA2, WPA3 encryption for secure access.
* Supports MAC filtering, 802.1X authentication, and firewall policies.

5. Multiple SSID & VLAN Support

* Can broadcast multiple SSIDs (e.g., Guest Wi-Fi, Corporate Wi-Fi).
* Assigns different VLANs for network segmentation.

6. Roaming & Handoff (in ESS networks)

* Enables seamless roaming between APs in an Extended Service Set (ESS).
* Uses Fast Roaming (802.11r, k, v) for smooth transitions.

7. Frequency & Channel Management

* Operates on 2.4GHz, 5GHz, or 6GHz bands (depending on Wi-Fi version).
* Uses channel selection & DFS (Dynamic Frequency Selection) to avoid interference.

8. QoS (Quality of Service)

* Prioritizes network traffic using WMM (Wi-Fi Multimedia).
* Ensures low latency for VoIP, gaming, and video streaming.

9. Power Management (PoE Support)

* Some APs support Power over Ethernet (PoE), allowing them to be powered via Ethernet cables.

10. Mesh & Extender Functionality (Advanced APs)

* Supports Wi-Fi Mesh networking for larger coverage areas.
* Can function as a Wi-Fi Extender to boost signals

**5. Difference between Bridge mode and Repeater mode**

1. Bridge Mode  
Bridge mode allows a networking device (like a router or AP) to function as a transparent bridge between two networks, merging them into a single network.

Purpose:

* Connects two or more separate networks.
* Eliminates Double NAT (Network Address Translation) when using multiple routers.
* Extends wired networks without creating a separate subnet.

How It Works:

* Disables the router’s NAT, DHCP, and firewall functions.
* Passes all traffic directly to the main router.
* Devices connected through the bridge function as part of the same network as the main router.

Use Cases:

Used when connecting multiple routers without creating a new subnet.  
Useful in corporate networks to connect different LANs.  
Helps in ISP-provided modems when using a third-party router.

Example:

if you have a main router and want to use another router without creating a new subnet, you enable bridge mode on the second router.

2. Repeater Mode (Wi-Fi Extender Mode)

A Wi-Fi repeater (or extender) amplifies an existing Wi-Fi signal and retransmits it to extend coverage.

Purpose:

* Increases Wi-Fi coverage in dead zones.
* Does not create a new subnet—it just extends the same Wi-Fi network.
* Can slightly reduce network speed due to retransmission.

How It Works:

* Connects wirelessly to the main router.
* Receives the Wi-Fi signal and rebroadcasts it under the same SSID or a different one.
* Creates a new "hop" for wireless devices to connect through.

Use Cases:  
When a Wi-Fi signal is weak in some areas.  
Used in homes, offices, and large buildings where a single router doesn’t cover all areas.

Example:

* If your router is placed in the living room but the signal is weak in the bedroom, a Wi-Fi repeater can extend the signal there.

6. what are the differences between 802.11a and 802.11b.

1. 802.11a

🔹 Frequency: 5 GHz  
🔹 Speed: Up to 54 Mbps  
🔹 Range: ~35 meters indoors, ~120 meters outdoors  
🔹 Interference Resistance: High (fewer devices use 5 GHz, so less congestion)

2. 802.11b

🔹 Frequency: 2.4 GHz  
🔹 Speed: Up to 11 Mbps  
🔹 Range: ~38 meters indoors, ~140 meters outdoors  
🔹 Interference Resistance: Low (more devices use 2.4 GHz, leading to congestion)

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

1. Login to your Router/Hotspot settings
   * Open a browser and enter 192.168.1.1 or 192.168.0.1 (check your router’s IP).
   * Login with the admin username/password (usually found on the device).
2. Disable 5GHz and Enable Only 2.4GHz
   * Go to Wireless Settings > Wi-Fi Band Selection.
   * Disable 5GHz and keep 2.4GHz enabled.
   * Save settings and restart the router/hotspot.
3. Connect Your Laptop to the 2.4GHz Wi-Fi
4. Check Wi-Fi Properties in Your Device
5. Note Down the Following:
   * Radio Type (802.11 version)
   * Frequency Band
   * Channel
   * Receive/Transmit Rate (Mbps)
   * Signal Strength (%)

**8. What is the difference between IEEE and WFA**

The **Institute of Electrical and Electronics Engineers (IEEE)** and the **Wi-Fi Alliance (WFA)** are two key organizations involved in the development and adoption of Wi-Fi technology. While IEEE defines the technical standards, WFA ensures their implementation and interoperability.

**IEEE (Institute of Electrical and Electronics Engineers)**

IEEE is responsible for developing and maintaining the **802.11 standards**, which define the technical specifications for Wi-Fi, including speed, frequency bands, and security protocols.

**WFA (Wi-Fi Alliance)**

The Wi-Fi Alliance is a non-profit organization that **certifies** Wi-Fi devices for interoperability and compliance with IEEE standards. It ensures that different manufacturers' products work seamlessly together.

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

* Fiber Optic (FTTH - Fiber to the Home)
  + Speed: Up to 10 Gbps
  + Latency: Very low
  + Best For: High-speed broadband, gaming, and business networks
* Ethernet (LAN Cable - Cat5e/Cat6/Cat7)
  + Speed: Up to 10 Gbps (depending on cable type)
  + Latency: Low
  + Best For: Offices, data centers, and homes needing stable connectivity
* DSL (Digital Subscriber Line - Copper Telephone Lines)
  + Speed: Up to 100 Mbps (VDSL)
  + Latency: Moderate
  + Best For: Rural areas with no fiber access
* Coaxial Cable (Cable Internet - DOCSIS)
  + Speed: Up to 1 Gbps
  + Latency: Low to moderate
  + Best For: Home broadband in urban areas

Wi-Fi networks can be deployed using different topologies based on the requirements of the network, coverage area, and number of connected devices. These topologies determine how devices communicate and interact within the network. The key Wi-Fi topologies include Infrastructure Mode, Extended Service Set (ESS), Ad-Hoc Mode, Mesh Wi-Fi Network, and Wi-Fi Direct. Each has its own unique advantages and use cases.

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

1. Infrastructure Mode (Basic Service Set - BSS)

Description:

Infrastructure mode is the most commonly used Wi-Fi topology. In this setup, a Wi-Fi Access Point (AP) acts as a central hub, and all devices (stations) communicate through it. The AP is connected to a wired network, allowing devices to access the internet.

Use Cases:

* Home Wi-Fi networks where a router provides internet access.
* Office networks with multiple employees connected wirelessly.
* Public hotspots such as cafes, airports, and malls.

2. Extended Service Set (ESS)

Description:

An Extended Service Set (ESS) consists of multiple access points connected to the same network. These APs are linked via a wired or wireless backhaul, providing seamless roaming across a large area.

Use Cases:

* Corporate offices, universities, and hospitals requiring wide coverage.
* Airports and shopping malls with multiple APs ensuring seamless connectivity.
* Smart city projects providing continuous Wi-Fi across different locations.

3. Ad-Hoc Mode (Independent Basic Service Set - IBSS)

Description:

In Ad-Hoc mode, devices communicate directly with each other without requiring a central access point. This peer-to-peer (P2P) communication is useful for temporary and small-scale networks.

Use Cases:

* Quick file transfers between laptops and mobile devices.
* Temporary wireless networks for gaming LAN parties.
* Emergency communication networks in disaster-hit areas.

4. Mesh Wi-Fi Network

Description:

A Mesh Wi-Fi network consists of multiple nodes (access points) that communicate wirelessly, extending coverage over large areas. Unlike traditional infrastructure mode, mesh networks do not rely on a single access point, making them more fault-tolerant.

Use Cases:

* Large homes and multi-floor buildings where one router is insufficient.
* Smart homes with IoT devices like cameras, smart lights, and sensors.
* Warehouses, factories, and industrial setups requiring extensive coverage.

5. Wi-Fi Direct

Description:

Wi-Fi Direct allows devices to connect directly without an access point, but one device acts as a controller. It is commonly used for wireless file sharing and device connectivity.

Use Cases:

* Wireless printing (e.g., phone to printer connection).
* File transfer between devices (e.g., Android’s Wi-Fi Direct, Apple’s AirDrop).
* Smart TV casting and screen mirroring.