**VISHAL G WIFI Assignment MODULE 1**

**1. In which osi layer the WIFI standard/ protocol fits**

The Wi-Fi standard/protocol primarily operates at the Data Link Layer (Layer 2) and the Physical Layer (Layer 1) of the OSI model. At the Physical Layer, it handles the transmission of raw data bits over radio waves. At the Data Link Layer, specifically in the MAC (Media Access Control) sublayer, it manages packet framing, addressing, and error detection to ensure reliable data transfer. Protocols like IEEE 802.11 define how devices communicate over Wi-Fi networks, including authentication, encryption, and access control.

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

Smartphone (Samsung Galaxy S22)

Wireless Capabilities: Supports Wi-Fi 6 (802.11ax), dual-band (2.4 GHz and 5 GHz), MU-MIMO (Multiple-User, Multiple-Input, Multiple-Output), and OFDMA (Orthogonal Frequency Division Multiple Access) for better efficiency.

Wi-Fi Generation: Wi-Fi 6 (6th generation).

Laptop

Wireless Capabilities: Supports Wi-Fi 6E (802.11ax), tri-band (2.4 GHz, 5 GHz, and 6 GHz), improved speed, and reduced latency.

Wi-Fi Generation: Wi-Fi 6E (Enhanced version of Wi-Fi 6).

Smart TV

Wireless Capabilities: Supports Wi-Fi 5 (802.11ac), dual-band (2.4 GHz and 5 GHz), and beamforming for focused signal transmission.

Wi-Fi Generation: Wi-Fi 5 (5th generation).

Smart Watches

Wireless Capabilities: Generally, supports Wi-Fi 4 (802.11n) or Wi-Fi 5 (802.11ac), mostly 2.4 GHz for better range.

Wi-Fi Generation: Wi-Fi 4 or Wi-Fi 5.

Wi-Fi Routers

Wireless Capabilities: Supports Wi-Fi 6 or 6E (802.11ax), multi-band (2.4 GHz, 5 GHz, and 6 GHz), MU-MIMO, OFDMA, Beamforming.

Wi-Fi Generation: Wi-Fi 6 or 6E.

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

Basic Service Set (BSS):

A Basic Service Set (BSS) is the fundamental building block of a Wi-Fi network, consisting of a single access point (AP) and all associated wireless devices communicating directly with that AP. Each BSS is uniquely identified by a Basic Service Set Identifier (BSSID), which is the MAC address of the AP.

Extended Service Set (ESS):

An Extended Service Set (ESS) is a network composed of multiple interconnected Basic Service Sets (BSSs) operating under the same Service Set Identifier (SSID). ESS allows seamless communication and roaming across different access points within the same network, providing broader coverage and enhanced connectivity over larger areas.

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

Wireless Signal Transmission & Reception: Transmits and receives radio signals to enable wireless communication with devices within its coverage area.

Data Framing & Packet Forwarding: Breaks down data into frames, manages addressing, and forwards data packets between devices and the wired network.

Network Bridging: Acts as a bridge between wireless devices and the wired network (e.g., LAN), enabling communication across different network segments.

Authentication & Encryption: Ensures network security by providing authentication mechanisms (e.g., WPA3, WPA2) and encrypting data to prevent unauthorized access.

Channel Management: Manages and selects appropriate frequency channels to reduce interference and improve network performance.

Roaming Support: Facilitates seamless handoff between multiple APs in an Extended Service Set (ESS) for uninterrupted connectivity.

Bandwidth Control & Quality of Service (QoS): Prioritizes traffic to maintain the quality of high-demand services like video streaming and online gaming.

DHCP Relay: Relays IP address assignments from the DHCP server to connected wireless clients, if configured.

Access Control: Restricts or permits devices to join the network based on MAC filtering, VLANs, or other policies.

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

Bridge Mode:

Bridge mode is a network configuration where a device, like a Wi-Fi router or access point, connects two separate networks and allows communication between them. It acts as a bridge between different network segments, such as connecting a wired network to a wireless network. In this mode, devices connected to the bridge receive IP addresses from the primary network's DHCP server, maintaining a single network segment. It provides better performance since it directly forwards data without duplicating signals. Common use cases include connecting remote wired devices to a wireless network.

Repeater Mode:

Repeater mode is a network configuration used to extend the coverage area of an existing wireless network by amplifying and retransmitting the original signal. Unlike bridge mode, it simply extends the range of a single network without creating a separate network segment. Devices connected to the repeater share the same IP range as the main network. However, since it duplicates and retransmits signals, it may introduce some latency and reduced speed. Repeater mode is commonly used to eliminate dead zones and improve Wi-Fi coverage in larger areas.

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

**802.11a:**

Operates at 5 GHz with data rates up to 54 Mbps.

Shorter range but less interference; ideal for indoor use.

Not compatible with 802.11b devices.

Commonly used in high-speed indoor networks like offices.

**802.11b:**

Operates at 2.4 GHz with data rates up to 11 Mbps.

Longer range but more interference from devices like microwaves and Bluetooth.

Compatible with older 802.11 devices.

Typically used for low-speed applications like home networks.

**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.**

2.4Ghz Configuration of the Wifi on the laptop, showing its properties:

SSID: JioFiber-TSbaf

Protocol: Wi-Fi 4 (802.11n)

Security type: WPA2-Personal

Manufacturer: Intel Corporation

Description: Intel(R) Wi-Fi 6 AX201 160MHz

Driver version: 22.240.0.6

Network band (channel): 2.4 GHz (6)

Aggregated link speed (Receive/Transmit): 144/65 (Mbps)

IPv6 address: 2405:201:e028:f136:2092:cacd:593:ee89

Link-local IPv6 address: fe80::3b6d:32af:500b:9229%19

IPv6 default gateway: fe80::aa88:1fff:fe05:ccc5%19

IPv6 DNS servers: 2405:201:e028:f136::c0a8:1d01 (Unencrypted)

2405:201:e028:f136::c0a8:1d01 (Unencrypted)

IPv4 address: 192.168.29.191

IPv4 DNS servers: 192.168.29.1 (Unencrypted)

Physical address (MAC): 10-3D-1C-48-F2-79

Similarly configuring the Router to 5Ghz and the properties of the connected Wifi:

SSID: JioFiber-TSbaf\_5G

Protocol: Wi-Fi 5 (802.11ac)

Security type: WPA2-Personal

Manufacturer: Intel Corporation

Description: Intel(R) Wi-Fi 6 AX201 160MHz

Driver version: 22.240.0.6

Network band (channel): 5 GHz (153)

Aggregated link speed (Receive/Transmit): 292/780 (Mbps)

IPv6 address: 2405:201:e028:f136:2092:cacd:593:ee89

Link-local IPv6 address: fe80::3b6d:32af:500b:9229%19

IPv6 default gateway: fe80::aa88:1fff:fe05:ccc5%19

IPv6 DNS servers: 2405:201:e028:f136::c0a8:1d01 (Unencrypted)

2405:201:e028:f136::c0a8:1d01 (Unencrypted)

IPv4 address: 192.168.29.191

IPv4 DNS servers: 192.168.29.1 (Unencrypted)

Physical address (MAC): 10-3D-1C-48-F2-79

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

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

The IEEE is a professional organization that develops global standards for technologies, including Wi-Fi through the 802.11 family of standards (e.g., 802.11a, 802.11b, 802.11n, 802.11ac, 802.11ax). Its focus is on creating technical specifications, protocols, and communication mechanisms, particularly related to the physical (PHY) and medium access control (MAC) layers. IEEE’s standards ensure robust and efficient wireless communication.

**Wi-Fi Alliance (WFA)**

The Wi-Fi Alliance (WFA) is a non-profit organization that certifies Wi-Fi devices to ensure compatibility and interoperability. It provides the "Wi-Fi Certified" label to devices that meet performance, security, and compatibility standards based on IEEE’s specifications. WFA’s certifications, such as WPA3, Wi-Fi Direct, and Wi-Fi 6, ensure smooth operation across devices from different manufacturers.

**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 Backhaul: Fiber optic backhaul uses thin strands of glass or plastic fibers to transmit data as light signals over long distances with incredible speed and reliability. It offers the highest bandwidth capacity, minimal signal loss, and extremely low latency (1-5 ms), making it the preferred choice for ISPs, data centers, enterprise networks, and high-speed internet services. Fiber optic backhaul is essential for delivering Gigabit and even Terabit speeds, supporting applications like 4K/8K streaming, cloud computing, and large-scale industrial networks.

MoCA (Multimedia over Coaxial Alliance) Backhaul: MoCA technology uses existing coaxial TV cables in buildings to create high-speed, low-latency backhaul connections. It provides reliable connectivity up to 2.5 Gbps, making it ideal for extending wired networks to areas where Wi-Fi signals are weak, such as basements or far-off rooms. MoCA is commonly used in home networks to improve coverage and performance without requiring new cabling.

Satellite Backhaul: Satellite backhaul uses satellites orbiting the Earth to transmit internet data to and from remote or rural locations where terrestrial infrastructure is unavailable. While it offers global coverage, it suffers from high latency (typically 500 ms or more) due to the long distance signals must travel. Speeds are generally lower compared to fiber or Ethernet, but advancements like Low Earth Orbit (LEO) satellite constellations (e.g., Starlink) are improving latency and bandwidth.

Cellular Backhaul (4G/5G): Cellular backhaul utilizes mobile networks such as 4G LTE and 5G to provide internet connectivity to Wi-Fi networks. It is commonly used for mobile hotspots, temporary networks, and areas lacking traditional wired infrastructure. With 5G, cellular backhaul can offer ultra-low latency (as low as 1 ms) and high speeds up to 10 Gbps, making it suitable for smart cities, industrial IoT, and real-time applications.

Powerline Backhaul (PLC - Power Line Communication): Powerline backhaul uses existing electrical wiring within a building to transmit internet data. It provides a convenient way to extend network coverage to areas where Wi-Fi signals are weak without installing additional cables. Speeds can reach up to 2 Gbps depending on the quality of the wiring and interference levels. Powerline backhaul is commonly used for home networking and smart home applications where reliable connectivity is required across multiple rooms.

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

Infrastructure Mode: Infrastructure mode is the most commonly used Wi-Fi mode where devices connect to a central Access Point (AP) that manages communication between all connected devices. The AP acts as a bridge between the wireless network and a wired network (like the internet), providing centralized management, better security, and enhanced performance. This mode is widely used in homes, offices, campuses, and public hotspots.

Repeater Mode: Repeater mode is designed to extend the coverage area of an existing wireless network. A repeater captures the Wi-Fi signal from the main router and rebroadcasts it, effectively increasing the network's range. This mode is ideal for eliminating dead spots in homes or buildings where signal strength is weak due to physical obstructions or distance from the primary router.

Bridge Mode: Bridge mode allows two or more network segments to communicate with each other by connecting separate networks, typically a wired network and a wireless network. It is commonly used to link two distinct LANs without causing IP conflicts. This mode is essential when integrating devices that require seamless communication between wired and wireless components, such as connecting smart devices to a home network.

Ad-Hoc Mode: Ad-Hoc mode enables direct communication between devices without using an Access Point or router. Devices form a peer-to-peer network where each device acts as both client and server. This mode is suitable for temporary networks, such as file sharing between laptops, offline multiplayer gaming, or establishing emergency networks during natural disasters.

Mobile Hotspot Mode: Mobile Hotspot mode allows a device, usually a smartphone, to share its cellular internet connection with other Wi-Fi-enabled devices by creating a small, local wireless network. It is commonly used for providing internet access to laptops, tablets, and other devices when a traditional Wi-Fi network is unavailable, such as during travel or outdoor activities.

Mesh Mode: Mesh mode involves a network of interconnected Access Points (APs) working together to provide consistent and expansive coverage. Instead of relying on a single router, data is dynamically routed across multiple nodes, ensuring reliability even if one node fails. Mesh networks are highly effective for large areas, such as smart homes, corporate offices, hotels, and outdoor campuses where seamless coverage is essential.

Work Group Bridge Mode: Work Group Bridge mode is a specialized mode where a wireless bridge connects a group of wired devices to a wireless network. Acting as a client device, the bridge allows non-wireless devices to communicate over Wi-Fi. This mode is often used in industrial and enterprise environments where legacy devices lacking Wi-Fi capability need network connectivity.

IoT Gateway Mode: IoT Gateway mode is designed to facilitate communication between IoT devices and the internet or cloud services. Acting as a protocol converter, it bridges various communication standards like Zigbee, Bluetooth, and Wi-Fi, enabling seamless connectivity. This mode is essential for smart homes, industrial IoT, and sensor networks where different protocols need to be unified for monitoring and control.