MODULE 4 ASSIGNMENT – WIFI TRAINING

1) What is the significance of MAC layer and in which position it is placed in the OSI model

Significance of the MAC Layer:

The **MAC (Medium Access Control) layer** is a sublayer of the **Data Link Layer** in the **OSI model**. It plays a crucial role in managing access to the shared physical medium (such as radio waves in Wi-Fi) and ensuring the reliable transmission of data between devices in a network.

Here's the significance of the **MAC layer**:

1. **Frame Construction and Formatting**:
   - The MAC layer is responsible for framing the data from the network layer (Layer 3) into **MAC frames** for transmission.
   - It adds necessary headers (like the source and destination MAC addresses) and tailing information (like CRC for error checking).
2. **Access Control**:
   - The MAC layer handles **media access control**, which means determining how multiple devices share the same communication channel (especially in wireless networks).
   - It uses various methods like **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance) to avoid collisions and manage the access to the medium.
3. **Error Detection and Handling**:
   - The MAC layer checks for transmission errors using a **Frame Check Sequence (FCS)** in the frame's tail.
   - If a frame has errors, it requests retransmission, ensuring reliable communication.
4. **Flow Control**:
   - The MAC layer is responsible for flow control in some cases, preventing buffer overflow at the receiving end and ensuring smooth data transmission.
5. **Addressing**:
   - The MAC layer uses **MAC addresses** (unique hardware addresses assigned to network interfaces) to identify devices in a network.
   - These addresses help route the data to the correct device within a local network.

Position of the MAC Layer in the OSI Model:

- The **MAC layer** is part of the **Data Link Layer** (Layer 2) in the OSI model.
- The **Data Link Layer** itself is divided into two sublayers:
  1. **LLC (Logical Link Control)**: Deals with logical addressing and communication management between devices.

2. **MAC (Medium Access Control)**: Manages access to the physical transmission medium and handles addressing at the hardware level (using MAC addresses).

2) Describe the frame format of the 802.11 MAC header and explain the purpose of each fields

Field	Size	Purpose
Frame Control	2 bytes	Defines frame type, subtype, and various flags like retry, power management, etc.
Duration/ID	2 bytes	Specifies the duration for channel reservation.
Address 1	6 bytes	Destination MAC address (or address of the recipient device).
Address 2	6 bytes	Source MAC address (or address of the sender).
Address 3	6 bytes	Address for routing or the next hop (for multi-hop or AP networks).
Sequence Control	2 bytes	Contains sequence number and fragment information for fragmentation.
Address 4	6 bytes	Optional, used in certain 4-address configurations like mesh networks.
Frame Body	Variable	Contains data or management/control information.
FCS	4 bytes	Frame Check Sequence (error checking).

3) Please list all the MAC layer functionalities in all Management, Control and Data plane

Plane	Functionality
Management Plane	- Association/Disassociation (AP & client) - Authentication/Deauthentication - Beaconing (AP advertising its presence) - Probe Request/Response - Power Management (client sleep modes) - Key Management (WPA, WPA2, etc.) - Roaming and Handoff between APs
Control Plane	- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) - RTS/CTS (Request to Send / Clear to Send) - ACK (Acknowledgement) - Frame Fragmentation and Reassembly - Collision Avoidance using RTS/CTS - Traffic Management (priority handling for different types of traffic) - Channel Reservation (e.g., via RTS/CTS)
Data Plane	- Data Frame Transmission (Encapsulation of user data) - Encryption/Decryption (WEP, WPA, WPA2) - Frame Delivery (Unicast, Broadcast, Multicast) - Fragmentation and Reassembly of large frames

Plane	Functionality
	- Error Checking using FCS - Buffering and Flow Control (managing congestion) - QoS (Quality of Service) Support - Retransmission in case of error (via ACK or Block ACK)

4) Explain the scanning process and its types in detail

The **scanning process** in Wi-Fi allows a client device (such as a laptop, smartphone, or tablet) to detect and connect to available wireless networks. It is a crucial step in the process of network discovery, where a device identifies all nearby access points (APs) and evaluates which one to connect to.

There are **two main types of scanning**: **Active Scanning** and **Passive Scanning**. Each scanning method has its unique characteristics, advantages, and use cases.

1. Active Scanning:

In **active scanning**, the client actively seeks out networks by broadcasting **Probe Requests** on specific channels. This process allows the client to receive **Probe Responses** from nearby access points.

Process:

1. **Probe Request**:
    - The client sends a **Probe Request** frame to search for available networks. This frame may include specific parameters, such as the **SSID** (Service Set Identifier) of the network the client is looking for.
2. **Probe Response**:
    - APs in the vicinity that are configured to support the requested SSID will reply with a **Probe Response** frame, containing information about the network, such as the SSID, supported data rates, security settings (e.g., WPA, WPA2), and other capabilities.
3. **Channel Hopping**:
    - The client may send probe requests on various channels, hopping across different frequency bands (2.4 GHz or 5 GHz) to discover all the available networks.
4. **Network Selection**:
    - Once the client receives responses from nearby APs, it evaluates the available networks based on criteria such as signal strength, security settings, and network load, and selects an AP to associate with.

Advantages of Active Scanning:

- **Faster Discovery**: Active scanning is typically faster because the client is actively requesting information from APs.
- **Specific Network Requests**: Clients can target specific SSIDs or channels if needed.

Disadvantages of Active Scanning:

- **Increased Traffic**: Because the client actively sends probe requests on each channel, it can cause a small increase in network traffic.
- **Privacy Concerns**: Some clients may disclose the SSID they are looking for, which could be a privacy issue if not managed properly.

2. Passive Scanning:

In **passive scanning**, the client listens to the broadcasted **Beacon Frames** from nearby APs without sending out probe requests. This process is more **quiet** and requires no active requests from the client.

Process:

1. **Listening to Beacon Frames**:
   - Access Points periodically broadcast **Beacon Frames** containing information about the network, such as SSID, supported data rates, security features, and other network capabilities.
2. **Channel Hopping**:
   - The client scans through each channel at regular intervals, waiting to listen for **Beacon Frames** from APs on those channels.
3. **Network Discovery**:
   - Upon receiving a **Beacon Frame**, the client gathers information about the AP and evaluates the network for association.
4. **Network Selection**:
   - The client chooses the best AP to associate with based on received Beacon information, including signal strength, security features, and network performance.

Advantages of Passive Scanning:

- **Low Overhead**: Passive scanning doesn’t generate any extra traffic since the client only listens to the APs, making it more efficient in terms of network traffic.
- **Less Intrusive**: The client doesn’t actively send probes, thus avoiding disclosing information about which SSID it’s searching for.

Disadvantages of Passive Scanning:

- **Slower Discovery**: Since the client is only listening for beacons, the process of discovering networks can take longer compared to active scanning.
- **No Specific SSID Requests**: The client can only learn about networks that are currently broadcasting beacons, limiting the client’s ability to search for specific networks.

3. Scanning Process in Different Wi-Fi Generations:

In each Wi-Fi generation, the scanning process has evolved to include improved efficiency, faster network discovery, and better handling of multiple networks.

802.11a/b/g/n/ac/ax:

- **802.11a/b/g**: These early standards primarily used passive scanning for network discovery. Active scanning was introduced but was less common due to the limitations in hardware and network complexity.
- **802.11n/ac**: With the introduction of **MIMO** (Multiple Input Multiple Output) and **channel bonding**, the scanning process was improved to support multi-channel operations, allowing devices to discover and select networks faster.
- **802.11ax (Wi-Fi 6)**: This generation introduces features like **OFDMA** (Orthogonal Frequency Division Multiple Access), **BSS Coloring**, and **target wake time** (TWT), which optimize the scanning process by reducing interference and improving power efficiency, especially in environments with high device density.

4. Scan Algorithms and Timers:

Different Wi-Fi devices and access points may implement scanning algorithms that determine when and how often they perform scans. Here are a few examples:

1. **Scan Interval**:
    - The **scan interval** refers to the period between scans. Devices may have a fixed or adjustable scan interval, which balances power consumption and responsiveness to network changes.
2. **Scan Time**:
    - This is the duration the client spends on each channel while scanning for networks. A longer scan time can improve the chances of discovering networks, but it may also cause delays in network selection.
3. **Background Scanning**:
    - In some cases, devices perform background scans to periodically check for new networks or network changes without actively disrupting the user's current network connection.

5) Brief about the client association process

Step	Description
1. Scanning	Client scans for available APs (Active or Passive scanning).
2. Authentication	Client authenticates with the AP using either Open, Shared Key, or 802.1X authentication methods.
3. Association	Client sends an **Association Request**; AP responds with **Association**

Step	Description
	Response and assigns an **Association ID (AID)**.
4. IP Address Assignment	Client obtains an IP address using DHCP (Discovery, Offer, Request, Acknowledgment).
5. Data Transfer	Client and AP exchange data using the established connection.
6. Reassociation	If the client moves between APs, it may go through **Reassociation** (Request/Response).

6) Explain each steps involved in EAPOL 4-way handshake and the purpose of each keys derived from the process

Step 1: Message 1 - AP to Client (Nonce and Key Information)

- **Message Type**: The Access Point (AP) sends the first message (Message 1) to the client (supplicant).
- **Purpose**: The AP sends the **ANonce** (AP Nonce) and other information such as the **Pairwise Master Key (PMK)** identifier, as well as some other configuration parameters.
- **Key Information**:
  - **ANonce**: A random number generated by the AP used to ensure the freshness of the key material.
  - **PMK**: This is the secret key derived from the authentication phase (e.g., 802.1X or PSK).

The AP's message essentially indicates that it is ready to proceed with the key exchange, and it introduces the first random number (ANonce) to be used in the process.

Step 2: Message 2 - Client to AP (Nonce, MIC, and Key Information)

- **Message Type**: The client responds with the second message (Message 2).
- **Purpose**: The client (supplicant) generates its own **SNonce** (Client Nonce) and sends it to the AP along with the **Message Integrity Code (MIC)** to ensure integrity and prevent tampering.
- **Key Information**:
  - **SNonce**: A random number generated by the client to be used in the key generation process, ensuring that both sides (AP and client) have unique, fresh inputs.
  - **MIC**: A hash value that ensures the integrity of the message.
  - **Key Confirmation**: The client verifies that it knows the PMK by providing a **Key Confirmation** message to the AP.

At this point, the client generates the **PTK (Pairwise Transient Key)** using both the **ANonce** (from the AP) and **SNonce** (from the client), along with the PMK. This key is used for encryption during data transmission.

Step 3: Message 3 - AP to Client (Key Confirmation and Pairwise Key Distribution)

- **Message Type**: The AP responds with the third message (Message 3).
- **Purpose**: The AP confirms that it has received the **SNonce** and sends a confirmation message back to the client. The AP also provides the **GTK (Group Temporal Key)** to the client, which is used to encrypt multicast and broadcast traffic.
- **Key Information**:
    - **GTK**: The Group Temporal Key is used to encrypt broadcast and multicast traffic. It is the same for all clients associated with the AP and helps secure group communications.
    - **Key Confirmation**: The AP confirms to the client that the key exchange is complete.

The AP finalizes the **PTK** generation process by sending back the confirmation and GTK.

Step 4: Message 4 - Client to AP (Key Confirmation)

- **Message Type**: The client sends the final message (Message 4) to the AP.
- **Purpose**: The client confirms that it has successfully received the **GTK** and **PTK** and is ready for data transmission.
- **Key Information**:
    - **Key Confirmation**: This ensures that both the AP and the client are synchronized and have derived the same keys, confirming the handshake is complete.
    - **MIC**: Again, the message is integrity-checked with a Message Integrity Code (MIC) to ensure its authenticity.

Key Derivation Process:

During the **4-Way Handshake**, several keys are derived and used for different purposes:

1. **Pairwise Master Key (PMK)**:
    - **Source**: This key is derived during the initial authentication phase (802.1X or PSK).
    - **Purpose**: The PMK is the base key from which all other keys are derived. It is used to derive the **PTK**.
2. **Pairwise Transient Key (PTK)**:
    - **Source**: Derived using the **PMK**, **ANonce** (from AP), and **SNonce** (from client).
    - **Purpose**: The PTK is used to encrypt unicast traffic between the client and AP. It is unique to each client-AP pair and ensures that each session has its own encryption key, preventing data from being intercepted by other clients.
3. **Group Temporal Key (GTK)**:
    - **Source**: The AP generates the GTK and sends it to the client in Message 3.

  - **Purpose**: The GTK is used to encrypt multicast and broadcast traffic. It is shared among all clients connected to the same AP and ensures that group traffic remains encrypted.

4. **Message Integrity Code (MIC)**:
   - **Purpose**: The MIC is used to ensure the integrity of the messages exchanged during the handshake. It prevents tampering or modification of the handshake messages, providing protection against man-in-the-middle attacks.

Purpose of the 4-Way Handshake:

- **Key Derivation**: The primary purpose is to securely derive encryption keys (PTK and GTK) that will be used for data transmission.
- **Mutual Authentication**: Both the client and the AP prove to each other that they possess the shared secret (PMK) and are authorized to communicate.
- **Security**: The process ensures that the communication is protected using **AES** or **TKIP** encryption (depending on WPA or WPA2). The exchange of nonces (ANonce and SNonce) guarantees the freshness of the keys, preventing replay attacks.
- **Confidentiality and Integrity**: The derived keys are used to encrypt unicast traffic (PTK) and group traffic (GTK), ensuring the confidentiality of the data. The MIC ensures message integrity, protecting the handshake process from tampering.

7) Describe the power saving scheme in MAC layer and explore on the types of Power saving mechanisms

The **Power Saving Mechanism (PSM)** in the MAC layer of Wi-Fi is designed to optimize battery life in wireless devices, such as laptops, smartphones, or IoT devices, by reducing power consumption when the device is not actively transmitting or receiving data.

Wi-Fi devices (especially mobile devices) rely on **Power Saving** mechanisms to extend battery life while maintaining a connection to the wireless network. The MAC layer defines several techniques to achieve this power efficiency.

Mechanism	Description	Used In	Power Efficiency	Latency Impact
Legacy PSM (802.11b/g)	Device sleeps for set intervals, wakes up to receive data.	Older Wi-Fi Standards	Moderate	High (due to sleep cycles)
802.11 PSM (Listen Interval)	Device listens at periodic intervals specified in the beacon frame.	802.11a/b/g/n/ac	Moderate to High	Moderate
TWT (Target Wake Time)	Device and AP negotiate specific wake-up times to reduce idle time.	802.11ax (Wi-Fi 6)	High (most efficient)	Low (more synchronized)

8) Describe the Medium Access Control methodologies

Methodology	**Key Feature**	**Purpose**	**Use Case**
DCF	Random backoff and listen	Collision avoidance	Normal data traffic
PCF	Centralized polling	Contention-free communication	Voice, video (rare use)
HCF (EDCA + HCCA)	QoS support	Prioritized traffic	VoIP, gaming
OFDMA (802.11ax)	Parallel transmissions	Efficiency in dense areas	Wi-Fi 6 deployments

9) Brief about the Block ACK mechanism and its advantages

Block ACK Mechanism (in Wi-Fi)

- **Purpose**:
  - To **acknowledge multiple frames** with a single ACK instead of sending an ACK for every frame individually.
- **How it Works**:
  - The sender transmits **a burst of data frames** (called an Aggregated MPDU - A-MPDU).
  - Instead of sending ACK after every frame, the receiver sends **one Block Acknowledgment** after receiving multiple frames.
  - The Block ACK contains a **bitmap** indicating which frames were received successfully and which were lost.
  - Only the missing frames are retransmitted if needed.

Advantages of Block ACK:

- **Reduces Overhead**:
  Fewer ACKs = less control traffic = more efficiency.
- **Increases Throughput**:
  Sending multiple frames at once without waiting boosts the speed.
- **Improves Efficiency in High-Speed Networks**:
  Essential for 802.11n, 802.11ac, and 802.11ax standards where speeds are very high.
- **Better Performance in Noisy Environments**:
  Selective retransmission (only missing frames are resent) saves time.
- **Supports Frame Aggregation**:
  Works perfectly with A-MPDU aggregation to maximize wireless capacity.

10) Explain about A-MSDU, A-MPDU and A-MSDU in A-MPDU

1. A-MSDU (Aggregated MAC Service Data Unit)

- **What it is**:
  Multiple **MSDUs** (data packets) are combined into **one large frame** at the MAC layer before transmission.
- **Key Points**:
  - Combines several upper-layer packets into a single 802.11 frame.
  - **Single MAC header** for all the combined MSDUs.
  - Efficient when destination addresses are the same or similar.
- **Advantages**:
  - **Reduces MAC header overhead**.
  - Improves transmission efficiency for small packets.
- **Drawback**:
  - If one part of A-MSDU is corrupted, the **entire frame** must be retransmitted.

2. A-MPDU (Aggregated MAC Protocol Data Unit)

- **What it is**:
  Multiple **MPDUs** (each with its own MAC header and trailer) are grouped together for transmission.
- **Key Points**:
  - Each subframe is independently CRC-protected.
  - Aggregated at the PHY layer.
- **Advantages**:
  - **Error isolation**: Only the corrupted MPDU needs retransmission.
  - **Higher efficiency** for large amounts of data.
  - Works with **Block ACK** for selective retransmission.
- **Drawback**:
  - Slightly more overhead due to multiple headers compared to A-MSDU.

3. A-MSDU inside A-MPDU

- **What it is**:
  You can **combine** both aggregation methods:

    - **First**, group several MSDUs into an **A-MSDU**.
    - **Then**, bundle multiple A-MSDUs into an **A-MPDU**.
- **Key Points**:
    - Maximizes bandwidth efficiency.
    - Reduces both MAC and PHY overheads.
- **Use case**:
    - Very high-throughput operations (like Wi-Fi 5 and Wi-Fi 6).