Wi-Fi Training Program
Assignment Questions -Module 3

Q1: What is the significance of MAC layer and in which position it is placed in the OSI model?

1. **Medium Access Control:**
   It ensures fair access to the wireless medium using protocols like CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
2. **Addressing:**
   It adds source and destination MAC addresses to frames, enabling proper data delivery on the local network.
3. **Frame Construction and Parsing:**
   It builds and processes frames, including management, control, and data frames.
4. **Error Detection:**
   Uses CRC (Cyclic Redundancy Check) to detect frame errors through the Frame Check Sequence (FCS).
5. **Retransmission and Acknowledgment:**
   Handles reliable transmission using ACK frames and retransmissions in case of errors.
6. **Power Management:**
   Supports power-saving features like sleep mode and wake-up notifications.
7. **Security Functions:**
   Plays a role in authentication and encryption key exchange (e.g., during the EAPOL handshake).

OSI Model Placement:

- **Layer 2 – Data Link Layer**, which is divided into two sublayers:
  - **LLC (Logical Link Control) sublayer** – manages communication with the network layer.
  - **MAC sublayer** – manages access to the physical medium.

Q2: Describe the frame format of the 802.11 MAC header and explain the purpose of each field

1. **Frame Control (2 bytes)**
   - Contains control information about the frame type and flags.
   - Subfields include:
     - Protocol Version (2 bits)
     - Type (2 bits) – Management, Control, Data
     - Subtype (4 bits)
     - To DS/From DS (1 bit each) – used in determining the frame's direction
     - More Fragments (1 bit), Retry (1 bit), Power Management (1 bit)
     - More Data, Protected Frame, Order
2. **Duration/ID (2 bytes)**
   - Indicates the time (in microseconds) the channel will be reserved for the frame transmission.
   - Also used for NAV (Network Allocation Vector) settings to avoid collisions.
3. **Address Fields (6 bytes each)**
   - Up to **four address fields**, depending on the frame direction:
     - Address 1: Destination MAC address
     - Address 2: Source MAC address
     - Address 3: BSSID or forwarding address
     - Address 4: Used in WDS (Wireless Distribution System) for mesh or bridging
4. **Sequence Control (2 bytes)**
   - Contains a **sequence number** and **fragment number**.
   - Used to reassemble fragmented frames and detect duplicates.
5. **QoS Control (2 bytes) [Optional]**
   - Present in QoS Data frames.
   - Indicates traffic priority, ACK policies, and other QoS settings.
6. **HT/VHT/HE Control (4+ bytes) [Optional]**
   - Present in high-efficiency (802.11n/ac/ax) data frames.
   - Used for advanced modulation, coding, and scheduling information.

7. **Frame Body (variable)**
    - Carries the actual data or management/control information (e.g., probe requests, beacons, authentication info).
8. **FCS – Frame Check Sequence (4 bytes)**
    - Used for error detection using CRC (Cyclic Redundancy Check).

Q3: Please list all the MAC layer functionalities in all Management, Control and Data planes

1. Management Plane Functionalities

These functions manage the connection and maintenance of communication between devices (stations and access points):

- **Beaconing:**
  Access Points (APs) periodically send beacon frames to announce their presence and capabilities.
- **Authentication/Deauthentication:**
  Handles verification of client identities. Authentication frames are exchanged before a station is allowed to join a network.
- **Association/Reassociation/Disassociation:**
    - **Association** allows a client to connect to an AP.
    - **Reassociation** allows a client to move between APs within the same network.
    - **Disassociation** informs that the client is disconnecting.
- **Probing:**
  Stations send **probe request** frames to discover APs, and APs respond with **probe response** frames.
- **Capability Exchange:**
  During association/authentication, devices share supported features (e.g., data rates, security options).

2. Control Plane Functionalities

These are short frames that assist in the coordination of data frame delivery and medium access:

- **RTS/CTS (Request to Send / Clear to Send):**
  Used to avoid collisions, especially in hidden node scenarios.
- **ACK (Acknowledgment):**
  Confirms successful reception of a unicast frame.
- **PS-Poll (Power Save Poll):**
  Sent by stations in power-saving mode to retrieve buffered data from the AP.
- **CF-End/CF-Ack (Contention-Free End/Acknowledgment):**
  Used in PCF (Point Coordination Function) mode, less commonly used today.

3. Data Plane Functionalities

These functions handle the actual transmission of user data across the network:

- **Data Transmission/Reception:**
  Encapsulation and delivery of higher-layer data (e.g., IP packets).
- **Fragmentation and Reassembly:**
  Breaks large frames into smaller fragments to improve reliability over unreliable links.
- **Encryption and Decryption:**
  Protects data confidentiality using security protocols like WPA2/WPA3.
- **QoS Support (802.11e):**
  Prioritizes traffic types (voice, video, best-effort, background).

Q4: Explain the scanning process and its types in detail

1. Passive Scanning

In passive scanning, the client device listens for **beacon frames** that are periodically transmitted by access points on each channel. These beacons contain essential network information, such as:

- Service Set Identifier (SSID)
- Supported data rates
- Security protocols (e.g., WPA2, WPA3)
- Channel and frequency information

Operational Steps:

1. The client tunes to a specific channel.

2. It listens for a predefined time interval (dwell time).
3. If a beacon is detected, the network information is recorded.
4. The client then switches to the next channel and repeats the process.

2. Active Scanning

In active scanning, the client device initiates the discovery process by transmitting **probe request frames** across each channel. Access points that receive these requests respond with **probe response frames**, containing similar information as beacon frames.

Operational Steps:

1. The client sends a probe request on a specific channel.
2. Nearby APs on that channel respond with probe responses.
3. The client collects and evaluates the responses.
4. The client moves to the next channel and repeats the process.

Q5: Explain the client association process

1. Authentication

This is the initial step where the client and the access point mutually identify each other.

- **Open System Authentication** (most common):
    - The client sends an **Authentication Request** frame.
    - The AP responds with an **Authentication Response** indicating success or failure.
- **Shared Key Authentication** (deprecated for security reasons):
    - Involves WEP keys and a challenge-response mechanism.

Note: This is not the same as upper-layer (e.g., WPA2/WPA3) authentication, which occurs later during security key exchange (via EAPOL/4-way handshake).

2. Association

Once authentication is successful, the client initiates the association process.

- The client sends an **Association Request** frame, which includes:
    - Supported data rates

    - Capability information
    - SSID
    - Power management and QoS features
- The AP processes the request and, if accepted, responds with an **Association Response** frame containing:
    - Association ID (AID)
    - Supported features confirmation
    - Status code (success or failure)

Q6: Explain each step involved in EAPOL 4-way handshake and the purpose of each key derived from the process

The **EAPOL (Extensible Authentication Protocol over LAN) 4-way handshake** is a critical security process in WiFi networks (specifically under WPA2 and WPA3 standards) that occurs after the client and the access point have successfully authenticated. Its primary goal is to confirm that both parties share the same **Pairwise Master Key (PMK)** and to securely derive session keys that will be used for encrypted communication. The handshake ensures mutual authentication, prevents replay attacks, and facilitates the secure exchange of encryption keys.

Steps Involved in the 4-Way Handshake:

1. **Message 1 – Authenticator to Supplicant:**
    - The authenticator (typically the AP) generates a random number called the **ANonce (Authenticator Nonce)** and sends it to the client.
    - **Purpose:** Initiates the key exchange process and provides input for PTK generation.
2. **Message 2 – Supplicant to Authenticator:**
    - The supplicant (client) generates its own **SNonce (Supplicant Nonce)** and derives the **Pairwise Transient Key (PTK)** using PMK, ANonce, SNonce, and the MAC addresses of both devices.
    - It sends the SNonce and a **Message Integrity Code (MIC)** computed using the PTK.
    - **Purpose:** Proves possession of the PMK and provides necessary elements for key derivation.

3. **Message 3 – Authenticator to Supplicant:**
    - The authenticator computes the same PTK and verifies the MIC from the client.
    - It then sends the **Group Temporal Key (GTK)** encrypted with a portion of the PTK and includes its own MIC.
    - **Purpose:** Confirms both sides have the same PTK and distributes the GTK securely.
4. **Message 4 – Supplicant to Authenticator:**
    - The supplicant installs the keys and sends a final message to confirm that the handshake is complete.
    - **Purpose:** Finalizes the key installation and signals readiness for secure communication.

Q7: Describe the power saving scheme in MAC layer and explore the types of power saving mechanisms

1. **Power Save Mode (PS Mode):**
    - When enabled, the client device notifies the AP via a Power Management bit set in the MAC frame header.
    - The AP buffers data for the client while it is asleep.
2. **Traffic Indication Map (TIM):**
    - Periodically sent in **beacon frames**.
    - TIM indicates which stations have buffered data waiting at the AP.
    - The client wakes up at each beacon interval to check the TIM.
3. **PS-Poll (Power Save Poll):**
    - If the TIM shows buffered data, the client sends a **PS-Poll** frame to the AP.
    - The AP then sends the buffered data to the client.

Types of Power Saving Mechanisms:

1. **Legacy Power Save Mode (802.11 Standard):**
    - Basic sleep and wake-up scheduling using TIM and PS-Poll.
    - Introduced in the original 802.11 standard.

    - Suitable for low-throughput and delay-tolerant applications.

2. **Unscheduled Automatic Power Save Delivery (U-APSD):**
    - Introduced in 802.11e for **QoS-enabled** networks.
    - Reduces overhead by eliminating the need for PS-Poll frames.
    - The client triggers data delivery by sending an uplink frame.
    - Ideal for real-time applications like VoIP.
3. **Scheduled Automatic Power Save Delivery (S-APSD):**
    - Pre-arranged data delivery schedules between AP and client.
    - Used in environments with predictable traffic patterns.
4. **Target Wake Time (TWT) – 802.11ax (Wi-Fi 6):**
    - Allows devices to negotiate specific times to wake and communicate.
    - Highly efficient for dense IoT deployments.
    - Significantly reduces idle listening and improves battery life.

Q8: Describe the Medium Access Control methodologies

1. Distributed Coordination Function (DCF):

- **Type:** Contention-based, decentralized
- **Mechanism:** Uses **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**.
- **Process:**
    - Devices sense the channel before transmitting.
    - If the medium is idle, they transmit after a random backoff period.
    - If busy, they defer until it becomes idle.
- **Acknowledgement:** Each successful transmission is followed by an **ACK frame** to confirm reception.
- **Usage:** Default access method in most Wi-Fi networks.

2. Point Coordination Function (PCF):

- **Type:** Contention-free, centralized

- **Mechanism:** Uses a **Point Coordinator (typically the AP)** to poll stations for data in a scheduled manner.
- **Operation:** Occurs during a **Contention-Free Period (CFP)** that alternates with DCF.
- **Usage:** Rarely used in practice due to complexity and limited support in devices.

3. Hybrid Coordination Function (HCF):

- **Introduced in:** IEEE 802.11e (QoS enhancement)
- **Includes:**
  - **Enhanced Distributed Channel Access (EDCA):**
    - Prioritizes traffic using multiple access categories (voice, video, best effort, background).
    - Offers better Quality of Service (QoS) by allowing time-sensitive traffic to access the medium faster.
  - **HCF Controlled Channel Access (HCCA):**
    - A centralized method where the **Hybrid Coordinator** schedules transmission opportunities (TXOPs) for QoS streams.

Q9: Brief about the Block ACK mechanism and its advantages

Concept of Block ACK Mechanism:

- In traditional 802.11 communication, each unicast frame must be individually acknowledged by an **ACK** frame.
- The Block ACK mechanism allows a sender to transmit a series of frames (aggregated or sequentially) without waiting for an individual ACK after each one.
- After sending a group of frames (called a **Block of frames**), the receiver sends a single **Block ACK frame** indicating the successful reception status of all frames within that block.

Types of Block ACK:

1. **Immediate Block ACK:**
   - The receiver responds with a Block ACK frame immediately after receiving the block of frames.
2. **Delayed Block ACK:**

  - The receiver waits for a short time before sending the Block ACK, allowing more flexibility in handling network conditions.

Advantages of Block ACK Mechanism:

- **Increased Throughput:**
  - Reduces the overhead caused by multiple individual ACK frames.
  - Especially beneficial for high data rate transmissions like video streaming and large file transfers.
- **Improved Efficiency:**
  - Decreases the amount of control traffic, freeing up the channel for actual data transmission.
  - Reduces contention and backoff time between transmissions.
- **Better QoS Support:**
  - Works efficiently with QoS mechanisms by supporting the quick and reliable delivery of grouped packets, essential for real-time applications.
- **Enhanced Aggregation:**
  - Works alongside frame aggregation techniques such as **A-MPDU** (Aggregated MAC Protocol Data Unit) to maximize the utilization of the channel.
- **Lower Latency:**
  - Reduces delay in acknowledging frames, making communication smoother, especially under heavy network loads.

Q10: Explain about A-MSDU, A-MPDU, and A-MSDU in A-MPDU

In IEEE 802.11n and subsequent standards, frame aggregation techniques were introduced to enhance data throughput and transmission efficiency. The two primary methods of aggregation are **A-MSDU (Aggregated MAC Service Data Unit)** and **A-MPDU (Aggregated MAC Protocol Data Unit)**. An A-MSDU aggregates multiple MAC Service Data Units into a single MAC Protocol Data Unit. These MSDUs share a single MAC header, resulting in lower overhead and improved channel efficiency. However, because the entire A-MSDU is treated as a single frame, if any part of it is corrupted during transmission, the entire frame must be retransmitted, making it less robust in error-prone environments.

On the other hand, **A-MPDU** aggregates multiple MPDUs into a single physical layer transmission (PPDU). Each MPDU retains its own MAC header and checksum, and they are separated by delimiters. This structure allows for selective retransmission of only the corrupted MPDUs, offering higher reliability and better error handling, especially in high-interference environments. While this adds slightly more overhead than A-MSDU, it provides a more robust solution for high-throughput communications.

Further enhancement is achieved by combining both techniques—**A-MSDU within A-MPDU**—where multiple MSDUs are grouped into A-MSDUs, and several A-MSDUs are then packed into separate MPDUs that are aggregated into an A-MPDU. This nested aggregation maximizes channel efficiency while preserving reliability through individual MPDU checksums and retransmissions. This hybrid approach is particularly useful in modern Wi-Fi standards, balancing overhead reduction with error resilience for optimal performance.