MODULE 4

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

   The MAC (Medium Access Control) layer is responsible for controlling how devices on a network gain access to the medium and permission to transmit data along with targeted frame delivery. It ensures reliable data transmission by managing collisions (CSMA/CD) and regulating traffic over the shared medium.
   The MAC layer is a sublayer of the **Data Link Layer (Layer 2)** in the OSI model, along with the Logical Link Control (LLC) sublayer.

2. Describe the frame format of the 802.11 MAC header and explain the purpose of each field.

   The 802.11 MAC header is part of every Wi-Fi frame and contains control information for managing wireless communication. The IEEE 802.11 MAC frame consists of several fields, divided into the MAC header, frame body, and FCS (Frame Check Sequence). The MAC header contains control information essential for communication.

FIELD	SIZE (BYTES)	FUNCTION
Frame Control	2	Indicates the type of frame (Management, Control, or Data). Contains flags like To DS, From DS, More Fragments, Retry, Power Management, etc.
Duration/ID	2	Specifies the time duration the medium will be reserved (used for NAV - Network Allocation Vector). In some control frames, it carries association ID.
Address 1 (Receiver Address)	6	MAC address of the receiver.
Address 2 (Transmitter Address)	6	MAC address of the sender.
Address 3 (BSSID or destination)	6	Can be the BSSID, source, or destination depending on the frame type.
Sequence Control	2	Includes the sequence number and fragment

		number for packet ordering and reassembly.
Address 4 (only in WDS)	6	Used only in frames when both ToDS and FromDS bits are set (WDS – Wireless Distribution System).
QoS Control	2	Present in QoS data frames; helps prioritize traffic types (voice, video, etc.).
Frame Body	Upto 2304	Contains the data or management information being transferred.
FCS – Frame Check Sequence	4	CRC used for error detection of the entire frame.

Each field in the MAC header plays a role in addressing, sequencing, controlling access, and ensuring reliability of wireless communication, adapting to infrastructure or ad-hoc modes and supporting features like QoS and HT capabilities.

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

- ❖ Management plane: handle network setup, maintenance, and teardown.
  - Authentication: Verifies identity of stations (STA).
  - Deauthentication**:** Invalidates the authentication between STA and AP.
  - Association/Reassociation: Establishes a connection between STA and AP.
  - Disassociation**:** Terminates an existing connection.
  - Beacon Transmission: Periodic broadcast for network discovery.
  - Probe Request/Response**:** Used during active scanning to discover networks.
  - Timing Synchronization**:** Maintains clock alignment across devices (via timestamps in beacons).
- ❖ Control plane: These support efficient and collision-free data transmission.
  - RTS/CTS (Request to Send / Clear to Send): Avoids hidden node collision.
  - ACK (Acknowledgement): Confirms successful frame reception.
  - Contention Window Management: Controls backoff timing in CSMA/CA.
  - NAV (Network Allocation Vector): Virtual carrier sensing to avoid overlapping transmission.

- PS-Poll (Power Save Poll): Used by STA to retrieve buffered frames from AP during power-saving mode.
- TXOP (Transmission Opportunity): Allocates a specific time interval for a device to transmit.

❖ Data plane: These deal with actual user data delivery.
- Frame Aggregation: Combines multiple frames for efficiency (A-MPDU, A-MSDU).
- Addressing: Uses MAC addresses for delivery.
- Sequence Control: Maintains correct frame order.
- Fragmentation and Reassembly**:** Splits large frames for transmission and reassembles them.
- Error Detection and Recovery: Uses CRC (FCS field) and ACK-based recovery.
- Multicast and Broadcast Handling: Delivers to multiple or all stations.

4. Explain the scanning process and its types in detail.

The scanning process is how a wireless station (STA) discovers nearby wireless networks before associating with an Access Point (AP). Scanning allows the STA to identify available networks (SSIDs), their capabilities, and signal strength. There are mainly two types of scanning: active and passive.

- Active Scanning: A proactive network discovery method where the wireless station (STA) actively transmits probe request frames on each channel. Access points (APs) receiving these requests respond with probe response frames, allowing the STA to quickly identify and gather information about available networks. This method is faster but consumes more power and is easily detectable.

- Passive Scanning: A network discovery method where a wireless station (STA) listens for beacon frames periodically broadcast by nearby access points (APs) on each channel without sending any probe frames. It is a silent process and consumes low power, making it ideal for energy-efficient or stealth operations.

Feature	Passive Scanning	Active Scanning
Process	STA listens for beacon frames broadcast by Aps. Switches channel and waits for beacons.	STA broadcasts probe request frames on each channel. APs respond with probe response frames.
Information Collected	SSID, supported rates, security capabilities, timestamp.	SSID, supported rates, security capabilities, timestamp.

Transmission by STA	No	Yes
Power Consumption	Low	High
Speed	Slow	Fast
Detectability	Undetectable	Detectable
Best Use Case	Power-saving or stealthy operations.	Fast network discovery or urgent connection.
Limitations	May miss networks with long beacon intervals.	Not ideal for stealth or low-power devices.

5. Brief about the client association process.

   The client association process is the procedure by which a wireless station (STA) connects to an access point (AP) to become part of a Wi-Fi network. It typically involves three main steps:

   i. Scanning
   - The STA scans available channels to discover nearby APs using passive or active scanning.
   - It collects information like SSID, signal strength, supported rates, and security features.

   ii. Authentication
   - STA initiates the connection by sending an **authentication request** frame.
   - AP responds with an **authentication response**.
   - This can be **open system** (no real security) or **shared key** (WEP, WPA/WPA2/WPA3).

   iii. Association Request/ Response
   - After successful authentication, the STA sends an association request frame to the AP. This includes capabilities, supported rates, SSID, etc.
   - The AP replies with an association response frame, completing the process.
   - STA is now associated and can exchange data with the AP.

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

   The EAPOL (Extensible Authentication Protocol over LAN) 4-way handshake is a crucial process that occurs after association in a secure Wi-Fi network (WPA2/WPA3). Its purpose is to establish encryption keys between the client (STA) and the Access Point (AP) for secure data transmission.

Purpose:

- Verify both client and AP have the same Pairwise Master Key (PMK).
- Derive and install a Pairwise Transient Key (PTK) for encryption.
- Establish Group Temporal Key (GTK) for broadcast/multicast traffic.

Steps:

- AP → STA (Message 1)
  AP sends an ANonce (Authenticator Nonce) to the STA.
  Used to begin the PTK generation process.

- STA → AP (Message 2)
  STA generates SNonce (its own nonce).
  STA derives the PTK using PMK (from previous authentication), ANonce (from AP), SNonce (STA's own random value), MAC addresses of AP and STA.
  Sends SNonce and Message Integrity Code (MIC) to AP.

- AP → STA (Message 3)
  AP generates the same PTK using PMK, ANonce, SNonce, and MACs.
  AP sends Group Temporal Key (GTK) encrypted with PTK.
  STA installs both PTK and GTK.

- STA → AP (Message 4)
  STA sends a final ACK to confirm installation of keys.
  Data encryption begins.

- Pairwise Master Key (PMK): Acts as the root key used to derive the Pairwise Transient Key (PTK).
- Pairwise Transient Key (PTK): Used for **unicast** (STA ↔ AP) encryption and message integrity.
- Group Temporal Key (GTK): Used for encrypting broadcast and multicast traffic from the AP to all associated STAs.
- ANonce and SNonce: Provide randomness to the PTK derivation process, ensuring that keys are unique for every session.

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

   The MAC layer power saving mechanism in IEEE 802.11 is designed to help wireless devices, especially battery-powered ones, reduce energy consumption by limiting radio activity when not engaged in data transmission or reception.

   Working:

- Devices (STAs) enter sleep mode to save power.
- AP buffers data for sleeping STAs.
- STAs wake up periodically (based on beacon intervals) to check if there's data for them.

  Mechanisms

  - Power Save Mode (PS Mode):
    The STA informs the AP that it is entering sleep mode. The AP buffers all incoming frames for that STA. The STA wakes up at each beacon interval to read the Traffic Indication Map (TIM) in the beacon frame. If its ID is listed, it sends a PS-Poll frame to the AP to retrieve the buffered data.

  - U-APSD (Unscheduled Automatic Power Save Delivery):
    Commonly used with Wi-Fi Multimedia (WMM) features, this mechanism eliminates the need for sending PS-Poll frames. The STA triggers data delivery by sending an uplink frame (e.g., a VoIP packet), and the AP automatically responds with the buffered downlink frames. This mechanism reduces latency, making it ideal for real-time voice and video applications.

  - TWT (Target Wake Time) (Introduced in 802.11ax – Wi-Fi 6):
    STAs negotiate specific wake-up times with the AP. This allows devices to remain in sleep mode for extended periods while ensuring they don't miss important data. It is highly efficient for dense networks and IoT devices, where long sleep cycles are desirable for battery longevity.

8. Describe the Medium Access Control methodologies.

   In Wi-Fi networks (IEEE 802.11), the Medium Access Control (MAC) layer defines different functions to manage how devices access the shared communication medium. These include Point Coordination Function (PCF), Distributed Coordination Function (DCF), and Enhanced Distributed Channel Access (EDCA), which are essential for managing channel access and ensuring efficient and fair communication.

   Point Coordination Function (PCF):
   - PCF is a contention-free access mechanism, primarily used in infrastructure mode with an Access Point (AP) controlling the medium access. It operates in polling mode, where the AP controls when stations (STAs) are allowed to transmit.
   - The AP periodically sends a polling frame to each STA, asking if they have data to send. Only the polled STA is allowed to transmit, eliminating collisions and ensuring a more predictable transmission.

- PCF is ideal for time-sensitive applications (like VoIP or streaming) because it reduces contention and delay, but it requires a point coordinator (typically the AP) and is not commonly used in practical, high-throughput Wi-Fi networks due to overhead.

Distributed Coordination Function (DCF):

- DCF is the fundamental mechanism used in most Wi-Fi networks for managing access to the medium. It is a contention-based access method, where devices listen to the channel to determine if it's free or busy before transmitting.
- The Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol is used by DCF to avoid collisions. Devices first check if the channel is idle for a specific duration (called the DIFS - Distributed Interframe Space). If idle, they transmit; if busy, they wait and back off.
- Backoff is a random time delay that is computed using a backoff counter. This reduces the likelihood of multiple devices transmitting at the same time (collision).
- DCF is flexible and works in both ad-hoc and infrastructure modes, providing basic access control but without strict priority or guarantees for real-time applications.

Enhanced Distributed Channel Access (EDCA):

- Prioritizes traffic into 4 Access Categories (AC): Voice, Video, Best Effort, Background.
- High-priority traffic is assigned smaller contention windows, allowing for quicker access to the channel. This supports applications such as VoIP and streaming, ensuring lower latency and better performance.

9. Brief about the Block ACK mechanism and its advantages.

The Block ACK mechanism in IEEE 802.11 enhances data transmission efficiency, particularly in high-throughput networks. Instead of sending an acknowledgment for each individual frame, the receiver sends a single acknowledgment for a group of frames. This reduces the overhead and increases throughput, especially during large data transfers, such as video streaming or file uploads.
Working

a) The transmitter sends a Block ACK Request after transmitting a set of frames.
b) The receiver responds with a Block ACK Response, indicating which frames were successfully received.
c) If any frames are lost, they can be retransmitted selectively.

Advantages

- By sending a single acknowledgment for a block of frames instead of individual ACKs for each frame, the control frame overhead is significantly reduced. This is especially beneficial in high-speed networks.
- With fewer control frames (ACKs), more bandwidth is available for actual data transmission, resulting in higher overall throughput.
- The Block ACK frame uses a bitmap to indicate which frames were successfully received. Only the lost or corrupted frames need to be retransmitted, saving time and bandwidth compared to retransmitting all frames.
- The sender doesn't need to wait for an acknowledgment after every individual frame, reducing transmission delays and allowing faster data flow.
- Block ACKs are particularly effective for burst data transmissions (e.g., video or large file transfers), where a lot of data is sent quickly, as they ensure efficient and quick transmission without excessive overhead.
- The mechanism allows for more efficient communication in networks with multiple devices, making it easier to manage higher data rates and multiple connections simultaneously.

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

These frame aggregation techniques, introduced in Wi-Fi (starting from 802.11n), are designed to improve efficiency and reduce overhead.

A-MSDU (Aggregated MAC Service Data Unit):

- Combines multiple MSDUs (upper-layer data units) into a single MAC frame. All subframes within the aggregation share a single MAC header. All subframes must have the same Traffic ID (TID) and destination.
- Reduces MAC header overhead, making it more efficient for small payloads.
- If any part of the A-MSDU is corrupted, the entire frame must be retransmitted.

A-MPDU (Aggregated MAC Protocol Data Unit):

- Aggregates multiple MPDUs (complete MAC frames with headers). Each MPDU can be retransmitted independently. Sent as a single PHY frame with support for Block ACK.
- Selective retransmission: If any MPDU is lost, only that specific MPDU needs to be retransmitted. More robust and flexible compared to A-MSDU.
- Slightly more PHY-layer overhead than A-MSDU due to the additional MPDU headers.

A-MSDU in A-MPDU (Two-Level Aggregation):

- Aggregates multiple A-MSDUs, which are then packaged into multiple MPDUs within an A-MPDU.

- Reduces overhead through A-MSDU aggregation, Supports retransmission through A-MPDU aggregation.
- Maximizes throughput and efficiency, especially used in Wi-Fi 6 and later standards.