Module 4

1. What is the significance of the MAC layer and its position in the OSI model?

- **OSI Layer Position:** The MAC layer is part of the **Data Link Layer (Layer 2)** in the OSI model.
- **Significance:**
    - Handles **frame delivery** across local networks.
    - Controls access to the shared transmission medium (e.g., air or cable).
    - Responsible for **collision avoidance**, **addressing (MAC addresses)**, and **channel access protocols** like CSMA/CA.
    - Works closely with the **Physical Layer** to transmit data.

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

802.11 MAC Header Structure:

- **Frame Control (2 bytes):** Indicates type of frame (management/control/data) and various flags.
- **Duration/ID (2 bytes):** Used for NAV (Network Allocation Vector) to reserve time on medium.
- **Address 1:** Receiver Address.
- **Address 2:** Transmitter Address.
- **Address 3:** BSSID (Basic Service Set Identifier).
- **Sequence Control (2 bytes):** Contains fragment number and sequence number.
- **Optional Address 4:** Used in WDS (Wireless Distribution System).
- **Frame Body:** Actual payload data.
- **FCS (4 bytes):** Frame Check Sequence for error detection.

3. List all MAC layer functionalities in Management, Control, and Data planes.

- **Management:**
    - Beacon transmission
    - Association & disassociation
    - Authentication & deauthentication

    - Scanning (passive/active)
- **Control:**
    - RTS/CTS (Request to Send / Clear to Send)
    - ACK (Acknowledgment)
    - Power-save poll
- **Data:**
    - Data frame transfer
    - Fragmentation & reassembly
    - Sequence numbering

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

- **Scanning:** The process by which a client discovers available wireless networks.
- **Types:**
    - **Passive Scanning:**
        - Listens for **beacons** sent by access points.
        - Consumes less power but slower.
    - **Active Scanning:**
        - Sends **probe request** and waits for **probe response**.
        - Faster but consumes more power.

5. Brief about the client association process.

1. **Scanning:** Client detects APs via passive or active scanning.
2. **Authentication:** Client and AP exchange authentication frames.
3. **Association Request:** Client sends request frame with capabilities.
4. **Association Response:** AP approves or denies the request.
5. **Client is associated:** Can begin data transfer.

6. Explain each step in the EAPOL 4-way handshake and key derivation.

Used in WPA/WPA2 for secure key exchange.

Steps:

1. **Message 1:** AP sends ANonce to the client.

2. **Message 2:** Client generates PTK using ANonce, SNonce, and PMK, sends SNonce to AP.
3. **Message 3:** AP computes PTK, installs key, and sends GTK (Group Temporal Key).
4. **Message 4:** Client installs key and sends acknowledgment.

Keys Derived:

- **PMK (Pairwise Master Key):** From passphrase or 802.1X.
- **PTK (Pairwise Transient Key):** Derived during handshake.
- **GTK (Group Temporal Key):** For multicast/broadcast.

7. Describe power saving scheme in MAC layer and types of power-saving mechanisms.

- **Purpose:** Extend battery life of wireless clients.
- **Mechanisms:**
    - **Power Save Poll (PS-Poll):** Client asks AP for buffered frames.
    - **Listen Intervals:** Clients wake up periodically to check beacons.
    - **U-APSD (Unscheduled Automatic Power Save Delivery):** Frames are delivered with data trigger.

8. Describe the Medium Access Control methodologies.

- **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):**
    - Used in Wi-Fi.
    - Devices sense channel before transmission.
- **RTS/CTS:** Helps avoid hidden node problem.
- **Backoff Algorithm:** Random delay before retrying transmission to prevent collisions.

9. Brief about Block ACK mechanism and its advantages.

- **Block ACK (BA):** A single acknowledgment frame is sent for a block of data frames instead of one by one.
- **Advantage:**
    - Reduces overhead
    - Improves throughput
    - Efficient for burst data (e.g., video streaming)

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

- **A-MSDU (Aggregated MAC Service Data Unit):**
    - Multiple MSDUs in one MPDU.
    - Saves header overhead.
    - Shared MAC header.
- **A-MPDU (Aggregated MAC Protocol Data Unit):**
    - Multiple MPDUs in one PHY frame.
    - Each MPDU has its own MAC header and FCS.
    - More robust error handling.
- **A-MSDU in A-MPDU:**
    - Nested aggregation.
    - Several A-MSDUs within individual MPDUs.
    - Improves bandwidth efficiency with some complexity.