**1. Significance of MAC Layer and OSI Position**

The **MAC (Medium Access Control) layer** controls how devices access and use the shared wireless medium.  
It manages framing, addressing, access coordination, security, and reliability.

* **OSI Model Position**: It belongs to the **Data Link Layer (Layer 2)**, just above the Physical Layer.

**2. Frame Format of 802.11 MAC Header**

The MAC header in 802.11 frames consists of several fields:

* **Frame Control (2 bytes)**: Defines type (Management, Control, Data), and control flags.
* **Duration/ID (2 bytes)**: Indicates duration needed for transmission.
* **Address Fields (6 bytes × 3 or 4)**:
  + Address 1: Receiver address.
  + Address 2: Transmitter address.
  + Address 3: BSSID or destination/source.
  + Address 4: Used in mesh networks (optional).
* **Sequence Control (2 bytes)**: Frame number and fragmentation control.
* **QoS Control (optional)**: For Quality of Service (in 802.11e onwards).
* **HT/VHT/HE Control (optional)**: For higher throughput features.

Each field ensures correct delivery, security, and traffic handling.

**3. MAC Layer Functionalities: Management, Control, and Data Planes**

* **Management Plane**:
  + Authentication and Deauthentication.
  + Association and Reassociation.
  + Beaconing and Probing.
  + Power management.
* **Control Plane**:
  + RTS (Request to Send)/CTS (Clear to Send).
  + Acknowledgments (ACK).
  + Power Save Poll (PS-Poll).
* **Data Plane**:
  + Data frame delivery.
  + Fragmentation and reassembly.
  + Encryption and decryption.

**4. Scanning Process and Types**

**Scanning** helps clients discover Access Points (APs).

* **Passive Scanning**: Client listens for Beacons broadcasted by APs periodically.  
  (Energy-saving, but slower connection.)
* **Active Scanning**: Client sends Probe Requests; APs respond with Probe Responses.  
  (Faster discovery but consumes more power.)

**5. Client Association Process**

The process where a client connects to an AP:

* **Scanning**: Detect APs.
* **Authentication**: Establish identity (open or secure).
* **Association**: Join the AP network.
* **Key Exchange**: (If secured) 4-way handshake to establish encryption.  
  Successful association enables the client to send/receive data on the Wi-Fi network.

**6. EAPOL 4-Way Handshake and Key Derivation**

The **4-Way Handshake** secures the communication after association:

* **Step 1**: AP sends **ANonce** to Client.
* **Step 2**: Client uses ANonce + SNonce + PMK to generate the PTK, then sends SNonce back.
* **Step 3**: AP computes PTK, validates, and sends Group Temporal Key (GTK).
* **Step 4**: Client confirms successful setup.

**Keys Derived**:

* **PMK (Pairwise Master Key)**: Base key from authentication.
* **PTK (Pairwise Transient Key)**: For encrypting unicast traffic.
* **GTK (Group Temporal Key)**: For encrypting broadcast/multicast traffic.

**7. Power Saving Scheme in MAC Layer**

Wi-Fi devices enter **sleep mode** to save battery and wake up when needed:  
**Types**:

* **Legacy Power Save**: Client sleeps and periodically wakes up to check the Traffic Indication Map (TIM) in Beacons.
* **WMM Power Save (U-APSD)**: Faster, efficient power save for VoIP.
* **Target Wake Time (TWT)** (introduced in Wi-Fi 6): Client negotiates scheduled wake/sleep times with AP for even better battery life.

**8. Medium Access Control Methodologies**

To avoid collisions, Wi-Fi uses:

* **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**:
  + Listen before transmit.
  + If busy, wait random time (backoff) and retry.
* **RTS/CTS Handshake**: Optional; used to avoid collisions for large packets.
* **NAV (Network Allocation Vector)**: A timer that indicates when medium will be busy.

**9. Block ACK Mechanism and Advantages**

Instead of acknowledging each frame individually, multiple frames are acknowledged at once.

* **Process**: Sender transmits multiple data frames → Receiver responds with a Block ACK summarizing all received frames.
* **Advantages**:
  + Reduces overhead.
  + Improves throughput.
  + Especially beneficial for high-bandwidth or real-time applications like video.

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

* **A-MSDU (Aggregated MAC Service Data Unit)**:  
  Multiple MSDUs combined into a single MPDU payload. Saves header overhead but if one fails, entire A-MSDU must be retransmitted.
* **A-MPDU (Aggregated MAC Protocol Data Unit)**:  
  Multiple MPDUs transmitted together but each retains its own header and can be retransmitted separately. More robust.
* **A-MSDU inside A-MPDU**:  
  A-MSDUs can be further packed inside A-MPDUs for maximum efficiency and minimal overhead.