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

* MAC is the Media Access Control Layer which is a sub layer of the data link layer in the OSI model.
* The two sublayers of the data link layer are : LLC (Logical Link Control) and MAC Layer.
* It controls access to the physical transmission medium.
* Assigns unique MAC address to devices for identification.
* Handles frame creation and addressing (adds MAC source and destination) and ensures proper delivery of data between devices on the same local network.
* Manages collision detection/avoidance in shared networks (like CSMA/CA).

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

* **Frame Control**-2 Bytes

Contains control flags like frame type, subtype, to/from DS, etc

* **Duration/ID** – 2 bytes  
  Used for setting the Network Allocation Vector (NAV), which helps coordinate medium access and avoid collisions.
* **Address 1** – 6 bytes  
  Usually the receiver address.
* **Address 2** – 6 bytes  
  Usually the transmitter address.
* **Address 3** – 6 bytes  
  Can be the BSSID or destination address, depending on the frame type.
* **Sequence Control** – 2 bytes  
  Contains the sequence number and fragment number; used to identify frame fragments and their order.
* **Address 4 (Optional)** – 6 bytes  
  Used only in Wireless Distribution Systems (WDS).
* **QoS Control (Optional)** – 2 bytes  
  Contains Quality of Service (QoS) information; used in QoS data frames.
* **HT Control (Optional)** – 4 bytes  
  Used in High Throughput (HT) networks (802.11n and above) for control information.
* **Frame Body** – Variable length  
  Contains the actual data being transmitted in the frame.
* **FCS (Frame Check Sequence)** – 4 bytes  
  A Cyclic Redundancy Check (CRC) value used for error detection.

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

**1. Management Plane**

Handles network joining, maintenance, and disconnection.

**Key Functions:**

* Client association and disassociation
* Power management
* Security management
* Traffic priority management
* Beacon generation
* Authentication and deauthentication
* Association and reassociation
* Probe request and response
* Timing synchronization
* Capability exchange

**2. Control Plane**

Manages medium access coordination and transmission control.

**Key Functions:**

* RTS (Request to Send) / CTS (Clear to Send)
* ACK (Acknowledgment)
* NAV (Network Allocation Vector)
* Power Save Control
* Backoff algorithm (CSMA/CA)
* Flow control
* Medium access control

**3. Data Plane**

Responsible for actual data transmission between devices.

**Key Functions:**

* Data transmission between two endpoints
* Frame fragmentation and reassembly
* Frame sequencing
* MAC addressing
* QoS (Quality of Service) handling
* Encryption and decryption hooks

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

**1. Passive Scanning**

The STA listens for beacon frames broadcasted periodically by APs on different channels.

**How It Works:**

* The STA tunes to a specific channel.
* Waits to receive beacon frames, which are broadcast by APs every 100 milliseconds (by default).
* Each beacon contains information such as SSID, supported data rates, security capabilities, and timing info.
* After collecting information from available APs on all channels, the STA selects the best AP to associate with.

**2. Active Scanning**

The STA actively sends probe request frames on each channel and waits for probe responses from APs.

**How It Works:**

* The STA sends a probe request frame on a specific channel (can be directed or broadcast).
* APs receiving the probe request reply with a probe response.
* The probe response contains the same information as a beacon.
* STA moves through channels rapidly, collecting responses to build a list of available APs.

**5. Brief about the client association process**

**Steps in the Association Process**

**1. Scanning**

* The STA uses passive or active scanning to gather information about nearby Aps
* Collects SSID, channel, signal strength, supported rates, and security settings.

**2. Authentication**

* In Open System Authentication, this is a simple two-message handshake:

1. Authentication Request sent by STA to AP.
2. Authentication Response sent by AP (grant or deny).

* For WPA/WPA2/WPA3, authentication continues later via key exchange (4-way handshake).

**3. Association**

* The STA sends an Association Request frame containing:
  + Supported data rates
  + Security capabilities
  + SSID and other capabilities
* The AP replies with an Association Response, which includes:
  + Association ID
  + Status code (success/failure)

Once associated, the AP allocates resources (like buffer space) for the client.

**4. Data Transmission**

* Once associated and authenticated, the STA can start exchanging data with the AP.
* The AP routes traffic between the STA and external networks (e.g., the internet).

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

**4-Way Handshake Process**

1. AP → Client (EAPOL Msg 1):  
   The Access Point (AP) sends a random nonce (Anonce) to the client to initiate the handshake. This gives the client the AP’s random value.
2. Client → AP (EAPOL Msg 2):  
   The client generates its own nonce (Snonce) and derives the PTK (Pairwise Transient Key) using the formula:  
   PTK = PRF(PMK, ANonce, SNonce, AP MAC, Client MAC)  
   The client then sends Snonce along with a MIC (Message Integrity Code). The MIC proves that the client possesses the PMK (Pairwise Master Key), a shared secret.
3. AP → Client (EAPOL Msg 3):  
   The AP verifies the MIC, derives the same PTK, and sends the encrypted GTK (Group Temporal Key), a replay counter, and a new MIC. This securely shares the group key with the client.
4. Client → AP (EAPOL Msg 4):  
   The client sends a final ACK to confirm the installation of both the PTK and GTK, completing the handshake. At this point, both the AP and the client can securely communicate.

* PTK is used for encrypting unicast data.
* GTK is used for broadcast/multicast data.
* Both parties now share identical keys.

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

The MAC Layer in WLAN plays a key role in conserving battery life of wireless clients (STAs) like phones, laptops, etc.

* **Client Sleep State:**  
  When idle but still associated with the AP, the client sends a QoS NULL frame.  
  This frame has the Power Management bit set to 1 in the 802.11 frame control field.  
  The client then switches off its radio to save power.
* **Waking Up and Checking for Data:**  
  The client wakes up at defined intervals based on the DTIM (Delivery Traffic Indication Message) in the Beacon frame sent by the AP.  
  It checks the TIM (Traffic Indication Map) Information Element for its AID (Association ID) in the Partial Virtual Bitmap (PVB).
* **Checking the PVB:**  
  Each bit in the PVB corresponds to a client's AID.  
  If a client’s AID bit is 1, it means the AP has data buffered for that client.
* **Retrieving the Data:**  
  The client sends a PS-Poll (Power Save 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 (PSM):**
   * Based on polling using PS-Poll frames.
   * Clients sleep and periodically wake up to check Beacon frames.
2. **Unscheduled Automatic Power Save Delivery (U-APSD):**
   * Used in QoS-enabled networks (WMM Power Save).
   * Triggers data delivery without waiting for beacon or polling.
   * More efficient for voice/video traffic.
3. **Target Wake Time (TWT):**
   * Introduced in Wi-Fi 6.
   * Clients negotiate specific times to wake up and receive/send data.
   * Improves power efficiency in IoT devices.

**8. Describe the Medium Access Control methodologies**

**1. PCF (Point Coordination Function)**

* Old and deprecated method.
* The AP maintains a list of clients and polls them from the available pool to schedule communication.
* Only the clients polled by the AP can perform data transfer.

**2. DCF (Distributed Coordination Function)**

* Uses CSMA/CA: The system physically senses the energy level of the medium.
* In addition to CSMA/CA, it uses CTS (Clear to Send), RTS (Request to Send), and other mechanisms to virtually sense the medium and control access.
* Distributed coordination, meaning there is no central coordinator like the AP.
* No QoS: Does not provide Quality of Service (QoS) features, but improves spectral usage.
* Contention Time: Same contention time for all traffic types.

**3. EDCA (Enhanced Distributed Channel Access)**

* Extends DCF by incorporating QoS (Quality of Service).
* Different contention times and periods are assigned to various traffic types.
* Priority traffic is given less contention time by adjusting parameters like CWmin and CWmax.
* This reduces backoff time and ensures that QoS is maintained for high-priority traffic.

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

**Flow Control in WiFi**

Flow control in WiFi ensures that data is sent at a rate the receiver can handle, avoiding buffer overflow and packet loss. In WiFi, which is half-duplex, the sender waits for an ACK before sending more data.

**Types of ACKs:**

* Single ACK – one ACK per frame
* Block ACK – one ACK for multiple frames

**Block ACK Process:**

* The sender transmits a burst of multiple data frames.
* Instead of getting ACKs one by one, the receiver sends a single Block ACK frame.
* This Block ACK tells the sender which frames were received and which are missing.
* Only the missing frames are retransmitted.

**Advantages of Block ACK:**

* Reduces control overhead which means fewer ACKs.
* Improves throughput, especially in high speed networks.
* Efficient use of bandwidth.
* Faster recovery from lost frames.
* Better performance for real-time apps.

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

**1. A-MPDU (Aggregated MAC Protocol Data Unit)**

* Multiple MPDUs with separate MAC headers are aggregated under a single PHY layer header.
* Each frame has its own CRC.
* If any one subframe is corrupted, only the corrupted frame is retransmitted.
* High overhead due to multiple MAC headers.

**2. A-MSDU (Aggregated MAC Service Data Unit)**

* Multiple MSDUs are aggregated with a single MAC and PHY header.
* Overhead is reduced significantly.
* However, if any one subframe fails, all aggregated frames must be retransmitted.

**3. A-MSDU inside A-MPDU**

* Multiple MSDUs (e.g., 2 or 3) are aggregated with a single MAC header.
* These are further grouped into MPDU chunks, which are aggregated under the same PHY header.
* This method is a middle ground between A-MSDU and A-MPDU.