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

The **MAC (Media Access Control) layer** is a sublayer of the **Data Link Layer (Layer 2)** in the **OSI model**. It plays a crucial role in enabling devices on the same network to communicate efficiently and without interference.

Key Functions:

- **Addressing:** Uses MAC addresses (unique hardware identifiers) to identify devices on the network.
- **Access Control:** Determines how devices take turns accessing the shared medium (e.g., Ethernet, Wi-Fi).
- **Frame Delimiting & Error Checking:** Ensures frames are correctly formed and detects errors using checksums (e.g., CRC).
- **Flow Control & Synchronization:** Helps manage data rate between sender and receiver.

Position in OSI Model:

- **Layer:** 2 (Data Link Layer)
- **Sublayers of Layer 2:**
    - **LLC (Logical Link Control)**
    - **MAC (Media Access Control) ← This is where MAC layer resides**

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

Fields ?

802.11 MAC Frame Format and Purpose of Each Field:

1. **Frame Control (2 bytes):** Contains control information about the frame type and subtype, protocol version, and various control flags such as To DS, From DS, Retry, More Fragments, and Power Management.
2. **Duration/ID (2 bytes):** Specifies how long the channel will be reserved for the frame transmission (for NAV – Network Allocation Vector). In Power Save Poll (PS-Poll) frames, it carries the association ID (AID).
3. **Address Fields (6 bytes each × 3 or 4):**
    - Address 1: Receiver address
    - Address 2: Transmitter address
    - Address 3: BSSID (Basic Service Set Identifier)
    - Address 4 (optional): Used in Wireless Distribution System (WDS)

4. **Sequence Control (2 bytes):** Contains a sequence number to detect duplicate frames and a fragment number for fragmented frames.
5. **QoS Control (2 bytes) (optional):** Used in Quality of Service data frames to prioritize traffic such as voice or video over regular data.
6. **HT Control (4 bytes) (optional):** Used for high-throughput (802.11n) control features like beamforming and antenna selection.
7. **Frame Body (0–2304 bytes):** The actual data or management information being transmitted.
8. **FCS – Frame Check Sequence (4 bytes):** Contains a CRC checksum used for error detection.

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

1. Management Plane MAC Functions:

- Beacon generation and processing
- Authentication and deauthentication
- Association and disassociation
- Reassociation
- Scanning (active/passive)
- Timing synchronization
- Capability exchange
- Parameter negotiation (e.g., supported data rates, QoS)

2. Control Plane MAC Functions:

- RTS (Request to Send) / CTS (Clear to Send) handshake
- ACK (Acknowledgment) frame handling
- NAV (Network Allocation Vector) management
- Power Save coordination (e.g., PS-Poll frames)
- Channel access coordination
- Contention window management (e.g., in CSMA/CA)
- Transmission opportunity (TXOP) control
- Rate adaptation decisions

3. Data Plane MAC Functions:

- Data frame generation and parsing
- Frame fragmentation and reassembly
- Addressing (source, destination, BSSID)
- Sequence control and duplicate detection
- Encryption and decryption (WEP, WPA, WPA2 handling)
- QoS prioritization (WMM)
- Data transmission and retransmission
- Error detection (using FCS)

4 . Explain the scanning process and its types in detail

Scanning in Wireless Networks (IEEE 802.11)

Scanning is the process by which a wireless device (station or client) searches for available wireless networks (Access Points or APs) in its vicinity. This is essential for **network discovery**, **association**, **roaming**, and **handover**.

Types of Scanning:

1. Passive Scanning

- **How it works:**
  The station listens for **beacon frames** periodically sent by Access Points on each channel.
- **Steps:**
  1. The station switches to a channel.
  2. It listens for beacon frames without sending any frames.
  3. If a beacon is detected, it gathers the information (SSID, BSSID, supported rates, etc.).
  4. Repeats the process on other channels.
- **Pros:**
  - No frame is transmitted (conserves battery).
  - Stealthy – ideal for environments where transmissions should be minimized.
- **Cons:**
  - Slower – relies on APs sending beacons (usually every 100 ms).

2. Active Scanning

- **How it works:**
  The station actively sends **Probe Request** frames and waits for **Probe Responses** from APs.
- **Steps:**
  1. The station switches to a channel.
  2. It broadcasts a **Probe Request** (can be directed to a specific SSID or to any).
  3. APs receiving the request respond with a **Probe Response**.
  4. The station collects the responses and moves to the next channel.
- **Pros:**
  - Faster discovery of networks.
  - Can be used to discover hidden SSIDs (if AP responds).
- **Cons:**
  - More power consumption.
  - Not stealthy – generates traffic.

5. Brief about the client association process

Client Association Process:

The association process allows a wireless client (station) to connect to an Access Point (AP) and become part of the wireless network. It involves the following steps:

1. **Scanning:**
   - The client searches for available networks using **active** or **passive scanning**.
2. **Authentication:**
   - The client sends an **Authentication Request** to the AP.
   - The AP responds with an **Authentication Response**.
   - In open system authentication (most common), this is a simple one-step approval.
3. **Association Request:**
   - The client sends an **Association Request** frame, which includes SSID, supported data rates, and capabilities.
4. **Association Response:**
   - The AP responds with an **Association Response** frame indicating success or failure.
   - If successful, the client is now associated and can begin data communication.

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

derived from the process ?

EAPOL 4-Way Handshake (Used in WPA/WPA2/WPA3 Security)

The **4-way handshake** is performed between the **client (supplicant)** and the **Access Point (authenticator)** after successful authentication to securely generate and exchange encryption keys.

Keys Involved:

1. **PMK (Pairwise Master Key):**
    - Derived from **pre-shared key (PSK)** or **802.1X authentication**.
    - Shared between client and AP before the handshake.
2. **PTK (Pairwise Transient Key):**
    - Derived during handshake using:
      PTK = PRF(PMK + ANonce + SNonce + MAC_AP + MAC_Client)
3. **GTK (Group Temporal Key):**
    - Used for broadcast/multicast traffic.
    - Distributed by AP in Message 3.

Steps in the 4-Way Handshake:

Message 1 (AP → Client):

- AP sends **ANonce** (a random number) to the client.
- Purpose: Initiate key generation by providing a nonce for PTK derivation.

Message 2 (Client → AP):

- Client generates **SNonce** and derives the **PTK**.
- Sends **SNonce + MIC (Message Integrity Code)** back to AP.
- Purpose: Proves it has the PMK and shares SNonce for PTK derivation.

Message 3 (AP → Client):

- AP also derives the same PTK.
- Sends **GTK (encrypted)** + **MIC** to client.
- Purpose: Distributes GTK securely and confirms successful PTK derivation.

Message 4 (Client → AP):

- Client sends an acknowledgment (with MIC).
- Purpose: Confirms installation of keys and completes the handshake.

Purpose of Keys:

Key	Purpose
PMK	Base key from which PTK is derived
PTK	Used for securing unicast data (encryption and MIC)
GTK	Used for encrypting broadcast/multicast traffic
ANonce / SNonce	Random values used to ensure PTK uniqueness and security

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

saving mechanisms

Power Saving in MAC Layer (IEEE 802.11)

Power saving in the MAC layer is designed to **extend battery life** of wireless devices (especially mobile stations) by minimizing active radio usage.

Basic Power Saving Mechanism (802.11 Standard):

1. **Sleep Mode:**
   - The station turns off its radio to save power.
2. **Awake Mode:**
   - Periodically wakes up to check for buffered frames at the AP.
3. **Beacon Frames:**
   - AP sends beacon frames at regular intervals containing **Traffic Indication Map (TIM)**.
4. **TIM:**
   - Informs which clients have data buffered at the AP.
5. **PS-Poll Frame:**
   - If a client sees its ID in the TIM, it sends a **PS-Poll** to request the data.
6. **Data Delivery:**
   - AP responds with the data frame, after which the station may go back to sleep.

Types of Power Saving Mechanisms:

1. Legacy Power Save Mode:

- Based on beacon and PS-Poll method.
- Simple but causes delay in data access.

2. Automatic Power Save Delivery (APSD – 802.11e):

- Supports **scheduled** or **unscheduled** data delivery.

- Mainly used for voice/video (QoS traffic).
- Reduces latency and improves battery performance.

3. Unscheduled APSD (U-APSD):

- Client triggers data delivery by sending any uplink frame.
- Used in VoIP and low-latency applications.

4. Scheduled APSD (S-APSD):

- AP delivers data at predefined intervals.
- Synchronizes with the station's wake-up schedule.

5. Target Wake Time (TWT – 802.11ax):

- Stations negotiate with AP to **wake up at specific times**.
- Highly efficient, reduces contention, ideal for IoT devices.

8. Describe the Medium Access Control methodologies

Medium Access Control (MAC) Methodologies in Wireless Networks

The **Medium Access Control (MAC)** layer controls access to the shared communication medium (the wireless channel) in wireless networks. Different MAC methodologies define how stations (client devices) contend for access to the medium, manage data transmission, and ensure efficient, collision-free communication.

Below are the key **MAC methodologies** in wireless communication, particularly in IEEE 802.11 standards.

1. Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- **Used in:** Wi-Fi (IEEE 802.11) networks.
- **How it works:**
    - o **Carrier Sense (CS):** A station listens to the channel to detect if it is idle or busy before transmitting.
    - o **Collision Avoidance (CA):** If the channel is idle, the station waits for a random backoff time and then transmits. If it detects that the channel is busy, it waits.
    - o **RTS/CTS (Request to Send / Clear to Send):** In environments with high traffic, stations use RTS/CTS to reserve the channel and reduce collisions.
- **Purpose:** To avoid collisions by ensuring that only one device transmits at a time.

2. Time Division Multiple Access (TDMA)

- **Used in:** Some wireless communication systems (e.g., cellular networks).
- **How it works:**

    - The available time is divided into **time slots**.
    - Each device is assigned a specific time slot to transmit its data, avoiding collision with other devices.
    - Devices only transmit in their allocated time slot, ensuring that there is no interference from other devices.
- **Purpose:** To prevent collisions by coordinating transmissions in time.

3. Frequency Division Multiple Access (FDMA)

- **Used in:** Some wireless systems (e.g., traditional analog cellular systems).
- **How it works:**
    - The available frequency spectrum is divided into **frequency bands**.
    - Each device is assigned a specific frequency band for communication.
    - Devices transmit on their assigned frequency, preventing interference from other devices.
- **Purpose:** To enable multiple users to transmit simultaneously on different frequency channels.

4. Code Division Multiple Access (CDMA)

- **Used in:** Cellular networks (e.g., 3G networks).
- **How it works:**
    - Each device is assigned a unique **code** to encode its data.
    - All devices transmit simultaneously, but because each transmission is encoded with a unique code, receivers can separate them based on the code used.
    - This allows multiple devices to share the same frequency spectrum at the same time without interference.
- **Purpose:** To enable simultaneous communication on the same frequency by using unique codes for each user.

5. Polling (Polling MAC)

- **Used in:** Some wireless LANs and Bluetooth.
- **How it works:**
    - The Access Point (AP) or master device polls client stations to check if they have data to send.
    - The client responds when it has data to transmit, ensuring that the AP knows when a station is ready to communicate.
- **Purpose:** To prevent collision by controlling when each station transmits.

6. Token Passing (Token-based MAC)

- **Used in:** Token Ring networks (older standard) and some industrial networks.
- **How it works:**
    - A **token** is passed around the network in a predetermined order.
    - Only the station holding the token is allowed to transmit data.
    - After transmitting, the station passes the token to the next station.
- **Purpose:** To eliminate collisions by granting permission to transmit in a controlled manner.

7. Slotted ALOHA

- **Used in:** Early wireless communication protocols, such as in satellite communications.
- **How it works:**
    - The time is divided into **slots**.
    - Each station sends data in a specific time slot, but if two stations transmit in the same slot, a collision occurs.
    - The stations then retransmit after a random time.
- **Purpose:** To reduce collisions by synchronizing transmissions into time slots.

8. Unslotted ALOHA

- **Used in:** Simple communication systems, such as in some early RFID systems.
- **How it works:**
    - Stations transmit data at any time without synchronization.
    - If a collision occurs, stations retransmit their data after a random delay.
- **Purpose:** To provide a simple and flexible medium access mechanism, though it has higher collision probability compared to slotted ALOHA.

9. Brief about the Block ACK mechanism and its advantages

Block ACK Mechanism in 802.11

The **Block ACK (Acknowledgement)** mechanism is used in the **IEEE 802.11** wireless networking standard, specifically in the **802.11e** (Quality of Service) and **802.11n/ac/ax** (High-Throughput) standards, to improve the efficiency of data transmission by reducing the overhead of acknowledgment (ACK) frames.

How Block ACK Works:

1. **Initiation:**
    - A **Block ACK** is requested by a station (client) during the transmission of a sequence of data frames, typically in an **HT (High Throughput) frame exchange**.

- The client sends a **Block ACK Request** to the Access Point (AP) indicating that it is ready to receive multiple frames without individual acknowledgments.

2. **Transmission:**
   - The sender (usually the AP) sends a **block of data frames** to the receiver (client) in a burst, without waiting for ACKs after each frame.
   - These frames are part of a **sequence** of frames.
3. **Block ACK:**
   - After receiving the data frames, the client sends a **Block ACK frame** to the AP, which acknowledges all the frames in the sequence at once, rather than acknowledging each frame individually.
   - The Block ACK frame includes a **Bitmap** to indicate which frames were successfully received and which need retransmission.

Key Features of Block ACK:

- **Bitmap:** The Bitmap in the Block ACK frame indicates which data frames were successfully received. Each bit in the Bitmap represents a frame in the sequence.
- **Efficiency:** Multiple frames can be acknowledged in a single Block ACK, reducing the number of required ACK frames.
- **Retransmission:** If any frame in the sequence is lost or corrupted, only the lost frames need to be retransmitted, as indicated by the Bitmap.

Advantages of Block ACK Mechanism:

1. **Reduced Overhead:**
   - **Fewer ACK frames** are needed, reducing the overhead of sending individual ACKs for each frame, especially in high-throughput networks.
2. **Improved Throughput:**
   - By reducing the number of ACKs and increasing the data transmission burst, **throughput is improved**, especially for large data transfers.
3. **Efficient Retransmission:**
   - Only the **lost or corrupted frames** need to be retransmitted, reducing unnecessary retransmissions of successfully received frames.
4. **Lower Latency:**
   - Block ACKs allow for more continuous transmission without waiting for ACKs after each frame, **reducing latency**.
5. **Better Performance in High-Throughput Networks:**
   - In scenarios with large file transfers or streaming, Block ACK helps maintain **high data rates** by reducing channel contention and congestion caused by frequent ACKs.

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

In IEEE 802.11 wireless networks, there are various ways to enhance throughput and reduce overhead during data transmission. The **A-MSDU** (Aggregated MAC Service Data Unit) and **A-MPDU** (Aggregated MAC Protocol Data Unit) are two key mechanisms used to aggregate multiple frames into a single transmission. Let's explore each of these concepts and their relationship.

1. A-MSDU (Aggregated MAC Service Data Unit)

- **Definition:**
  - **A-MSDU** is a method to **aggregate multiple MSDUs** (MAC Service Data Units) into a single MAC frame for transmission.
  - Each MSDU within an A-MSDU is an independent data frame, typically coming from different applications or service flows, but they are transmitted together within a single frame.
- **Structure:**
  - The **A-MSDU** consists of a single MAC header followed by multiple **MSDUs** that share the same MAC header.
  - Each MSDU is independent but encapsulated within the A-MSDU. The data is placed contiguously, and a **length field** is used to specify the size of each individual MSDU.
- **Advantages:**
  - **Reduced overhead**: The MAC header is sent only once for all aggregated MSDUs.
  - **Increased throughput**: By aggregating multiple MSDUs into one frame, the transmission efficiency improves, as less time is spent on control overhead.
- **Disadvantages:**
  - **Frame size limit**: A-MSDUs are limited by the **maximum frame size** defined in the standard (typically 3839 bytes).
  - **Error propagation**: If one MSDU is corrupted, all the MSDUs in the A-MSDU may need to be retransmitted.

2. A-MPDU (Aggregated MAC Protocol Data Unit)

- **Definition:**
  - **A-MPDU** is a method to **aggregate multiple MPDUs** (MAC Protocol Data Units) into a single transmission.
  - Unlike A-MSDU, which aggregates multiple MSDUs, A-MPDU aggregates whole MPDUs, including their MAC headers.
- **Structure:**

  - The **A-MPDU** consists of several **MPDUs** (each with its own MAC header and payload), and the transmission is managed using a **sequence number** to distinguish between the MPDUs.
  - A special **delimiter** is added between each MPDU within the A-MPDU to allow the receiver to identify the boundaries of each MPDU.
- **Advantages:**
  - **High robustness**: A-MPDU can carry multiple MPDUs, and if an MPDU is lost or corrupted, only that particular MPDU needs to be retransmitted.
  - **Efficient retransmission**: Each MPDU is independently acknowledged, so only the corrupted frames need retransmission.
- **Disadvantages:**
  - **Higher overhead per frame**: Since each MPDU carries its own MAC header, the overhead is higher compared to A-MSDU.
  - **More complex error handling**: Since MPDUs have separate headers, it might involve more complex error handling.

3. A-MSDU in A-MPDU (A-MSDU Aggregated Inside A-MPDU)

- **Definition:**
  - The concept of **A-MSDU in A-MPDU** combines both techniques, allowing **A-MSDUs** to be placed within **A-MPDU**.
  - This means that multiple **A-MSDUs** (each containing multiple MSDUs) are aggregated into an **A-MPDU** (which contains multiple MPDUs).
- **Structure:**
  - **A-MPDU** carries multiple **A-MSDUs**, and within each A-MSDU, there are multiple **MSDUs**.
  - The aggregation is done at two levels:
    - The first level aggregates **multiple MSDUs into an A-MSDU**.
    - The second level aggregates **multiple A-MSDUs into an A-MPDU**.
- **Advantages:**
  - **Highly efficient**: By combining the aggregation of both MSDUs (A-MSDU) and MPDUs (A-MPDU), the system minimizes the overhead while still ensuring that multiple units of data are transmitted efficiently.
  - **Higher throughput**: Since it aggregates both MSDUs and MPDUs, it reduces the overall transmission time and increases throughput, particularly in high-throughput scenarios.
- **Disadvantages:**
  - **Complexity**: Managing both levels of aggregation can be more complex.

- **Error handling**: If an error occurs, it could affect multiple layers of aggregation, making error recovery more challenging.