**Name:** Afreen S

**University:** Vellore Institute of Technology (VIT)

# WiFi Training Program

## Assignment – Module 4

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 **sub-layer** of the Data Link Layer in the OSI model. Its key roles are:

- **Controls access to the shared medium** (e.g., deciding who can transmit and when in wireless networks).
- **Handles frame delivery** between devices on the same network.
- **Manages addressing** using MAC addresses.
- **Avoids collisions** using protocols like CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

**Position in OSI Model:**

The **MAC layer** is part of **Layer 2: Data Link Layer**.

OSI Layers (Top to Bottom):

1. Application
2. Presentation
3. Session
4. Transport
5. Network
6. **Data Link**
    - **MAC sub-layer**
    - LLC (Logical Link Control) sub-layer
7. Physical

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.

**802.11 MAC Header Format:**

| **Field** | **Size (bytes)** | **Purpose** |
|---|---|---|
| **Frame Control** | 2 | Indicates type of frame (Data, Control, Management), version, flags like To/From DS, Retry, etc. |
| **Duration/ID** | 2 | Used for network allocation vector (NAV) – helps avoid collisions by reserving the channel. |
| **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 | Depends on type – often used as BSSID in infrastructure mode. |
| **Sequence Control** | 2 | Frame number + fragment number for ordering and reliability. |
| **Address 4** *(only in WDS)* | 6 | Used in special cases like mesh or bridge mode. |
| **Frame Body** | Variable | Contains actual data (payload). |
| **FCS (Frame Check Sequence)** | 4 | CRC for error checking. |

**Purpose of the MAC Header:**

- Identifies who is sending and receiving the frame.
- Helps manage delivery in complex wireless environments.
- Supports **fragmentation, retransmission, QoS**, and **collision avoidance**.

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

◆ **Management Plane Functions (for setup, maintenance, and teardown of communication)**

- **Authentication** – Verifies identity of stations (STA).
- **Association/Disassociation** – Manages joining/leaving an AP (Access Point).
- **Beacon Transmission** – Periodic broadcast for network discovery.
- **Probe Request/Response** – Used by STAs to find APs and initiate connection.
- **Reassociation** – Moves STA from one AP to another.
- **Timing Synchronization** – Keeps devices synced using timestamps in beacons.

◆ **Control Plane Functions (for coordination of access to the medium)**

- **RTS/CTS (Request to Send / Clear to Send)** – Avoids hidden node collision.
- **ACK (Acknowledgement)** – Confirms successful frame delivery.
- **Contention Window Management** – Controls backoff timing in CSMA/CA.
- **NAV (Network Allocation Vector)** – Virtual carrier sensing to avoid overlapping transmission.
- **TXOP (Transmission Opportunity)** – Grants time slot to transmit without interruption (used in QoS).

◆ **Data Plane Functions (for actual data transmission)**

- **Frame Construction and Parsing** – Encodes/decodes data in MAC frames.
- **Addressing** – Uses MAC addresses for delivery.
- **Sequence Control** – Maintains correct frame order.
- **Fragmentation and Reassembly** – Splits/rejoins large data packets.
- **Error Detection** – Uses FCS (Frame Check Sequence) to detect errors.
- **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 device (STA – Station) searches for available **Access Points (APs)** before connecting to a network. It's part of the **MAC Management functionalities**.

**Types of Scanning:**

🔹 **Passive Scanning**

- **How it works**:
    - The STA **listens** for **beacon frames** broadcasted by APs.
    - Each AP sends beacons periodically (usually every 100 ms).
    - The STA gathers info like SSID, BSSID, channel, and capabilities.
- **Pros**:
    - Energy efficient
    - Stealth mode (STA doesn't reveal itself)
- **Cons**:
    - **Slower** (must wait for beacons on each channel)

🔹 **Active Scanning**

- **How it works**:
    - The STA **sends Probe Request** frames on each channel.
    - APs respond with **Probe Response** frames.
    - STA collects info and selects AP to associate with.
- **Pros**:
    - **Faster** discovery
    - Finds hidden SSIDs
- **Cons**:
    - Consumes more **power**
    - **Reveals STA identity**

| Feature | Passive Scanning | Active Scanning |
|---|---|---|
| Initiated By | AP (beacons) | STA (probe requests) |
| Speed | Slower | Faster |
| Power Usage | Low | Higher |
| Hidden SSID support | No | Yes |
| Privacy | Better (silent) | Less (reveals MAC) |

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

The **client association process** refers to how a wireless station (**STA**) connects to an **Access Point (AP)** to become part of the wireless network.

**Process:**

**1. Scanning**

- The STA discovers nearby APs using **passive** (beacon listening) or **active** (probe requests) scanning.

**2. Authentication**

- STA sends an **authentication request** to AP.
- AP responds with an **authentication response**.
- In open system, this step is simple; in secured networks, involves credentials (e.g., WPA2).

**3. Association Request**

- After successful authentication, STA sends an **association request** to AP.
- This includes capabilities, supported rates, SSID, etc.

**4. Association Response**

- AP replies with **association response**, assigning an **Association ID (AID)** to the STA.
- STA is now officially connected to the AP and can send/receive data.

6. **Explain each steps 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 process used in WPA2/WPA3 Wi-Fi security to establish **encryption keys** between a **client (STA)** and an **Access Point (AP)** after authentication.

**Purpose:**

- To generate and exchange **encryption keys** securely.
- To confirm both parties have the **same Pairwise Master Key (PMK)**.
- To derive the **Pairwise Transient Key (PTK)** for data encryption.

**Steps of the 4-Way Handshake:**

**Step 1: AP → STA**

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

**Step 2: STA → AP**

- **STA generates PTK** using:
  - PMK (from previous authentication)
  - ANonce (from AP)
  - SNonce (STA's own random value)
  - MAC addresses (AP & STA)
- Sends **SNonce** and **Message Integrity Code (MIC)** to AP.

**Step 3: AP → STA**

- 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**.

**Step 4: STA → AP**

- STA sends a final **ACK** to confirm installation of keys.
- Data encryption begins.

**Keys Derived in the Process:**

| Key | Purpose |
|---|---|
| **PMK (Pairwise Master Key)** | Derived from passphrase or 802.1X. Used as the base key for all derivations. |
| **PTK (Pairwise Transient Key)** | Generated per session; used to encrypt unicast traffic between STA and AP. |
| **GTK (Group Temporal Key)** | Used for broadcast/multicast traffic encryption. |
| **MIC (Message Integrity Code)** | Ensures message has not been tampered with. |

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

The **MAC layer power saving scheme** in IEEE 802.11 helps wireless devices **conserve battery** by minimizing radio usage when not actively transmitting or receiving data.

**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 in Power Saving:**

◆ **Power Save Mode (PS Mode):**

- STA notifies AP of entering **sleep mode**.
- AP stores (buffers) the frames destined for that STA.
- STA wakes at **beacon intervals** and checks **Traffic Indication Map (TIM)** in the beacon.
- If data is pending, STA sends **PS-Poll frame** to retrieve it.

◆ **U-APSD (Unscheduled Automatic Power Save Delivery):**

- Used in **Wi-Fi Multimedia (WMM)**.
- STA doesn't have to send PS-Poll.
- Data is delivered automatically after the STA sends a trigger (e.g., VoIP packet).
- Reduces delay → Good for **voice/video apps**.

◆ **TWT (Target Wake Time)** ***(Introduced in 802.11ax – Wi-Fi 6)*****:**

- Devices negotiate **specific wake times** with AP.
- Greatly improves efficiency in **IoT** and **dense networks**.
- Allows STAs to sleep for long durations without missing critical transmissions.

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

The **MAC layer** manages how devices access the **shared wireless medium** without collision. In IEEE 802.11 (Wi-Fi), several methods are used to efficiently share the channel.

**Key MAC Methodologies:**

◆ **Distributed Coordination Function (DCF) – Mandatory**

- Based on **CSMA/CA** (Carrier Sense Multiple Access with Collision Avoidance).
- Devices listen to the channel:
    - If idle → transmit.

- If busy → wait and back off randomly.

- Uses **ACK**, **RTS/CTS**, and **NAV** to avoid collisions.
- Default method in all 802.11 networks.

◆ **Point Coordination Function (PCF) – Optional**

- Uses a **central coordinator (usually the AP)**.
- Works in a **contention-free** period.
- AP polls each STA to give it permission to send.
- Not widely used due to complexity and inefficiency in real-world Wi-Fi.

◆ **Hybrid Coordination Function (HCF) – 802.11e**

- Combines both **DCF + PCF**.
- Introduces **HCCA (HCF Controlled Channel Access)** for time-sensitive traffic.
- Enables **QoS (Quality of Service)** support.

◆ **EDCA (Enhanced Distributed Channel Access) – 802.11e**

- Prioritizes traffic into **4 Access Categories (AC)**: Voice, Video, Best Effort, Background.
- High-priority traffic gets **shorter contention windows**.
- Supports applications like **VoIP and streaming**.

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

The **Block ACK** mechanism is an enhancement in IEEE 802.11 to improve the **efficiency** of data transmission, especially for high-throughput networks.

**Block ACK:**

- Instead of sending an **ACK for each frame**, the receiver sends a **single acknowledgment** for a **block of frames**.
- This reduces overhead and improves throughput, especially for **large data bursts** like video or file transfers.

**Working:**

1. **Block ACK Request** is sent by the transmitter after sending a group of frames.
2. **Block ACK Response** is sent by the receiver indicating which frames were received successfully.
3. Lost frames can be **retransmitted selectively**.

**Advantages:**

| Benefit | Description |
|---|---|
| **Efficiency** | Fewer ACKs = reduced overhead. Boosts speed. |
| **High Throughput** | Ideal for multimedia, VoIP, large file transfers. |
| **Selective Retransmission** | Only lost frames are retransmitted — saves time. |
| **Better Channel Utilization** | Minimizes control traffic, uses bandwidth effectively. |

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

These are **frame aggregation techniques** used in Wi-Fi (starting from **802.11n onwards**) to increase efficiency and **reduce overhead**.

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

- **Combines multiple MSDUs** (upper-layer data units) into **one MAC frame**.
- Shared **single MAC header**.
- All subframes must have the **same TID (traffic ID)** and **destination**.

**Advantages:**

- Reduces MAC header overhead.
- More efficient for small payloads.

**Drawbacks:**

- If the A-MSDU is corrupted, **entire frame is retransmitted**.

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

- Aggregates **multiple MPDUs** (complete MAC frames with headers).
- Each MPDU can have its own **retransmission**.
- Sent as one PHY frame with **Block ACK support**.

**Advantages:**

- Supports **selective retransmission**.
- More **robust** and flexible.

**Drawbacks:**

- Slightly more **PHY-layer overhead** compared to A-MSDU.

**3. A-MSDU in A-MPDU (Two-Level Aggregation)**

- Combines **multiple A-MSDUs**, and then aggregates them inside multiple MPDUs in an **A-MPDU**.
- Best of both:
  - Reduces overhead (via A-MSDU)
  - Supports retransmission (via A-MPDU)

**Most efficient**, used in **Wi-Fi 6** and later for maximum throughput.