Moulik Tammana

Wi-Fi Training Program Module – 4

Q1. What is the significance of MAC layer and in which position it is placed in the OSI model.

The MAC (Medium Access Control) layer is a sub-layer of the Data Link Layer in the OSI model. It plays a critical role in managing how data is transmitted over a shared communication medium—especially in wireless networks like Wi-Fi.

Key Responsibilities of the MAC Layer:

- **Access Control to the Medium: Determines when a device can transmit data over the channel. Uses techniques like CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) in wireless.**
- **Frame Delimiting and Addressing: Adds MAC addresses (unique hardware addresses) to frames to identify sender and receiver.**
- **Error Detection (Not Correction): Adds a CRC (Cyclic Redundancy Check) to detect errors in frames.**
- **Frame Construction and Parsing: Builds frames for data transmission and extracts data upon receipt.**
- **Acknowledgment and Retransmission: In wireless, often includes ACK frames to confirm successful delivery.**
- **Management and Control Frames Handling: Handles connection setup, authentication, and mobility (association, reassociation, etc.).**

Q2. Describe the frame format of the 802.11 MAC header and explain the purpose of each fields.

General MAC Header Structure (for Data/Control/Management Frames) are in the following manner:

Field	Size (bytes)	Purpose
Frame Control	2	Identifies the type of frame.
Duration/ID	2	Used for setting NAV (Network Allocation Vector) for virtual carrier sensing.
Address 1	6	Receiver Address which is usually the MAC of the destination.
Address 2	6	Transmitter Address which is the MAC of the device sending the frame.
Address 3	6	Depending on frame type can be BSSID, destination, or source.
Sequence Control	2	Contains sequence number and fragment number for reassembly.
Address 4	6	Present only in Wireless Distribution System mode – used for source/destination behind APs.
QoS Control	2	Present in QoS data frames (802.11e) – manages traffic priority.
HT Control	4	Present in HT frames (802.11n) – used for MIMO/beamforming.
FCS (Frame Check Seqence)	4	CRC value, Hammers used for error detection at the MAC layer.

The Frame Control field is subdivided into the following fields:

Sub-field	Size (bits)	Purpose
Protocol Version	2	Usually 00. Used for versioning; future use.
Type	2	Specifies if the frame is Management (00), Control (01), or Data (10).
Subtype	4	Further classifies the frame type (e.g., Beacon, RTS, Data+ACK, etc.).
To DS	1	Frame destined to the Distribution System (AP).
From DS	1	Frame coming from the Distribution System.
More Fragments	1	Set if more fragments of this frame will follow.
Retry	1	Set if this frame is a retransmission.
Power Management	1	Indicates if sender will go to sleep after this frame.
More Data	1	Indicates buffered data available for the client at the AP.
Protected Frame	1	Set if frame body is encrypted (e.g., WPA/WPA2).
Order	1	Set if frames must be processed in order (used for QoS).

Q3. Please list all the MAC layer functionalities in all Management, Control and Data plane.

Management Frame Functions

- **Handles network discovery and maintenance through Beacon, Probe, Association, and Authentication frames.**
- **Manages station joining/leaving via association/disassociation and authentication/deauthentication.**
- **Supports scanning, timing synchronization (TSF), and power-saving coordination.**
- **Examples of Management Frames are: Beacon, Probe Request and Response, Association Request, Channel Switch Announcement Frame.**

Control Frame Functions

- **Regulates channel access using RTS/CTS and collision avoidance via CSMA/CA and NAV management.**
- **Provides acknowledgment mechanisms (ACK, Block ACK) to ensure reliable frame delivery.**
- **Implements backoff algorithms, TXOP management, and QoS-based traffic prioritization.**
- **Examples of Control Frames are: RTS, OTS, Block ACK, PS-Poll.**

Data Frame Functions

- **Delivers user data and control info between devices with fragmentation and reassembly support.**
- **Performs addressing, encryption/decryption, and sequence numbering for integrity and security.**
- **Enables QoS through A-MSDU/A-MPDU aggregation, traffic classification, and scheduling.**
- **Examples of Data Frames are: QoS Data frame, Qos NULL data frames.**

Q4. Explain the scanning process and its types in detail.

Scanning allows a Wi-Fi client (STA) to discover available wireless networks (SSIDs) and gather info about nearby Access Points (APs).

There are two types of scanning processes:

Active Scanning Process:

- **The client sends Probe Request frames on each channel.**
- **APs within range respond with Probe Response frames containing network info (SSID, supported rates, RSN, etc.).**
- **Faster than passive scanning, but consumes more power and may cause interference.**

Passive Scanning Process:

- **The client listens silently on each channel for Beacon frames broadcasted periodically by APs.**
- **No frames are sent by the client, making it more power-efficient and stealthy.**
- **Slower than active scanning since it waits for beacons.**

Different frames in Scanning (Management Frames):

1. **Probe Request Frame (Active Scan)**

- **Contains: SSID (can be wildcard or specific), supported rates, etc.**
- **Sent to broadcast address to discover all networks, or a specific SSID.**

2. **Probe Response Frame (Active Scan)**

- **Sent by an Access Point (AP) in response to a Probe Request from a client during active scanning, to advertise its presence and capabilities.**
- **Contains: BSSID, supported data rates, channel info, security settings (RSN), and timing parameters to help the client decide whether to join.**

3. **Beacon Frame (Passive Scan)**

- **Periodically sent by APs (typically every 100 ms).**
- **Contains: SSID, BSSID, channel info, RSN, capabilities, supported data rates, etc.**

Q5. Brief about the client association process.

Beacon Listening

- **Beacon frames are periodically transmitted by the Access Point (AP) to announce the presence of the network.**
- **Beacon Listening involves a client (STA) silently listening for these Beacon frames during passive scanning.**

Scanning

- **The client discovers nearby Access Points (APs) via active or passive scanning.**

Authentication

- **Ensures the client device is legitimate and authorized to join the network.**
- **The client sends an Authentication Request to the AP.**
- **The AP replies with an Authentication Response.**
- **This is the initial authentication (Open or Shared Key), not yet full security (WPA/WPA2 handshake happens later).**

Association

- **Establishes a communication link between the client and AP for data exchange.**
- **The client sends an Association Request with its capabilities (e.g., supported rates).**
- **The AP responds with an Association Response if it accepts the client.**

(Optional) 4-Way Handshake

- **If using WPA/WPA2, the 4-way handshake is performed to establish encryption keys (PTK/GTK).**

Client is now connected

- **The client can start exchanging data frames securely with the AP.**

Connection	Purpose	Details
Probe Request to AP	The client (STA) sends a Probe Request frame to discover nearby networks.	• The client either sends a broadcast probe (wildcard SSID) to find all available networks or a specific probe (with an SSID) to look for a particular network. • This happens during active scanning.
Probe Response to Client	The AP responds to the Probe Request with a Probe Response frame.	• The AP provides information about the network, including SSID, BSSID, supported data rates, and security protocols. • The client uses this information to determine if it wants to associate with this AP.
Authentication Request to AP	The client sends an Authentication Request to the AP.	• This step involves the client trying to authenticate with the AP, which may be using Open System Authentication or Shared Key Authentication (if WEP is used). • The AP checks if it will allow the client to connect.
Authentication Response to Client	The AP responds with an Authentication Response to acknowledge or reject the authentication request.	• If successful, the client is now authenticated, but not yet associated (authenticated means it is allowed to connect, but they still need to establish a proper connection). • For WPA/WPA2, 802.1X authentication will occur before this step, involving a RADIUS server for stronger security.
Association Request to AP	The client sends an Association Request to the AP.	• This step involves the client formally requesting to join the AP's network, including additional information like supported data rates, power management options, and capabilities. • It essentially sets up the connection parameters for the client and the AP.
Association Response to Client	The AP sends an Association Response to the client.	• The AP replies with an Association Response that includes a status code (whether the association was successful or not) and assigns an Association Identifier (AID) to the client.

		• If successful, the client is now officially associated with the AP and can start communication.
Data Transfer Between AP and Client	After successful authentication and association, the client and AP can now exchange data frames.	• Data transfer begins, and encrypted data frames are exchanged using the encryption keys established during the 4-way handshake (if WPA/WPA2 is used). • The client and AP can now send and receive unicast, multicast, and broadcast data.

Q6. Explain each steps involved in EAPOL 4-way handshake and the purpose of each keys derived from the process

Message 1: AP → Client

- **AP sends a nonce (ANonce) to the client.**
- **ANonce is a random value used for key generation.**

Message 2: Client → AP

- **Client generates its own nonce (SNonce).**
- **Client now has PMK, ANonce, and SNonce — uses them to derive the PTK (Pairwise Transient Key).**
- **Sends SNonce to AP.**
- **Also includes a Message Integrity Code (MIC) to prove it has the PMK.**

Message 3: AP → Client

- **AP now has PMK, ANonce, SNonce — so it derives the same PTK.**
- **Sends Group Temporal Key (GTK) (encrypted) to the client for broadcast/multicast traffic.**
- **Includes a MIC to verify integrity.**

Message 4: Client → AP

- **Client sends an acknowledgment to confirm installation of the keys.**
- **The handshake is now complete, and both devices can securely communicate.**

Q7. Describe the power saving scheme in MAC layer and explore on the types of Power saving mechanisms.

Basic Power Saving Mechanism (802.11 Standard)

Sleep Mode:

- **The client (STA) enters a low-power state (sleep).**
- **It periodically wakes up to listen for beacon frames from the AP.**

Beacon Frames:

- **APs broadcast beacon frames at regular intervals.**
- **These beacons contain a Traffic Indication Map (TIM) that shows which clients have buffered data waiting.**

Traffic Indication Map (TIM):

- **Indicates which clients have pending unicast data at the AP.**
- **If the client's AID (Association ID) is listed, it sends a PS-Poll to request the data.**

PS-Poll Frame:

- **Sent by a sleeping client when it finds that data is pending.**
- **AP responds with the buffered data, and the client can then return to sleep.**

Types of Power Saving Mechanisms

1. Unscheduled Power Save Delivery (U-APSD / WMM-PS):

- **Used in QoS-enabled networks (WMM).**
- **The client controls when it wants data, often triggered by sending an uplink frame.**
- **More efficient and flexible than legacy power save.**

2. Scheduled Power Save Delivery (S-APSD / Scheduled Service Periods):

- **Client and AP agree on scheduled service times.**
- **The AP transmits data only during pre-agreed service periods, minimizing wake-ups.**

3. Target Wake Time (TWT) – (802.11ax / Wi-Fi 6):

- **Clients negotiate with the AP to wake up at specific times.**
- **Great for IoT devices that don't need constant communication.**
- **Reduces channel contention and improves battery life.**

4. Legacy Power Save Mode (802.11b/g):

- **Based on TIM and PS-Poll frames.**
- **Still widely supported, but less efficient compared to modern methods.**

Q8. Describe the Medium Access Control methodologies.

Medium Access Control (MAC) Methodologies

The goal of MAC is to control how multiple devices share the wireless medium (radio channel) without collisions and with fairness.

Distributed Coordination Function (DCF)

- **Based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).**
- **Devices listen before transmitting.**
- **If the medium is busy, they wait for a random backoff time.**
- **Uses ACK frames to confirm successful reception.**
- **Uses Interframe spaces (IFS) like DIFS/SIFS.**
- **Avoids collisions using Random Backoff.**
- **RTS/CTS (Request to Send / Clear to Send) optional to avoid hidden node problem.**

Point Coordination Function (PCF)

- **Works in infrastructure mode (with Access Point).**
- **AP uses a polling mechanism to control who can transmit.**
- **Ensures contention-free communication.**
- **Rarely used in real-world Wi-Fi.**
- **Time is divided into Contention-Free Period (CFP) and Contention Period (CP).**
- **Used where timing-sensitive delivery is needed (e.g., voice).**

Hybrid Coordination Function (HCF)

Combines both DCF and PCF.

EDCA:

- **Priority-based access using different Access Categories (AC).**
- **Higher-priority traffic (like voice) gets smaller contention window and shorter AIFS.**

HCCA:

- **Centralized scheduling by Hybrid Coordinator (usually the AP).**
- **Ensures QoS guarantees by reserving time slots.**

Time Division Multiple Access (TDMA)

- **Time is divided into slots, and each device is assigned a specific time slot to transmit.**
- **No collisions, as access is pre-scheduled.**
- **More common in LTE, 5G, and sensor networks.**

MAC Methodology	Standard	Access Type	Key Use Case
DCF	802.11	CSMA/CA (random backoff)	Basic Wi-Fi access
PCF	802.11	Polling-based	Contention-free (rarely used)
EDCA (HCF)	802.11e	Priority-based CSMA/CA	QoS for voice/video
HCCA (HCF)	802.11e	Scheduled/polling	Guaranteed QoS (e.g., VoIP)
TDMA	Non-WiFi	Time-slotted	Industrial/IoT/5G systems

Q9. Brief about the Block ACK mechanism and its advantages.

Block ACK Mechanism (Block Acknowledgment)

What it is:

- **A method to acknowledge multiple data frames with a single acknowledgment frame.**
- **Introduced in IEEE 802.11e and enhanced in 802.11n and later.**

Block ACK works in the following manner:

1. **The sender and receiver agree to use Block ACK through a setup (Add Block ACK Request and Response).**
2. **The sender transmits a burst of data frames (MPDUs).**
3. **Instead of acknowledging each frame individually, the receiver sends one Block ACK.**
4. **This ACK includes a bitmap indicating which frames were successfully received.**

Advantages of Block ACK:

- **Reduces overhead. One ACK instead of many and saves time and bandwidth.**

Improves throughput:

- **Higher efficiency, especially with high data rates and long frame bursts.**

Supports QoS:

- **Enhances real-time performance for multimedia (voice/video).**

Efficient retransmissions:

- **Only the missing frames (not acknowledged in bitmap) are retransmitted.**

Better channel utilization:

- **Less time spent on control frames, more on actual data transfer.**

Q10. Explain about A-MSDU, A-MPDU and A-MSDU in A-MPD.

In wireless communication, there's a lot of overhead: each frame carries its own header, acknowledgments, and waits between transmissions. Aggregation reduces this overhead by combining multiple data units into one transmission, increasing throughput and efficiency.

A-MSDU (Aggregated MAC Service Data Unit)

- **A-MSDU aggregates multiple MSDUs into a single MPDU to reduce protocol overhead.**
- **All MSDUs in an A-MSDU must be destined to the same receiver and have the same TID (Traffic Identifier).**
- **The aggregation happens above the MAC header, and a single MAC header is used for all MSDUs.**
- **Each MSDU inside has its own subframe header (DA, SA, Length) and padding for 4-byte alignment.**
- **A-MSDU is more efficient for small packets, but a single error may corrupt the entire frame.**

A-MPDU (Aggregated MAC Protocol Data Unit)

- **A-MPDU aggregates multiple MPDUs into one PHY layer frame using a common PHY header.**
- **Each MPDU in an A-MPDU has its own MAC header and FCS (Frame Check Sequence).**
- **A-MPDU allows selective retransmission of failed MPDUs (better reliability).**
- **This method is robust and widely used in 802.11n/ac/ax for high throughput.**
- **The receiver uses a Block ACK with a bitmap to indicate successfully received MPDUs.**

MSDU inside A-MPDU

- **This technique combines both aggregations: multiple A-MSDUs packed as MPDUs into a single A-MPDU.**
- **Each A-MSDU becomes one MPDU within the A-MPDU structure.**
- **Nested aggregation provides maximum efficiency, reducing both MAC and PHY overhead.**
- **This is used in high-throughput Wi-Fi (like 802.11n and 802.11ac) to support bulk data transfer.**
- **It allows fine-grained error recovery (thanks to A-MPDU) while still reducing header overhead (via A-MSDU).**