Module 4 Assignment

Wi-Fi Training Program

Siddharth Balaji

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

MAC layer corresponds to the second layer of the OSI model which plays a vital role in managing access to the medium (wireless in this case), ensuring there is no collision, error detection but no correction and is responsible for converting message into MAC frame before sending it to the physical layer.

The MAC layer is part of the Data Link Layer (Layer 2) in the OSI model. It is divided into two sublayers:

1.Logical Link Control (LLC) – responsible for identifying network protocols and error checking.

2.Media Access Control (MAC) - responsible for controlling access to the physical transmission medium.

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

The MAC layer frame consists of 9 fields and subfields, each adding information to the packet.

Frame control	Duration/ID	Address 1	Address 2	Address 3	SC (Sequence Control)	Address 4	Data	CRC
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes	0–2312 bytes	4 bytes

The following are the 9 fields along with their purposes:

FRAME CONTROL: It is 2 bytes long field which defines type of frame and some control information.

DURATION: It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied (in µs).

ADDRESS 1 TO 4: These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.

SEQUENCE CONTROL (SC): It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits). Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.

DATA: It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).

CRC (Cyclic Redundancy Check): It is 4 bytes long field which contains a 32-bit CRC error detection sequence to ensure error free frame.

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

MANAGEMENT PLANE:

The purposes of management plane are establishing, maintaining, and terminating connections between stations and access points.

- Beacon Generation
- Authentication
- Association/Re-association
- Deauthentication
- Disassociation
- Probe Request/Response
- Timing Synchronization
- Capability Information Exchange
- SSID & BSSID Handling
- Power Management Support

CONTROL PLANE:

The purpose of control plane is to assist in medium access control, avoiding collisions and acknowledging transmissions.

- Medium Reservation
- Acknowledgement
- Block Acknowledgement
- PS-Poll Frame Handling
- Clear Channel Assessment (CCA)
- Contention-based Access (CSMA/CD)
- Control Frame Exchange

DATA PLANE: (Data Frames)

The purpose of control plane is to transmit actual user data (like IP packets, voice, video).

- Frame Fragmentation/Reassembly
- Addressing
- QoS Handling
- Data Encryption/Decryption
- Sequence Numbering
- Multicast and Broadcast Handling
- Frame Aggregation
- Error Detection

Q4. Explain the scanning process and its types in detail

Scanning is the process by which a station (STA) discovers nearby Access Points (APs) before connecting to a network. This step is used for network discovery, roaming, and initial association.

There are two types of scanning, passive scanning and active scanning.

PASSIVE SCANNING:

- 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.

ACTIVE SCANNING:

- 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.

The frames in Scanning (Management Frames):

We can use a Wireshark filter to view the fames for a Wi-Fi capture and it will contain the following frames

1. Beacon Frame (Passive Scan)

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

2.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.

3. 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.
- It contains BSSID, supported data rates, channel info, security settings (RSN), and timing parameters to help the client decide whether to join.

USE CASE:

SCENARIO	SCANNING TYPE
Device boot-up/first time connect	Passive or Active
Roaming between APs in same network	Active (fast handover)
Hidden SSID (not in beacon)	Active alone
Power-saving sensor mode	Passive

Q5. Brief about the client association process.

The client association process is the set of steps that a Wi-Fi station (STA) follows to connect to an Access Point (AP). This process ensures that the station is authenticated, associated, and ready to exchange data.

STEPS IN THE PROCESS:

SCANNING:

- STA discovers nearby APs using passive or active scanning.
- Collects information like SSID, BSSID, signal strength, supported rates, etc.

AUTHENTICATION:

- The STA sends an Authentication Request to the AP.
- The AP responds with an Authentication Response.
- For Open System Authentication (default in most networks), this is just a 2-frame

ASSOCIATION:

- After successful authentication, the STA sends an Association Request.
- The AP replies with an Association Response, assigning an Association ID (AID) to the client.
- From this point onwards, the STA is logically connected to the AP and can send/receive frames.

4-WAY HANDSHAKE:

If the AP uses WPA/WPA2/WPA3, a 4-way handshake occurs.

- It derives encryption keys (PTK, GTK) using pre-shared key or 802.1X authentication.
- After this, encrypted communication begins.

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

The EAPOL 4-Way Handshake is a critical security process used in Wi-Fi (WPA2/WPA3) networks to securely derive encryption keys between the client (STA) and the Access Point (AP) after association. It ensures that both sides share the same secret key without directly sending it over the air.

KEYS USED:
PMK (PAIRWISE MASTER KEY): It is the hared secret key derived from PSK (password) or EAP (802.1X). Basis for further key generation.
PTK (PAIRWISE TRANSIENT KEY): It is the unique encryption key for each STA-AP session, used for unicast traffic.
GTK (GROUP TEMPORAL KEY): It is the encryption key used to protect broadcast and multicast traffic.

MESSAGE	SENDER TO RECIEVER	ACTION	PURPOSE
Message 1	AP to STA	Sends ANonce (AP's random number).	Start handshake, provide fresh randomness
Message 2	STA to AP	STA generates SNonce (STA's random number), calculates PTK, and sends SNonce to AP.	Share client's random value, prove it knows the PMK.
Message 3	AP to STA	AP now computes PTK, generates and sends the GTK encrypted with PTK.	Deliver broadcast/multicast key (GTK) securely.
Message 4	STA to AP	STA acknowledges receipt and successful install of PTK and GTK.	Final confirmation to start encrypted communication.

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

The MAC layer in Wi-Fi includes power saving mechanisms to help reduce energy consumption, especially for battery-powered devices like smartphones, tablets, and IoT sensors.
There are two standard modes:
Active Mode: The STA is always awake.
Power Save Mode (PSM): The station sleeps most of the time and wakes up periodically.

POWER SAVING MECHANISMS:
LEGACY POWER SAVING MODE (PSM):

- This is the standard sleep/wake mechanism using PS-Poll and TIM in beacons.
- It is simple but adds latency for real-time traffic.

U-APSD (UNSCHEDULED AUTOMATIC POWER SAVE DELIVERY):

- It is used in VoIP/Multimedia applications.
- The STA sends a trigger frame (e.g., data frame), and AP responds with multiple buffered frames.
- It eliminates the need for PS-Poll and reduces delay.
- It is used in 802.11e for QoS support.

TWT (TARGET WAKE TIME):

- STA and AP negotiate a schedule during which the STA will be awake.
- The AP only transmits to the STA during agreed TWT periods.
- It is ideal for IoT devices that can sleep for long durations.
- Used in 802.11ax or Wi-Fi 6

WNM-SLEEP MODE (WIRELESS NETWORK MANAGEMENT):

- It lets STA sleep for extended time without losing association.
- AP can send buffered frames when STA wakes up based on negotiated rules.

Q8. Describe the Medium Access Control methodologies

Medium Access Control (MAC) techniques are essential to coordinate which station among multiple that can transmit and avoid collisions.

There are two types of MAC methodologies used in 802.11:

1. Contention-based: CSMA/CA
2. Contention-free: PCF, HCCA, EDCA

CARRIER SENSE MULTIPLE ACCESS WITH COLLISION AVOIDANCE (CSMA/CA):

1. Listens to the medium (carrier sense).
2. If the medium is idle, it waits for a short Interframe Space (IFS) and transmits.
3. If the medium is busy, it waits and selects a random backoff timer.
4. When the backoff timer expires and the medium is still idle, the transmission begins.

POINT COORDINATION FUNCTION (PCF):

- The PCF allows users to transmit by granting access to the stations by polling them.
- By reserving the medium, AP ensures that stations cannot transmit data unless polled by the AP.
- The stations are polled in a Round Robin method.

DISTRIBUTED CO-ORDINATION FUNCTION (DCF):

- DCF is a hybrid methodology which uses PCF with distributed control. In this method, everyone including the Access Point are considered as participants contending for the wireless medium.
- It operates based on CSMA/CA mechanism where data is transmitted when a participant senses a medium to be idle.
- If a collision takes place, the station waits for particular amount of time called backoff before retransmitting the same signal.

ENHANCED DISTRIBUTION CHANNEL ACCESS (EDCA):

- EDCA is QoS enhanced DCF where in traffic priority is given to stations contending for medium access.
- By taking various parameters into consideration, traffic is transmitted into separate queues in the Radio Hardware.

HCF CONTOLLED CHANNEL ACCESS (HCCA):

- Advanced polling system controlled by the AP.
- AP can reserve time slots for QoS stations.
- Suitable for guaranteed latency (e.g., VoIP).
- Rarely used in normal Wi-Fi networks due to complexity.

Hybrid Coordination Function (HCF) is a combination of both PCF and DCF.

Q9. Brief about the Block ACK mechanism and its advantages

Block ACK is a mechanism where acknowledgement to multiple frames is given at a time. This is a very efficient mechanism that is popularly used. It was introduced in IEEE 802.11e and improved in later amendments like 802.11n. Block ACK is used during aggregation.

1. The transmitter initiates the process by sending Add Block ACK (ADDBA) to find out if receiver supports Block ACK and it receives an acknowledgement from the receiver.
2. After transmitting the data, the transmitter asks for Block ACK with a request and it sends an acknowledgement. This session can be deleted by sending Delete Block ACK(DELBA) by the transmitter.

The two types of Block ACK are Immediate BLOCK ACK and Delayed BLOCK ACK.

WORKING:

1. The ender (STA/AP) transmits a burst of data frames (called MPDUs) using Block ACK-enabled transmission.
2. After the burst, it sends a Block ACK Request (BAR).
3. The receiver replies with a Block ACK, indicating which frames were received successfully (using a bitmap).
4. If some frames failed, may be due to interference), only those are retransmitted.

ADVANTAGES:

- Reduces overhead by avoiding per-frame ACKs.
- Faster transmission of multiple frames, especially in video/voice.
- Only lost frames are resent, not the whole sequence.
- More time spent sending data than control frames.

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

A-MSDU (AGGREGATE MAC SERVICE DATA UNIT):
A-MSDU stands for Aggregate MAC Service Data Unit which is aggregation of two or more MSDU. MSDUs are data packet which are received by the MAC layer from the layers above it.

A-MPDU (AGGREGATE MAC PROTOCOL DATA UNIT):
A-MPDU stands for Aggregate MAC Protocol Data Unit which is aggregation of two or more MPDU. MPDUs are data packets which are received by the physical layer from the MAC layer. Multiple MPDUs are aggregated together which is transmitted with a PHY header by the radio.

MSDU inside A-MPDU:
A-MSDU in A-MPDU refers to a scenario where multiple A-MSDUs are bundled together to create an A-MPDU. This approach can be beneficial for scenarios where there are many smaller MSDUs to transmit, allowing for further aggregation and overhead reduction