Name: J Kevin Immanuel

College: VIT Chennai

Module 4 Assessment Wifi Training

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

MAC layer is responsible for several functions:
1) It is responsible for medium access control

2) Framing: It adds MAC headers with source and destination MAC address

3) Error detection

MAC layer is part of the Data Link Layer (Layer 2)

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

The 802.11 MAC frame format consists of:

Header | Frame Body | FCS

Header: Header consists of the following sub components:

Field	**Size**	**Description**
Frame Control	2 bytes	Type, subtype, control flags (To DS, From DS, retry, etc.)
Duration/ID	2 bytes	Used for NAV (Network Allocation Vector)
Address 1	6 bytes	Receiver Address
Address 2	6 bytes	Transmitter Address
Address 3	6 bytes	Destination, source, or BSSID
Sequence Control	2 bytes	Sequence number & fragment number
(Optional) Address 4	6 bytes	Present in WDS or mesh frames
QoS Control (optional)	2 bytes	For QoS traffic prioritization
HT Control (optional)	4 bytes	High throughput control field

Frame body: Contains the actual payload

FCS (Frame Check Sequence): Used for CRC error detection

Q3) List all MAC layer functionalities in management, control and data plane.

Management plane: Handles client association, power management, security management, traffic priority management, scanning, QoS management and load balancing

Control Plane: Handles flow control and medium access control

Data plane: Handles data transmission between 2 end points of the networks

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

Scanning is the process of a wifi client discovering a wifi access point.

There are two types of scanning :
1) Active scanning: In this, the wifi client first sends a Probe request management frame, which contains all the capabilities of the client. When received by the AP, it processes the frame and sends back a probe response frame containing the AP's capabilities. It is upto the client to select the AP.

2) Passive scanning: In this, the AP sends a beacon frame periodically, which contains the AP's capabilities. This frame is received by the clients.

Q5) Briefly explain the client association process

When a client is connecting to an AP to share data to a wireless network, it follows the following steps:

1) Scanning: This process is done either through active scanning or passive scanning as discussed above.
2) Authentication: The client first sends an authentication request to the AP. When the AP receives this, it sends back the authentication response. In modern secure connection like WPA2/3, there is 4 way handshake for authentication.
3) Association: The client sends an association request to join the AP. The AP sends back an association response, assigning the client an association ID
4) Data can now be shared.

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

Steps:
1) Access point sends an ANonce message (bunch of random numbers) to the client

2) Client receives the ANonce, creates SNonce (random numbers) and generates the PTK using the ANonce, SNonce, PMK and MAC address.

3) The client sends back the SNonce and a Message Integrity Check (MIC) to the AP, to check if the message is not corrupted.

4) The AP then sends the GTK to the client. AP creates the GTK using the GMK without the client's activity.

5) The client sends back an EAPOL message to AP, ending the process.

Keys:
1) PSK – Preshared Master Key – This key is same for all clients logged into the network.

2) PMK – Pairwise Master Key – This key is unique for each client.

3) PTK – Pairwise Transient Key – This key is used to encrypt and decrypt unicast information traffic at that particular session. It is generated on the client.

4) GMK – Groupwise Master Key

5) GTK – Groupwise Temporal Key – This key is used to encrypt/decrypt multicast and broadcast information traffic

Q7) Describe the power saving scheme in MAC layer and explore the types of power saving mechanisms

One of the functionalities of WLAN MAC layer is to perform power management in devices. Client and AP are running on battery so there is a need to conserve power.

When a client is idle, the client sends a QoS NULL frame (no data), with the power management bit in frame control set to 1, and turn of radio.

When the client sends NULL frame to AP, AP sends beacon with the AID of the client set.

After waking, Client will receive beacons and all beacons will have a bitmap. Client will check the TIM IE (Traffic Indication Element) if the AID of client is set. If it is set, client will send a Power Save Poll to the AP

AP will send the buffer frame with more data(if there is any more)

Client will keep sending PS Poll to AP to continually receive buffer frames if there are more.

Q8) Describe Medium access control methodologies

1) Point Coordination Function:
   AP acts as the coordinator. It has a polling list of stations. It sends a CF Poll frame to the station in the list. When the station receives the frame, it is allowed to share data in the medium. Once the CFP MAX Duration expires, the station is not allowed to access the medium and the AP sends the CF Poll frame to the next station in the list
   This method is obsolete now due to various reasons:
   a) Polling time increases when number of stations increase so it is not scalable
   b) Type of traffic (QoS) is not considered
   c) If a station is asleep/does not respond, the time is wasted.
2) Distributed Coordination Function:
   This method is based on CSMA/CA. In this, the AP and the clients participate together in contending for access to the wireless medium. Each transmitter senses if the channel is available for transmission. If not available, it will keep waiting. If the channel is available, it will start the backoff process. This means that it waits for a random amount of time that is calculated using the backoff time formula. The countdown from the start of the time to 0 happens only when the channel if free. Once the timer reaches 0, it sends the message and waits for ACK from receiver. If it does not receive, the sender increases the backoff time and again counts down to retransmit the message.
   Disadvantages are that
   a) No QoS Consideration
   b) Insufficient in dense networks
3) Enhanced Distribution Channel Access (EDCA): This is similar to DCF, except that the traffic type is considered for priority. Firstly, the message that is to be transmitted is assigned an access category (voice, video, etc).
   There are separate queues for each category. Each category has:
   a) Arbitrary Inter Frame Space: Time to wait after channel becomes idle
   b) CWMin/CWMax: Used to calculate random backoff
   c) TXOP: Transmission Opportunity

Q9) Briefly explain about block ACK mechanisms and its advantages

Block ack is part of flow control of MAC layer. Instead of sending a single frame and receiving a single ACK from receiver, the sender sends multiple frames as a "block" and waits for the receiver's ACK. The ACK sent by receiver is a single ACK, which is a bitmap of each frame, indicating which frames have been received and which have not.

Advantages:

1) Reduces overhead: Instead of sending one ACK for every frame, you send one Block ACK for multiple frames – much less control traffic
2) Higher Throughput: More time is spent actually sending data, less time wasted sending ACKs - increases overall data rate.
3) Efficient for Bulk Transfers: Ideal when sending many frames at once (like video streaming, file downloads, or aggregated frames).
4) Selective Retransmission: Only the missing or corrupted frames are retransmitted (not the entire burst), saving bandwidth and time.
5) Better Use of Airtime: Especially important in high-speed Wi-Fi (802.11n/ac/ax) where small ACK frames could otherwise waste valuable wireless airtime.

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

A-MSDU: Layer 3 to 5 are combined. All the MSDU in a MAC frame are combined together into a single frame. This means that instead of sending one frame at a time and waiting for ack, we can send multiple MSDUs at the same time in a single frame and get back a single ACK. The frame has a single MAC header.

The problem with A-MSDU is that if the sender does not get back the ACK, it has to once again send a frame with the same MSDUs in it.

A-MPDU: Similar to A-MSDU, but instead of having a single MAC header, each MSDU will have a separate MAC Header. In doing this, the ACK received by the sender will be a block ACK, meaning we can check which MSDU is missing and retransmit only the missing MSDU.

A-MSDU inside A-MPDU: Combination of both the aggregation techniques. Instead of having a single MSDU with a single MAC header, there will be 2 MSDU with a single MAC header. This gives us better performance.