WiFi Assessment 4 - Module 4

Name	T K Gowtham
Email ID	gowthamkamalasekar@gmail.com
College	VIT Chennai

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

- MAC is the Media Access Control Layer which is a sub layer of the data link layer in the OSI model.
- The two sublayers of the data link layer are : LLC (Logical Link Control) and MAC Layer.
- It controls access to the physical transmission medium.
- Assigns unique MAC address to devices for identification.
- Handles frame creation and addressing (adds MAC source and destination)
- Ensures proper delivery of data between devices on the same local network.
- Manages collision detection/avoidance in shared networks (like CSMA/CA in WiFi).

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

Field	**Size**	**Purpose**
Frame Control	2 Bytes	Contains control flags like frame type, subtype, to/from DS, etc
Duration/ID	2 Bytes	Used for setting Network Allocation Vector for medium access.
Address 1	6 Bytes	Usually the receiver address
Address 2	6 Bytes	Usually the transmitter address

Address 3	6 Bytes	Can be BSSID or destination address (depend on frame type)
Sequence Control	2 Bytes	Identifies frame fragments and order (sequence number + fragment id)
Address 4 (Optional)	6 Bytes	Used only in wireless distribution systems (WDS).
QoS control (optional)	2 Bytes	Quality of Service info
HT Control (optional)	4 Bytes	Used in High Throughput (802.11n and above)
Frame Body	variable	Actual Data
FCS (Frame Check Seq)	4 Bytes	CRC used for error detection.

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

- Management Plane - Handles network joining, maintenance and disconnection
    - Handles client association, power management, security management, traffic priority management
    - Beacon generation, Authentication, Association/Reassociation, Disassociation/Deauthentication, probe request/response, timing synchronization, capability exchange.
- Control Plane - handles medium access coordination and transmission control.
    - RTS/CTS, ACK, NAV (Network Allocation Vector), Power Save Control, Backoff Algorithm (CSMA/CA).
    - Handles flow control, medium access control
- Data Plane - Handles actual data transmission between devices.
    - Handles data transmission between two endpoints of the wireless network.
    - Frame fragmentation and reassembly, frame sequencing, MAC addressing, QoS Handling, Encryption/Decryption Hooks.

4. Explain the scanning process and its types in detail

- Passive Scanning
    - Client listens on each channel for beacon frames sent by APs
    - Beacon broadcasts every 100ms and contains SSID, Supported data rates, security info, BSSID, channel info.
    - Client tunes to a channel.
    - Waits for a beacon from any AP
    - Collect info and move to the next channel.
    - Repeat until all channels are scanned.

- Active Scanning:
    - Client sends a probe request on each channel and APs respond with a probe response containing network info.
    - Client tunes to a channel.
    - Sends probe requests (can be broadcast or with a specific SSID).
    - APs on that channel respond with probe response.
    - Client collects response and moves to the next channel.

5. Brief about the client association process

- Beacon listening → The client listens for beacon frames from nearby access points. These beacons advertise the presence of WiFi networks.
- Scanning → The client sends a probe request to search for available networks. The AP replies with a probe response, containing its details (SSID, capabilities, etc.).
- Authentication → The client sends an authentication request to the AP. The AP replies with an Authentication response. This step ensures the client is allowed to attempt a connection.
- Association → The client then sends an Association Request. The AP replies with an Association Response if successful. Now the client is officially connected to the AP and given Association ID (AID).
- Data Transfer → After association, data transfer begins.
- So, flow of client connection with AP will be as follows :
    - Probe Request to AP
    - Probe Response to Client
    - Authentication Request to AP
    - Authentication Response to Client
    - Association Request to AP
    - Association Response to Client
    - Data transfer between AP and Client

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

- The 4 way handshake is a process between the WiFi client (supplicant) and the Access point (authenticator) to prove both sides know the same Pairwise Master Key(PMK), derive fresh session keys, and secure the wireless connection.

- The keys involved are :
    - PMK - Pairwise Master Key : Shared secret derived from the WiFi password or 802.1x authentication.
    - PTK - Pairwise Transient Key : Derived during the handshake, used for encrypting unicast traffic.
    - GTK - Group Temporal Key : Used for encrypting broadcast and multicast traffic.

- 4-Way Handshake Process :
    - AP → Client (EAPOL Msg 1) : AP sends a random nonce (Anonce) to the client to start the handshake and give the client the AP's random value.
    - Client → AP (EAPOL Msg 2) : Client generates its own nonce (Snonce) and derives the PTK using : PTK = PRF(PMK, ANonce, SNonce, AP MAC, Client MAC). Client sends SNonce + MIC (Message Integrity Code). MIC proves the client has the PMK (shared secret).
    - AP → Client (EAPOL Msg 3) : AP verifies MIC, derives the same PTK, and sends encrypted GTK, replay counter, MIC, so as to share the group key (GTK) securely with the client.
    - Client → AP (EAPOL Msg 4) : Client sends final ACK to confirm installation of PTK and GTK, to complete handshake, both sides now securely communicate.

- PTK is used for encrypting unicast data, GTK is used for Broadcast/Multicast. Both parties will now have identical keys.

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

- Power saving scheme in MAC Layer (802.11 WLAN) → The MAC Layer in WLAN plays a key role in conserving battery life of wireless clients (STAs) like phones, laptops, etc.
    - Sleep and Wake up Mechanism is used in MAC Layer as the power saving scheme.

    - Client goes to sleep when idle but still associated with the AP, the client sends a QoS NULL frame. This frame has the power management bit set to 1 in the 802.11 frame control field. The client then switched off its radio to save power.

    - Waking up and Checking for data : the client wakes up at defined intervals by the DTIM (Delivery Traffic Indication Message) in the Beacon frame sent by the AP. It checks the TIM (Traffic Indication Map) IE for its AID (Association ID) in the Partial Virtual Bitmap (PVB).

    - Checking the PVB : Each bit in the PVB corresponds to a client's AID. If a client's AID bit is 1, it means the AP has data buffered for that client.

    - Retrieving the Data : The client sends a PS-Poll (Power Save Poll) frame to the AP. The AP then sends the buffered data to the client.

- Types of Power Saving Mechanisms :

    - Legacy Power Save Mode (PSM) : based on polling using PS-Poll frames. Clients sleep and periodically wake up to check Beacon frames.

    - Unscheduled Automatic Power Save Delivery (U-APSD) : Used in QoS enabled networks (WMM power save). Triggers data delivery without waiting for beacon or polling and more efficient for voice/video traffic.

    - Target Wake Time (TWT) : Introduced in WiFi 6. Clients negotiate specific times to wake up and receive/send data. It also improves power efficiency in IoT devices.

8. Describe the Medium Access Control methodologies

- Point Coordination Function (PCF)
    - It is a contention free type.
    - It is used in Real time traffic (voice/video)/
    - AP acts as a central controller (point coordinator).
    - AP polls devices one by one to transmit without collision.
    - Time is divided into Contention-Free Period (CFP) and Contention Period (CP).
    - Rarely used in practice due to complexity.

- Distributed Coordination Function (DCF)
    - It is contention based type
    - It uses CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
    - Device listens to the channel before sending.
    - If the medium is idle → waits for a short time(DIFS) and sends
    - If busy then waits, then picks a random backoff time and tries again.
    - ACK : after successful data transfer, the receiver sends an ACK to confirm.
    - It is used in all WiFI devices by default.

- Enhanced Distribution Channel Access (EDCA)
    - EDCA is an improved version of DCF used in 802.11e standard to provide QoS for applications like voice, video, and real-time traffic.
    - In DCF, all data has equal priority but in reality voice needs fast, low latency access, video needs good bandwidth, background downloads can wait.
    - So, EDCA prioritizes traffic into different categories.
    - It divides traffic into four Access categories from highest to lowest priority : AC_VO (Voice/VoIP), AC_VI (Video Streaming), AC_BE (Best effort for Browsing), AC_BK (Background like update and sync).
    - Each category has its own contention parameters like : AIFS (Arbitration Inter-Frame Space) that is how long to wait before contending, CWmin/CWmax (Context Window) which is the backoff range.

    - Higher the priority, shorter the AIFS and smaller backoff range which means it gets to access the channel faster.
    - Each AC in the same device works like Virtual station as they compete for the channel independently. If two categories collide inside the same device, a rule is applied to resolve it (higher priority wins or perform backoff again i.e. double their contention window and retry later).

9. Brief about the Block ACK mechanism and its advantages

- Flow control in WiFi ensures that data is sent at a rate the receiver can handle, avoiding buffer overflow and packet loss. In WiFi, which is half-duplex, the sender waits for an ACK before sending more data. There are two types of ACKs.
    - Single ACK - one ACK per frame
    - Block ACK - one ACK for multiple frames

- The sender transmits a burst of multiple data frames.
- Instead of getting ACKs one by one, the receiver sends a single Block ACK frame.
- This block ACK tells the sender which frames were received and which are missing.
- Only the missing frames are retransmitted.

- Advantages of Block ACK are :
    - Reduces control overhead which means fewer ACKs.
    - Improves throughput, especially in high speed networks.
    - Efficient use of bandwidth.
    - Faster recovery from lost frames.
    - Better performance for real-time apps.

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

- Aggregation improves efficiency by sending multiple data units together instead of one-by-one. This reduces overhead (like PHY/MAC headers, ACKs, backoff delays).
- A-MPDU (Aggregated MAC Protocol Data Unit) is a frame aggregation technique in WiFi where multiple MPDUs (each with its own MAC header) are combined into a single PHY layer transmission.

- A-MSDU (Aggregated MAC service data unit) :
    - Combines multiple MSDUs into one big frame
    - One PHY + MAC header for the whole A-MSDU
    - Receiver processes all MSDUs together
    - If any part is lost, the entire A-MSDU is retransmitted.
    - Good for small, reliable transmission.
    - A-MSDU has 1 PHY + 1 MAC header, followed by MSDU1 + MSDU2 + MSDU3 → then ACK.

- A-MPDU (Aggregated MAC Protocol Data Unit) :
    - Combines multiple MPDUs (each with its own MAC header) under one PHY frame.
    - If one MPDU is lost, only that one is retransmitted.
    - More robust than A-MSDU
    - Each MPDU can carry one MSDU
    - Each MSDU has its own MAC header, combined into one PHY → followed by ACK.

- A-MSDU inside A-MPDU
    - Combining both methods, each MPDU contains an A-MSDU (which contains multiple MSDUs).
    - So inside each MPDU : multiple MSDUs.
    - Combines flexibility of A-MPDU with efficiency of A-MSDU.
    - Complex but best performance.
    - Each MPDU has multiple MSDUs (A-MSDU), and multiple such MPDUs are packed in one PHY transmission → then ACK.