Wi-Fi Module 4

1. What is the significance of MAC layer and in which position it is placed in the OSI model
   - MAC layer stays in the 2nd layer of OSI model.
   - It is responsible for,
   - Error detection
   - Effective sharing of medium
   - Flow control
   - Effective sharing of medium

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

1. Protocol - 00 for wifi

2. Type - Defines whether the frame is Management (00), Control (01), or Data (10)

3. Subtype - Identifies the specific type of frame (e.g., Beacon, RTS, CTS, Data)

4. To DS - Set if the frame is heading to the Distribution System (AP)

5. From DS - Set if the frame is coming from the Distribution System (AP)

6. More Fragments - Set if the frame is fragmented

7. Retry - Set if this is a retransmitted frame

8. Power Management - Indicates whether the STA is in power-saving mode

9. More Data - Indicates additional buffered data at the AP for power-saving STAs

10. Protected Frame - Set if the frame is encrypted (WEP, WPA, WPA2)

11. Order - Set for strictly ordered frames

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

A. Management Plane Functions

These are used to **establish, maintain, and tear down connections** in a wireless network.

1. **Authentication**
    - Verifies the identity of a device before joining the network.
2. **Association / Reassociation**
    - Establishes a connection between a station (STA) and an Access Point (AP).
    - Reassociation allows a STA to move from one AP to another.
3. **Beacon Frame Transmission**
    - APs send beacon frames periodically to advertise their presence and capabilities.
4. **Probe Request / Response**
    - Used by stations to discover available wireless networks.
5. **Disassociation**
    - Cleanly ends an association between STA and AP.
6. **Deauthentication**
    - Terminates the authentication relationship.

B. Control Plane Functions

Control frames **assist in the delivery and reliability** of data and management frames.

1. **RTS (Request to Send) / CTS (Clear to Send)**
    - Avoids collisions in environments with hidden nodes using virtual carrier sensing.
2. **ACK (Acknowledgment)**
    - Confirms successful reception of a frame.
3. **PS-Poll (Power Save Poll)**
    - Station asks AP for buffered data when waking up from power-saving mode.

4. **Block ACK / Block ACK Request**
    - Efficient acknowledgment of multiple frames in bulk (used in high-throughput modes).
5. **CF-End (Contention-Free End)**
    - Ends contention-free period in PCF (Point Coordination Function), though rarely used now.
6. **Control Wrapper**
    - Encapsulates control information in 802.11n/ac/ax enhancements.
7. **Trigger Frame (802.11ax)**
    - Schedules uplink transmissions in OFDMA (Orthogonal Frequency Division Multiple Access).

C. Data Plane Functions

Handles **actual data transmission** between devices.

1. **Frame Aggregation (A-MSDU, A-MPDU)**
    - Combines multiple data frames for efficient transmission.
2. **Fragmentation and Reassembly**
    - Splits large frames to avoid retransmission of whole frames on errors.
3. **QoS Management (EDCA, HCCA)**
    - Prioritizes traffic types (e.g., voice, video) using Enhanced Distributed Channel Access.
4. **Traffic Scheduling**
    - Ensures fair and efficient use of the medium based on traffic priority.
5. **Encryption / Decryption**
    - Secures data with WEP, WPA2, WPA3 (at MAC sublayer before PHY).
6. **Error Detection (FCS)**
    - Checks for transmission errors using CRC in the MAC footer.
7. **Rate Adaptation**
    - Dynamically adjusts data transmission rate based on channel conditions.

1. Explain the scanning process and its types in detail

A. Passive Scanning

How it works:

1. The STA **listens** for **beacon frames** sent periodically by APs (typically every 100 ms).

B. Active Scanning

How it works:

1. The STA actively **sends Probe Request frames** on each channel.

2. Brief about the client association process
   - Beacon frame
   - Probe request/ response
   - Auth request/response
   - Assoc request/response

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

- AP sends Anonce to STA
- STA sends Snonce to STA
- PTK is generated using Passphrase Anonce Snonce Ap mac and STA mac
- GTK is send from AP to STA

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

The STA informs the **Access Point (AP)** that it's entering **power save (PS) mode**.

In PS mode:

- STA turns off its radio to save power.
- AP **buffers** any frames destined for the STA.

STA **periodically wakes up** (e.g., at beacon intervals) to:

- Check the **Traffic Indication Map (TIM)** in the beacon frame.

- If TIM indicates pending data, STA sends a **PS-Poll** frame to retrieve it.

Legacy power save mode

Target Wake time

8. Describe the Medium Access Control methodologies

- Distributed Coordinated Function
- Point Coordination Function
- EDCA

9. Brief about the Block ACK mechanism and its advantages

Immediate Block ACK: Sent immediately after frame burst (used when latency is critical).

Delayed Block ACK: Sent after a delay (less common, may be used when power saving is a concern).

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

There are three types of MAC AGGREGATION. They are

1. A-MPDU aggregation - Here, under single PHY hdr, multiple frames with MAC headers for each frame will be sent as single entity therefore BLOCK ack after single SIFS can be expected.

2. A-MSDU Aggregation - Under single PHY and MAC headers, multiple frames will be embedded. though looks efficient, it might be difficult to organize and retransmit incase of any errors.

3. A-MSDU inside A-MPDU aggregation - it is the mix of above two types by which under single PHY hdr, frames will be grouped such that each group contains one MAC header making it easier to track and organize.