Name: Aswath S
College: Vellore Institute of Technology, Vellore
Reg.No: 21BEC2188

WiFi Training Program 2025
Module 4

Question 3:
Please list all the MAC Layer Functionalities in all management, control, data planes

Solution:

MAC Layer functionalities:

1. **Management plane-** The MAC layer handles various management tasks that ensure network formation, maintenance, and disassociation
    a. **Scanning-** Scanning is the process by which a wireless device (STA - Station) discovers nearby wireless networks (BSS/ESS) before initiating a connection. It allows the station to find available Access Points (APs), determine their capabilities, and select the best one to associate with.
        i. **Passive Scanning:** In passive scanning, a wireless station (STA) listens for beacon frames that are periodically transmitted by nearby access points (APs). These beacon frames contain critical information about the wireless network, such as the SSID, supported data rates, channel information, and security capabilities. The STA does not transmit any frames during this process.However, it can be slower, especially if the STA has to wait for the next scheduled beacon on each channel.
        ii. **Active Scanning:** In active scanning, the wireless station (STA) proactively sends probe request frames on each channel to discover available wireless networks. Access points (APs) that receive the probe request respond with probe response frames, providing information such as the SSID, capabilities, and supported data rates. Active scanning is generally faster than passive scanning because the STA doesn't need to wait for beacons—it actively triggers a response. However, it consumes more power and creates additional traffic, which can be a consideration in power-sensitive or congested environments.
    b. **Client Association:**
        i. **Scanning (Discovery Phase)**
            - The STA first scans to discover nearby networks.
                - Passive Scanning: STA listens for Beacon frames from APs.
                - Active Scanning: STA sends a Probe Request, and APs respond with Probe Response frames.
        ii. **Probe Request**
            - Sent by the STA to actively search for APs.
            - Can include SSID (specific or broadcast) and supported capabilities.
        iii. **Probe Response**
            - Sent by APs in reply to probe requests.
            - Contains network details such as SSID, capabilities, supported rates, and security features.

iv. **Authentication**
   - The STA sends an Authentication Request frame to the selected AP.
   - The AP replies with an Authentication Response frame.
   - This establishes initial trust (often "Open System" or "Shared Key").

v. **Association**
   - After successful authentication, the STA sends an Association Request frame to join the AP.
   - The AP responds with an Association Response frame.
   - If accepted, the STA is now associated with the AP and can start data communication.

vi. **Data Transfer happens after successful association.**

c. **Security management:**

   i. Wi-Fi security involves encryption and key management to ensure data confidentiality, integrity, and authentication. Two key elements involved in protecting wireless communications are the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK), which are both established during the 4-Way Handshake after a successful association.

d. **QoS Management:**

   i. QoS (Quality of Service) management in the management plane of IEEE 802.11 involves mechanisms that ensure efficient handling and prioritization of different types of network traffic, especially when bandwidth is limited or the network is congested. Within the management plane, QoS features are primarily responsible for identifying the capabilities of both the client and the access point, negotiating QoS parameters during association, and managing traffic categories for services like voice, video, and data. For instance, during the association process, QoS support is communicated through information elements in management frames. Standards like IEEE 802.11e introduce enhancements such as the Enhanced Distributed Channel Access (EDCA) and Hybrid Coordination Function (HCF), which allow for traffic prioritization based on predefined access categories (ACs). These categories ensure that time-sensitive applications like VoIP and video streaming are given higher priority over regular data traffic. QoS management at the MAC layer thus plays a critical role in improving user experience by minimizing delay, jitter, and packet loss for high-priority services.

e. **Power Management:**

   i. Power management in IEEE 802.11 is a MAC layer mechanism designed to conserve energy, especially for battery-powered devices like laptops, smartphones, and IoT devices. It allows stations (STAs) to alternate between active and sleep (doze) states without losing connection to the network.

   ii. When a STA is in Power Save Mode, it informs the Access Point (AP) through a flag in the Association Request or reassociation frame. The AP then buffers any incoming frames destined for that STA while it sleeps. These buffered frames are advertised in the Traffic Indication Map (TIM) field of the periodic beacon frames sent by the AP. The STA periodically wakes up to listen to these beacons. If the TIM indicates buffered data for the STA, it sends a PS-Poll (Power Save Poll) frame to request delivery of the data, after which it can return to sleep.This system allows clients to save energy by avoiding constant radio activity while still receiving important network data.

Advanced protocols like WMM-Power Save (WMM-PS) and Target Wake Time (TWT) in newer standards (like 802.11ax) offer even more efficient power scheduling, particularly for latency-sensitive and low-power IoT devices.

f. **Load Balancing:**

   i. Load balancing in the management plane of IEEE 802.11 refers to techniques used to distribute client devices (STAs) evenly across multiple access points (APs) to prevent congestion and improve overall network performance. In a wireless environment with multiple APs (like in an enterprise or campus setting), clients often tend to associate with the AP that has the strongest signal, even if that AP is already overloaded. This leads to performance degradation for users connected to congested APs, while nearby APs may remain underutilized.To manage this, APs and wireless controllers implement load balancing by influencing the association and roaming behavior of clients. This is often done during the association and reassociation phases, which are part of the management plane. Techniques include:

      - Association control, where the AP may reject or delay association requests if it's heavily loaded.
      - Band steering, which encourages dual-band clients to connect to the less congested 5 GHz band instead of the 2.4 GHz band.

2. Control Plane:

a. **Flow control:**

   i. Flow control in the control plane of IEEE 802.11 is a mechanism that ensures the reliable and orderly delivery of data frames between wireless stations and access points, particularly under conditions of varying network load or congestion. Since wireless communication is subject to interference, collisions, and bandwidth limitations, flow control helps manage the rate at which frames are sent to avoid overwhelming the receiver or the medium. This is achieved through control frames such as ACK (Acknowledgment), RTS (Request to Send), and CTS (Clear to Send). These frames coordinate access to the wireless medium and confirm successful reception, allowing the sender to pace its transmissions. For instance, the RTS/CTS handshake helps prevent collisions in scenarios where hidden nodes are present, effectively regulating the flow of data. By ensuring that only one station transmits at a time and that receivers are not flooded with data faster than they can process it, flow control contributes to the efficiency and reliability of the wireless link.

b. **Media Access Control:**

   i. MAC layer is responsible for coordinating access to the shared wireless medium, ensuring that multiple devices can communicate efficiently and without collision.Methods of MAC are :

      1. **Distributed Coordination Function (DCF)**
         - Mandatory access method in all 802.11 devices.
         - Uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).
         - Before transmitting, a device senses the medium:

        - If idle, it waits for a DIFS (Distributed Interframe Space), then transmits.
        - If busy, it defers and enters a random backoff before retrying.
    - Optionally uses RTS/CTS frames to reduce hidden node issues.
    - After successful frame delivery, an ACK is sent by the receiver.

2. **Point Coordination Function (PCF)**
    - A contention-free polling-based method.
    - The Access Point (AP) controls who transmits and when.
    - Uses a Point Coordinator to poll stations in a specific order.
    - Rarely implemented due to complexity and inefficiency.
3. **Enhanced Distributed Channel Access (EDCA)**
    - Extension of DCF to support Quality of Service (QoS).
    - Divides traffic into 4 Access Categories (ACs): Voice, Video, Best Effort, Background.
    - Each AC has different priorities and contention parameters.
    - Ensures time-sensitive data (e.g., VoIP, video) gets faster access.

3. **Data Plane:**

a. **Frame aggregation:**

i. Data aggregation in the data plane of IEEE 802.11 is a performance-enhancing technique used to increase transmission efficiency by combining multiple data frames into a single larger frame before sending it over the wireless medium. This reduces overhead and improves throughput, especially in high-speed standards like 802.11n, 802.11ac, and 802.11ax.

ii. Types of Frame Aggregation are:

1. **A-MSDU (Aggregated MAC Service Data Unit)**
    - Combines multiple **MSDUs** (higher-layer packets like IP packets) into a **single MAC frame**.
    - All packets must be from the **same source and destination** and have the same QoS.
    - Smaller header overhead but **less flexible**.
2. **A-MPDU (Aggregated MAC Protocol Data Unit)**
    - Combines multiple **MPDUs** (complete MAC frames) into a **single PHY frame**.
    - More robust: Each MPDU can be **individually acknowledged (Block ACK)**.
    - Widely used in **802.11n and newer**.