Name: Devansh Srivastava

Registration number: 21BCE0527

Wi-Fi Training Programme

Module 4

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

Ans. The Medium Access Control (MAC) layer plays a vital role in networking because it is situated in the lower half of the Data Link Layer (Layer 2) in the OSI model. What makes it vital is controlling how devices access and share the channel of communication. This involves controlling which devices can broadcast at what time, preventing collisions, and ensuring fair access to the shared electromagnetic spectrum for wireless networks. It is the interface of the logical link control sublayer with the physical layer.Logical link control sublayer controls MAC addresses (48-bit hardware addresses) to perform addressing; medium access control is performed through methods of coordination; data encapsulation and framing is controlled; and these functionalities are crucial in the case of wireless networks where high medium contention is involved.

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

Ans. The 802.11 MAC header consists of several fields, each serving a specific purpose:

- **Frame Control (2 bytes)**: Contains protocol version, frame type (management, control, data), power management indicators, and other control flags
- **Duration/ID (2 bytes)**: Indicates time needed to transmit the frame (used for virtual carrier sensing)
- **Address Fields (6 bytes each)**: Usually contains up to 4 address fields:
    - Address 1: Receiver address
    - Address 2: Transmitter address
    - Address 3: Typically, destination address or BSSID
    - Address 4: Used in special cases for wireless bridging
- **Sequence Control (2 bytes)**: Contains fragment number and sequence number for frame ordering
- **QoS Control (2 bytes)**: Present in QoS data frames, contains traffic priority information
- **HT Control (4 bytes)**: Optional field for high throughput operations
- **Frame Body**: Variable length payload containing the actual data
- **FCS (4 bytes)**: Frame Check Sequence for error detection

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

Ans.

Management Plane:

- Beacon generation
- Authentication & association
- Scanning & probing
- Disassociation & deauthentication

Control Plane:

- RTS/CTS (Request to Send/Clear to Send)
- ACK (Acknowledgement)
- NAV setting
- Power Save Poll

Data Plane:

- Frame fragmentation/reassembly
- Access control
- Addressing and sequence numbering
- Reliable delivery using ACKs

4. Explain the scanning process and its types in detail

Scanning is the process by which wireless clients discover available networks. There are two primary types:

Passive Scanning

- Client listens on each channel for beacon frames
- No transmission from client, only reception
- Energy efficient but slower
- Client builds list of BSSIDs, SSIDs, and capabilities
- Process:
    1. Switch to channel
    2. Wait for beacons (typically 100ms per channel)
    3. Record information
    4. Repeat for all channels

Active Scanning

- Client actively sends probe request frames
- More efficient for discovering networks quickly
- Higher power consumption
- Process:
    1. Switch to channel
    2. Transmit probe request (broadcast or directed)
    3. Wait for probe responses (typically 10-30ms)
    4. Process responses and record information
    5. Repeat for all channels

5. Brief about the client association process

Ans. The following steps are a part of the association process, which associates a client device (STA) with an AP:

1. **Scan:** STA finds existing APs.

2. **Authentication:** An open or shared key is used to make it through the initial authentication request and response.

3. **Association Request/Response:** STA initiates an association request to a chosen AP, who responds with an association response if the request is accepted.

4. **4-Way Handshake:** The last step in getting the connection and encrypting if security has been turned on.

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

Ans. The EAPOL (Extensible Authentication Protocol Over LAN) 4-way handshake establishes encrypted communications:

1. **Message 1** (AP → Client):
    - AP sends Authenticator Nonce (ANonce)
    - Purpose: Provide random data to client
    - No encryption yet
2. **Message 2** (Client → AP):
    - Client generates Supplicant Nonce (SNonce)
    - Client computes Pairwise Transient Key (PTK) from PMK, ANounce, SNounce, and MAC addresses

    - Client sends SNounce and MIC (integrity check)
    - Purpose: Prove client has correct PMK without revealing it
3. **Message 3** (AP → Client):
    - AP computes PTK
    - AP sends GTK (Group Temporal Key) encrypted with KEK (Key Encryption Key, part of PTK)
    - Includes MIC for verification
    - Purpose: Deliver broadcast/multicast key securely
4. **Message 4** (Client → AP):
    - Client acknowledges receipt and installation of keys
    - Purpose: Confirm successful key installation

Key hierarchy:

- **PMK (Pairwise Master Key)**: Derived from initial authentication
- **PTK (Pairwise Transient Key)**: Derived during handshake, contains:
    - KCK (Key Confirmation Key): For message integrity
    - KEK (Key Encryption Key): For encrypting further key material
    - TK (Temporal Key): For actual data encryption
- **GTK (Group Temporal Key)**: For broadcast/multicast traffic

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

Ans. Wi-Fi power-saving techniques allow devices to conserve battery while staying online. Legacy mode enables clients to sleep since the AP buffers their traffic, indicated by TIM elements in beacons. When ready, clients wake up and receive frames through PS-Poll messages.

•WMM Power Save optimizes this further with trigger frames that initiate service periods when the AP transmits all buffered traffic at once. This is more appropriate for voice and video applications.

•PSMP takes this one step further in terms of efficiency by planning specific transmission windows, while TWT (introduced in Wi-Fi 6) enables devices to negotiate outright wake times, which is great for IoT devices that transmit very rarely.

•They balance connectivity against battery life with each successive Wi-Fi generation as mobile devices and sensor networks continue to advance.

•Furthermore, 802.11ah also introduced S1G power save for very long sleep cycles framed in hours or days with regard to long-range IoT applications and very long contention-free periods in addition to making room for simultaneous wake times between multiple devices in a group that has a time-bounded duty cycle.

•Recent power-saving implementation uses a hybrid approach, selecting the most appropriate one based on traffic flow, device capability, and network conditions. This adaptive policy optimizes battery life without sacrificing performance for time-sensitive applications.

.

8. Describe the Medium Access Control methodologies

Ans. The MAC layer controls media access in several different ways:

• **CSMA/CA (Carrier detect Multiple Access with Collision Avoidance): Devices** detect the channel prior to sending in order to avoid collisions.

• **RTS/CTS Mechanism:** Helps in avoiding hidden node collisions.

• **Backoff Algorithm:** Devices wait for a random time duration before attempting again upon sensing a busy medium.

• **Network Allocation Vector, or NAV:** Virtual carrier sensing for reservation of the channel.

9. Brief about the Block ACK mechanism and its advantages

Ans. The Block ACK method enables a sender to send multiple data frames and obtain one acknowledgment for all, instead of receiving one for each frame.

Advantages:

1. Decreases ACK overhead
2. Enhances throughput
3. Improves performance in fast wireless settings
4. Effective for tasks involving intermittent data, such as video streaming

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

Ans. These are frame aggregation techniques that improve efficiency by reducing overhead:

- **A-MSDU (Aggregate MAC Service Data Unit)**

1. Packs several MSDUs into one MPDU (literally, packets)
2. Uses a single MAC header and FCS for multiple pay loads
3. Most efficient in error-free conditions
4. Limited to 7935 bytes (802.11n) or 11,454 bytes (802.11ac/ax)
5. All subframes must have same receiver address

- **A-MPDU (Aggregate MAC Protocol Data Unit)**

1. Puts several full MPDUs into one transmission
2. Can be selectively received using Block ACK
3. 65,535 bytes (802.11n) or 1,048,575 bytes (802.11ac/ax).
4. More error-tolerant compared to A-MSDU

- **A-MSDU in A-MPDU**

1.Both techniques are used together for optimal efficiency

2.Multiple MSDUs are aggregated into A-MSDUs

3.Multiple A-MSDUs are aggregated into an A-MPDU

4.Accomplishes hierarchical aggregation for optimal performance

5.Optimal balance between efficiency and error-tolerance