Vivek Narayanan D
Coimbatore Institute of Technology

WI-FI MODULE 4 ASSIGNMENT

1. Significance of MAC Layer and Its Position in OSI Model

The Medium Access Control (MAC) layer plays a crucial role in managing how data is transmitted over the wireless medium in a network. The MAC layer is responsible for ensuring that multiple devices can share the same communication medium (radio spectrum) efficiently and without interference.

The MAC layer sits within the Data Link Layer (Layer 2) of the model. The MAC layer operates in the Data Link Layer (Layer 2), which is critical for managing direct communication between devices over the shared medium. The MAC layer provides essential services to devices within the same local network to ensure efficient and conflict-free data transfer. Within Wi-Fi networks, the MAC layer performs several critical tasks to ensure that devices can communicate without interference, collision, or data loss.

1. **Access Control**: Wi-Fi operates in a broadcast environment where multiple devices (stations) are often trying to communicate simultaneously. The MAC layer uses protocols like CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to prevent collisions. Before transmitting data, a device listens to the medium to check if it is idle. If the medium is busy, the device waits for a random period before attempting to transmit.

2. **Frame Management**: The MAC layer is responsible for encapsulating data into frames that can be transmitted over the air. These frames contain essential information like the source and destination addresses (MAC addresses), as well as control information (e.g., type of data being sent, sequence numbers for reordering packets).

3. **Collision Avoidance and Retransmission**: If a collision occurs (i.e., two devices transmit at the same time), the MAC layer detects this through acknowledgments (ACK) and uses techniques such as backoff to prevent further collisions. The retransmission of lost frames is managed through mechanisms like Automatic Repeat reQuest (ARQ), which ensures data integrity and reliability.

4. **Security**: It helps in the encryption and decryption of data frames using protocols like WPA2 (Wi-Fi Protected Access 2) and WPA3. The MAC layer works with the higher layers (like the network and transport layers) to authenticate devices, exchange keys,

and secure data during transmission through techniques like the 4-way handshake and AES (Advanced Encryption Standard).

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

The general frame structure consists of a MAC Header, Frame Body, and FCS (Frame Check Sequence). The MAC header itself varies based on the frame type (Management, Control, or Data), but a typical Data frame MAC header is 24–30 bytes long and includes the following key fields:

1. Frame Control (2 bytes):

- Contains information like the frame type (data, control, management), subtype, protocol version, and flags (e.g., To DS, From DS, More Fragments).
- Helps identify what kind of frame it is and how to handle it.

2. Duration/ID (2 bytes):

- Indicates the time (in microseconds) the channel will be occupied.
- Used in NAV (Network Allocation Vector) to avoid collisions.

3. Address Fields (6 bytes each):

- Address 1: Receiver MAC address.
- Address 2: Transmitter MAC address.
- Address 3: BSSID (AP's MAC or destination).
- Address 4 (optional): Used in WDS (Wireless Distribution System).

4. Sequence Control (2 bytes):

- Contains the sequence number and fragment number.
- Helps in frame reassembly and detecting duplicates.

5. QoS Control (2 bytes, optional):

- Present in QoS data frames.
- Manages priority and traffic categories.

6. HT/VHT/HE Control (optional, in advanced frames):

- Used in high throughput (802.11n/ac/ax) for extra control info.

b) Frame Body (0–2304 bytes):

- Actual data or management information carried in the frame.

c) Frame Check Sequence (FCS, 4 bytes):

- CRC used for error detection in the frame.

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

The MAC layer provides a variety of functions across three planes: Management, Control, and Data.

1) Management Plane:

- **Network Discovery**: Includes beaconing and scanning to identify available networks.
- **Authentication:** Verifies the identity of a device to ensure it's authorized to connect.
- **Association:** Handles the process of connecting to an access point or network.
- **De authentication and Disassociation:** Manages disconnections from the network.

2) Control Plane:

- **Channel Access:** Controls how devices access the wireless medium. This includes protocols such as CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).
- **Frame Fragmentation:** Breaks data into smaller pieces for transmission over the air.
- **Acknowledgments:** Ensures reliable transmission by requiring an acknowledgment (ACK) for each data frame sent.

3) Data Plane:

- **Data Transfer:** Handles the actual transmission of data packets between devices in the network.
- **Frame Buffering:** Manages frames that are waiting to be transmitted or need retransmission.
- **Flow Control:** Ensures efficient use of the communication medium by controlling the rate of data transfer.

4. Explain the scanning process and its types in detail

The scanning process allows wireless devices to discover and connect to available networks. The two main types of scanning are:

- **Passive Scanning**: In passive scanning, the device listens for beacon frames sent by access points (APs) at regular intervals. These beacons contain information such as the SSID (Service Set Identifier) and capabilities of the AP. This method is energy-efficient as it does not require the device to send out probe requests, but it can take longer to detect available networks.
- **Active Scanning**: In active scanning, the device sends out a probe request to all available channels. The access points that hear the probe respond with probe responses.

This allows the device to quickly discover available networks. However, active scanning consumes more power as the device has to transmit and receive probes.

The scanning process is essential for network discovery, allowing devices to select the most suitable access point to connect to the network.

5. Brief about the client association process

The client association process is a series of steps where a wireless device (client) establishes a connection to an access point (AP) in a Wi-Fi network. This process generally involves the following steps:

1. **Scanning**: The client scans for available networks using passive or active scanning.
2. **Authentication**: The client sends an authentication request to the AP to verify its identity.
3. **Association Request**: Once authenticated, the client sends an association request to the AP, indicating its intention to join the network.
4. **Association Response**: The AP responds with an association response, granting the client access to the network.
5. **IP Address Assignment**: The client is typically assigned an IP address via DHCP (Dynamic Host Configuration Protocol).
6. **Data Transfer**: The client is now associated with the network and can begin transferring data.

Each step ensures that the client and AP can securely and efficiently communicate.

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

The 4-Way Handshake is a critical part of the 802.11i (WPA/WPA2) authentication process. It establishes a secure session between a Supplicant (Client) and an Authenticator (Access Point) by deriving encryption keys. Below is a detailed breakdown of each step and the purpose of the keys involved.

Step-by-Step 4-Way Handshake Process

Step 1: AP → Client (Message 1 - ANonce)

- The AP sends a random number (ANonce) to the client.
- The client uses PMK + ANonce + SNonce (generated next) to compute the PTK.
- PTK = PRF(PMK, "Pairwise key expansion", ANonce + SNonce + AP MAC + Client MAC)

Step 2: Client → AP (Message 2 - SNonce + MIC)

- The client responds with its own random number (SNonce) and a MIC (Message Integrity Code).
- The AP now has both ANonce and SNonce, allowing it to compute the same PTK.
- The MIC ensures the message was not tampered with.

Step 3: AP → Client (Message 3 - Install PTK + GTK + MIC)

- The AP sends the GTK (Group Temporal Key) and confirms the PTK is installed.
- The GTK is used for broadcast/multicast traffic.
- The MIC ensures integrity.
- The client installs the PTK for unicast encryption.

Step 4: Client → AP (Message 4 - Acknowledgment)

- The client confirms that the PTK & GTK are installed.
- The AP marks the handshake as complete.
- Secure communication begins using AES-CCMP (WPA2) or TKIP (WPA).

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

Power saving is a critical feature in wireless networks, especially for battery-powered mobile devices like smartphones, laptops, and IoT sensors. The MAC (Medium Access Control) layer in IEEE 802.11 (Wi-Fi) plays a vital role in managing power consumption by allowing devices to enter low-power states when communication is not needed.

Standard MAC Layer Power Saving Mechanism:

The IEEE 802.11 standard defines a basic power-saving mechanism known as Power Save Mode (PSM):

1. **Sleep and Wake States**: The client device can switch between awake and sleep states. While sleeping, it turns off its radio to save power.
2. **AP Buffering**: When the STA is asleep, the Access Point (AP) buffers the incoming frames for that client.
3. **Beacon Frames**: The AP periodically sends beacon frames (usually every 100 ms) containing a Traffic Indication Map (TIM). This map tells which STAs have pending data at the AP.
4. **Polling**: If the STA sees its ID in the TIM of a beacon, it sends a PS-Poll frame to the AP to request the buffered data. After receiving the data, the STA can go back to sleep.

Types of Power Saving Mechanisms in MAC Layer

Beyond the standard PSM, several advanced mechanisms have been introduced in later 802.11 amendments to further improve efficiency:

1. Automatic Power Save Delivery (APSD – 802.11e)

- APSD is designed for Wi-Fi Multimedia (WMM) environments.
- It improves PSM by enabling scheduled or trigger-based delivery of data.

2. Power Save Multi-Poll (PSMP – 802.11n)

- Introduced in 802.11n for high-throughput devices.
- Allows AP to send a PSMP frame that schedules multiple STAs' sleep and wake times.
- STAs only wake up when they are scheduled to receive/transmit.

3. Target Wake Time (TWT – 802.11ax/802.11ah)

- Used in 802.11ax (Wi-Fi 6) and 802.11ah (Wi-Fi HaLow).
- TWT allows STAs and APs to agree on specific times when the STA will wake up to communicate.
- Between TWT sessions, the STA can remain asleep.

8. Describe the Medium Access Control methodologies

In Wi-Fi networks, multiple devices share a common wireless medium (air), making Medium Access Control (MAC) essential for organizing communication and avoiding collisions. The MAC layer in IEEE 802.11 is responsible for coordinating access to this shared medium using specialized techniques that balance fairness, efficiency, and performance.

1. CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

The primary MAC technique used in Wi-Fi is CSMA/CA, which prevents data collisions by sensing the channel before transmitting:

- **Carrier Sensing**: Before sending data, a device checks whether the channel is idle.
- **Random Backoff**: If the channel is busy, the device waits for a random backoff period before trying again.
- **Collision Avoidance**: Unlike wired Ethernet (which uses CSMA/CD), Wi-Fi cannot detect collisions directly due to the half-duplex nature of radios. Instead, it tries to avoid them using time-based mechanisms.

2. Interframe Spacing (IFS)

Wi-Fi defines different waiting times between frames to prioritize access:

- **SIFS (Short Interframe Space)**: Used for highest-priority frames like ACKs or CTS.
- **DIFS (DCF IFS)**: Used before normal data frames.

- **AIFS (Arbitration IFS)**: Used in QoS-aware networks (WMM) with different wait times for voice, video, best-effort, and background traffic.

3. DCF – Distributed Coordination Function

DCF is the basic MAC protocol in all Wi-Fi versions, operating in a decentralized way:

- Uses CSMA/CA with random backoff.
- Supports optional RTS/CTS (Request to Send / Clear to Send) to reduce hidden node collisions.
- Each station independently competes for channel access.

4. PCF – Point Coordination Function

PCF is a centralized protocol where the AP polls stations to grant them permission to transmit.

- Introduced to support real-time traffic, like voice.
- Uses a Contention-Free Period (CFP) during which only the AP coordinates access.

5. EDCA – Enhanced Distributed Channel Access (802.11e)

EDCA introduces QoS to the MAC layer by classifying traffic into four Access Categories (ACs):

- Voice, Video, Best Effort, and Background.
- Each category has its own contention parameters (AIFS, CWmin, CWmax).
- Higher-priority traffic gets faster access.

This methodology is crucial for applications like VoIP and video streaming.

9. Brief about the Block ACK mechanism and its advantages

The Block Acknowledgment (Block ACK) mechanism, introduced in IEEE 802.11e and enhanced in 802.11n/ac/ax, is designed to improve efficiency in high-throughput wireless networks. Unlike the traditional method of sending an individual ACK for every frame, Block ACK allows multiple data frames to be acknowledged together, reducing overhead.

How Block ACK Works:

1. **Block ACK Request (BAR):** The sender transmits a Block ACK Request after sending a series of data frames (MPDUs).
2. **Block ACK (BA):** The receiver replies with a Block ACK frame, which includes a bitmap indicating the successful receipt of each frame in the block.
3. **Selective Retransmission:** The sender only retransmits the frames marked as missing or erroneous in the bitmap, not the entire block.

Types of Block ACK:

- **Immediate Block ACK:** Receiver replies immediately after receiving the BAR.
- **Delayed Block ACK:** Receiver can delay the response to avoid channel contention or resource limitations.

Advantages of Block ACK:

1. **Reduced Overhead:** Acknowledging multiple frames with one Block ACK saves bandwidth compared to sending individual ACKs for each frame.
2. **Increased Throughput:** Aggregated frame acknowledgment minimizes inter-frame waiting times, allowing faster and more efficient data transmission.
3. **Better for High Data Rates:** Essential for high-throughput standards like **802.11n/ac/ax**, especially when using frame aggregation (A-MPDU).
4. **Selective Retransmission:** Only lost or corrupted frames are retransmitted, improving efficiency and reducing unnecessary traffic.
5. **Improved Network Performance:** Especially useful in environments with high contention or many clients, as it reduces acknowledgment traffic.

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

Wi-Fi standards introduced frame aggregation techniques to increase throughput by reducing overhead. These techniques combine multiple data units into a single transmission.

1. A-MSDU (Aggregated MAC Service Data Unit):

- Aggregates multiple MSDUs (data units from the upper layers) into a single MAC Protocol Data Unit (MPDU).
- All MSDUs share the same destination and QoS parameters.
- Reduces MAC header overhead since one header is shared for all MSDUs.
- **Limitation**: If any part is corrupted, the whole A-MSDU is retransmitted.

2. A-MPDU (Aggregated MAC Protocol Data Unit):

- Aggregates multiple MPDUs into a single PHY-layer transmission.
- Each MPDU has its own MAC header and FCS (Frame Check Sequence).
- If one MPDU is corrupted, only that part is retransmitted, not the entire A-MPDU.
- More robust than A-MSDU, especially in noisy environments.

3. A-MSDU in A-MPDU (Two-Level Aggregation):

- Combines both methods: Each MPDU in an A-MPDU may itself contain an A-MSDU.
- Maximizes throughput by minimizing both MAC and PHY overhead.
- Requires device support and negotiation.