Module 4 Assignment answers

Sri Gnana Saravan.N

VIT Chennai

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

Solution:

The MAC (Medium Access Control) layer is a sublayer of the Data Link Layer (Layer 2) in the OSI model. Its main function is to manage protocol access to the physical network medium. It is responsible for coordinating when and how data is transmitted over the wireless medium to avoid collisions and ensure successful communication.

Position in OSI Model:

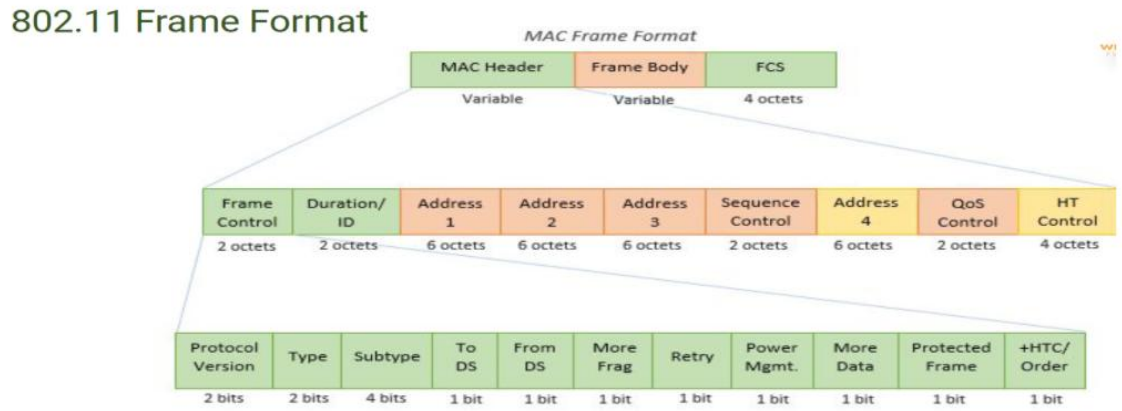
- Layer 2: Data Link Layer
  - Sublayers: Logical Link Control (LLC) and MAC

Significance:

- Provides addressing (MAC addresses)
- Controls frame delivery reliability
- Implements access control protocols like CSMA/CA
- Supports fragmentation, encryption, and retransmission

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

Solution:



Field Name	Description
Frame Control	Contains information like frame type, subtype, protocol version, etc.
Duration/ID	Specifies the duration for which the channel is reserved
Address 1	Usually the receiver's MAC address
Address 2	Usually the transmitter's MAC address
Address 3	Depends on the frame type; could be source/destination/AP address
Sequence Control	Helps in tracking fragmented frames
Address 4	Present in WDS (Wireless Distribution System) frames
Frame Body	Contains the actual data (MSDU)
FCS (Frame Check Sequence)	Error checking field using CRC

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

Solution:

Management Plane:
- Scanning (active & passive)
- Authentication
- Association/Reassociation
- Disassociation/Deauthentication
- Beaconing

Control Plane:
- RTS/CTS exchange
- ACK (Acknowledgment)
- PS-Poll
- CF-End, CF-Poll

Data Plane:
- Frame fragmentation and reassembly
- Encryption/Decryption (WEP/WPA/WPA2/WPA3)
- Sequence numbering
- MAC addressing
- QoS control

4. Explain the scanning process and its types in detail?

Solution:

Scanning is the process where a Wi-Fi client searches for nearby Access Points (APs).

Active Scanning:

In active scanning, **the client takes the initiative** to find APs.

Process:

1. The client sends a **Probe Request** frame on each channel.
2. The **Probe Request** contains:
    - Supported rates
    - SSID (can be specific or broadcast)
    - Security capabilities
3. Any APs listening on that channel respond with a **Probe Response**.
4. The client compares responses and chooses an AP to associate with

Passive Scanning:

In passive scanning, the client simply **listens** for **Beacon frames** that are **periodically** broadcast by APs (typically every 100ms).

Process:

1. Each AP broadcasts a **Beacon Frame** regularly.
2. The Beacon contains:
    - SSID
    - Supported data rates
    - Security settings
    - Channel and timing information
3. The client receives these beacons and gathers info about available networks.

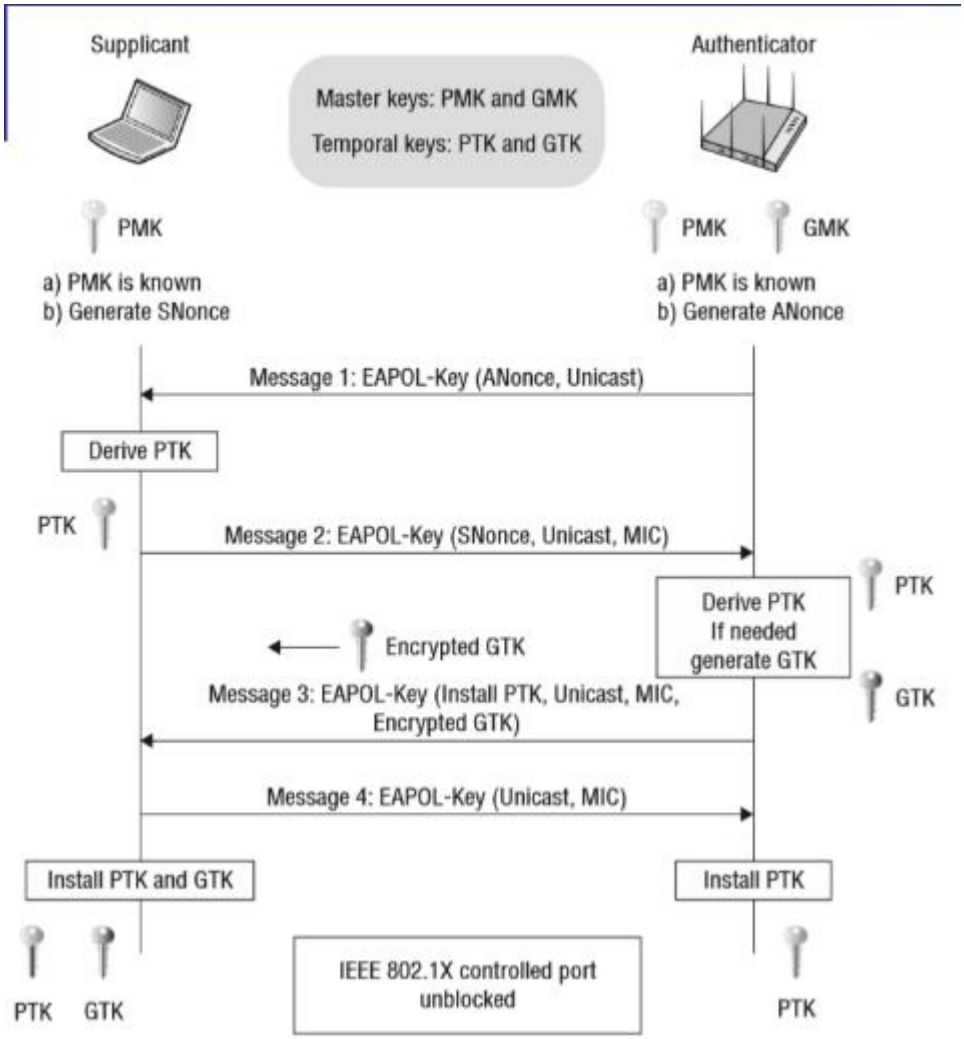
5. Brief about the client association process?

Solution:

- Scanning: Client discovers Aps
- Authentication: Basic open system or shared key
- Association Request: Client sends capability info
- Association Response: AP assigns Association ID (AID)
- EAP-based Authentication for WPA/WPA2 enterprise

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

Solution:



The **EAPOL 4-Way Handshake** is a process used in **WPA/WPA2/WPA3 (Personal and Enterprise)** Wi-Fi networks to securely establish encryption keys between a **Wi-Fi client (supplicant)** and an **Access Point (authenticator)** after initial authentication.

Purpose of the 4-Way Handshake:

To derive and securely install the following:

- **PTK (Pairwise Transient Key):** Used for encrypting unicast traffic.
- **GTK (Group Temporal Key):** Used for encrypting broadcast/multicast traffic.

These keys are derived from the **PMK (Pairwise Master Key)**.

PMK- Pre-shared or derived master key (from passphrase or 802.1X)

PTK- Derived from PMK + nonces + MAC addresses (used for unicast encryption)

GTK- Broadcast/multicast key generated by AP, distributed securely

Steps of the 4-Way Handshake:

Precondition:

Both client and AP know the **PMK** (via password or authentication server).

Message 1: AP → Client (ANonce)

- AP sends a **random number** called **ANonce** (Authenticator Nonce).
- This message also includes MAC addresses of the AP and client.
- Purpose: Starts the handshake and provides entropy to derive PTK.

Message 2: Client → AP (SNonce, MIC)

- Client generates its own **SNonce** (Supplicant Nonce).
- Computes the **PTK** using:
- Sends the **SNonce** + **Message Integrity Code (MIC)** (to ensure data is not tampered).

Message 3: AP → Client (Install PTK, Encrypted GTK)

- AP uses the known PMK, SNonce, and ANonce to compute the same PTK.

- Sends:
    - **GTK encrypted** using the PTK
    - MIC to verify authenticity
- Instructs client to install the PTK and GTK.

Message 4: Client → AP (Handshake Complete)

- Client confirms that it successfully installed PTK and decrypted GTK.
- Sends acknowledgment with MIC.
- Secure connection is now established!

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

Solution:

To conserve energy, devices switch off radios and use scheduled wake-up times.

Mechanism:

- Device sends QoS NULL frame with Power Management bit = 1
- AP buffers incoming data
- Device wakes up during DTIM beacon interval
- Parses TIM bitmap to check for pending data
- Sends PS-Poll to retrieve data

Types:

- Legacy Power Save Mode
- U-APSD
- TWT (802.11ax)

8. Describe the Medium Access Control methodologies?

Solution:

1. Distributed Coordination Function (DCF)

- **Based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**
- Before sending, the device **senses the channel**:
    - If the channel is idle → sends data after a short wait (**DIFS**)
    - If the channel is busy → backs off for a random time (**Backoff algorithm**)

- **ACK frame** is used to confirm successful delivery.

Pros: Simple, decentralized
Cons: Not efficient for time-sensitive data

2. Point Coordination Function (PCF)(*rarely used)*

- **Centralized access method** using the AP as the **coordinator**
- Works in a **Contention-Free Period (CFP)**: AP polls clients in turn
- Ensures timely delivery of data (e.g., for voice/video)

Pros: Collision-free communication
Cons: Not widely supported in real-world networks

3. Enhanced Distributed Channel Access (EDCA) — *QoS support in DCF*

- Part of 802.11e standard
- Uses **traffic categories** (voice, video, best effort, background)
- Higher-priority traffic waits less time to access the medium

Example:

- Voice packets get priority over email or file downloads.

9. Brief about the Block ACK mechanism and its advantages?

Solution:

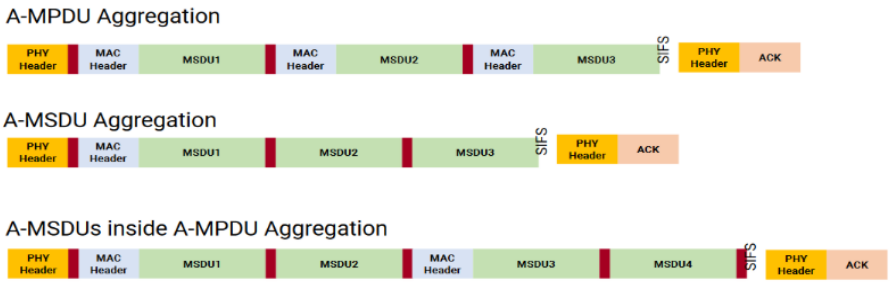
Used to improve efficiency by acknowledging multiple frames in one control message.

Advantages:

- Reduces overhead
- Increases throughput
- Minimizes retransmissions

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

Solution:



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

- Combines multiple **MSDUs** (MAC Service Data Units) into a **single MPDU** (MAC Protocol Data Unit).
- These MSDUs must all be destined for the same receiver.
- Aggregated at a **higher layer** in the MAC.
- Less overhead than sending each frame separately.
- More efficient in low-error environments.
- If one subframe fails CRC, **entire A-MSDU is retransmitted**.

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

- Combines multiple **MPDUs** into a **single transmission burst** at the physical layer.
- Each MPDU has its own MAC header and CRC.
- More robust — if one MPDU fails, only that one needs retransmission.
- More suited for error-prone environments.

Cons:

- Slightly higher overhead per MPDU (due to individual headers/CRC).

3. A-MSDU within A-MPDU

- Wi-Fi supports **nested aggregation**: an **A-MSDU** can be placed inside each MPDU of an A-MPDU.
- A-MSDU reduces header overhead within each MPDU.
- A-MPDU enables selective retransmission and higher reliability.