**Module 4**

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

The MAC (Medium Access Control) layer is a sublayer of the Data Link Layer (Layer 2) in the OSI model. It governs how devices on a network gain access to the medium and permission to transmit data.

**Significance:**

* Controls access to the physical transmission medium.
* Ensures reliable delivery using acknowledgment and retransmission.
* Maintains unique addressing (MAC address).
* Supports security features and QoS (Quality of Service).

**OSI Placement:**

* **Layer 2 (Data Link Layer)**
  + Sublayers:
    - Logical Link Control (LLC)
    - **Medium Access Control (MAC)**

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

The 802.11 MAC header consists of various fields used to manage wireless communication efficiently.

**Key Fields:**

* **Frame Control:** Identifies type/subtype (management, control, data), QoS, power mgmt.
* **Duration/ID:** Indicates duration the channel will be occupied.
* **Address 1, 2, 3 (and 4 if required):** Destination, source, BSSID, etc.
* **Sequence Control:** Handles fragmentation and reassembly.
* **QoS Control (optional):** Priority and traffic ID for QoS.
* **HT/VHT/HE Control (optional):** Info for high-throughput/very high-throughput enhancements.
* **FCS (Frame Check Sequence):** Used for error detection.

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

**Management Plane:**

* Beacon transmission
* Probe request/response
* Association & authentication
* Reassociation and disassociation

**Control Plane:**

* RTS/CTS (Request/Clear to Send)
* ACK (Acknowledgment)
* Power Save Poll
* Block ACK control

**Data Plane:**

* Frame transmission and retransmission
* Aggregation (A-MSDU, A-MPDU)
* Sequence control
* QoS support

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

**Scanning Process:** Used by wireless clients to find and connect to available wireless networks.

**Types:**

* **Passive Scanning:**
  + Listens for beacons from APs.
  + Low power consumption, no packet transmission.
* **Active Scanning:**
  + Sends probe requests and waits for probe responses.
  + Faster network discovery, more power-intensive.

**5. Brief about the client association process**

**Steps in Client Association:**

1. **Scanning:** Detect available APs (passive or active).
2. **Authentication:** Client requests to authenticate with AP.
3. **Association Request:** Sent by client with capability info.
4. **Association Response:** AP grants or denies association.
5. **Data Transfer Ready:** If successful, client is part of the WLAN.

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

**Purpose:** Establish encryption keys securely between client (STA) and AP after authentication.

**Steps:**

1. **Message 1:** AP sends ANonce to STA.
2. **Message 2:** STA generates PTK using ANonce, SNonce, PMK, and MACs; sends SNonce to AP.
3. **Message 3:** AP generates PTK and installs it; sends GTK to STA encrypted.
4. **Message 4:** STA installs PTK and confirms handshake completion.

**Keys:**

* **PMK (Pairwise Master Key):** Derived from EAP or PSK.
* **PTK (Pairwise Transient Key):** Used for unicast traffic.
* **GTK (Group Temporal Key):** Used for broadcast/multicast.

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

**MAC Layer Power Saving:**

* Clients can switch to sleep mode to conserve power.
* AP buffers frames and informs client via TIM in beacons.

**Mechanisms:**

* **Legacy Power Save Mode:** Client periodically wakes to receive beacon/TIM.
* **U-APSD (Unscheduled Automatic Power Save Delivery):** Improves VoIP performance by letting clients trigger delivery.
* **TWT (Target Wake Time - 802.11ax):** Negotiates specific wake times, reducing contention and saving power.

**8. Describe the Medium Access Control methodologies**

**Main MAC Methodologies in WLAN:**

* **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance):**
  + Sense the medium before transmission.
  + Use backoff timers to avoid collisions.
* **RTS/CTS Mechanism:**
  + Prevents hidden node problem.
* **DCF (Distributed Coordination Function):**
  + Basic access method using CSMA/CA.
* **PCF (Point Coordination Function):**
  + Optional, uses polling mechanism (rarely used now).

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

**Block Acknowledgement (Block ACK):**  
The Block ACK mechanism is a feature introduced in IEEE 802.11e and widely adopted in later 802.11 standards (including 802.11n/ac/ax) to enhance efficiency in wireless communication. It allows the receiver to acknowledge multiple data frames with a single acknowledgment (ACK), reducing control overhead and improving throughput in high-speed Wi-Fi networks.

**Working Principle:**

* Instead of sending an ACK for each data frame, the receiver sends **one Block ACK frame** that summarizes the status of multiple received frames.
* The transmitter sends a **burst of frames** (block of frames) and then waits for a **Block ACK** from the receiver.
* The **Block ACK frame** includes a bitmap that indicates **which frames were received successfully** and **which were lost**, enabling **selective retransmission**.
* This mechanism significantly improves performance in **high-throughput and high-latency environments**.

**Steps in the Block ACK Process:**

1. **Block ACK Agreement (Negotiation Phase):**
   * Sender and receiver exchange a **Block ACK Request** and **Block ACK Agreement** frame.
   * This establishes parameters like buffer size, timeout period, and window size.
2. **Data Transmission:**
   * The sender transmits a **burst of MAC frames** (e.g., A-MPDUs) to the receiver.
3. **Block ACK Response:**
   * The receiver replies with a **Block ACK frame**, which contains a **bitmap** indicating the status (received/missing) of each frame in the block.
4. **Selective Retransmission:**
   * The sender **retransmits only the missing frames**, identified using the bitmap from the Block ACK.

**Advantages of Block ACK:**

* **Reduced Overhead:**
  + One ACK for multiple frames minimizes control traffic.
  + Significantly reduces the number of ACK frames on the channel.
* **Improved Efficiency:**
  + Saves bandwidth and allows more time for data transmission.
  + Especially beneficial in scenarios with aggregated frames like A-MPDU.
* **Selective Retransmission:**
  + Only failed frames are retransmitted, optimizing resource usage and reducing delays.
* **Better Channel Utilization:**
  + Enhances performance in congested or high-error environments.

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

**1. A-MSDU (Aggregated MAC Service Data Unit):**  
A-MSDU aggregates multiple MAC Service Data Units (MSDUs) into a single MAC Protocol Data Unit (MPDU) to improve efficiency.

**Key Points:**

* Combines multiple higher-layer MSDUs into one MPDU.
* All MSDUs must be intended for the **same destination**.
* **Structure:**
  + Each MSDU has its own subframe header and payload.
  + The entire A-MSDU is wrapped in a single MAC header and Frame Check Sequence (FCS).
* Reduces MAC header overhead.
* Increases throughput by transmitting more data per frame.
* **Limitation:** If any subframe is corrupted, the **entire A-MSDU** must be retransmitted.

**2. A-MPDU (Aggregated MAC Protocol Data Unit):**  
A-MPDU aggregates multiple MPDUs into a single Physical (PHY) layer transmission, providing better reliability.

**Key Points:**

* Each MPDU in the A-MPDU has its own MAC header and FCS.
* **Structure:**
  + MPDUs are separated by delimiters in the PHY frame.
  + Each can be individually acknowledged or retransmitted.
* Allows selective retransmission of corrupted MPDUs.
* Better error handling than A-MSDU.
* More robust in high-throughput or lossy networks.

**3. A-MSDU inside A-MPDU (Two-Level Aggregation):**  
This method combines the advantages of both A-MSDU and A-MPDU.

**Key Points:**

* An A-MSDU is first created by aggregating MSDUs.
* Multiple such A-MSDUs are then packed into an A-MPDU (each as an MPDU).
* **Structure:**
  + Each MPDU contains an A-MSDU.
  + MPDUs are separated by delimiters and individually validated.
* Improves efficiency through reduced overhead and better error recovery.
* Supports high throughput and reliable data delivery.