**Wi-Fi Training Program**

**Assignment Solutions – 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 controls how devices access the shared physical medium, avoids collisions, and ensures reliable delivery of frames.  
It is positioned at the **Data Link Layer (Layer 2)** of the OSI model.

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

| **Field** | **Purpose** |
| --- | --- |
| Frame Control | Type of frame (management, control, data) and control flags |
| Duration/ID | Used for setting NAV (Network Allocation Vector) to reserve medium |
| Address 1 | Receiver address |
| Address 2 | Transmitter address |
| Address 3 | Final destination or BSSID |
| Sequence Control | Manages frame ordering and detects duplicates |
| Address 4 (optional) | Present in mesh or WDS networks |
| QoS Control (optional) | Used if QoS is enabled |
| HT Control (optional) | Used for High Throughput communications |
| Frame Body | Contains actual data or management information |
| FCS | Frame Check Sequence for error detection |

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

| **Plane** | **Functionalities** |
| --- | --- |
| Management | Beaconing, Scanning, Authentication, Association, Roaming |
| Control | RTS/CTS exchange, Acknowledgment (ACK), Power Save Poll, CF-End |
| Data | Frame Aggregation, Fragmentation, QoS handling, Error detection and recovery |

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

Scanning is the process where a client discovers available wireless networks.

* **Passive Scanning**:  
  The client listens for beacons that APs send periodically. It consumes less power but is slower.
* **Active Scanning**:  
  The client actively sends probe requests and waits for probe responses from APs. It is faster but uses more energy.

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

The client association process happens in three main steps:

* **Scanning**: The client scans and selects an AP to connect.
* **Authentication**: The client and AP exchange authentication frames to verify identity.
* **Association**: The client sends an association request and the AP responds with an acceptance.

Once associated, the client can send and receive data over the network.

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

The 4-way handshake ensures secure key exchange between the AP and the client.

* **Step 1**: AP sends a random number (ANonce) to the client.
* **Step 2**: Client generates another random number (SNonce), derives the PTK (Pairwise Transient Key) using both nonces and sends the SNonce to AP.
* **Step 3**: AP uses both nonces to derive the PTK, then sends the Group Temporal Key (GTK) securely to the client.
* **Step 4**: Client acknowledges receipt of keys, completing the handshake.

**Keys derived:**

* **PMK** (Pairwise Master Key): From pre-shared key or 802.1X.
* **PTK**: For encrypting unicast traffic.
* **GTK**: For encrypting multicast and broadcast traffic.

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

Power saving allows clients to conserve battery by reducing radio usage.

* **Legacy Power Save Mode**:  
  The client sleeps and periodically wakes up to receive buffered frames from the AP.
* **U-APSD (Unscheduled Automatic Power Save Delivery)**:  
  Optimized for low-latency traffic like VoIP; client triggers AP to send buffered packets.
* **TWT (Target Wake Time)**:  
  Clients negotiate with the AP to wake up at specific times, saving more power (mainly used in IoT).

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

MAC methodologies manage how devices access the medium:

* **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)**:  
  Devices sense the medium; if busy, they back off for a random time before retrying.
* **RTS/CTS (Request To Send / Clear To Send)**:  
  Used to avoid hidden node collisions by reserving the channel before actual data transmission.
* **NAV (Network Allocation Vector)**:  
  A timer that tells other devices how long the medium will be occupied.

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

Block ACK allows multiple frames to be acknowledged with a single acknowledgment frame, instead of one-by-one ACKs.

**Advantages:**

* Reduces protocol overhead.
* Increases network efficiency.
* Improves overall throughput, especially in high-speed WLANs.

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

1. **A-MSDU (Aggregated MAC Service Data Unit)**:  
   Multiple MSDUs are packed into one MPDU to reduce header overhead.
2. **A-MPDU (Aggregated MAC Protocol Data Unit)**:  
   Multiple MPDUs are sent together in one transmission for better reliability, with individual error checking.
3. **A-MSDU in A-MPDU**:  
   A-MSDUs are first aggregated into MPDUs, then these MPDUs are combined into an A-MPDU. This combines the benefits of both aggregation and error handling.