### Q2)802.11 MAC Frame Header Format and Field Explanations

The **802.11 MAC header** is a critical part of Wi-Fi communication, containing control information for addressing, sequencing, and frame management. Below is a detailed breakdown of its structure and fields.

**1. 802.11 MAC Frame Structure**

An 802.11 MAC frame consists of three main parts:

1. **MAC Header** (Variable length, typically **24–30 bytes**)
2. **Frame Body (Payload)** (0–2312 bytes)
3. **FCS (Frame Check Sequence)** (4-byte CRC for error detection)

**2. MAC Header Fields (Detailed)**

**A. Frame Control (2 Bytes)**

|  |  |  |
| --- | --- | --- |
| Subfield | Bits | Purpose |
| Protocol Version | 0–1 | Always 00 (current 802.11 standard). |
| Type | 2–3 | Frame type: **Management (00)**, **Control (01)**, **Data (10)**. |
| Subtype | 4–7 | Further classifies frame (e.g., **Beacon (1000)**, **ACK (1101)**). |
| To DS | 8 | 1 = Frame to **Distribution System** (e.g., AP → Router). |
| From DS | 9 | 1 = Frame from **Distribution System** (e.g., Router → AP). |
| More Fragments | 10 | 1 = More fragments follow. |
| Retry | 11 | 1 = Retransmitted frame. |
| Power Management | 12 | 1 = Device is entering sleep mode. |
| More Data | 13 | 1 = AP has buffered frames for a sleeping device. |
| Protected Frame | 14 | 1 = Frame is encrypted (WEP/WPA/WPA2). |
| Order | 15 | 1 = Strict ordering required (rarely used). |

**B. Duration/ID (2 Bytes)**

* **Purpose**:
  + In **Data/Control frames**: Specifies **time reserved for transmission** (μs) for NAV (Network Allocation Vector).
  + In **PS-Poll frames**: Contains the **Association ID (AID)** of a sleeping device.

**C. Address Fields (6 Bytes Each)**

802.11 uses **four address fields**, but only 3 are always present. Their meaning depends on **To DS/From DS** flags:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Address Field | To DS=0, From DS=0 (Ad-hoc) | To DS=1, From DS=0 (Client→AP) | To DS=0, From DS=1 (AP→Client) | To DS=1, From DS=1 (WDS) |
| Addr1 (RA) | Destination MAC | AP (BSSID) | Destination MAC | Receiver AP |
| Addr2 (TA) | Source MAC | Source MAC | AP (BSSID) | Transmitter AP |
| Addr3 | BSSID | BSSID | Source MAC | Destination MAC |
| Addr4 | N/A | N/A | N/A | Original Source MAC |

**Key Terms**:

* **RA (Receiver Address)**: Immediate recipient.
* **TA (Transmitter Address)**: Immediate sender.
* **BSSID**: MAC address of the AP.

**D. Sequence Control (2 Bytes)**

| **Subfield** | **Bits** | **Purpose** |
| --- | --- | --- |
| **Fragment Number** | 0–3 | Identifies fragments of the same frame. |
| **Sequence Number** | 4–15 | Unique ID for reassembling frames. |

**E. QoS Control (Optional, 2 Bytes)**

Present in **QoS Data frames** (802.11e/WMM):

* **TID (Traffic Identifier)**: Prioritizes traffic (0–7 for WMM: Voice, Video, Best Effort, Background).
* **ACK Policy**: Specifies if acknowledgment is required.

**3. Example: Data Frame (Client → AP)**

* **To DS=1, From DS=0**: Client sending to AP.
* **Addr1**: AP’s MAC (Receiver).
* **Addr2**: Client’s MAC (Transmitter).
* **Addr3**: BSSID (AP’s MAC again).

**4. Key Frame Types**

|  |  |  |
| --- | --- | --- |
| Type | Subtype Examples | Purpose |
| Management | Beacon, Probe Request/Response | Network discovery/maintenance. |
| Control | RTS, CTS, ACK | Medium access coordination. |
| Data | QoS Data, Null (no payload) | Actual user data transmission. |

* **MAC Header**: Manages addressing, fragmentation, and frame control.
* **Critical Fields**:
* **Frame Control**: Determines frame type and behavior.
* **Address Fields**: Flexible based on **To DS/From DS**.
* **Sequence Control**: Ensures ordered delivery.
* **Usage**: Essential for Wi-Fi communication (collision avoidance, encryption, QoS).

**Without the MAC header**, Wi-Fi devices couldn’t coordinate transmissions or route data correctly!