802.11 MAC Frame Format

An 802.11 frame consists of three main components:

1. **MAC Header**: Contains control and addressing information.
2. **Frame Body**: Carries the actual data (payload), which can be empty for control frames.
3. **Frame Check Sequence (FCS)**: Ensures data integrity.

The **MAC Header** is variable in length (typically 24–30 bytes, depending on the frame type and addressing mode).

Field	Size (Bytes)	Description and Purpose
Frame Control	2	Defines the frame type, subtype, and control flags for frame processing.
Duration/ID	2	Indicates the time the channel will be occupied or an association ID (for power save).
Address 1 (RA)	6	MAC address of the immediate receiver (Recipient Address).
Address 2 (TA)	6	MAC address of the transmitter (Transmitter Address).
Address 3	6	MAC address for routing (e.g., source/destination or BSSID, depending on frame type).
Sequence Control	2	Tracks frame sequence and fragmentation for reassembly.
Address 4 (optional)	6 (optional)	Used in wireless distribution system (WDS) for mesh or bridge networks.
QoS Control (optional)	2 (optional)	Manages Quality of Service for prioritized traffic (used in QoS data frames).

Following the MAC header, the **Frame Body** (0–2312 bytes) contains the payload, and the **FCS** (4 bytes) is a CRC for error detection.

802.11 MAC Header

1. Frame Control (2 bytes)

- **Structure**: Divided into several subfields:

    - **Protocol Version (2 bits)**: Indicates the 802.11 protocol version (usually 0 for current standards).
    - **Type (2 bits)**: Specifies the frame type (00: Management, 01: Control, 10: Data, 11: Reserved).
    - **Subtype (4 bits)**: Defines the specific function within the type (e.g., for Management: Beacon, Probe Request; for Control: RTS, CTS; for Data: QoS Data, Null Data).
    - **To DS (1 bit)**: Set to 1 if the frame is destined for the distribution system (DS), e.g., from a client to an access point (AP).
    - **From DS (1 bit)**: Set to 1 if the frame is coming from the DS, e.g., from an AP to a client.
    - **More Fragments (1 bit)**: Indicates if more fragments of the frame are to follow.
    - **Retry (1 bit)**: Set to 1 if the frame is a retransmission of a previously sent frame.
    - **Power Management (1 bit)**: Indicates the power-saving state of the sender (1 for power-save mode).
    - **More Data (1 bit)**: Signals that the sender has more data to send (used in power-save mode).
    - **Protected Frame (1 bit)**: Set to 1 if the frame body is encrypted (e.g., with WPA2).
    - **Order (1 bit)**: Set to 1 to indicate strict ordering of frames (rarely used).
- **Purpose**: Provides essential metadata about the frame's type, purpose, and processing requirements, allowing devices to interpret and handle the frame correctly.

2. Duration/ID (2 bytes)

- **Purpose**:
    - In **data and control frames**, it specifies the duration (in microseconds) that the wireless channel will be occupied, including the time for the frame, ACK, and interframe spaces. This is used to update the **Network Allocation Vector (NAV)**, which helps prevent other devices from transmitting and causing collisions (part of CSMA/CA).
    - In **power-save poll (PS-Poll) frames**, it contains the **Association ID (AID)** of the station, used to identify the client requesting buffered data from an AP.
- **Significance**: Ensures efficient medium access by reserving the channel and supports power-saving mechanisms.

3. Address 1 (RA - Recipient Address, 6 bytes)

- **Purpose**: Specifies the MAC address of the immediate recipient of the frame. This could be:
    - A client device (for frames sent from an AP).
    - An AP (for frames sent from a client).
    - A group address (for multicast or broadcast frames).
- **Significance**: Ensures the frame is processed only by the intended recipient, enabling targeted delivery in a shared medium.

4. Address 2 (TA - Transmitter Address, 6 bytes)

- **Purpose**: Specifies the MAC address of the device transmitting the frame (the sender's wireless interface).
- **Significance**: Identifies the source of the frame, allowing the recipient to send acknowledgments (ACKs) or responses back to the correct device.

5. Address 3 (6 bytes)

- **Purpose**: Provides additional addressing information, depending on the frame's context:
    - In **data frames**, it typically contains:
        - The **Source Address (SA)** (if the frame originates from a client).
        - The **Destination Address (DA)** (if the frame is headed to a client).
        - The **BSSID** (Basic Service Set Identifier, the AP's MAC address) in infrastructure networks.
    - In **management frames**, it often carries the BSSID to identify the network.
- **Significance**: Supports routing and filtering by providing context about the frame's ultimate source or destination, especially when frames traverse a distribution system.

6. Sequence Control (2 bytes)

- **Structure**:
    - **Sequence Number (12 bits)**: Assigns a unique number to each frame (0–4095) to track the order of frames.
    - **Fragment Number (4 bits)**: Identifies fragments of a larger frame (if fragmentation is used).
- **Purpose**: Ensures frames are reassembled correctly and detects missing or duplicate frames. This is crucial for reliable delivery in noisy wireless environments.
- **Significance**: Prevents data loss or corruption by maintaining frame order and supporting retransmission of lost fragments.

7. Address 4 (6 bytes, optional)

- **Purpose**: Used only in **Wireless Distribution System (WDS)** scenarios, such as mesh networks or wireless bridges, where frames are relayed between APs.
- **Details**: Contains the MAC address of the original source or final destination in a multi-hop wireless network.
- **Significance**: Enables complex network topologies by supporting frame forwarding across multiple wireless hops.

8. QoS Control (2 bytes, optional)

- **Purpose**: Present in **QoS Data frames** (used in IEEE 802.11e for enhanced performance).
- **Structure**:

    - **TID (Traffic Identifier, 4 bits)**: Specifies the priority level (0–7) for QoS traffic (e.g., voice, video).
    - **EOSP (End of Service Period, 1 bit)**: Indicates the end of a service period for power-saving devices.
    - **ACK Policy (2 bits)**: Defines acknowledgment behavior (e.g., normal ACK, no ACK, block ACK).
    - **TXOP (Transmission Opportunity, variable)**: Specifies the duration a station can transmit.
- **Significance**: Enhances network performance for time-sensitive applications by prioritizing traffic and managing channel access.