802.11 Wi-Fi Frame Injection Reference

802.11 Raw Frame Construction & Explanation

This document outlines the structure and purpose of various IEEE 802.11 Wi-Fi frames, including Management, Control, and Data frames. It is intended for use in Wi-Fi packet injection, testing, and analysis with hardware such as ESP8266/ESP32. Each section includes a brief explanation, the raw byte format, and configurable options for advanced control.

802.11 Wi-Fi Frame Injection Reference

1. Authentication Frame

Used by a client to initiate an authentication sequence with an AP. Typically follows with an Association Request.

```
uint8_t authPacket[26] = {
  0xB0, 0x00, // Frame Control: Authentication (Type: 0, Subtype: 11)
  0x00, 0x00, // Duration
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,  // Destination Address
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,  // Source Address
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,  // BSSID
  0x00, 0x00, // Sequence Control
  0x00, 0x00  // Authentication Algorithm: Open System (0x0000)
};
```

Notes: Authentication frames may include additional fields for sequence number or algorithm if using Shared Key instead of Open System.

802.11 Wi-Fi Frame Injection Reference

2. Deauthentication Frame

Sent by AP or client to terminate a session forcefully. Often used in Wi-Fi attacks to disconnect users.

```
uint8_t deauthPacket[26] = {
  0xC0, 0x00, // Frame Control: Deauthentication
  0x00, 0x00,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0x00, 0x00,
  0x07, 0x00  // Reason Code: 7 (Class 3 frame received from nonassociated STA)
};
```

Notes: Reason codes can vary depending on the situation (e.g., `1` = Unspecified, `4` = Inactivity timeout, `7` = Nonassociated STA).

802.11 Wi-Fi Frame Injection Reference

3. Association Request Frame

Sent after authentication, requesting the AP to allow the client to join the BSS (Basic Service Set).

```
uint8_t assocReqPacket[26] = {
  0x00, 0x00, // Frame Control: Association Request
  0x00, 0x00,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0x00, 0x00,
  0x00, 0x00  // Capability Information (Open System)
};
```

Notes: Optionally followed by SSID, supported rates, and other IEs (Information Elements).

4. Disassociation Frame

Used to notify an AP or STA that the sender is leaving the BSS or ending the session.

```
uint8_t disassocPacket[26] = {
  0xA0, 0x00, // Frame Control: Disassociation
  0x00, 0x00,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0x00, 0x00,
  0x08, 0x00  // Reason Code: Leaving BSS
};
```

Notes: Can be triggered by network change, user disconnect, or session timeout.

802.11 Wi-Fi Frame Injection Reference

5. Probe Request Frame

Broadcast by STAs to find nearby APs and networks.

```
uint8_t probeReqPacket[26] = {
  0x40, 0x00, // Frame Control: Probe Request
  0x00, 0x00,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0x00, 0x00
};
```

Notes: Can include optional SSID field to probe for specific networks.

6. Probe Response Frame

Sent by APs in response to Probe Requests, advertising their presence.

```
uint8_t probeRespPacket[38] = {
  0x50, 0x00, // Frame Control: Probe Response
  0x00, 0x00,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0x11, 0x22, 0x33, 0x44, 0x55, 0x66,
  0x11, 0x22, 0x33, 0x44, 0x55, 0x66,
  0x00, 0x00,
  0x64, 0x00, 0x01, 0x04, 0x00, 0x00,
  0x01, 0x04, 0x82, 0x84, 0x8B, 0x96
};
```

Notes: Includes timestamp, beacon interval, and IEs such as supported rates, SSID.

802.11 Wi-Fi Frame Injection Reference

7. Beacon Frame

Periodically transmitted by APs to announce network presence and parameters.

```
uint8_t beaconPacket[38] = {
  0x80, 0x00, // Frame Control: Beacon
  0x00, 0x00,
  0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
  0x11, 0x22, 0x33, 0x44, 0x55, 0x66,
  0x11, 0x22, 0x33, 0x44, 0x55, 0x66,
  0x00, 0x00,
  0x64, 0x00, 0x01, 0x04, 0x00, 0x00,
  0x01, 0x04, 0x82, 0x84, 0x8B, 0x96
};
```

Notes: Contains fixed parameters and several optional IEs like SSID, supported rates, and channel.

8. Acknowledgement (ACK) Frame

Sent to confirm receipt of data or management frames.

```
uint8_t ackPacket[16] = {
  0xD4, 0x00, // Frame Control: ACK
  0x00, 0x00,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0x00, 0x00, 0x00, 0x00, 0x00, 0x00,
  0x00, 0x00
};
```

Notes: Very short frame used to acknowledge unicast frames. No body content.

802.11 Wi-Fi Frame Injection Reference

9. Data Frame

Used to carry actual payloads between AP and STA.

```
uint8_t dataFrame[34] = {
  0x08, 0x00, // Frame Control: Data
  0x00, 0x00,
  0x11, 0x22, 0x33, 0x44, 0x55, 0x66,
  0xAA, 0xBB, 0xCC, 0xDD, 0xEE, 0xFF,
  0x11, 0x22, 0x33, 0x44, 0x55, 0x66,
  0x00, 0x00,
  0xDE, 0xAD, 0xBE, 0xEF
};
```

Notes: Can include encryption or QoS control fields depending on subtype.