Chapter 04: Frame Formats & Basic Operations

Dr. Mayank Agarwal

Department of CSE
IIT Patna

CS6206 Selected Topics in Wireless Networks

Lecture 4 Learning Objectives I

By the end of this lecture, you will be able to:

- Identify and explain the three main 802.11 frame types
- Decode MAC frame headers and understand each field's purpose
- Trace the complete station lifecycle: scanning, authentication, association
- Explain the beacon frame structure and its critical role
- Calculate frame sizes and transmission times
- Analyze address fields in different network configurations
- Understand power management mechanisms through frame analysis

802.11 Frame Types: The Three Categories I

- **Management Frames (Type = 00):** Establish and maintain connections
  - Beacon, Probe Request/Response, Authentication, Association, etc.
  - **Purpose:** Network discovery, connection setup, maintenance
- **Control Frames (Type = 01):** Assist in data frame delivery
  - RTS, CTS, ACK, PS-Poll, CF-End, etc.
  - **Purpose:** Medium reservation, acknowledgment, power save
- **Data Frames (Type = 10):** Carry upper-layer data
  - Simple Data, QoS Data, Null Data, etc.
  - **Purpose:** Transport user data and some management info

Frame Control Field: First 2 bytes of every frame determine type/subtype

Universal MAC Frame Format I

Frame Control	Duration/ID	Address 1	Address 2	Address 3	Sequence Control	Address 4
2 bytes	2 bytes	6 bytes	6 bytes	6 bytes	2 bytes	6 bytes

Plus: Optional Address 4, Frame Body (0-7955 bytes), FCS (4 bytes)

Variable Parts:

- **Address 4:** Only present in wireless distribution system (WDS)
- **QoS Control:** 2 bytes, present in QoS Data frames (802.11e)
- **HT Control:** 4 bytes, present in +HTC frames (802.11n)

Total Header Size: 24-36 bytes depending on frame type and options

Frame Control Field: The Master Key I

Protocol	Type	Subtype	To DS	From DS	More Frag	Retry	Pwr Mgmt
2 bits	2 bits	4 bits	1 bit	1 bit	1 bit	1 bit	1 bit

More Data	Protected	Order	(reserved)
1 bit	1 bit	1 bit	1 bit

Critical Fields:

- **Type/Subtype:** Identifies exact frame type
- **To/From DS**: Determines address field interpretation
- **Retry:** Indicates retransmission (important for duplicate detection)
- **Pwr Mgmt:** 1 = station going to sleep
- **More Data:** AP has more buffered frames for this station
- **Protected:** Frame body is encrypted

Duration/ID Field: Multi-Purpose Field I

- **When transmitting:** Sets NAV for other stations
  - Duration = time until end of ACK + SIFS
  - Maximum: 32767 μs (32.767 ms)
- **In PS-Poll frames:** Contains Association ID (AID)
  - AID (14 bits): 1-2007 identifies station to AP
  - Bits 14-15: 11 to indicate PS-Poll
- **In CF frames:** Contains CF parameters

Duration Calculation Example:

- DATA transmission: 500 μs
- SIFS: 16 μs
- ACK: 40 μs
- **Duration** = SIFS + ACK = 16 + 40 = 56 μs

Note: Duration protects only until end of ACK, not the DATA itself!

Address Field Interpretation (Recap and Extensions) I

To DS	From DS	Addr 1	Addr 2	Addr 3	Scenario
0	0	DA	SA	BSSID	Ad-hoc or Management
0	1	DA	BSSID	SA	AP to STA (WDS to STA)
1	0	BSSID	SA	DA	STA to AP (STA to WDS)
1	1	RA	TA	DA	Wireless bridge (WDS)

Where:

- **DA:** Ultimate destination MAC
- **SA:** Original source MAC
- **BSSID:** AP's MAC address (or IBSS generated)
- **RA:** Receiver address (next hop)
- **TA:** Transmitter address (previous hop)

Address 4: Present only when To DS=1 AND From DS=1 (WDS)

- Addr4 = SA (when To DS=1, From DS=1)

Sequence Control Field: Preventing Duplicates I

Fragment Number	Sequence Number
4 bits	12 bits

Purpose:

- **Sequence Number:** Increments by 1 for each new MSDU
  - Wraps at 4095 $\rightarrow$ 0
  - Same for all fragments of same MSDU
- **Fragment Number:** Increments for each fragment
  - 0 for unfragmented frames
  - Max 15 fragments per MSDU

Duplicate Detection:

- Receiver tracks (SA, Sequence, Fragment) tuples
- Discards duplicates (same tuple received again)
- Important because 802.11 doesn't guarantee exactly-once delivery

Management Frames: The Connection Lifecycle I

1. **Scanning:** Find available networks
   - Probe Request/Response
2. **Authentication:** Establish identity
   - Authentication (legacy Open/Shared Key)
   - 802.1X/EAP for WPA2-Enterprise
3. **Association:** Join the network
   - Association Request/Response
   - Reassociation for roaming
4. **Maintenance:** Stay connected
   - Beacon (periodic announcements)
   - Disassociation/Deauthentication (leave network)

The Beacon Frame: Network Advertisement I

Transmitted periodically by AP (typically every 100 ms)

Critical Information Elements (IEs):

- **Timestamp:** AP's clock (used for synchronization)
- **Beacon Interval:** Time between beacons (TU = 1024 μs)
- **Capability Info:** Network capabilities (privacy, QoS, etc.)
- **SSID:** Network name (0-32 bytes)
- **Supported Rates:** Data rates supported
- **DS Parameter Set:** Channel number
- **TIM (Traffic Indication Map):** Buffered frames for sleeping stations
- **Additional IEs:** Security, QoS, HT/VHT/HE capabilities

Example Beacon Interval: 100 TU $= 100 \times 1024\ \mu s = 102.4$ ms

Beacon Frame Structure Example I

- **MAC Header:** 24 bytes
- **Fixed Parameters:** 12 bytes
  - Timestamp (8 bytes)
  - Beacon Interval (2 bytes)
  - Capability Info (2 bytes)
- **Information Elements:** Variable
  - SSID IE (1+len bytes)
  - Supported Rates IE (1+len bytes)
  - DS Parameter Set IE (3 bytes)
  - TIM IE (4+ bytes)
  - Other IEs (variable)
- **FCS**: 4 bytes

Typical Size: 60-200 bytes depending on IE count

Transmission Time at 1 Mbps: 200 bytes $\times$ 8 bits/byte $\div$ 1 Mbps $=$ 1600 μs $=$ 1.6 ms

Numerical Example 1: Frame Control Example: 0x6D98 I

Given Frame Control Field:

$$0x6D98$$

Binary Representation:

$$0x6D98 = 0110\ 1101\ 1001\ 1000$$

Frame Control fields are interpreted in **little-endian order** (bit 0 is the LSB).

Frame Type and Direction I

Decoded Fields:

- Protocol Version (bits 0–1): 00 (0)
- Type (bits 2–3): 10 (2 = Data)
- Subtype (bits 4–7): 1001 (9 = QoS Data + CF-Ack)
- To DS (bit 8): 1
- From DS (bit 9): 0

This is a **QoS Data frame** transmitted **from a station to an access point**.

Control Flags I

Flag Interpretation:

- More Fragments: 1 (additional fragments follow)
- Retry: 1 (retransmission)
- Power Management: 0 (station awake)
- More Data: 1 (buffered frames exist)
- Protected: 1 (payload encrypted)
- Order: 0 (no strict ordering)

This frame represents an **encrypted QoS retransmission** with buffered data indicated.

Bit-Level Interpretation (0x6D98) I

Bit(s)	Field	Binary	Interpretation
0–1	Protocol Version	00	IEEE 802.11
2–3	Type	10	Data frame
4–7	Subtype	1001	QoS Data + CF-Ack
8	To DS	1	STA $\rightarrow$ AP
9	From DS	0	Not from DS
10	More Fragments	1	Fragmented MSDU
11	Retry	1	Retransmission
12	Power Mgmt	0	Station awake
13	More Data	1	Buffered frames exist
14	Protected	1	Encrypted payload
15	Order	0	No strict ordering

Final Interpretation I

Answer:
The Frame Control value **0x6D98** corresponds to a **QoS Data + CF-Ack frame** (Type 2, Subtype 9) transmitted **to the distribution system**. The frame is **encrypted**, **fragmented**, and marked as a **retransmission**. The **More Data** bit indicates buffered frames at the access point. Because To DS = 1 and From DS = 0, the address fields are:

$$\text{Addr1} = \text{RA}, \quad \text{Addr2} = \text{TA}, \quad \text{Addr3} = \text{DA}$$

This is a valid, complex IEEE 802.11 frame with all fields consistent.

Numerical Example 2: Beacon Overhead Calculation I

Problem: An AP transmits beacons every 100 TU (102.4 ms) at 1 Mbps mandatory rate. Beacon size is 150 bytes.

1. What percentage of airtime is consumed by beacons?
2. If 3 APs on same channel, what's combined beacon overhead?
3. What's the impact on VoIP capacity (VoIP packet every 20 ms)?

Solution Steps:

1. Beacon transmission time: $150 \times 8/1$ Mbps $= 1200\mu s = 1.2ms$
2. Beacon interval: $100 \times 1024\mu s = 102.4ms$
3. Percentage: $(1.2/102.4) \times 100\% \approx 1.17\%$
4. 3 APs: $3 \times 1.17\% \approx 3.51\%$ (if perfectly synchronized, worse)
5. VoIP: Packet every 20 ms = 50 packets/sec, each 1 ms airtime = 5% airtime

Numerical Example 2: Beacon Overhead Calculation II

Model Answer:

1. **1.17%** of airtime consumed by beacons from one AP
2. **3.51%** for 3 APs (could be higher with collisions)
3. Beacons consume **significant portion** of available airtime for low-rate traffic like VoIP. At 1.17% overhead, that's about 1/4 of the 5% needed for one VoIP call!

Probe Request/Response: Active Scanning I

- **Probe Request:** "Is anyone there with SSID X?"
  - Can be broadcast (SSID=0 length) or directed (specific SSID)
  - Contains supported rates, capabilities
  - Sent on each channel during scanning
- **Probe Response:** "Yes, I'm here with these capabilities"
  - Similar to Beacon but sent only in response to probe
  - Contains same IEs as Beacon

Scanning Types:

- **Active Scanning:** Send Probe Requests
- **Passive Scanning:** Listen for Beacons
- **Background Scanning:** Scan while connected (for roaming)

Timing: MinChannelTime (wait for response), MaxChannelTime (move on)

Authentication Frames: Legacy Mechanisms I

- **Open System Authentication:**
  1. Station → AP: Authentication (Algorithm=0, Seq=1)
  2. AP → Station: Authentication (Algorithm=0, Seq=2, Success)

  No actual authentication! Just formal handshake.
- **Shared Key Authentication:**
  1. Station → AP: Auth (Algorithm=1, Seq=1)
  2. AP → Station: Auth (Algorithm=1, Seq=2) with Challenge Text
  3. Station → AP: Auth (Algorithm=1, Seq=3) with Encrypted Challenge
  4. AP → Station: Auth (Algorithm=1, Seq=4, Success/Failure)

  Uses WEP encryption (broken, deprecated)

Modern Authentication: 802.1X/EAP happens **after** Open System auth

- Open System completes first
- Then 802.1X exchange occurs
- Finally, 4-way handshake for key derivation

Association Frames: Joining the BSS I

- **Association Request:** "Can I join your network?"
  - Contains capabilities, supported rates, SSID
  - May include Listen Interval (beacon intervals between wake-ups)
- **Association Response:** "Welcome, here's your AID"
  - Status code (0=success)
  - Association ID (AID, 1-2007)
  - Supported rates, etc.
- **Reassociation Request/Response:** For roaming between APs
  - Includes current AP address
  - Allows new AP to retrieve station context

AID (Association ID): 14-bit identifier

- Used in TIM to indicate buffered frames
- PS-Poll includes AID to identify station
- 0 and 2008-16383 reserved

Control Frames: The Supporting Cast I

- **ACK (Acknowledgment):** 14 bytes
  - RA = transmitter of DATA frame
  - Sent after SIFS
  - Duration = 0 (doesn't extend NAV)
- **RTS (Request To Send):** 20 bytes
  - RA = receiver (AP or STA)
  - TA = transmitter
  - Duration = time for CTS+DATA+ACK+3$\times$SIFS
- **CTS (Clear To Send):** 14 bytes
  - RA = transmitter of RTS
  - Duration = from RTS minus CTS and SIFS
- **PS-Poll (Power Save Poll):** 20 bytes
  - AID in Duration/ID field
  - Sent by station waking from sleep

Data Frames: Variations and Special Types I

- **Simple Data:** Carries MSDU (MAC Service Data Unit)
- **QoS Data:** Adds QoS Control field (802.11e)
- **Null Data:** No frame body, used for power management
  - Power Management bit indicates sleep mode
  - More Data bit indicates AP has buffered frames
- **Data+CF-Ack, Data+CF-Poll, etc.:** Combination frames
- **QoS Null:** QoS version of Null frame

Frame Body Contents:

- **LLC/SNAP Header:** 8 bytes (DSAP, SSAP, Control, OUI, Type)
- **Payload:** IP packet, ARP, etc.
- **Encryption:** WEP, TKIP, or CCMP overhead if Protected=1

Maximum Sizes:

- Without aggregation: 2304 bytes (MSDU)
- With A-MSDU: 7935 bytes (802.11n), 11454 bytes (802.11ac)

Power Management Frames and Mechanisms I

- **Power Management Bit:** In Frame Control field
  - 1 = station will sleep after this frame
  - AP starts buffering frames for sleeping station
- **Beacon TIM (Traffic Indication Map):**
  - Bitmap indicating which stations have buffered frames
  - AID corresponds to bit position
  - DTIM (Delivery TIM): Indicates broadcast/multicast frames
- **PS-Poll Frame:** Station requests buffered frames
- **More Data Bit:** In frames from AP, indicates more buffered frames
- **Null Data Frame:** Station can send to change power state

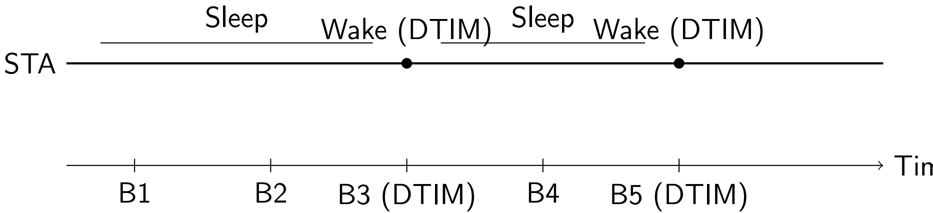
Example Sequence:

1. Station sets Power Management=1 in last data frame
2. AP buffers subsequent frames for station
3. Station wakes at Listen Interval, hears Beacon with TIM bit set

Power Management Frames and Mechanisms II

4. Station sends PS-Poll for each buffered frame
5. AP sends buffered frames with More Data bit as needed

Timing Diagram: Beacon, TIM, DTIM, Listen Interval I



Observation:

- STA sleeps for multiple Beacon Intervals
- STA wakes up at DTIM beacons to check buffered broadcast/multicast traffic

TIM vs DTIM in IEEE 802.11 I

Traffic Indication Map (TIM)

- Present in **every Beacon**
- Indicates buffered **unicast** data
- Bitmap indexed by Association ID (AID)
- STA wakes at its Listen Interval to check TIM

Delivery Traffic Indication Message (DTIM)

- Special Beacon that contains DTIM
- Indicates buffered **broadcast/multicast** data
- Occurs every **DTIM Interval** beacons
- All power-save STAs must wake up at DTIM

Disassociation & Deauthentication: Leaving Gracefully I

- **Disassociation:** "I'm leaving this BSS"
  - Reason codes: 3=STA is leaving, 8=STA has left
  - AP frees resources (AID, buffer space)
  - Station can reassociate later
- **Deauthentication:** "Our authentication is terminated"
  - More severe than disassociation to unauthenticated state
  - Must reauthenticate to reconnect
  - Reason codes: 2=Previous authentication no longer valid

Both are notifications, not requests:

- No response expected
- Not acknowledged
- Can be sent by either party

Security Issue: These frames are unencrypted and unauthenticated in basic 802.11, leading to "deauth attacks" to disconnect users.

Action Frames: For Extended Capabilities I

- **Category:** Management frame subtype 13
- **Various types for different purposes:**
  - Spectrum Management (802.11h)
  - QoS (802.11e)
  - Block Ack (802.11e)
  - Radio Measurement (802.11k)
  - Fast BSS Transition (802.11r)
  - Protected Management (802.11w)

Example: Measurement Request/Report (802.11k)

- AP can request client to measure channel conditions
- Client reports back noise, interference, neighbor APs
- Used for load balancing and roaming optimization

Protected Management Frames (802.11w):

- Encrypts certain management frames

Action Frames: For Extended Capabilities II

- Prevents deauth/disassociation attacks
- Requires WPA2/WPA3

Information Elements (IEs): The Extensible Part I

- **Structure:** ID (1 byte) + Length (1 byte) + Data (variable)
- **Common IEs:**
  - SSID (0), Supported Rates (1), DS Parameter Set (3)
  - TIM (5), ERP (42), HT Capabilities (45), VHT Capabilities (191)
  - Vendor Specific (221): Proprietary extensions

HT Capabilities IE Example (802.11n):

- 26 bytes of MIMO parameters
- Supported MCS sets, channel width, SM power save, etc.
- Allows devices to advertise advanced capabilities

Beacon/Probe Response contain many IEs:

- AP advertises all supported features
- Clients parse to determine compatibility
- Modern beacons can be 500+ bytes with all IEs

Fragmentation at MAC Layer I

- **Why:** Smaller frames have lower error probability
- **Fragmentation Threshold:** Maximum size before fragmenting
- **Process:**
  1. MSDU divided into fragments threshold
  2. Each fragment gets MAC header with same Sequence Number
  3. Fragment Number increments (0, 1, 2, ...)
  4. More Fragments bit = 1 except in last fragment
  5. Each fragment individually acknowledged
  6. Retransmit only failed fragments

Example: 1500-byte MSDU, threshold=500 bytes

- 3 fragments: 500+500+500 bytes (plus headers)
- Headers add 28-36 bytes each
- Total overhead: $3\times\ 30 = 90$ bytes vs. 30 for unfragmented
- But error in one fragment only loses 500 bytes, not 1500

Frame Exchange Sequences I

Basic Data Transfer:

1. DATA $\rightarrow$ SIFS $\rightarrow$ ACK

With RTS/CTS:

1. RTS $\rightarrow$ SIFS $\rightarrow$ CTS $\rightarrow$ SIFS $\rightarrow$ DATA $\rightarrow$ SIFS $\rightarrow$ ACK

Fragmented Data:

1. DATA(Frag0, MoreFrag=1) $\rightarrow$ SIFS $\rightarrow$ ACK $\rightarrow$ SIFS $\rightarrow$ DATA(Frag1, MoreFrag=1) $\rightarrow$ SIFS $\rightarrow$ ACK $\rightarrow$ SIFS $\rightarrow$ DATA(Frag2, MoreFrag=0) $\rightarrow$ SIFS $\rightarrow$ ACK

Power Save:

1. Beacon (TIM indicates buffered) $\rightarrow$ DIFS+Backoff $\rightarrow$ PS-Poll $\rightarrow$ SIFS $\rightarrow$ DATA $\rightarrow$ SIFS $\rightarrow$ ACK

Duration/NAV protects entire sequence

Retransmission and Error Recovery I

- **ACK Timeout:** If ACK not received within timeout
  - Default: few hundred μs to few ms
  - Station retransmits frame
  - Retry bit set to 1 in retransmissions
- **Retry Limits:**
  - Short Retry Limit (SRC): 7 for short frames
  - Long Retry Limit (LRC): 4 for long frames
  - After limit exceeded, frame discarded
- **Dynamic Rate Adaptation:** Based on retry statistics
- **Duplicate Detection:** Using Sequence Control field

Example: VoIP packet retransmission

- High priority, small size
- SRC=7, quick retries
- But each retry adds delay $\rightarrow$ may exceed playout buffer

Wireshark Analysis: Real Frame Examples I

Filter examples:

- `wlan.fc.type == 0` - Management frames
- `wlan.fc.type == 1` - Control frames
- `wlan.fc.type == 2` - Data frames
- `wlan.fc.subtype == 8` - Beacon frames

Key fields to examine:

- `wlan.fc` - Frame control flags
- `wlan.da`, `wlan.sa`, `wlan.bssid` - Addresses
- `wlan.duration` - NAV setting
- `wlan.seq` - Sequence and fragment numbers
- `wlan.tag` - Information elements

Exercise: Capture and analyze:

Wireshark Analysis: Real Frame Examples II

1. Complete association sequence
2. Data transfer with fragmentation
3. Power save operation

Frame Size Optimization Considerations I

- **Large Frames:**
  - Pros: Lower header overhead, better efficiency
  - Cons: Higher error probability, more airtime per transmission
- **Small Frames:**
  - Pros: Less lost on error, fairer sharing
  - Cons: High header overhead, more contention

Optimal Sizes:

- **Ethernet:** 1500 bytes (historical reasons)
- **Wi-Fi:** Depends on channel conditions
  - Good SNR: Large frames (1500+ bytes)
  - Poor SNR: Smaller frames (500-1000 bytes) or fragmentation

Modern Solution: Frame Aggregation (802.11n/ac/ax)

- Send multiple frames in one transmission
- Amortize overhead across many frames
- Achieve 70-80% efficiency

Security Implications in Frame Design I

- **Unprotected Fields:** Headers always unencrypted
  - Addresses, duration, sequence control visible
  - Traffic analysis possible
- **Management Frame Vulnerabilities:**
  - Deauth/disassociation attacks
  - Beacon spoofing (evil twin AP)
  - Probe request tracking (SSID broadcasting)
- **Countermeasures:**
  - 802.11w: Protected Management Frames
  - MAC address randomization (in probe requests)
  - WPA3: Simultaneous Authentication of Equals (SAE)

Privacy Consideration: Even with encryption, headers reveal:

- MAC addresses (tracking devices)
- Timing patterns (behavior analysis)
- Frame lengths (traffic fingerprinting)

Summary: Key Frame Concepts I

1. **Three frame types:** Management, Control, Data
2. **Frame Control field:** Determines type and important flags
3. **Address fields:** Interpretation depends on To/From DS bits
4. **Beacon frames:** Periodic advertisements with IEs
5. **Connection lifecycle:** Scan $\rightarrow$ Authenticate $\rightarrow$ Associate
6. **Power management:** TIM, PS-Poll, More Data bit
7. **Sequence control:** Prevents duplicate reception
8. **Fragmentation:** Reduces error impact at cost of overhead

Reading & Preparation for Next Lecture I

- **Required Reading:**
  - Textbook (Gast): Chapter 4 - "802.11 Framing in Detail"
  - Practice decoding frame control fields
- **Optional Reading:**
  - IEEE 802.11-2020: Clause 9 (MAC frame formats)
  - Wireshark 802.11 display filter reference
- **Next Lecture (Lecture 5): BSS, ESS & Network Topologies**
  - Infrastructure vs. ad-hoc modes
  - Distribution System concept
  - Roaming and mobility
  - Mesh networking (802.11s)

Review Questions I

1. Decode: Frame Control = 0x0108. What type of frame is this?
2. Why do beacons need to be transmitted at a low mandatory rate?
3. Explain the difference between Disassociation and Deauthentication.
4. How does a station know if the AP has buffered frames for it?
5. Calculate: 1000-byte data frame + 30-byte header at 54 Mbps. What's airtime?
6. Why is the Duration field in DATA frames set to cover only the ACK?
7. What problem does the Sequence Control field solve?
8. When should fragmentation be used vs. smaller MTU?

Discussion Question: "Given that MAC headers are always unencrypted, what privacy concerns does this raise for public Wi-Fi users? How could the protocol be redesigned to address these concerns while maintaining backward compatibility?"

Laboratory Exercise Preview I

Exercise: Frame Capture and Analysis

- **Objective:** Capture and analyze real 802.11 frames
- **Tools:** Wireshark, Wi-Fi adapter in monitor mode
- **Tasks:**
  1. Capture complete association sequence
  2. Decode frame control fields for various frame types
  3. Calculate NAV durations and verify timing
  4. Identify Information Elements in beacons
  5. Trace a complete data transfer with ACKs
- **Deliverable:** Annotated packet capture with analysis

Learning Outcome: Practical experience with 802.11 frame structures and sequencing.

Appendix: Common Frame Subtypes I

Type	Subtype	Name	Purpose
Management	0000	Association Request	Request to join BSS
	0001	Association Response	Response to join request
	0010	Reassociation Request	Request to roam to new AP
	0011	Reassociation Response	Response to roam request
	0100	Probe Request	Actively scan for networks
	0101	Probe Response	Response to probe
	1000	Beacon	Periodic network advertisement
	1001	ATIM	Ad-hoc traffic indication
	1010	Disassociation	Leave BSS
	1011	Authentication	Legacy authentication
	1100	Deauthentication	Terminate authentication
	1101	Action	Extended capabilities
Control	1011	RTS	Request to Send
	1100	CTS	Clear to Send
	1101	ACK	Acknowledgment
	1010	PS-Poll	Power Save Poll
Data	0000	Data	Simple data frame
	1000	QoS Data	Data with QoS
	0100	Null	No data (power management)

Appendix: Frame Size Calculations I

- **ACK Frame:** 14 bytes = 112 bits
- **RTS Frame:** 20 bytes = 160 bits
- **CTS Frame:** 14 bytes = 112 bits
- **PS-Poll Frame:** 20 bytes = 160 bits
- **Beacon Frame:** Typically 60-200 bytes = 480-1600 bits
- **Data Frame Header:** 24-36 bytes = 192-288 bits
- **LLC/SNAP Header:** 8 bytes = 64 bits (inside frame body)

Appendix: Frame Size Calculations II

Transmission Time Formula:

$$\text{Airtime} = \frac{\text{Frame Size (bits)}}{\text{PHY Rate (bps)}}$$

Example: 1500-byte data + 30-byte header at 54 Mbps:

$$\text{Size} = (1500 + 30) \times 8 = 12,240 \text{ bits}$$

$$\text{Time} = 12,240/54 \times 10^6 = 0.0002267 \text{ s} = 226.7\mu s$$

Important: Add PHY preamble/header (20 μs for OFDM)

Common Frame Analysis Mistakes I

1. **Ignoring PHY preamble:** Adds 16-20 μs per frame
2. **Misreading addresses:** Forgetting To/From DS determines meaning
3. **Overlooking Duration field:** It sets NAV for virtual carrier sense
4. **Misinterpreting Retry bit:** Not all retransmissions indicate problems
5. **Ignoring Sequence Control:** Can miss duplicate frames
6. **Not checking FCS:** Corrupted frames may still be captured
7. **Assuming all management frames are unencrypted:** 802.11w changes this
8. **Missing Information Elements:** Critical capabilities in IEs

Best Practice: Use Wireshark's 802.11 dissector which handles most interpretations correctly.

Thank you!