# Wi-Fi Technology Fundamentals


Module-3

**WLAN MAC Layer**

Session-3b

MAC Headers, Framing and Key Functions

# Last Session Recap……

Module-3

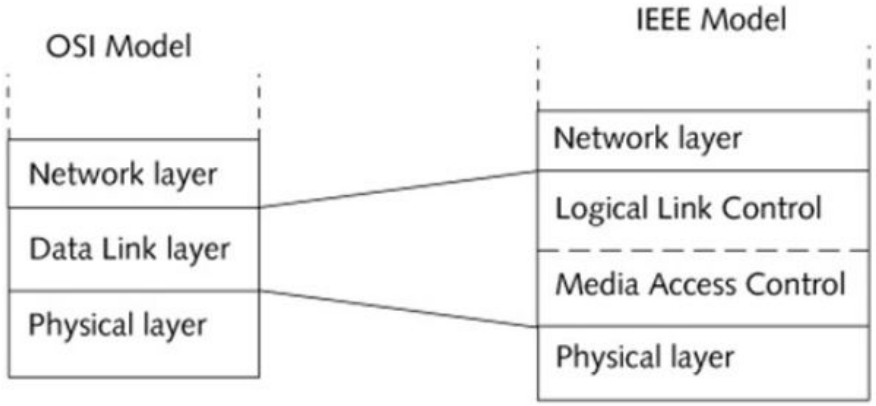
**WLAN MAC Layer**

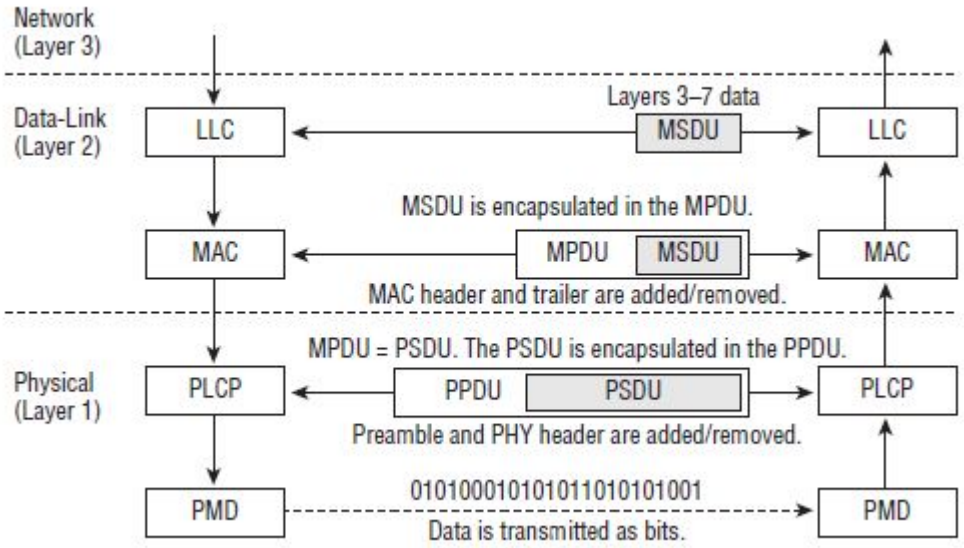
Session-3a

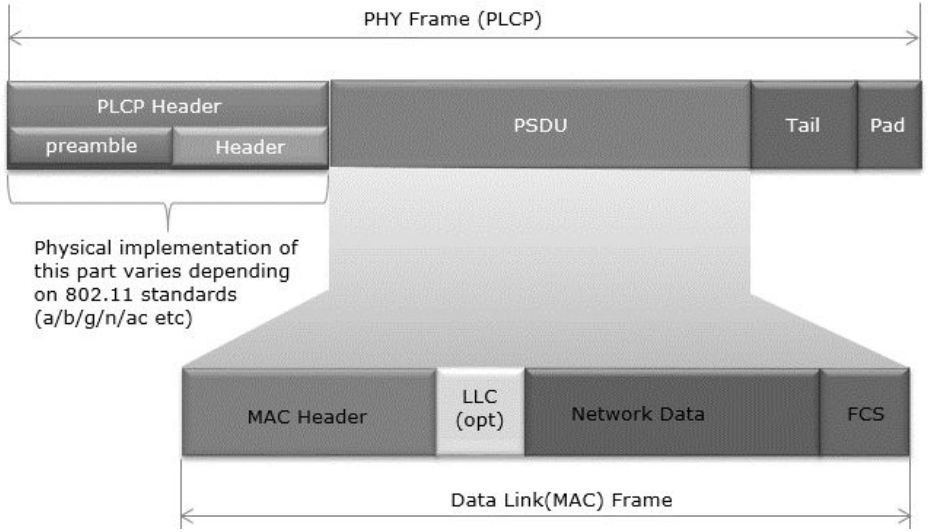
**Basic AP Management and Control Functions**

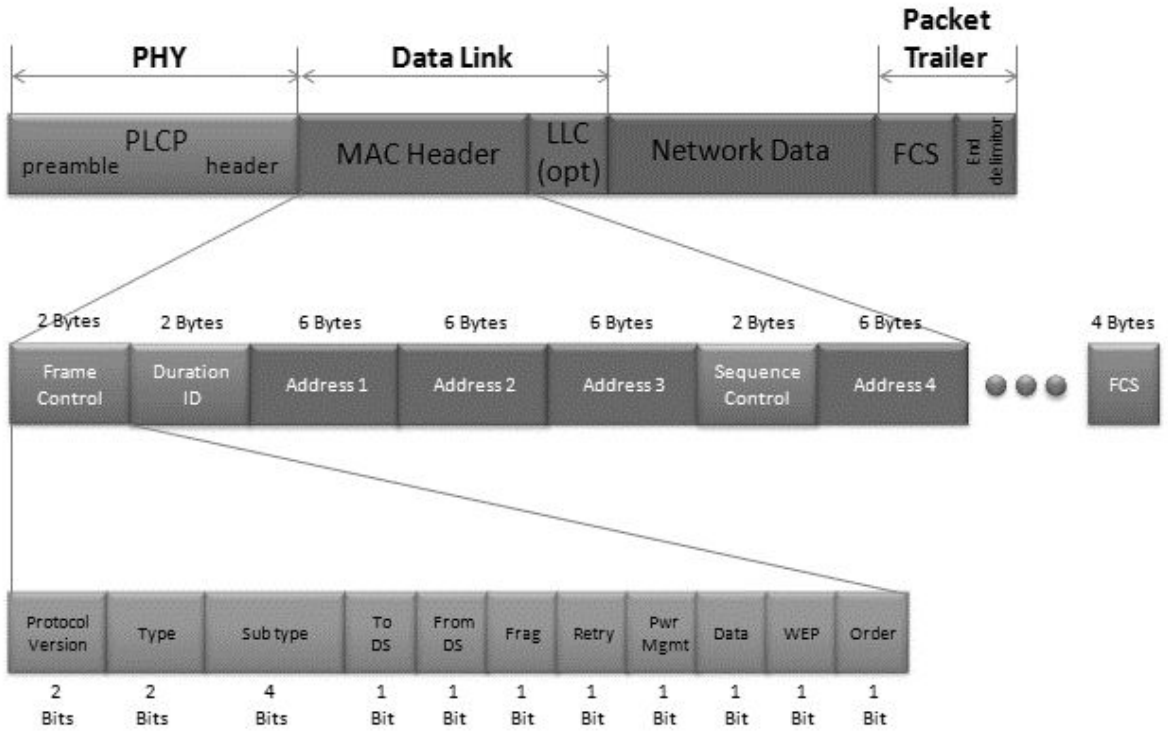
- ✔ Beaconing, Scanning
- ✔ Basic client connection
- ✔ Various Management and Control Functions

# PHY to MAC Header

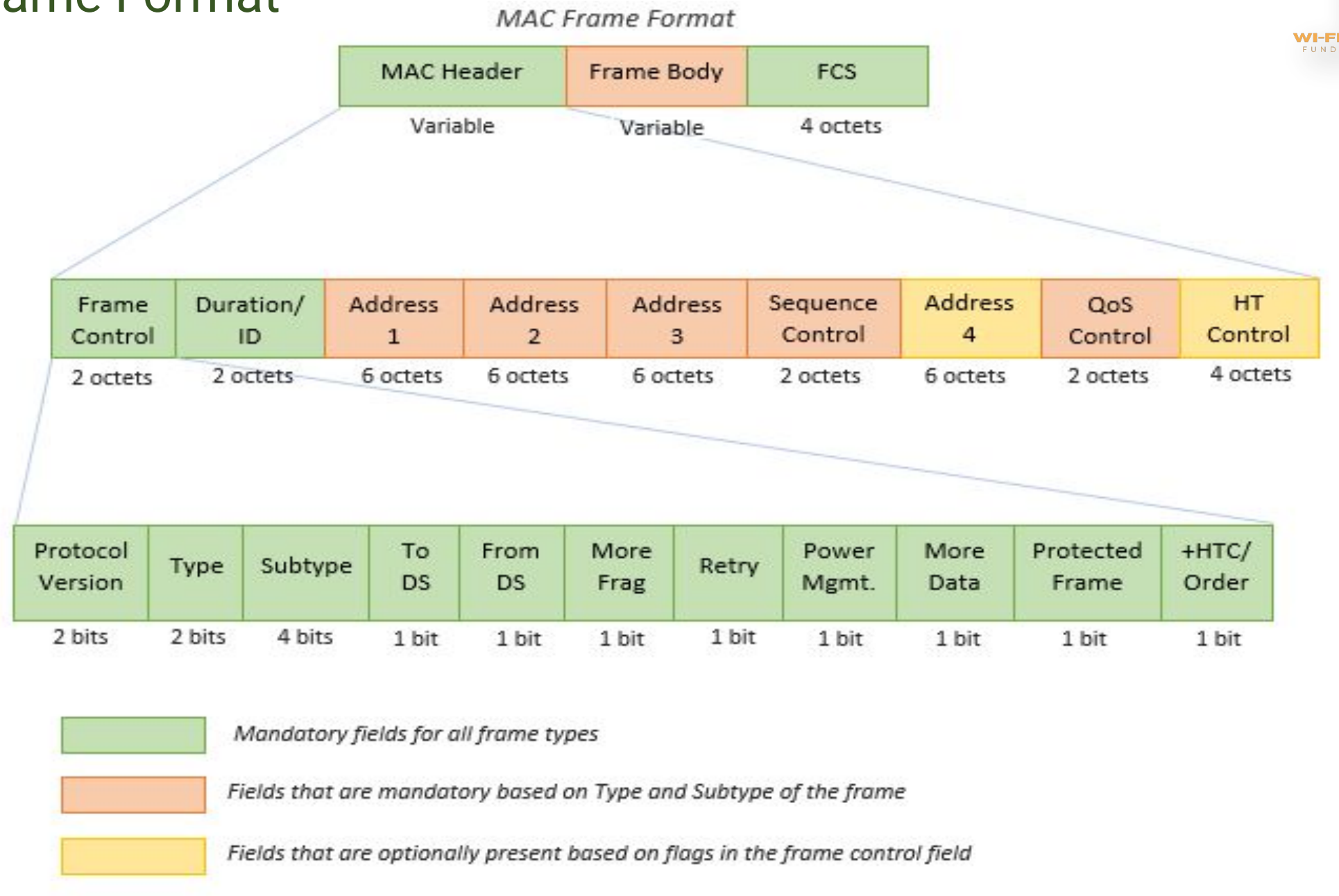


# 802.11 Frame Format

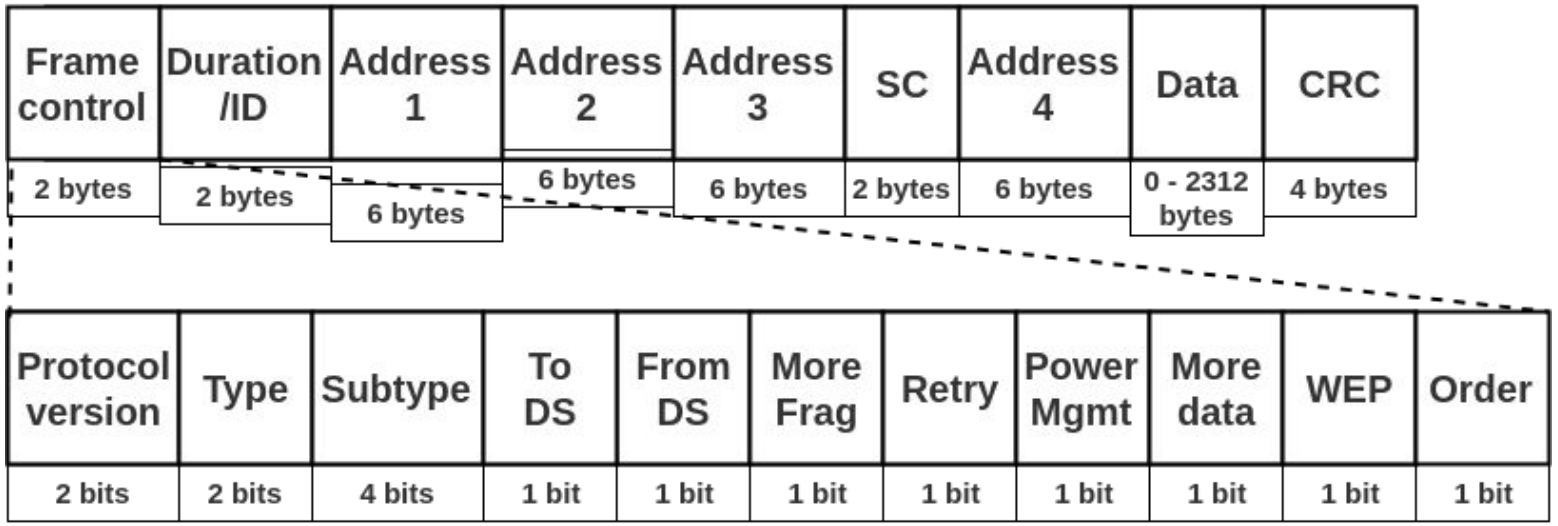


# 802.11 Frame Format

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

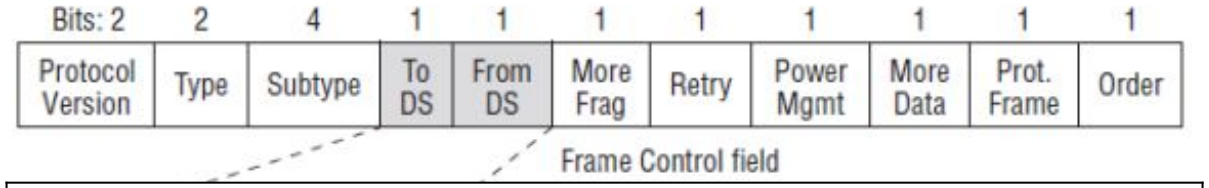
•**Frame Control(FC) –** It is 2 bytes long field which defines type of frame and some control information. Various fields present in FC are:

- **Version:** Current Protocol Version
- **Type:** Function of frame i.e management(00), control(01) or data(10).
- **Subtype:** It Indicates subtype such as Beacons, Probe Request etc..
- **To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
- **From DS:** It is a 1 bit long field which when set indicates frame coming from DS.
- **More frag (More fragments):** when set to 1 means frame is followed by other fragments.
- **Retry:** It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
- **Power Mgmt.:** Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
- **More data:** It is 1-bit long field that is used to indicate receiver that a sender has more data to send than the current frame.
- **WEP:** It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
- **Order:** It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.



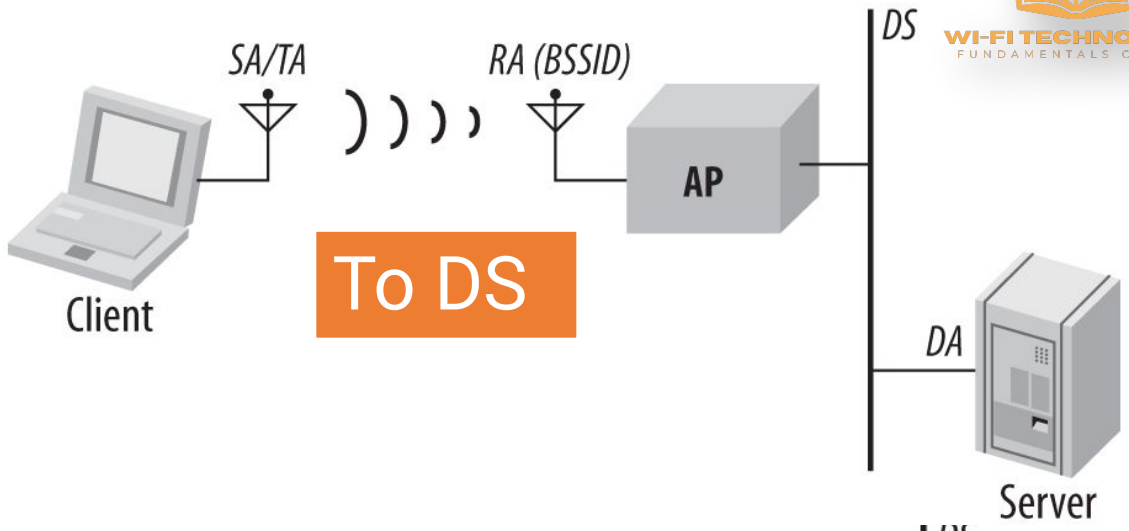

•**Duration/ID –** It is 4 bytes long field which contains the value indicating the period of time in which the medium is occupied(in μs).
•**Address 1 to 4 –** These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each).
•**SC (Sequence control) –** It is 16 bits long field which consists of 2 sub-fields, i.e., Sequence number (12 bits) and Fragment number (4 bits).
•**Data –** It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).
•**CRC (Cyclic redundancy check) –** It is 4 bytes long field which contains a 32 bit CRC error detection sequence to ensure error free frame.

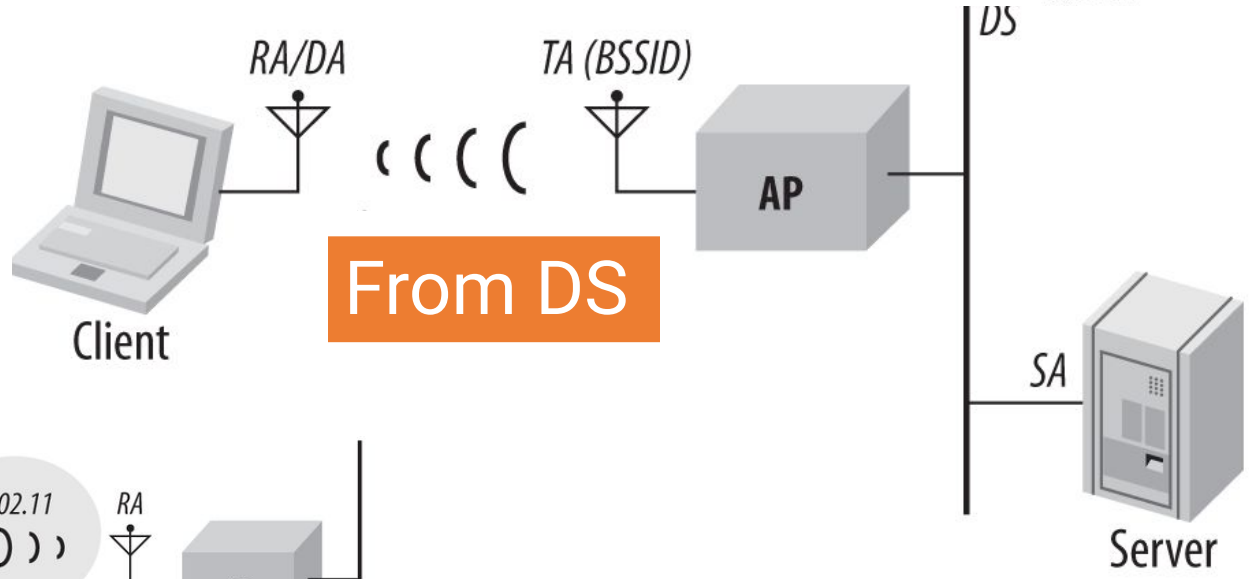
# The Address Fields

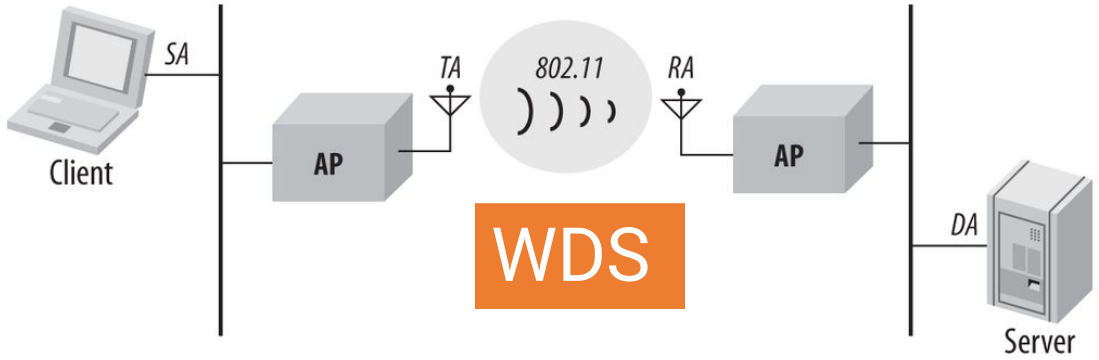



| Function | ToDS | FromDS | Address 1 (receiver) | Address 2 (transmitter) | Address 3 | Address 4 |
|---|---|---|---|---|---|---|
| IBSS | 0 | 0 | DA | SA | BSSID | Not used |
| To AP (infra.) | 1 | 0 | BSSID | SA | DA | Not used |
| From AP (infra.) | 0 | 1 | DA | BSSID | SA | Not used |
| WDS (bridge) | 1 | 1 | RA | TA | DA | SA |

- SA = MAC address of the original sender (wired or wireless)
- DA = MAC address of the final destination (wired or wireless)
- TA = MAC address of the transmitting 802.11 radio
- RA = MAC address of the receiving 802.11 radio
- BSSID = L2 identifier of the basic service set (BSS)



# Frame Type/Subtypes

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

## MANAGEMENT (00)

- Beacon
- Probe Request / Response
- Authentication
- Deauthentication
- Association Request / Response
- Reassociation Request / Response
- Disassociation
- ATIM

## ACTION

- Block ACK Request / Response
- Delete Block ACK
- ADDTS Request / Response
- Delete TS
- DLS Request / Response /Teardown
- TPC Request / Report
- Channel Switch Announcement.

## CONTROL (01)

- Block ACK Request
- Block ACK
- PS-Poll
- RTS
- CTS
- ACK

## DATA (10)

- Data
- Data + CF-ACK
- Data + CF-Poll
- Data + CF-ACK + CF-Poll
- Null (no data)
- CF-ACK (no data)
- CF-Poll (no data)
- CF-ACK + CF-Poll (no data)
- QoS Data
- QoS Data + CF-ACK
- QoS Data + CF-Poll
- QoS Data + CF-ACK + CF-Poll
- QoS Null (no data)
- Reserved
- QoS CF-Poll (no data)
- QoS CF-ACK + CF-Poll (no data)

# Frame Type/Subtypes

| Type | Type Description | Sub Type | Sub Type Description |
|---|---|---|---|
| 00 | Management | 0000 | Association Request |
| 00 | Management | 0001 | Association Response |
| 00 | Management | 0010 | Reassociation Request |
| 00 | Management | 0011 | Reassociation Response |
| 00 | Management | 0100 | Probe Request |
| 00 | Management | 0101 | Probe Response |
| 00 | Management | 0110 | Timing Advertisement |
| 00 | Management | 0111 | Reserved |
| 00 | Management | 1000 | Beacon |
| 00 | Management | 1001 | ATIM |
| 00 | Management | 1010 | Dissociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101 | Action |
| 00 | Management | 1110 | Action No Ack (NACK) |
| 00 | Management | 1111 | Reserved |
| 01 | Control | 0000-0010 | Reserved |
| 01 | Control | 0011 | TACK |
| 01 | Control | 0100 | BeamForming Report Poll |
| 01 | Control | 0101 | VHT/HE NDP Announcement |
| 01 | Control | 0110 | Control Frame Extension |
| 01 | Control | 0111 | Control Wrapper |
| 01 | Control | 1000 | Block Ack Request (BAR) |
| 01 | Control | 1001 | Block Ack (BA) |
| 01 | Control | 1010 | PS-Poll |
| 01 | Control | 1011 | RTS |
| 01 | Control | 1100 | CTS |
| 01 | Control | 1101 | ACK |
| 01 | Control | 1110 | CF End |
| 01 | Control | 1111 | CF End + CF ACK |

| Type | Type Description | Sub Type | Sub Type Description |
|---|---|---|---|
| 10 | Data | 0000 | Data |
| 10 | Data | 0001 | Reserved |
| 10 | Data | 0010 | Reserved |
| 10 | Data | 0011 | Reserved |
| 10 | Data | 0100 | Null (no data) |
| 10 | Data | 0101 | Reserved |
| 10 | Data | 0110 | Reserved |
| 10 | Data | 0111 | Reserved |
| 10 | Data | 1000 | QoS Data |
| 10 | Data | 1001 | Data + CF ACK |
| 10 | Data | 1010 | Data + CF Poll |
| 10 | Data | 1011 | QoS Data + CF ACK + CF Poll |
| 10 | Data | 1100 | QoS Null(No Data) |
| 10 | Data | 1101 | Reserved |
| 10 | Data | 1110 | QoS CF-Poll (no Data) |
| 10 | Data | 1111 | QoS CF ACK + CF Poll(no Data) |
| 11 | Extension | 0000 | DMG Beacon |
| 11 | Extension | 0001 | S1G Beacon |
| 11 | Extension | 0010-1111 | Reserved |

# Management and Control Frames



| 2 | 2 | 6 | 6 | 6 | 2 | 0 to 2312 octets | 4 |
|---|---|---|---|---|---|---|---|
| FC | D | DA | SA | BSSID | SC | Frame Body | FCS |

**Beacon**

| | |
|---|---|
| Timestamp | 8 |
| Beacon Interval | 2 |
| Capability Information | 2 |
| SSID | 2 to 34 |
| Supported Rates | 2 to 10 |
| FH Parameter Set | 7 |
| DS Parameter Set | 3 |
| CF Parameter Set | 8 |
| IBSS Parameter Set | 4 |
| Traffic Indication Map | 7 to 256 |

**Probe Request**

| | |
|---|---|
| SSID | 2 to 34 |
| Supported Rates | 2 to 10 |

**Probe Response**

| | |
|---|---|
| Timestamp | 8 |
| Beacon Interval | 2 |
| Capability Information | 2 |
| SSID | 2 to 34 |
| Supported Rates | 2 to 10 |
| FH Parameter Set | 7 |
| DS Parameter Set | 3 |
| CF Parameter Set | 8 |
| IBSS Parameter Set | 4 |

Management Frames

**Association Request**

| | |
|---|---|
| Capability Information | 2 |
| Listen Interval | 2 |
| SSID | 2 to 34 |
| Supported Rates | 2 to 10 |

**Association Response**

| | |
|---|---|
| Capability Information | 2 |
| Status Code | 2 |
| Association ID | 2 |
| Supported Rates | 2 to 10 |

**Disassociation**

| | |
|---|---|
| Status Code | 2 |

**Reassociation Request**

| | |
|---|---|
| Capability Information | 2 |
| Listen Interval | 2 |
| Current AP Address | 6 |
| SSID | 2 to 34 |
| Supported Rates | 2 to 10 |

**Reassociation Response**

| | |
|---|---|
| Capability Information | 2 |
| Status Code | 2 |
| Association ID | 2 |
| Supported Rates | 2 to 10 |

**[IBSS] Announcement Traffic Indication Map**

| | |
|---|---|
| <empty> | 0 |

**Authentication**

| | |
|---|---|
| Auth. Alg. No. | 2 |
| Auth. Trans. Seq. No. | 2 |
| Status Code | 2 |
| Challenge Text | 3 to 255 |

**Deauthentication**

| | |
|---|---|
| Reason Code | 2 |

**RTS**

| 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|
| FC | D | RA | TA | FCS |

**CTS or ACK**

| 2 | 2 | 6 | 4 |
|---|---|---|---|
| FC | D | RA | FCS |

**PS-Poll**

| 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|
| FC | AID | BSSID | TA | FCS |

**CF-End**

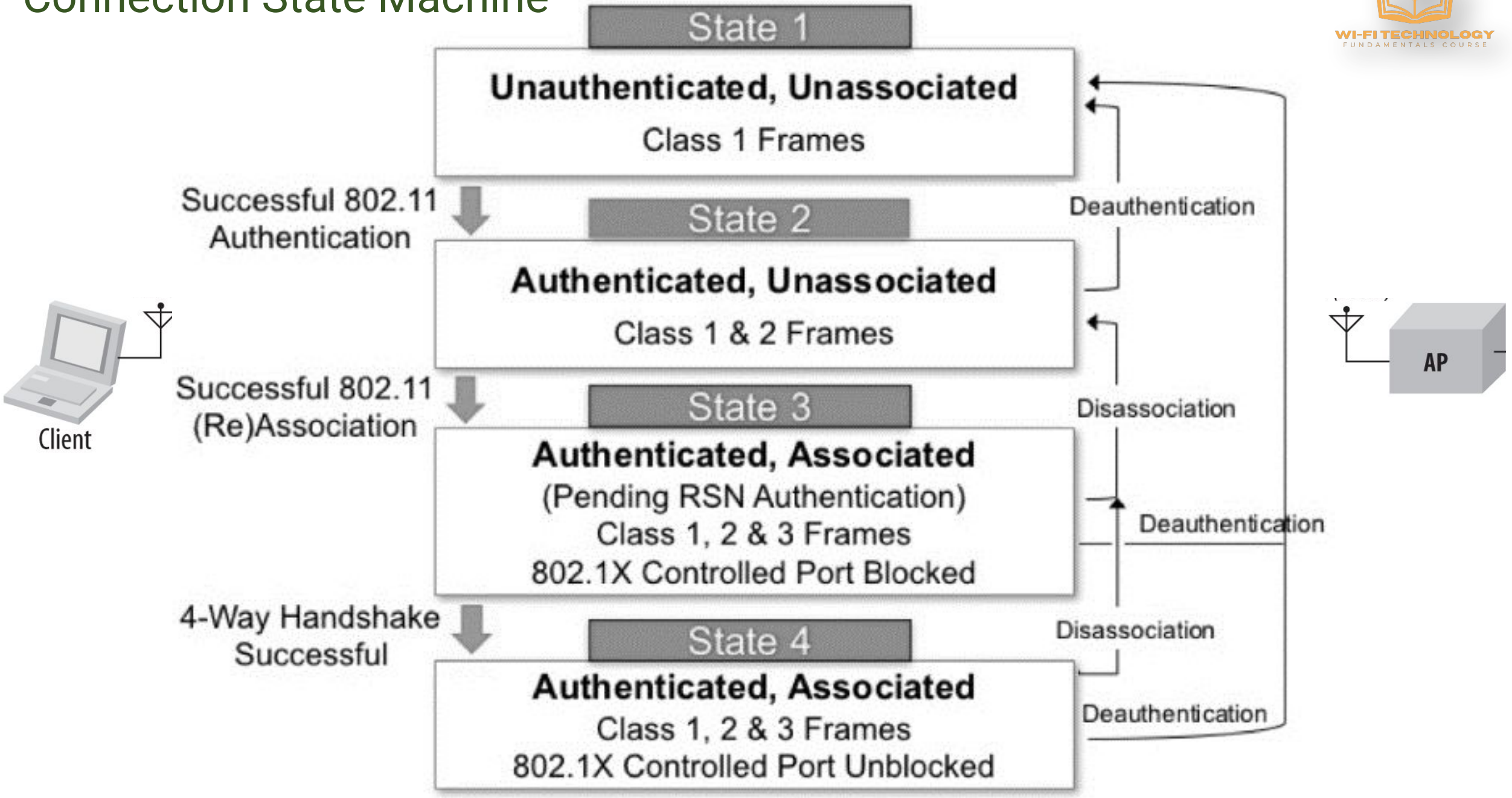
| 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|
| FC | D | RA | BSSID | FCS |

**CF-End + CF-ACK**

| 2 | 2 | 6 | 6 | 4 |
|---|---|---|---|---|
| FC | D | RA | BSSID | FCS |

Control Frames

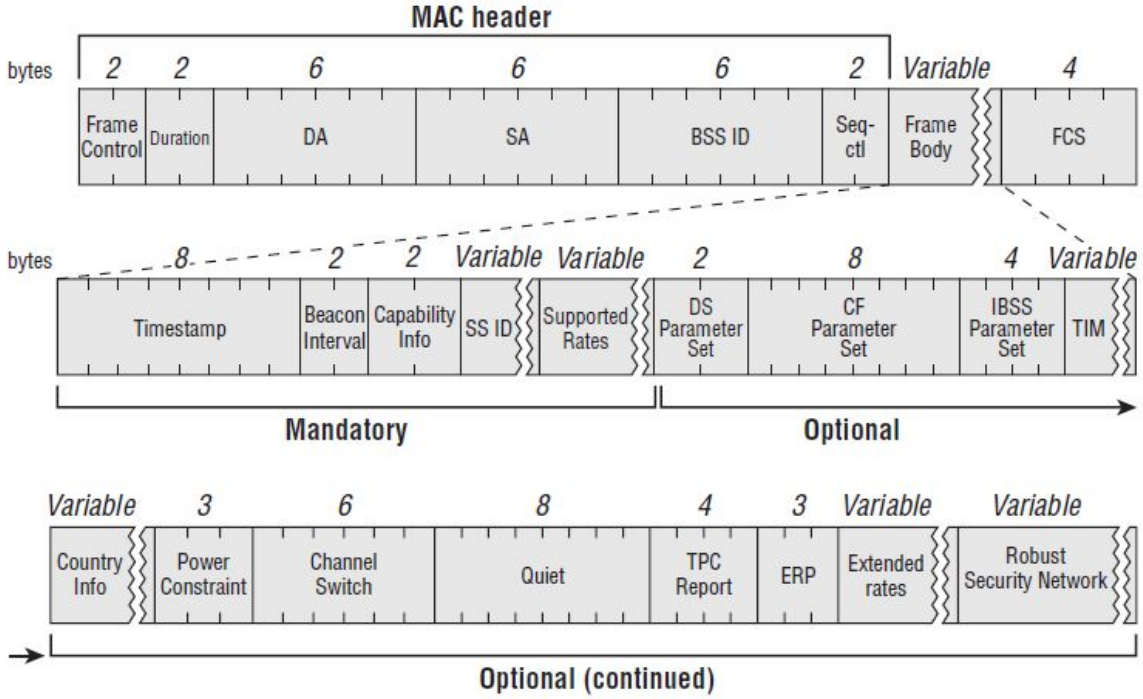
# Connection State Machine



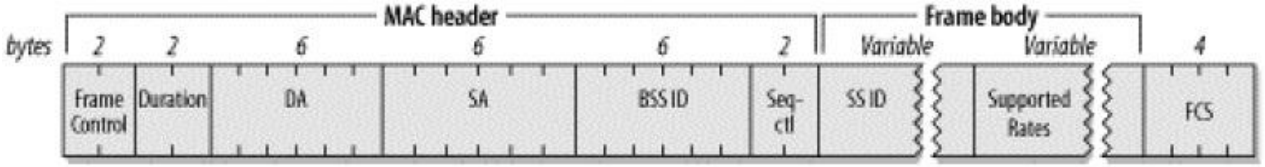
# Beacon Frame

**Beacon frame** is one of the management frames in IEEE 802.11 based WLANs. It contains all the information about the network. Beacon frames are transmitted periodically, they serve to announce the presence of a wireless LAN and to synchronize the members of the service set

- Fixed Parameters
  - Beacon interval -This represents the amount of time between beacon transmissions
  - Timestamp – The clock information of the AP that the stations can use to synchronize with the APs clock
  - Capabilities Information – Provides information about the various basic capabilities of the AP
- Tagged Parameters
  - Service Set Identifier (SSID) – is the name of the network
  - Supported Rates – Info about the various MCS rates supported by the AP.
  - DS Parameter Set – Provides information about channel used by AP
  - Country Code – which country regulations the AP is following
  - Traffic Indication Map – Indicates which stations have traffic buffered
  - BSS Load Element – Provide info about the APs medium utilization
  - TPC – Shows information about the transmit power of the AP
  - RSN IE – provides information about supported security mechanisms
  - EDCA parameter set – provide information about the various medium access parameters that are used to implement on the air QoS
  - HT information/capabilities – Indicated details about 802.11n capabilities of the AP
  - VHT information/capabilities – Indicated details about 802.11ac capabilities of the AP
  - HE information/capabilities – Indicated details about 802.11ax capabilities of the AP
  - EHT information/capabilities – Indicated details about 802.11be capabilities of the AP
  - Vendor Specific Tags – More vendor specific information.

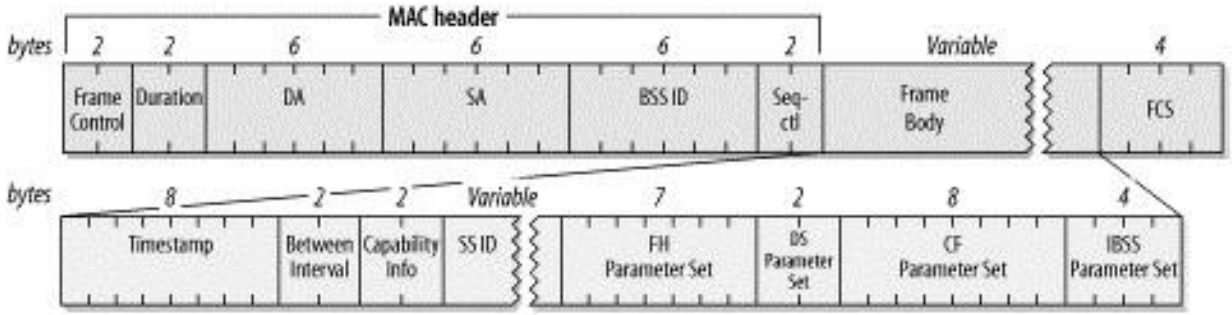


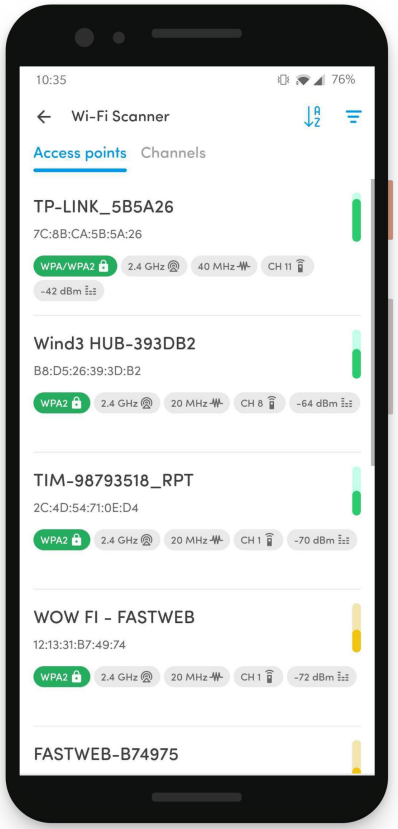
# Probe Request/Response Frames




Probe Request

Probe Response




A probe request frame is transmitted from a wireless station during active scanning.
Access points within reach respond by sending probe response frames.

Probe request frames contain the following information:

- SSID (0 ... 32 bytes), alphanumeric name
- Supported bit rates and other capabilities of the Station.

This is used by APs to see if the station can be permitted to join the network.

Probe response frames come from the AP to the station and contain the same information as in the beacons

# Authentication Frame

**Open System authentication**

There are two information elements in the body of the authentication request.

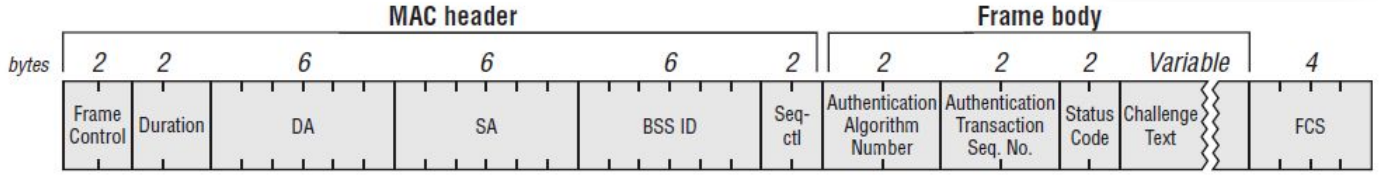
1. Authentication Algorithm Identification is set to 0 to indicate open-system method.
2. Authentication Transaction Sequence number is set to 1 to indicate first frame in the sequence.

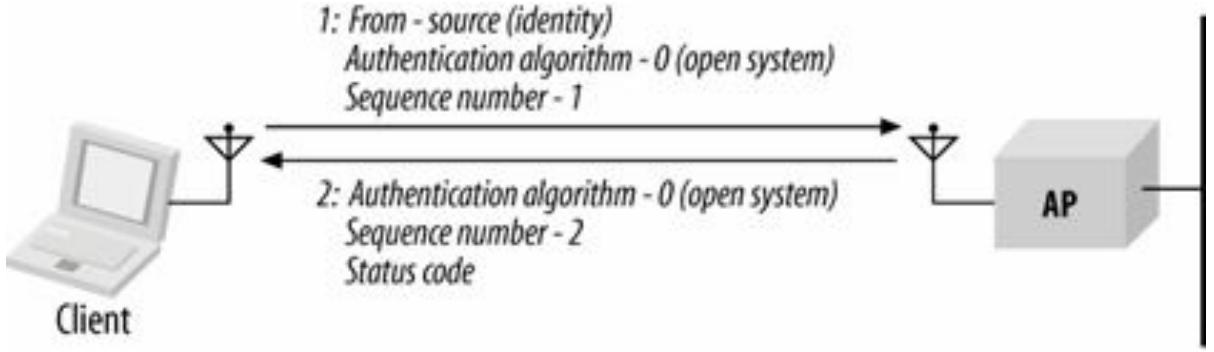
The access point then processes the authentication request and returns its response. Three information elements are present

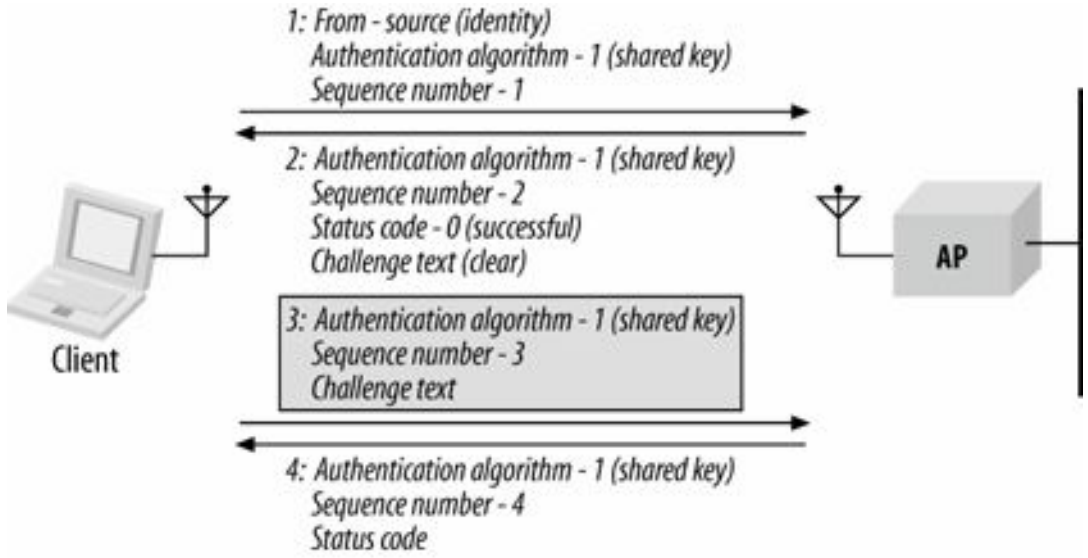
1. Authentication Algorithm Identification field is set to 0 to indicate open-system authentication.
2. Sequence Number is set to 2 to indicate response
3. Status Code indicates the outcome of the authentication request.

**Shared key authentication**

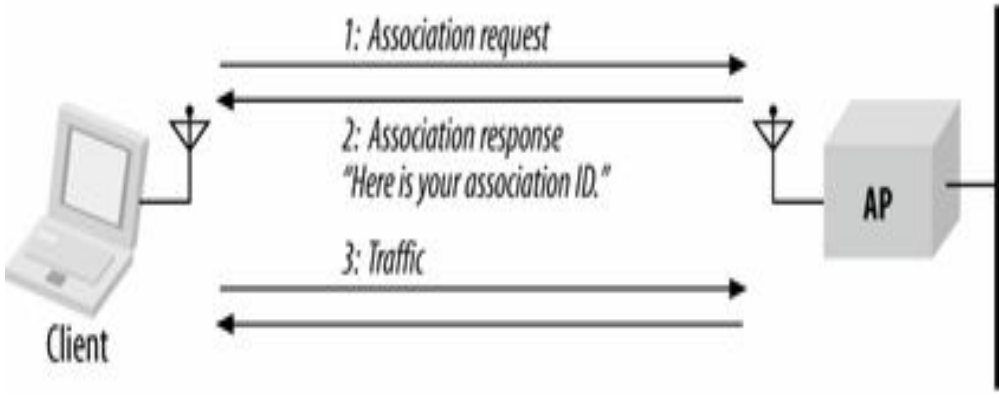
- Client sends Authentication request with Auth Algorithm set to 1 to indicate share key authentication
- AP responds with a text
- Station encrypts the text and sends it back
- AP decrypts and returns an authentication management frame



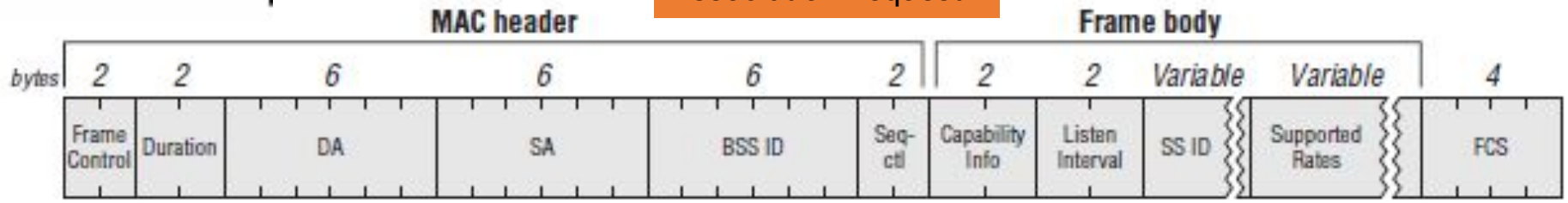



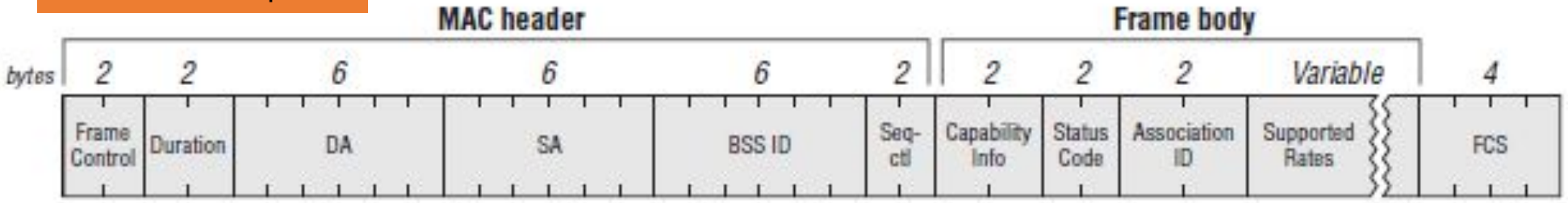
# Association Frames




Association Request




Association Response

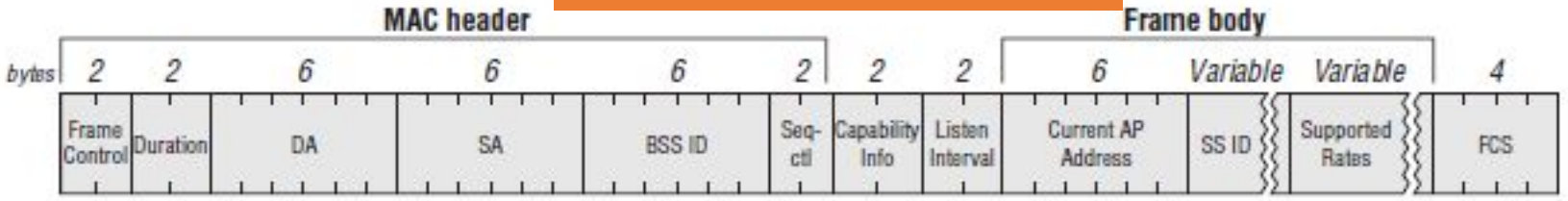



1. Once a mobile station has authenticated to an access point, it can issue an Association Request frame.
2. Stations that have not yet authenticated receive a Deauthentication frame from the access point in response.
3. One Association request is received, the access point then processes the association request. AP can chose to reject association.
4. When the association request is granted, the access point responds with a status code of 0 (successful) and the Association ID (AID).
5. The AID is a numerical identifier used to logically identify the mobile station to which buffered frames need to be delivered.

# Re-association Frames

Reassociation is the process of moving an association from an old access point to a new one. Over the air, it is almost the same as an association; on the backbone network, however, access points may interact with each other to move frames. When a station moves from the coverage area of one access point to another, it uses the reassociation process to inform the 802.11 network of its new location

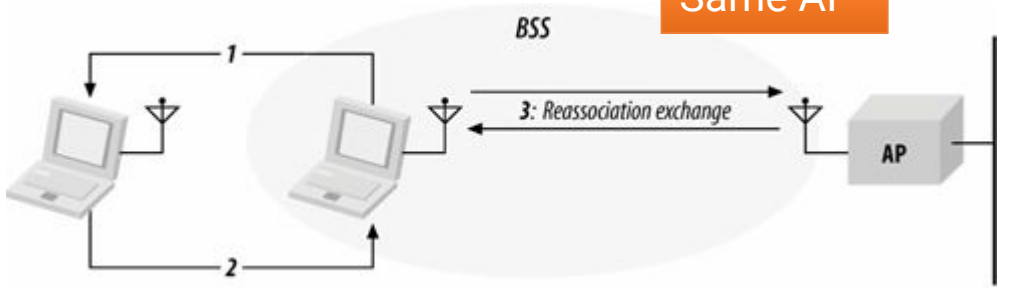
## Reassociation Frame Format



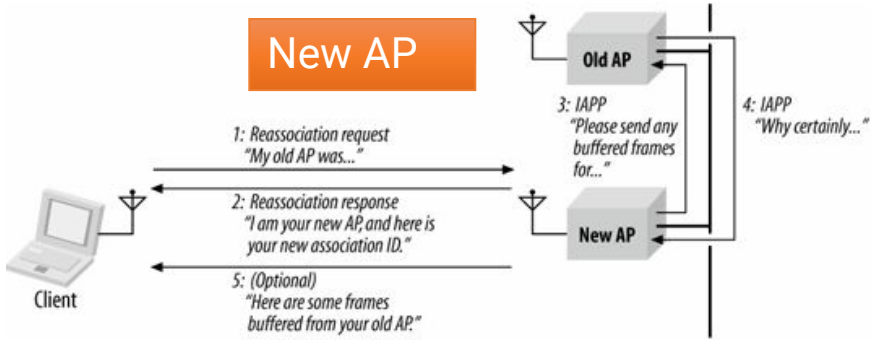

1. The mobile station issues a Reassociation Request to the new access point.
2. The access point processes the Reassociation Request:
    1. If the Reassociation Request is granted, the access point responds with a Status Code of 0 (successful) and the AID.
    2. Unsuccessful Reassociation Requests include just a Status Code, and the procedure ends.
3. The new access point contacts the old access point to finish the reassociation procedure. This communication is part of the IAPP.
4. The old access point sends any buffered frames for the mobile station to the new access point. 802.11 does not specify the communication between access points. At the conclusion of the buffered frame transfer:
    1. Any frames buffered at the old access point are transferred to the new access point so they can be delivered to the mobile station.
    2. The old access point terminates its association with the mobile station. Mobile stations are allowed to associate with only one access point at any given time.

Reassociation is also used to rejoin a network if the station leaves the coverage area and returns later to the same access point.

## Same AP



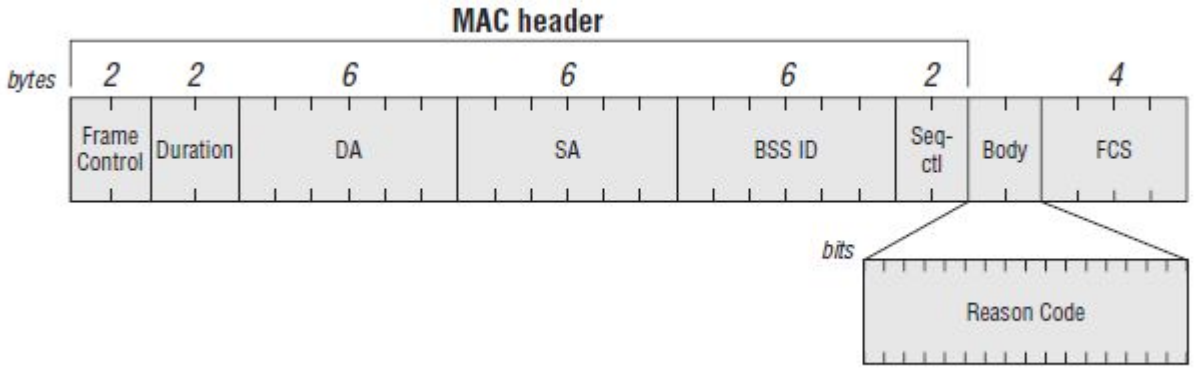

## New AP



# De-Authentication and Dis-association Frames

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

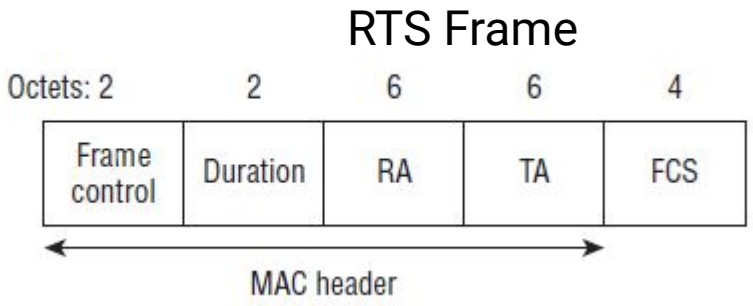
- Disassociate and Deauthenticate frames are management frames.
- Clients may disassociate prior to powering off.
- APs may disassociate clients for various reasons including failure to properly authenticate, for load balancing or timeout reasons, entering a state of maintenance, etc.
- When a station is disassociated it still maintains its authentication. This makes it easier for the client to associate again in the future.
- Deauthentication frames are used to reset the state machine back to state 1 for an associated client.
- The authentication process takes place prior to association therefor, if a station is deauthenticated, it is also disassociated.
- The body of Disassociate and Deauthentication frames includes a **reason code** explaining why the frame was sent.

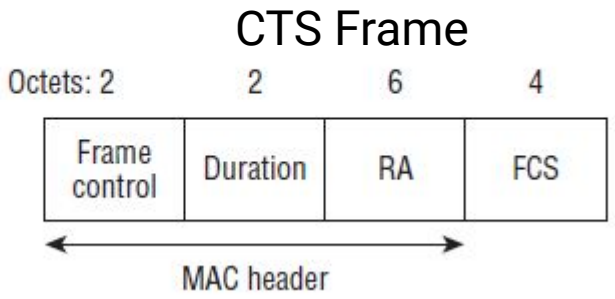



| Code | 802.11 definition | Explanation |
|---|---|---|
| 0 | Reserved | Normal working operation |
| 1 | Unspecified reason | We don't know what's wrong |
| 2 | Previous authentication no longer valid | Client has associated but is not authorised. |
| 3 | station is leaving (or has left) IBSS or ESS | The access point went offline, deauthenticating the client. |
| 4 | Disassociated due to inactivity | Client session timeout exceeded. |
| 5 | Disassociated because AP is unable to handle all currently associated stations | The access point is busy, performing load balancing, for example. |
| 6 | Class 2 frame received from nonauthenticated station | Client attempted to transfer data before it was authenticated. |
| 7 | Class 3 frame received from nonassociated station | Client attempted to transfer data before it was associated. |
| 8 | Disassociated because sending station is leaving (or has left) BSS | Operating System moved the client to another access point using non-aggressive load balancing. |
| 9 | Station requesting (re)association is not authenticated with responding station | Client not authorized yet, still attempting to associate with an access poin |
| 10 | Disassociated because the information in the Power Capability element is unacceptable | |

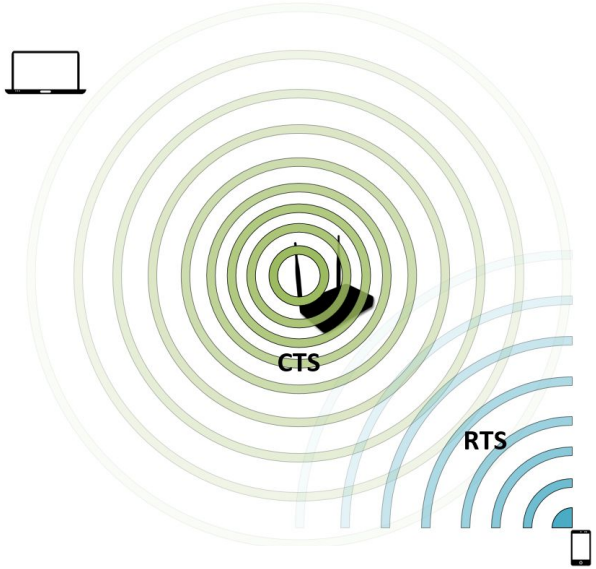
# RTS/CTS Frames





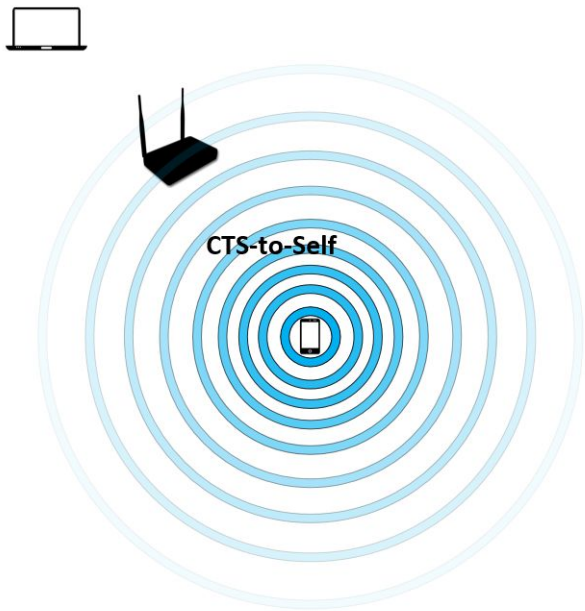




- Request to send (RTS) and clear to send (CTS) frames are used before each data frame transmission and are key to the virtual carrier sense process.
- When a station transmits a frame it will include a duration field. Stations nearby synchronize with this transmission, decode the frame, and update their NAV timers.
- A station will send an RTS frame, requesting to reserve the medium for the amount of time listed in the duration, but stations far away may not be able to decode the frame and not update their NAV timer.
- To resolve this issue, the CTS frame is used.
- CTS is a response from the AP, confirming medium reservation, which can be heard by all stations in the BSS.




## CTS-to-Self

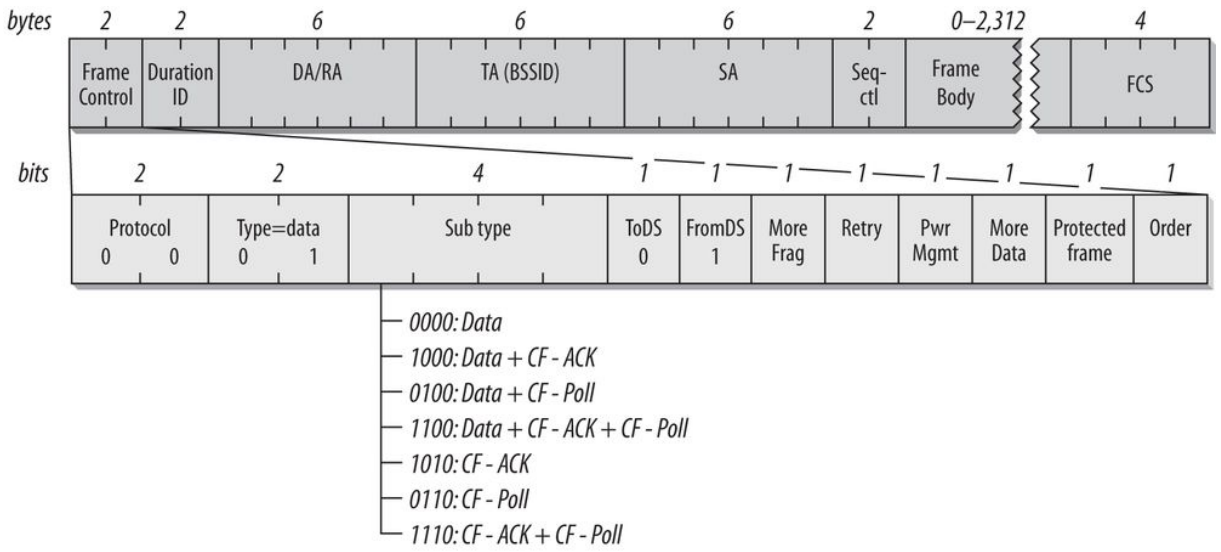
- CTS-to-Self is a simpler method of performing NAV distribution.
- It requires less overhead because only one frame is sent but risks collisions due to clients farther away potentially not being able to decode the CTA frame and set their NAV timers.
- The duration in the CTS-to-Self frame is the total time for data, ACK, and the interframe space
- CTS-to-Self is normally sent by the AP.



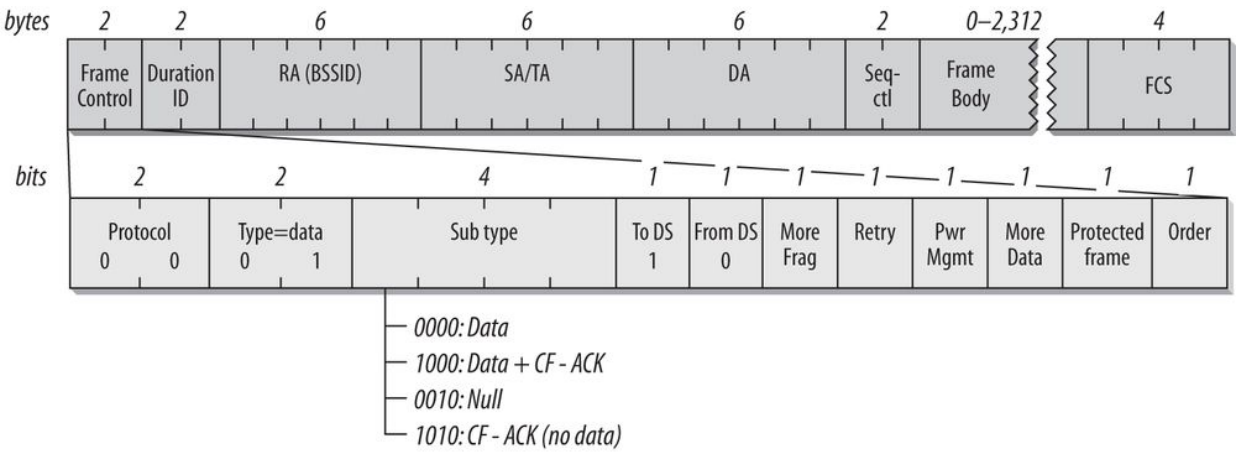
# Data Frames and Acknowledgements

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

## Data Frames from AP




## Data Frames to AP

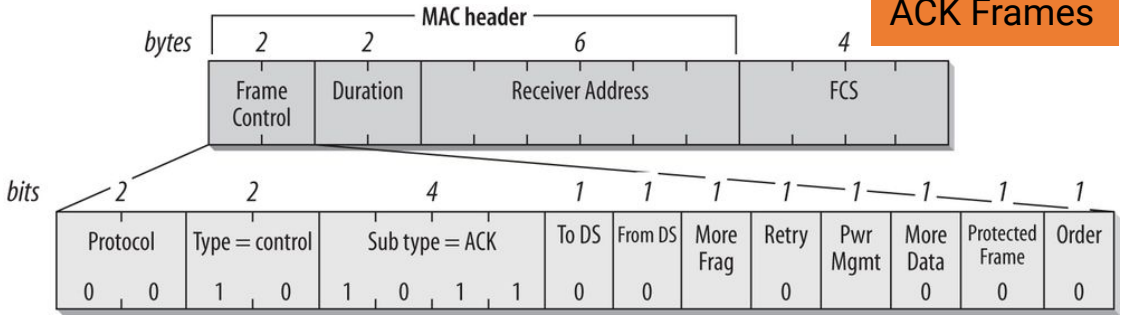



Data frames are used to transfer information or trigger an event. Data frames are the only type of frames that transfer actual useful payload.

Not all data frames contain a payload, some are “null data frames” and only contain a header and trailer.

ACK frames create a delivery verification method; they are expected after the transmission of data frames to confirm receipt of the frame. If the CRC check fails, the receiver will not send an ACK. If the sender does not receive an ACK, it will retransmit the frame.

## ACK Frames



# References

802.11 Framing in Detail
https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html

802.11 Wireless Networks: The Definitive Guide, Second Edition – Book Summary
https://flylib.com/books/en/2.519.1/

Management Frame Types
https://cciew2.rssing.com/chan-6090950/all_p14.html

802.11 Frame Types and Formats
https://howiwifi.com/2020/07/13/802-11-frame-types-and-formats/

WI-FI TECHNOLOGY
FUNDAMENTALS COURSE


?
QUIZ!
TIME

# Quiz 3a Results


**Md Sajjad Alam**

**INDIA**

Number of participants - 111