WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

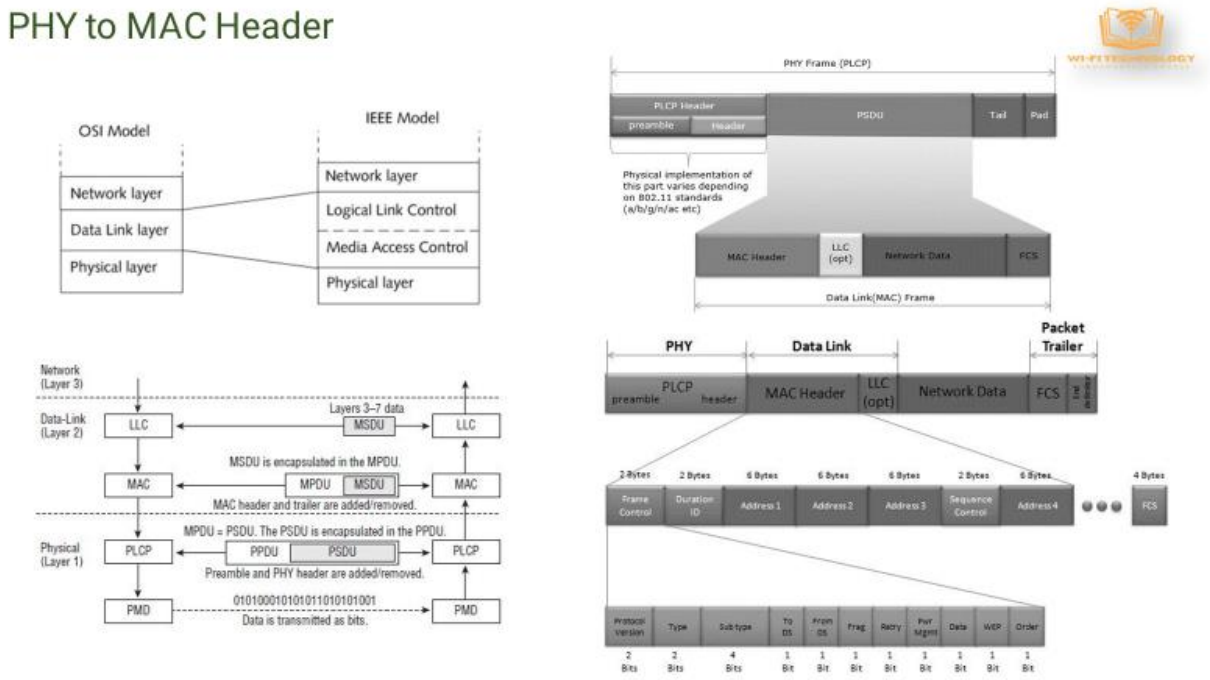
Module 3: WLAN MAC Layer

Session 3b:

MAC HEADERS, FRAMING AND KEY FUNCTIONS

Thanushya Mothikivalasa
Rohini kaparapu
Nishtala Kiranmai
Jami Harika
Shiny Sayyad

PHY to MAC Header:



Introduction to Data Link Layer:

- Transitioning from the physical (PHY) layer to the Medium Access Control (MAC) layer, the data link layer facilitates reliable communication. Within this layer, two sublayers, the PLCP (Physical Layer Convergence Procedure) and PMD (Physical Medium Dependent), play crucial roles in framing and encoding data for wireless transmission.

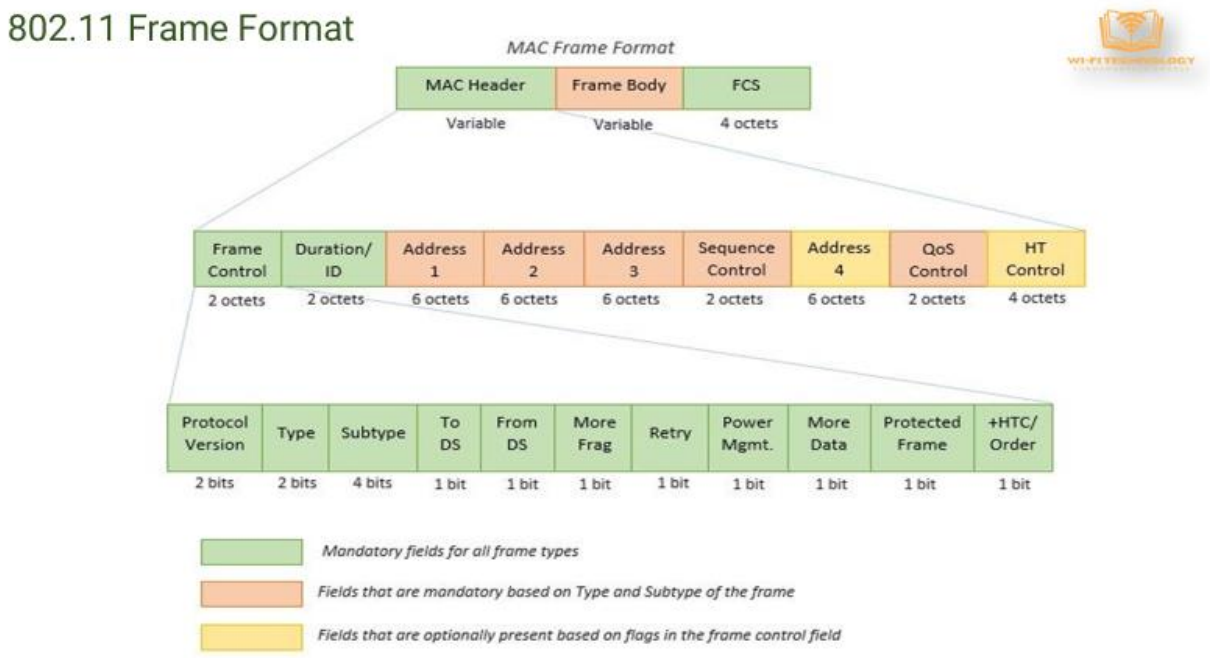
Overview of Data Link Layer Sublayers:

- At the data link layer, the Logical Link Control (LLC) and Medium Access Control (MAC) sublayers further refine the communication process. These sublayers contribute to the encapsulation and control of data for successful wireless networking.

MAC Frame Structure:

- Delving into the specifics of the MAC frame structure, it's essential to recognize the PS (Physical Layer Service) and PSDU (PLCP Service Data Unit) elements. The PSDU encapsulates the entire MAC frame, including headers and payloads, emphasizing the layered nature of network communication.

802.11 Frame Format:



Understanding the 802.11 Frame Components:

- Within the 802.11 frame format, distinctive components define the structure. The frame comprises a header, FCS (Frame Check Sequence), and body. This organization ensures systematic data transmission and reception.

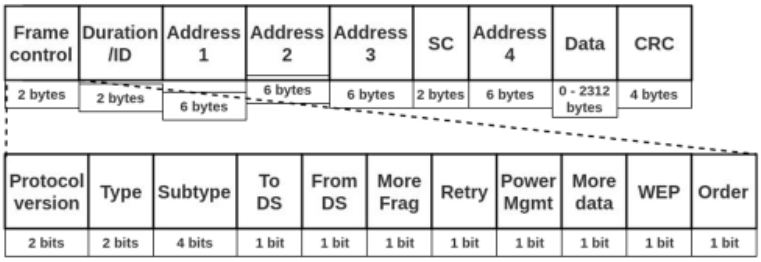
Significance of Frame Control Field:

- The Frame Control field serves as the cornerstone of frame interpretation. Elements like Protocol Version, Type, and Subtype guide the receiver in identifying the frame's nature and purpose within the communication process.

802.11 Frame Format (Frame Control Field Details):

802.11 Frame Format

- **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.

Crucial Subfields in Frame Control:

- Analyzing the Frame Control field in-depth, critical subfields emerge. Protocol Version ensures protocol compatibility, while Type and Subtype categorize frames into management, control, or data frames. DS (Distribution System) Bits provide insights into the frame's role within the distribution system, and the Duration Field specifies the time required for successful frame transmission.

The Address Fields

In the 802.11 frame format, which is commonly used for Wi-Fi communication, there are several address fields that play a crucial role in specifying the source and destination of a frame. The structure of these address fields can vary depending on the type of frame and

the mode of operation (e.g., infrastructure mode, ad-hoc mode, bridge mode).

Bits: 2	2	4	1	1	1	1	1	1	1	1
Protocol Version	Type	Subtype	To DS	From DS	More Frag	Retry	Power Mgmt	More Data	Prot. Frame	Order

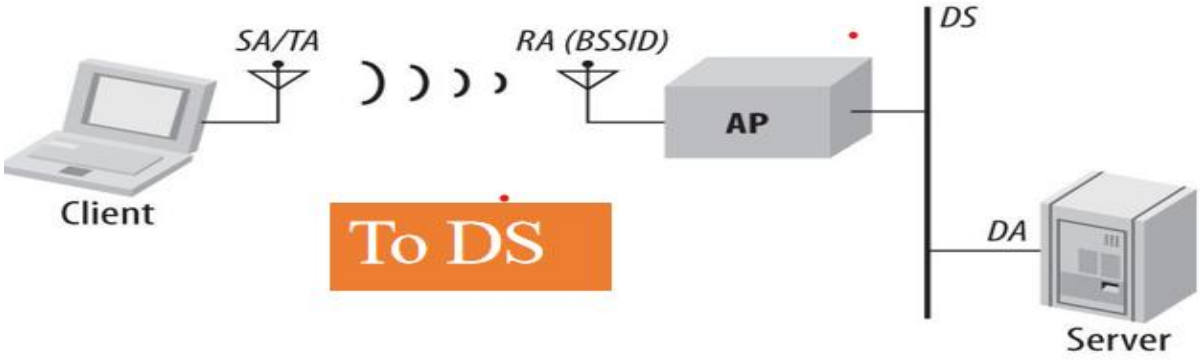
Frame Control field

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

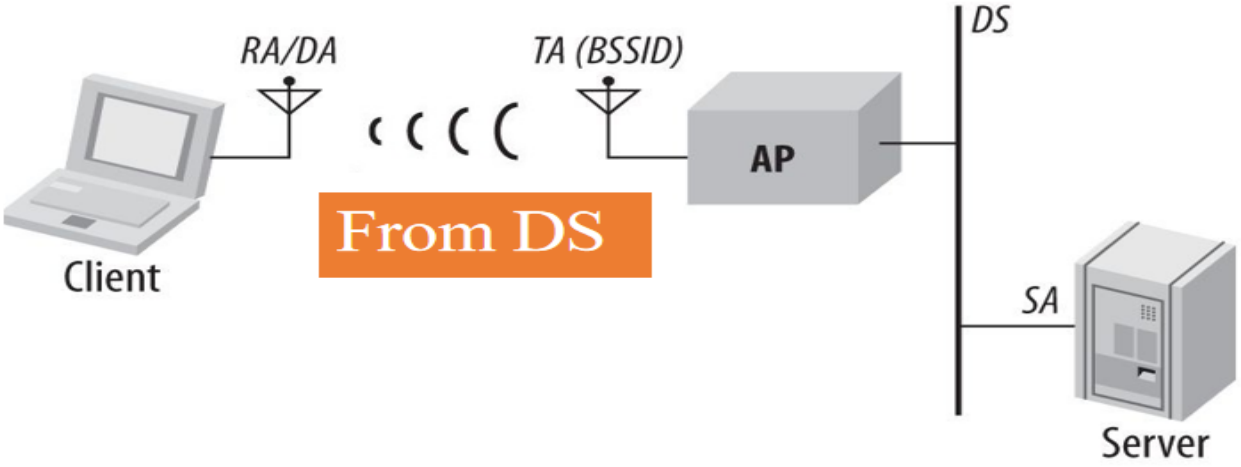
- SA = MAC address of the original sender (wired or wireless)
- DA = MAC address of the final destination (wired or wireless)
- TA = MAC address of the transmitting 802.11 radio
- RA = MAC address of the receiving 802.11 radio
- BSSID = L2 identifier of the basic service set (BSS)

DS (Distribution System):

DS refers to the distribution system or the network behind access points.
TO DS bit: Set indicates sending information from within the wireless LAN cell to the distribution system.



From DS: Set implies information coming from outside to inside the wireless LAN cell.



Frame Transmission Scenarios:

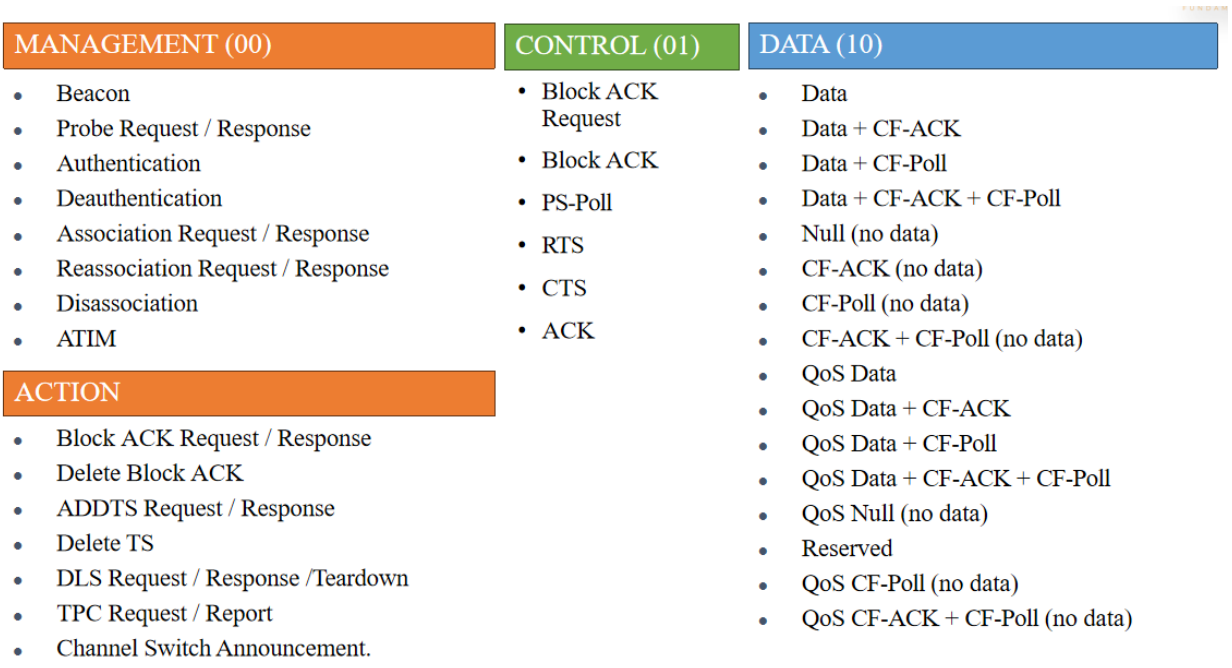
To DS and from DS bits both set to zero: Frames stay within the wireless LAN cell (management and control frames).
To DS set to one and from DS set to zero: Data frame from client to network.
To DS set to zero and from DS set to one: Data frame from network to client.
Both To DS and from DS bits set: Bridge mode, connecting two Wi-Fi networks.

Address Fields:

Address fields (address one to address four) vary based on 2DS and from DS bit settings. Different configurations for frames staying within the wireless LAN cell and frames going to/from the network.
An 802.11 frame can have up to four address fields. The four address fields vary according to the To DS/From DS sub-field in the Frame Control field. For example, the values of the four address fields are different when a frame is sent from a STA to an AP and when a frame is sent from an AP to a STATION. Rules for filling in the four address fields

Frame Type/Subtypes

Three main frame types: Management frames, Control frames, and Data frames.



Management Frames:

Management frames are used for the establishment, maintenance, and termination of network connections. They provide essential information about the network and its devices.

Examples:

Beacon: Broadcasted by an access point to announce its presence and network parameters.
Probe Request/Response: Used for network discovery and device probing.
Authentication: Initiates the authentication process between a station and an access point.
Association/Reassociation Request/Response: Used to join or rejoin a network.
Deauthentication/Disassociation: Signals the termination of an existing connection.

1.Beacon:

Broadcasted by an access point (AP) to announce its presence and provide information about the network.

Allows stations to discover and connect to available networks. Contains essential information like SSID, supported data rates, and other network parameters.

2. Probe Request / Response:

A station sends a Probe Request to discover nearby APs, and an AP responds with a Probe Response providing information about its capabilities.

Stations use Probe Requests to discover available networks, and APs respond with Probe Responses to attract potential associations.

3. Authentication:

A station initiates the authentication process with an AP to gain access to the network.
The station sends an Authentication frame to the AP, and the AP responds with an Authentication frame to confirm or deny access.

4. Deauthentication:
Used by an AP to terminate the association with a station or vice versa.
Sent when a station or AP decides to disconnect from the network.

5. Association Request / Response:
A station sends an Association Request to join a network, and the AP responds with an Association Response to either accept or reject the association.
Establishes a connection between a station and an AP, allowing the station to become part of the network.

6. Reassociation Request / Response:
Similar to Association but used when a station is already associated with one AP and wants to move to another AP within the same Extended Service Set (ESS).
Enables a station to seamlessly transition between APs while maintaining connectivity within the same network.

7. Disassociation:
A station or AP initiates this frame to terminate an existing association.
Sent when a station wants to disconnect from the network or when an AP decides to disassociate a station.

8. ATIM (Announcement Traffic Indication Message):
Used in infrastructure BSS to announce the presence of broadcast or multicast frames waiting for stations in power-saving mode.
Helps stations in power-saving mode to wake up and listen for pending broadcast or multicast frames.

ACTION

1. Block ACK Request / Response:
A station initiates this frame to request the establishment of a Block ACK agreement for the transmission of multiple frames.
Sent by the receiving station to acknowledge the Block ACK request and establish the Block ACK agreement.

2. Delete Block ACK:
Sent to terminate an existing Block ACK agreement between stations.

3. ADDTS Request / Response:
Used to request the setup of a Traffic Stream (TS) for Quality of Service (QoS).
Sent by the receiving station to acknowledge the ADDTS request and establish the requested TS.

4. Delete TS:
Sent to terminate an existing Traffic Stream (TS) that was previously established.

5. DLS Request / Response / Teardown:

A station sends a DLS (Direct Link Setup) request to establish a direct link with another station.
Sent by the other station to acknowledge the DLS request and establish the direct link.
Used to terminate an existing direct link between stations.

6. TPC Request / Report:

Sent to request a change in transmit power level.
A station sends a TPC (Transmit Power Control) report to inform other stations or the AP about its transmit power level.

7. Channel Switch Announcement:
Used to announce a channel switch, indicating that the sender is moving to a new operating channel.
Important for coexistence in scenarios where multiple APs or stations share the same frequency space.

2.Data Frames:

Data frames carry the actual payload or information that is being transmitted between devices within the network.

Examples:

QoS Data: Carries data with Quality of Service (QoS) parameters for improved performance.
Null Data: A frame without an actual data payload, used for control purposes.
QoS Null Data: Similar to Null Data but with QoS parameters.
Block ACK: Supports efficient transmission of multiple frames with acknowledgment.

1. Data:
This is a standard data frame used to transmit actual data from the sender to the receiver.

2.Data + CF-ACK:

This frame type includes data and is followed by a Contention-Free Acknowledgment (CF-ACK). CF-ACK is used in contention-free protocols.

3. Data + CF-Poll:
In this case, data is transmitted along with a Contention-Free Poll (CF-Poll). CF-Poll is used to initiate a request for data transmission.

4. Data + CF-ACK + CF-Poll:
This frame type combines data with both Contention-Free Acknowledgment (CF-ACK) and Contention-Free Poll (CF-Poll).

5. Null (no data):
A null data frame with no actual data payload. It may serve as a control frame in certain situations.

6. CF-ACK (no data):
This frame only contains a Contention-Free Acknowledgment (CF-ACK) and no data payload.

7. CF-Poll (no data):
Similar to CF-ACK (no data), this frame includes only a Contention-Free Poll (CF-Poll) with no data payload.

8. CF-ACK + CF-Poll (no data):
Combines a Contention-Free Acknowledgment (CF-ACK) and a Contention-Free Poll (CF-Poll), both without any actual data payload.

9. QoS Data:
Quality of Service (QoS) data frame is used to transmit data with QoS parameters for improved network performance.

10. QoS Data + CF-ACK:
Combines QoS data with a Contention-Free Acknowledgment (CF-ACK).

11. QoS Data + CF-Poll:
Combines QoS data with a Contention-Free Poll (CF-Poll).

12.QoS Data + CF-ACK + CF-Poll:
Combines QoS data with both Contention-Free Acknowledgment (CF-ACK) and Contention-Free Poll (CF-Poll).

13.QoS Null (no data):

A QoS null frame with no actual data payload. It serves a similar function as the regular null frame but with QoS parameters.

14.Reserved:
This frame type is reserved for future use and may not be currently defined or utilized.

15. QoS CF-Poll (no data):
A QoS frame that includes only a Contention-Free Poll (CF-Poll) without any data payload.

16.QoS CF-ACK + CF-Poll (no data):
Combines QoS parameters with both Contention-Free Acknowledgement (CF-ACK) and Contention-Free Poll (CF-Poll) without any actual data payload.

3.Control Frames:

Control frames are used to manage the flow of data and coordinate communication between devices. They handle tasks such as flow control, acknowledgment, and contention resolution.

Examples:

RTS (Request to Send): Initiates a reservation of the medium for data transmission.
CTS (Clear to Send): Sent by the receiver to grant permission for data transmission.
ACK (Acknowledgment): Confirms successful reception of a data or management frame.
PS-Poll (Power Save Poll): Allows a station in power-saving mode to request pending data from the access point.
Block ACK Request/Response: Manages the efficient transmission of multiple frames.

1.RTS (Request to Send):
Used in a wireless network to initiate a reservation of the medium for the transmission of a data frame.
The sender (station) sends an RTS frame to the receiver, requesting permission to send a data frame.

2. CTS (Clear to Send):
Sent by the receiver in response to an RTS frame, granting permission for the sender to transmit a data frame.
Acknowledges the receipt of the RTS frame and indicates that the medium is clear for the sender to transmit.

3. ACK (Acknowledgment):
Confirms the successful reception of a data or management frame.
After receiving a data frame, the recipient sends an ACK frame to confirm successful reception.

4. PS-Poll (Power Save Poll):

Allows a station in power-saving mode to request data pending for it at the access point (AP).
A station in power-saving mode sends a PS-Poll frame to the AP, and the AP responds with buffered data.

5. Block ACK Request:

Initiates the setup of a Block ACK agreement between the sender and receiver for the transmission of multiple frames.
The sender requests the receiver to establish a Block ACK agreement to improve efficiency for multiple frame transmissions.

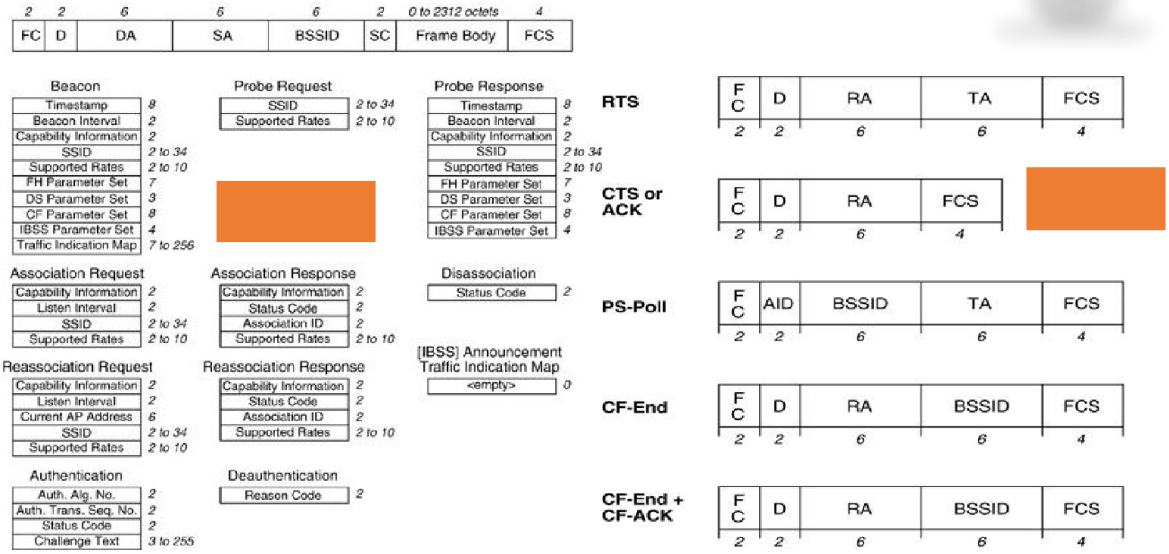
6. Block ACK:

Confirms the establishment of a Block ACK agreement between the sender and receiver.
Sent by the receiver in response to a Block ACK Request, indicating readiness for efficient multiple frame transmissions.

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



Management Frames:

Management frames are used for the establishment and management of communication between devices in a WLAN.They handle tasks such as network association, authentication, and disassociation.

Examples:

- Beacon Frames: Sent periodically by an access point to announce its presence and provide information about the network.
- Probe Request/Response Frames: Used to discover nearby networks or to respond to such requests.
- Association Request/Response Frames: Used to request and acknowledge the association of a station (device) with an access point.
- Authentication Frames: Used to authenticate a station with an access point.
- Disassociation Notification: Sent when a device wants to leave the network.

Frame Format:

Frame Control (2 bytes):

- Protocol Version (2 bits): Indicates the version of the IEEE 802.11 protocol.
- Type (2 bits): Specifies the frame type (Management frames have a type value of 0).
- Sub-type (4 bits): Defines the sub-type of the Management frame (e.g., Association Request, Beacon, Probe Response, etc.).

- To DS (1 bit): Indicates if the frame is destined for the distribution system (DS).
- From DS (1 bit): Indicates if the frame is from the distribution system (DS).
- More Fragments (1 bit): Indicates whether there are more fragments of this frame to follow.
- Retry (1 bit): Indicates if the frame is a re-transmission.
- Power Management (1 bit): Indicates power management mode.
- More Data (1 bit): Used to indicate if there are more frames to be sent.
- WEP (1 bit): Indicates whether the frame is encrypted using WEP (Wired Equivalent Privacy).

Duration/ID (2 bytes):

- Duration (in Time Units): Specifies the duration for which the medium will be reserved for the transmission of the frame.

Address Fields (6 bytes each for Receiver and Transmitter):

- Receiver Address (RA): The MAC address of the station intended to receive the frame.
- Transmitter Address (TA): The MAC address of the station that transmitted the frame.

Sequence Control (2 bytes):

- Fragment Number (4 bits): Indicates the sequence number of the fragment.
- Sequence Number (12 bits): Represents the sequence number of the frame.

Frame Body (Variable length):

- Contains information specific to the Management frame subtype. For example, in an Association Request frame, the body includes information like supported rates, SSID, and other parameters.

Frame Check Sequence (FCS) (4 bytes):

- A cyclic redundancy check (CRC) or Frame Check Sequence to ensure the integrity of the frame during transmission.

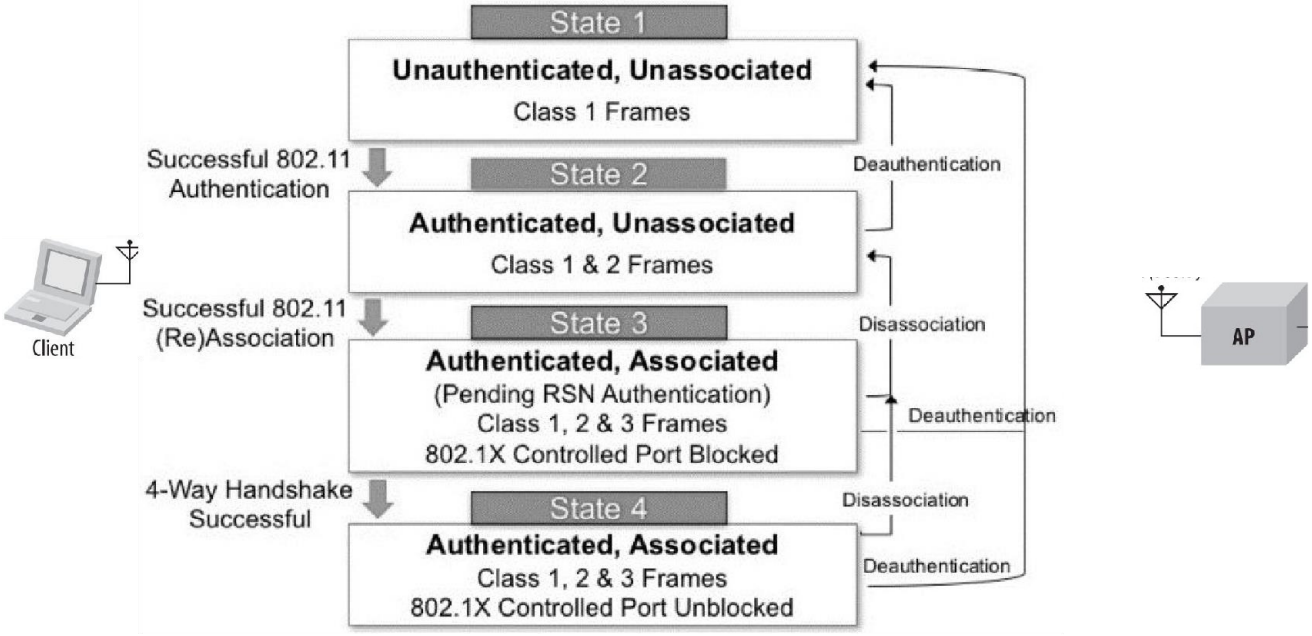
Control Frames:

Control frames are used for the management of data transmission between devices.They provide mechanisms for handling frame acknowledgment, power management, and fragmentation.

Examples:

- Clear-to-Send (CTS) Frames:Used in the Request-to-Send/Clear-to-Send (RTS/CTS) mechanism to avoid collisions.
- Acknowledgment Frames (ACK):Sent by the receiving station to confirm the successful reception of a data frame.
- Power Save Frames: Used to indicate power save mode for a station.
- Block Acknowledgment (BA): Used to acknowledge the receipt of a block of data frames, improving efficiency.

Connection State Machine



The connection state machine of a client with an access point in a wireless network is crucial for understanding the different phases a client goes through during the connection process.

Unauthenticated, Unassociated (State 1):

- In this initial state, the client is aware of the existence of the access point but has not yet completed the authentication process or associated with it.
- This state reflects the starting point of the connection process, where the client begins by recognizing available access points.

Authenticated, Unassociated (State 2):

- After successfully authenticating with the network, the client enters this state. Although authenticated, it has not yet been associated with a specific access point.
- Authentication is a crucial step in ensuring that the client is allowed to join the network. This state prepares the client for the next step of associating with a particular access point.

Authenticated, Associated (State 3):

- Upon completing the association process, the client is now fully authenticated and associated with a specific access point.
- This state signifies that the client is now an active member of the network, capable of communication with the access point. However, it may not have full data access until additional security measures are taken.

Authenticated, Associated, Ready to Send Data (State 4):

- After successfully completing all security handshakes, the client is now not only authenticated and associated but also ready to send and receive data.
- This is the final state, indicating that the client has undergone all necessary processes to ensure a secure and reliable connection. It can actively participate in data exchange within the WLAN.

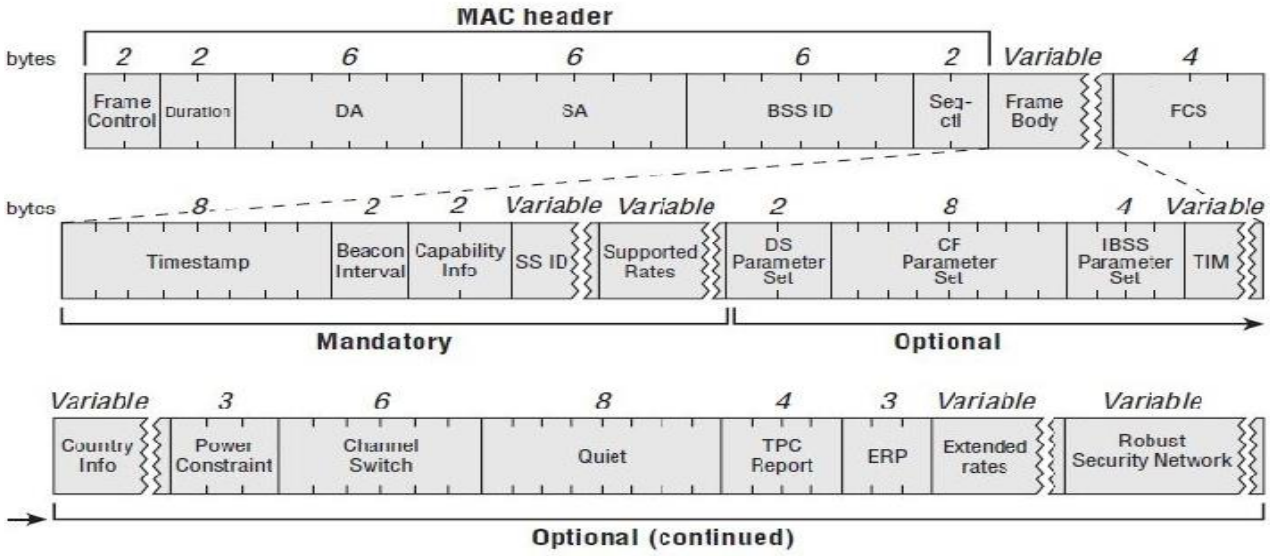
State Transitions and Continuity:

- Dynamic Transition: The client can dynamically transition between states based on its activities. For example, sending a deauthentication frame to the access point can move it back to the unauthenticated and unassociated state.
- Continuous Transition: The client's ability to move between states reflects the dynamic nature of wireless networks. This flexibility allows the client to adapt to changing conditions, such as roaming between access points or responding to network events.

Importance of State Machine:

- Systematic Connection Process:The state machine ensures a systematic and secure process for a client to establish and maintain a connection with an access point.
- Security: Each state represents a specific level of security clearance, with authentication and association serving as checkpoints before full participation in the network.
- Efficiency: The state machine helps in optimizing the efficiency of the connection process by guiding the client through well-defined steps.

Beacon Frame



Beacon frame: It 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.

Frame and Its Significance:

The Beacon frame is a pivotal element in the world of wireless networks, akin to a menu provided by an access point (AP) to all potential clients within its range. This broadcasted frame contains crucial information about the access point and is transmitted approximately once every 100 milliseconds, although this interval can be adjusted by the access point based on its configuration.

Frame Format:

As with many frames, the Beacon frame consists of a header and a body. The header includes standard elements such as frame control, duration, and address fields. The body, however, is where the real richness lies. The body is composed of fixed parameters, which are consistent across all Beacon frames, and tag parameters, which are optional and can vary based on the AP's capabilities.

Fixed Parameters:

Fixed parameters are essential and mandatory in every Beacon frame. One such critical fixed parameter is the timestamp. This timestamp essentially reflects the clock information of the access point. For seamless communication within the Basic Service Set (BSS), every connecting station needs to synchronize with the AP's clock. This synchronization is crucial for various time-sensitive operations, such as determining when a device should go to sleep or wake up to receive critical information. The timestamp is broadcasted every 100 milliseconds.

Another vital fixed parameter is the beacon interval, which specifies the timing at which beacons are transmitted. Typically set to around 100 milliseconds, this interval signifies how often the AP sends out Beacon frames. Some AP’s might adjust this interval, choosing to send beacons less frequently (e.g., every 200 milliseconds) to reduce overhead.

Tag Parameters:

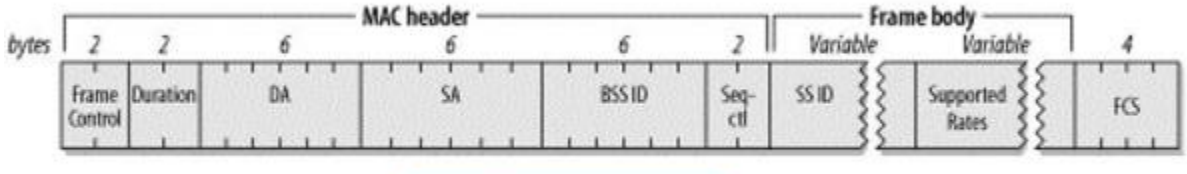
Tag parameters, on the other hand, introduce variability to the Beacon frame. These optional parameters can differ among beacons based on the capabilities of the access point. Like items on a restaurant menu, the number and type of tag parameters can vary. For instance, one AP might include three tag parameters, while another, with more capabilities, might feature five or even ten.

Importance of Timestamp:

The timestamp serves as a synchronization mechanism, analogous to students synchronizing their watches with the classroom clock. For example, if the classroom clock dictates that a surprise quiz will occur at 4:15 PM, students need to follow that clock for accurate timing.

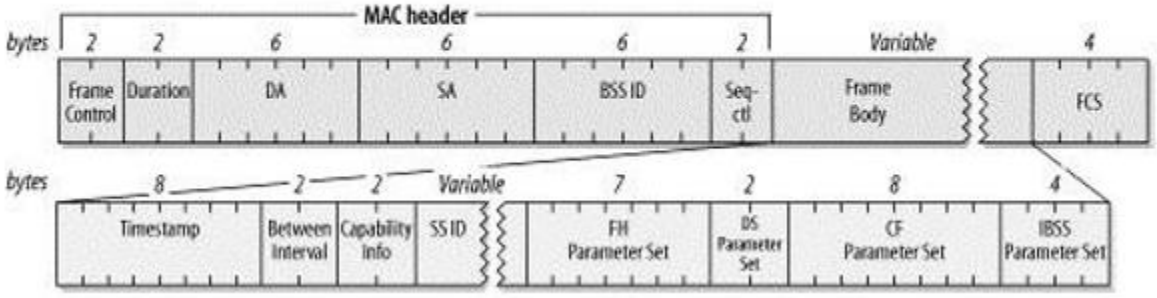
Similarly, devices connecting to an access point must synchronize with the AP's clock to receive time-sensitive information effectively. This synchronization ensures that devices receive critical data at the right time.

Probe Request/Response Frames



Probe Request

Probe Response

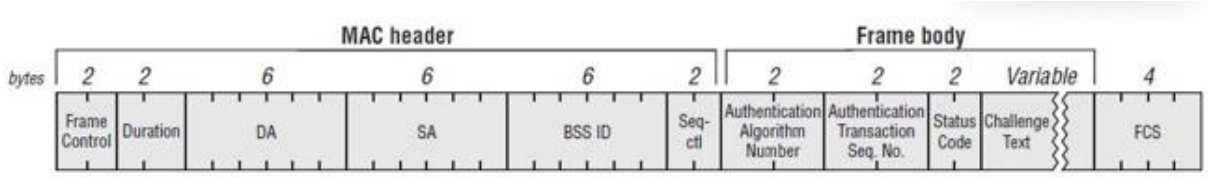


A probe request frame is transmitted from a wireless station during active scanning. Access points within reach respond by sending probe response frames.Probe request frames contain the following information:

- 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.To understand it in much simpler words we can Think of a probe request like a device asking, "Hey, any Wi-Fi networks around here?" It's a signal sent out by your device to see what Wi-Fi networks are available nearby.When an access point receives this request, it replies with a probe response. It's like the access point saying, "Yes, I'm here! Here's info about my Wi-Fi network, like its name and what it offers."So, the probe request is your device looking for Wi-Fi, and the probe response is the network saying, "Hey, here I am! Here's what I've got."

Authentication Frame



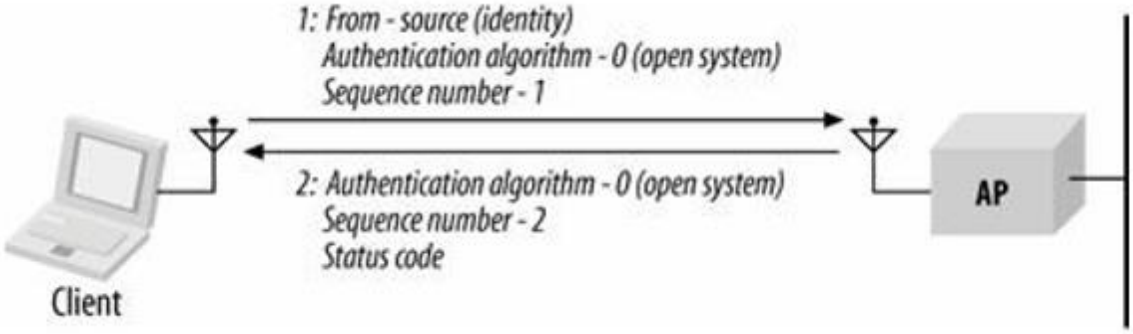
Open System authentication

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

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

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

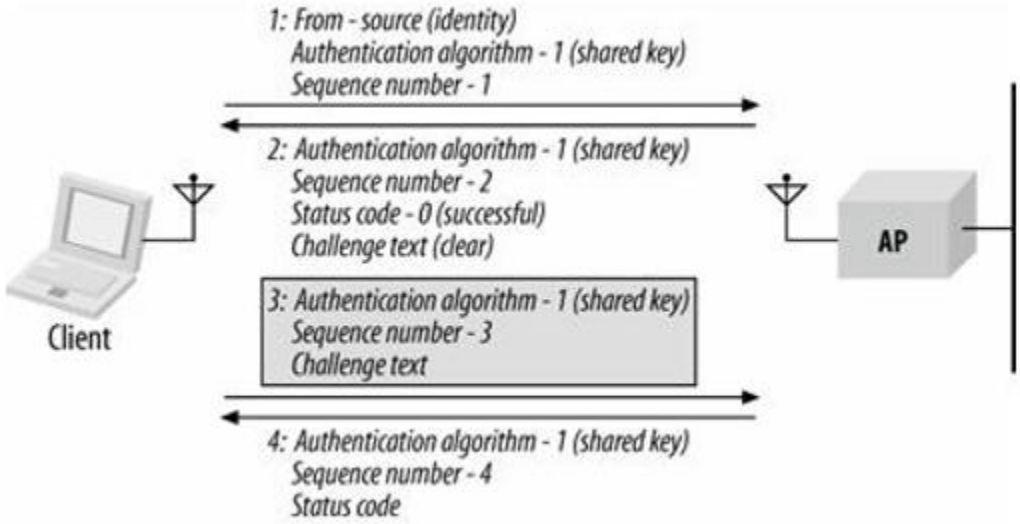
- Authentication Algorithm Identification field is set to 0 to indicate open-system authentication.
- Sequence Number is set to 2 to indicate response
- Status Code indicates the outcome of the authentication request.



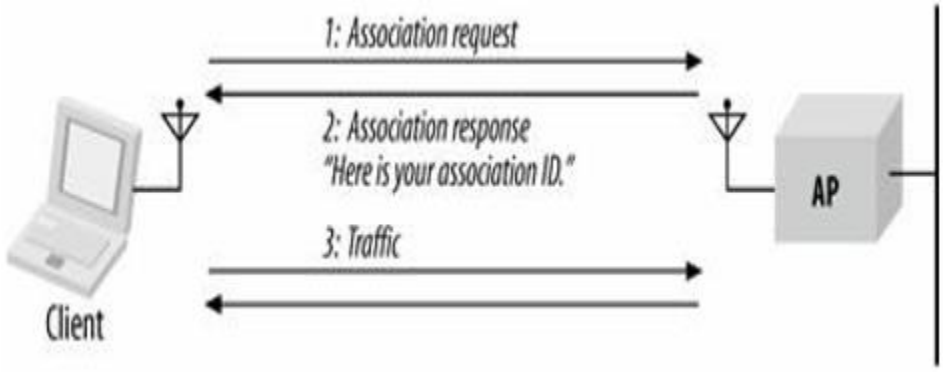
Shared key authentication

- Client initiates authentication request, specifying shared key authentication by setting the authentication algorithm to 1.
- Access Point (AP) responds by sending a piece of text to the client.

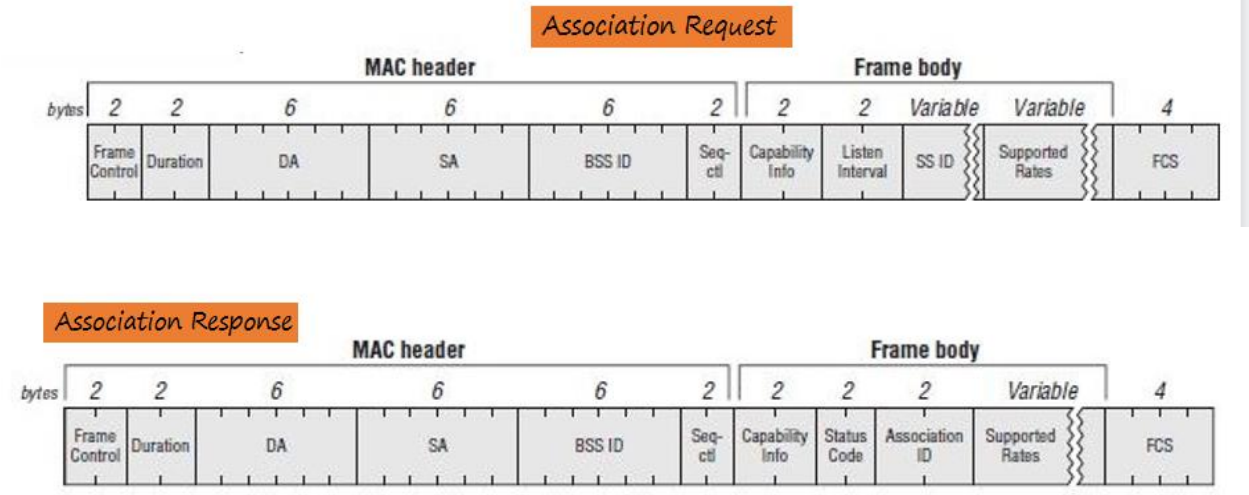
- The client encrypts this text using a specific encryption method.
- Encrypted text is sent back to the AP by the client.
- The AP decrypts the received text using the shared key.
- Successful decryption confirms the correct key usage by the client.
- The AP generates an authentication management frame.
- This frame signifies the completion of the authentication process, enabling the client to securely access the Wi-Fi network using the shared key method.



Association frames



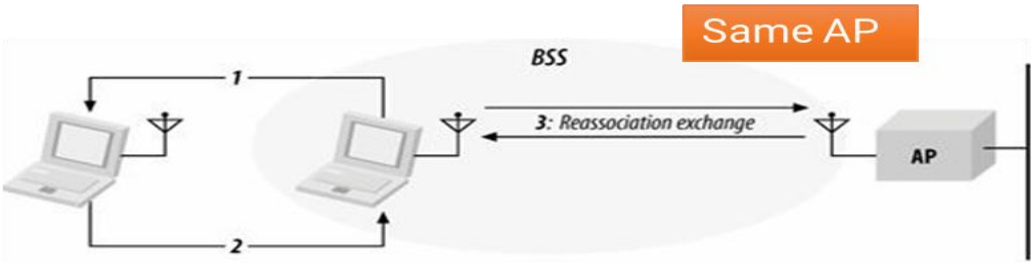
1. Once a mobile station has authenticated to an access point, it can issue an Association Request frame.
2. Stations that have not yet authenticated receive a Deauthentication frame from the access point in response.
3. One Association request is received, the access point then processes the association request. AP can choose 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.

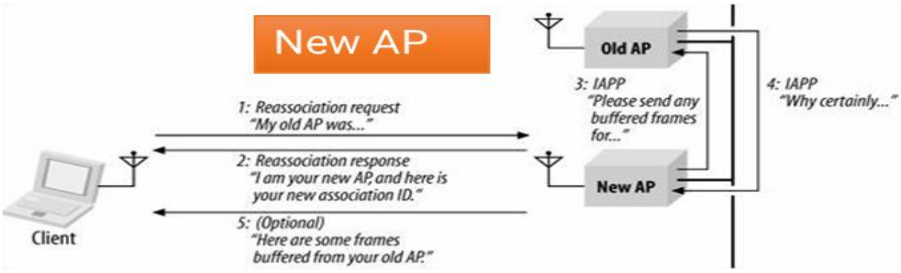


Here's the step by step representation of how the association frame works :

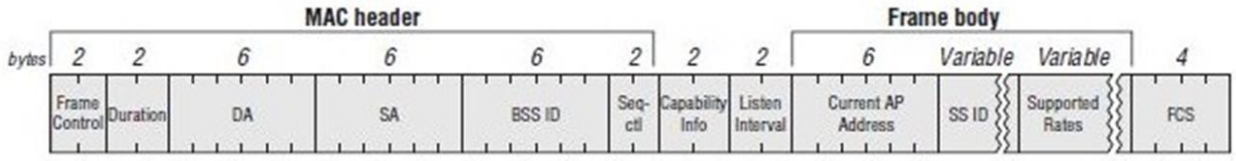
1. **Client's Introduction:** When your device wants to join a Wi-Fi network, it sends what's called an association request to the access point. This request is like your device saying, "Hey, I'd like to join your network! Here are the things I can do, like the speed I can handle."
2. **Access Point Evaluation:** The access point then checks this request. It's like the AP saying, "Let me see if we can be friends." It looks at your device's capabilities and checks if it has enough space and speed to accommodate your device.
3. **Compatibility Check:** For example, if the access point can support a certain speed (let's say 24 Mbps), and your device also works at that speed, it means you both are compatible.
4. **Association Response:** If everything checks out and the access point is happy to have your device join, it sends back an association response. This response says, "You're in!" It includes a special ID number for your device to recognize it within the network.

Re-association Frames



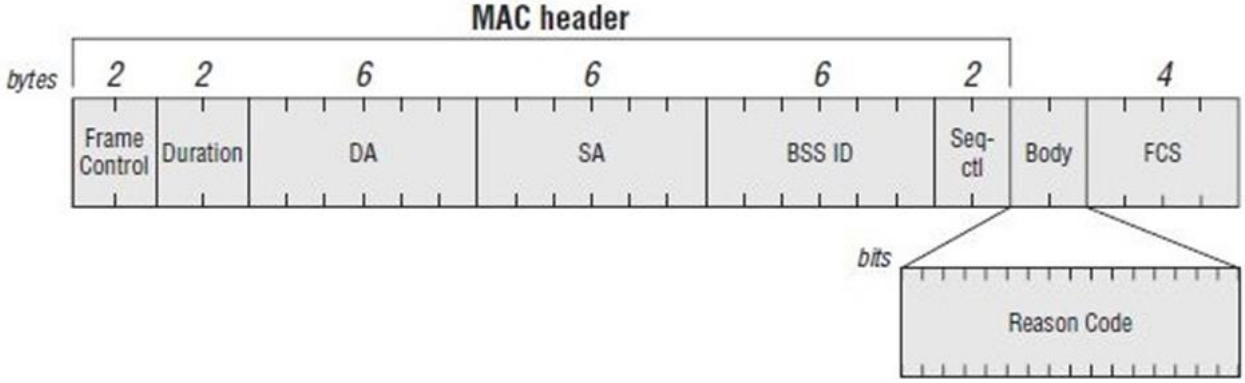


Reassociation Frame Format



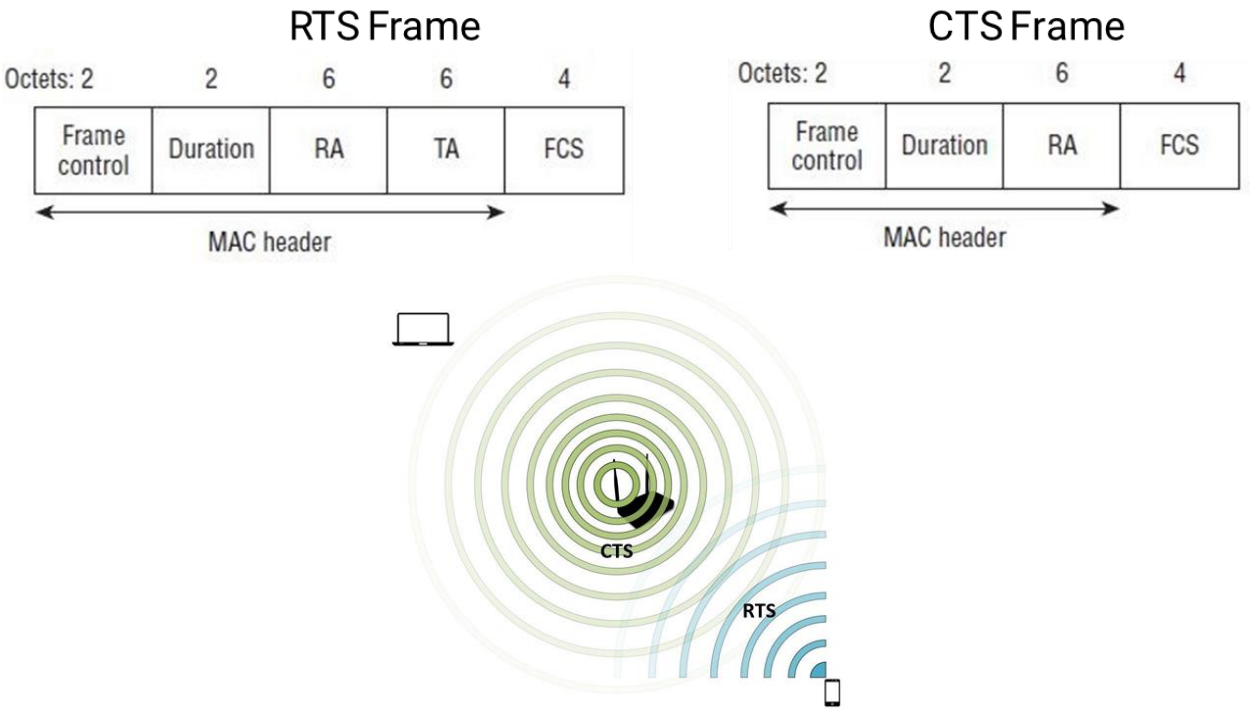
The concept of reassociation comes into play when a device that was previously associated with an access point (AP) temporarily loses its association and needs to reconnect. Instead of going through the entire process of probing and authentication again, the device can use reassociation frames. These frames allow the device to quickly reconnect to the same AP or associate with a new AP while maintaining its authenticated state. Reassociation frames streamline the reconnection process, avoiding unnecessary repetitions of authentication steps.

De-Authentication and Dis-association Frames



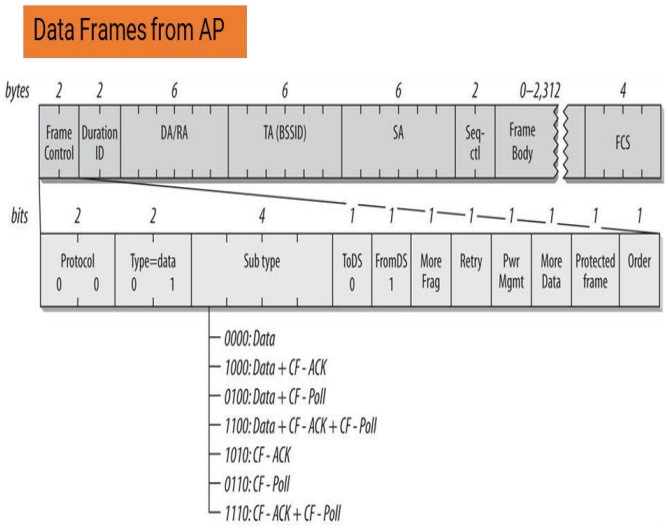
Deauthentication frames serve the purpose of disconnecting a device from a Wi-Fi network. When a client wants to disconnect, it can send a deauthentication frame to the access point, indicating a reason for the disconnection through a reason code. Similarly, an access point can also send a deauthentication frame to a client, either to force it to disconnect or to kick it out of the network. The deauthentication frame is a type of management frame used to manage the association and disassociation of devices within a Wi-Fi network.

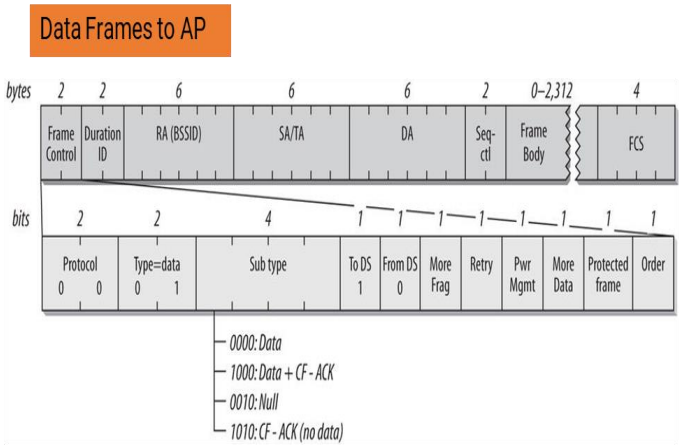
RTS/CTS Frames

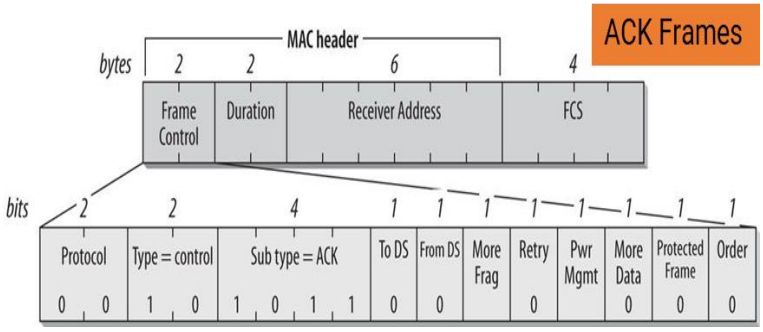


Wi-Fi networks use RTS (Request to Send) and CTS (Clear to Send) frames to solve the "hidden node problem." This problem arises when two stations cannot hear each other directly, trying to transmit data simultaneously to a shared destination. To prevent collisions, the station initiating communication sends the RTS frame to the destination, goes there, and determines the desired duration of the journey - specifies the time. This process enables remote stations to disconnect for a certain period of time, avoid collisions, and increase network performance. The RTS/CTS tool facilitates a form of "virtual bearer sensing" to reduce the hidden node challenge.

Data Frames and Acknowledgements







1. Data Frames:

Think of data frames as messengers carrying the actual stuff you want to send over Wi-Fi—like pictures, documents, or videos.

2. Headers Everywhere:

But these messengers come with a bit of paperwork, called headers. These headers are like tags on the message, telling the Wi-Fi network where it's from, where it's going, and other important details.

3. Acknowledgment Frames (ACK):

After sending your message (data frame), the network sends a tiny acknowledgment (ACK) back, just to say, "Got it, everything's cool."

4. Overhead Reality:

However, there's a catch. Besides your message, there's some extra stuff flying around—like network management messages (probes, associations, etc.). This extra stuff takes up airtime and slows things down a bit.

5. Capture File Peek:

Looking at a Wi-Fi capture file is like checking out a log of all the messages and paperwork flying through the air—probes, connection requests, and more.

6. Deauthentication Frame:

If a device wants to leave the Wi-Fi party, it sends a "goodbye" message (Deauthentication frame) with a reason, like "I'm moving elsewhere."

Simply put, data frames act as messengers carrying your important files or messages over Wi-Fi. However, just as the transmitter includes documentation (headers) indicating the message's origin and destination, these data frames also introduce additional features over the air—such as network control messages (which have a high impact) that can slow things down a bit.

Looking at the Wi-Fi activity log is like watching a mix of messages flying around, including connection requests, acknowledgments, and farewells when a device decides to leave the Wi-Fi network. So, in the world of Wi-Fi, it's not just about sending your data; it also involves managing certain documents and processing messages.