Wi-Fi TRAINING - MODULE 4

Akash S, embedUR Systems

Qn 1:

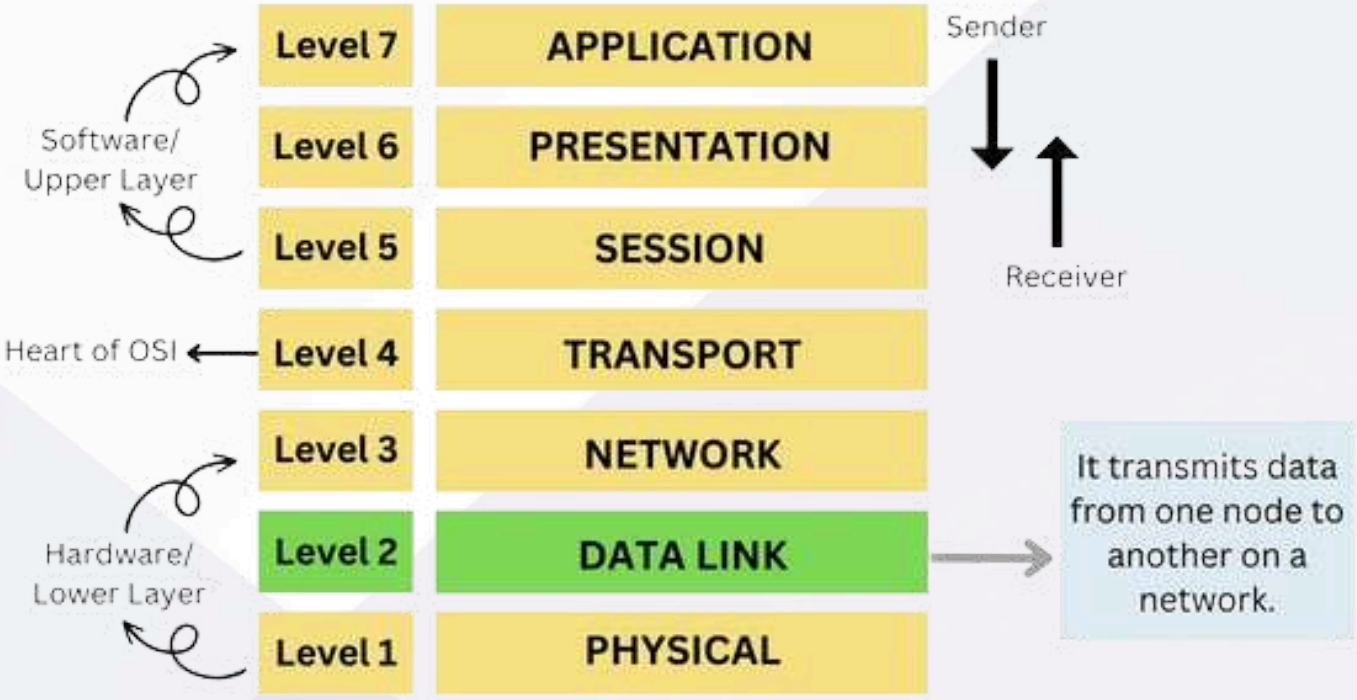
What is the significance of MAC layer and in which position it is placed in the OSI model

MAC Layer:

- The MAC layer is like the traffic cop of Wi-Fi, managing how devices share the wireless airwaves
- It handles addressing so each device knows where data is going
- It controls access to the medium, ensuring fair play among all connected devices
- It adds error checking to catch and fix data hiccups
- It’s key for security features like encryption in wireless networks

Position in OSI layer:

- Layer 2 - **Data Link Layer**

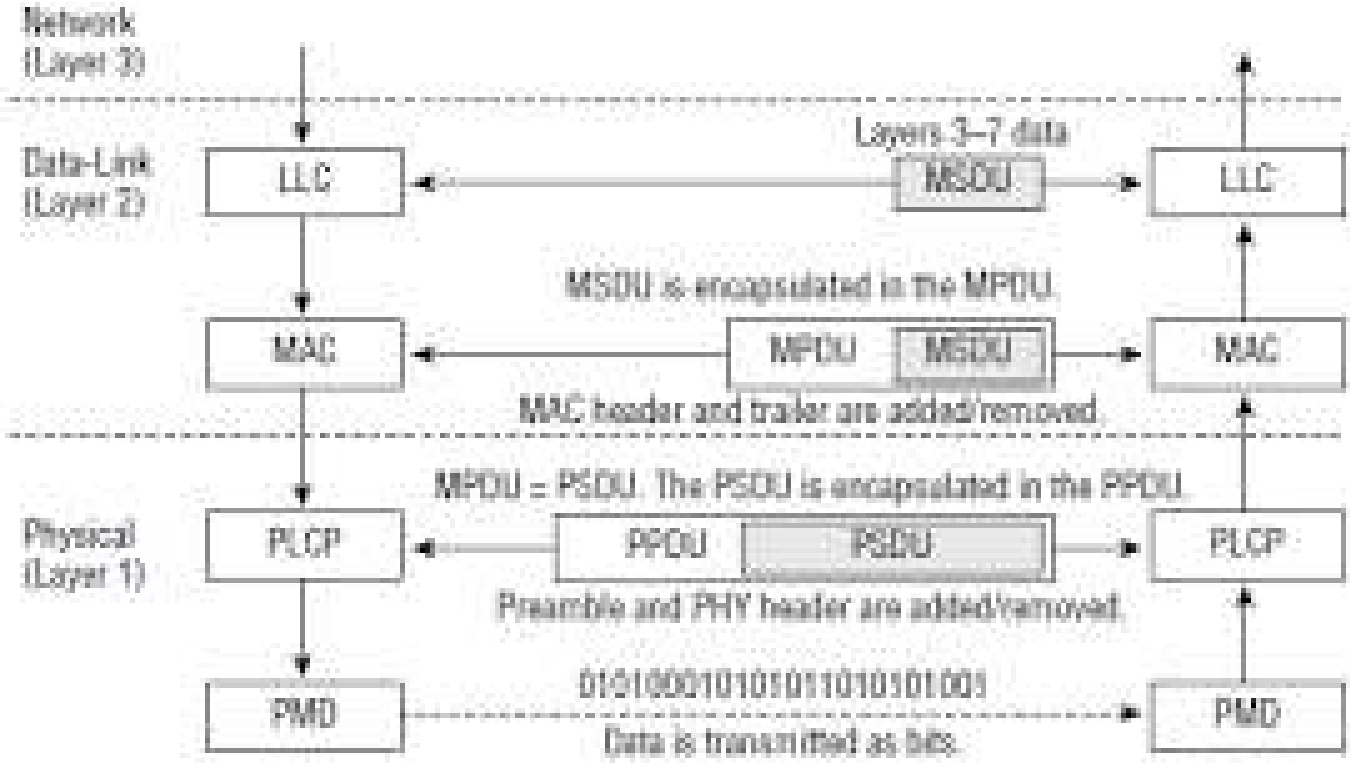


Speciality:

- Without the MAC layer, Wi-Fi would be chaos with no order or security
- Its position in Layer 2 makes it the heart of local network communication
- It supports features like roaming and QoS, vital for smooth networks

MAC in modern Networks:

- The MAC layer adapts to new tech like faster Wi-Fi standards
- It enables devices to switch APs without dropping connections
- It helps prioritize traffic, like video calls over emails
- It works with higher layers to deliver reliable data everywhere
- Its flexibility keeps wireless networks growing strong



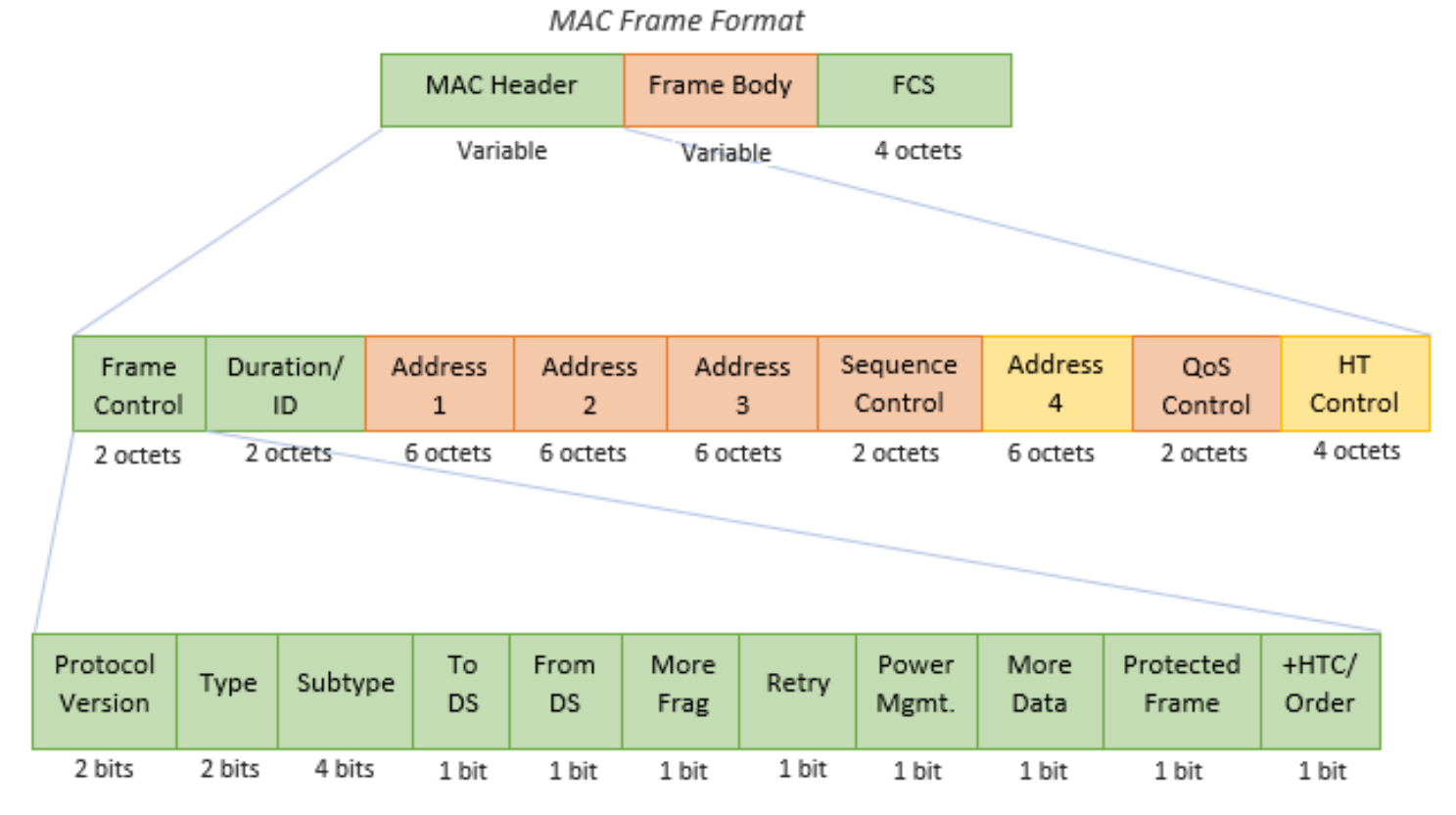
Qn 2:

Describe the frame format of the 802.11 MAC header and explain the purpose of each field

Overview:

- The 802.11 MAC header is the backbone of every Wi-Fi frame, shaping how data moves wirelessly
- It's a structured layout packed with 30 bytes, split into fields that tell a story of communication
- It adapts based on frame type
    - management
    - control
    - data
- This header ensures every device knows its role in the wireless dance

Frame Format:



Breakdown:

- **Frame Control** - indicates the frame type and subtype for proper processing
- **Duration/ID** - specifies the duration of channel reservation or serves as a network identifier
- **Address 1** - contains the MAC address of the receiving device
- **Address 2** - holds the MAC address of the transmitting device
- **Address 3** - includes the MAC address of the final destination or original source
- **Sequence Control** - manages the sequence number and fragment number for frame ordering
- **Address 4** - provides an additional MAC address for complex network scenarios
- **QoS Control** - defines priority levels for quality of service handling
- **HT Control** - manages high-throughput settings for advanced Wi-Fi features

Technical edge:

- The variable field length optimizes header size based on need
- It integrates with modern standards like 802.11n and 802.11ac
- Sequence tracking reduces errors in high-speed transmissions
- It supports advanced features like multi-user MIMO

Qn 3:

Please list all the MAC layer functionalities in all Management, Control, and Data planes

Management Plane:

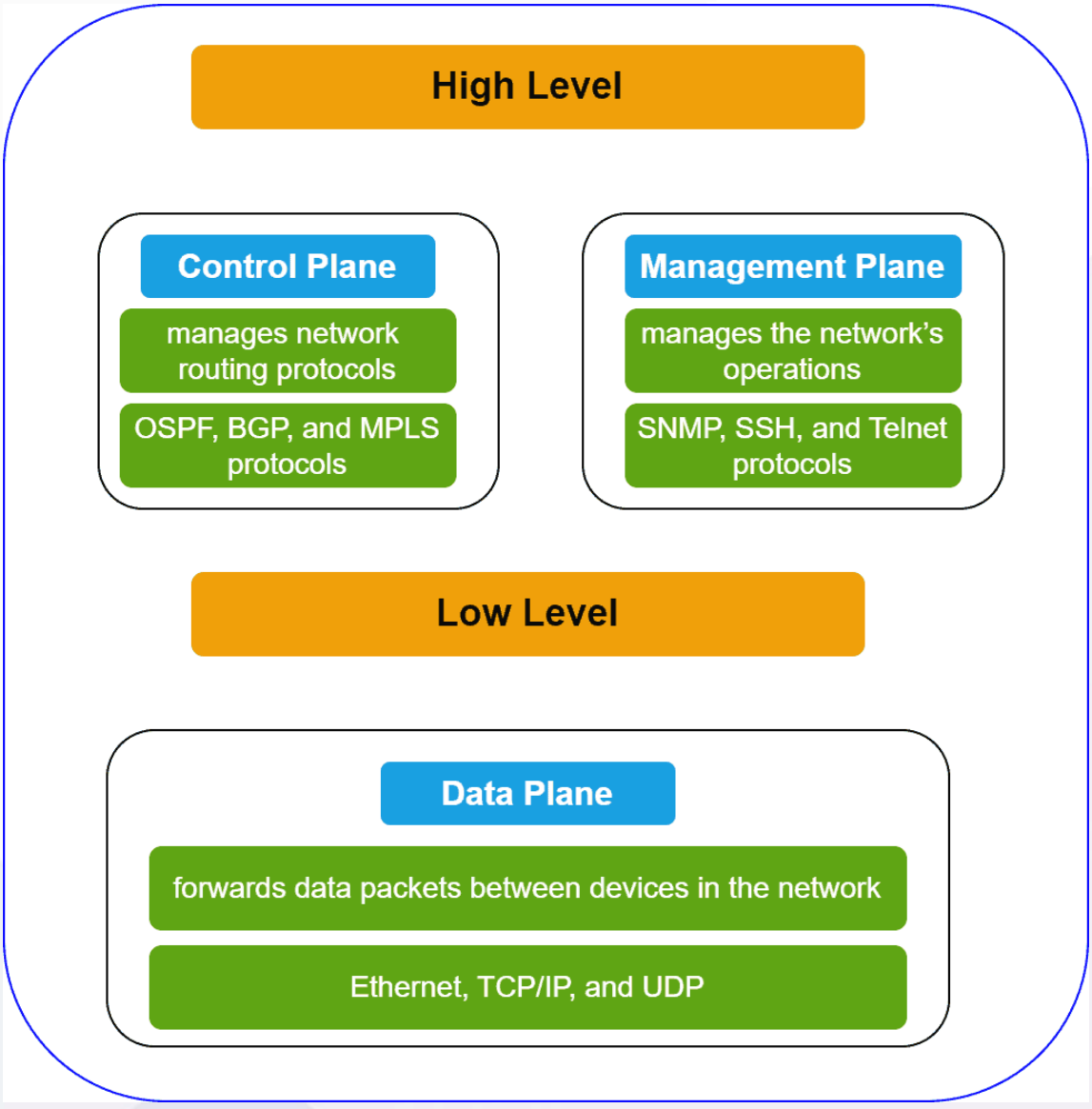
- Beacon generation sends periodic signals to announce the network
- Probe request/response handles device discovery and network scanning
- Authentication manages initial security checks for joining devices
- Association establishes a connection between client and access point
- Deauthentication/disassociation ends connections cleanly when needed
- Timing synchronization keeps all devices on the same clock
- Power save polling supports devices in sleep mode to wake for data
- Channel switching adjusts frequencies to avoid interference

Control Plane:

- Request to send (RTS) signals intent to transmit, reducing collisions
- Clear to send (CTS) grants permission to proceed with data
- Acknowledgment (ACK) confirms successful frame reception
- Block acknowledgment (Block ACK) groups confirmations for efficiency
- Contention window management sets wait times to avoid clashes
- Power save mode coordination lets devices sleep and wake smartly
- Request for power save multi-poll (RPSM) optimizes sleep schedules
- Frame fragmentation splits large data into manageable pieces

Data Plane:

- Frame transmission sends actual user data over the air
- Frame reception captures and processes incoming data
- Error detection checks for corruption using FCS (Frame Check Sequence)
- Retry mechanism resends failed frames to ensure delivery
- Frame aggregation combines multiple frames to boost speed
- QoS scheduling prioritizes traffic like video over regular data
- Encryption/decryption secures data with protocols like WPA3
- Rate adaptation adjusts speed based on signal quality



Qn 4:

Explain the scanning process and its types in detail

Scanning:

- Scanning is the process where a Wi-Fi client searches for available networks to connect
- The client starts by listening for beacon frames sent by access points
- It can also send probe requests to actively ask for network info
- The device collects responses with details like SSID, signal strength, and channel
- It ranks the options based on signal quality and security settings
- Finally, it picks the best network and begins the association process

Types of Scanning:

- **Passive scanning** involves listening quietly for beacon frames from access points
    - It saves power as the client doesn't transmit anything
- **Active scanning** means sending probe requests to force responses from APs
    - It's faster but uses more battery and can cause more network traffic
- Hybrid scanning mixes both, starting passive then switching to active if needed

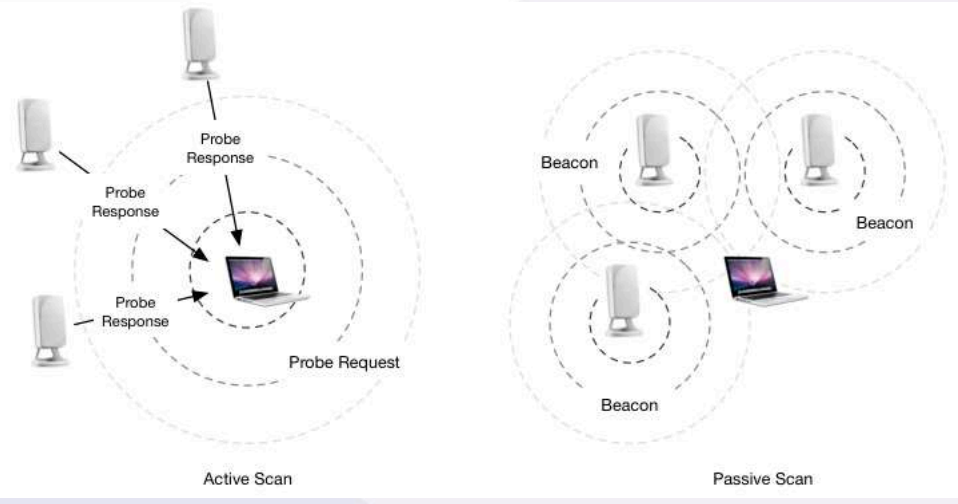
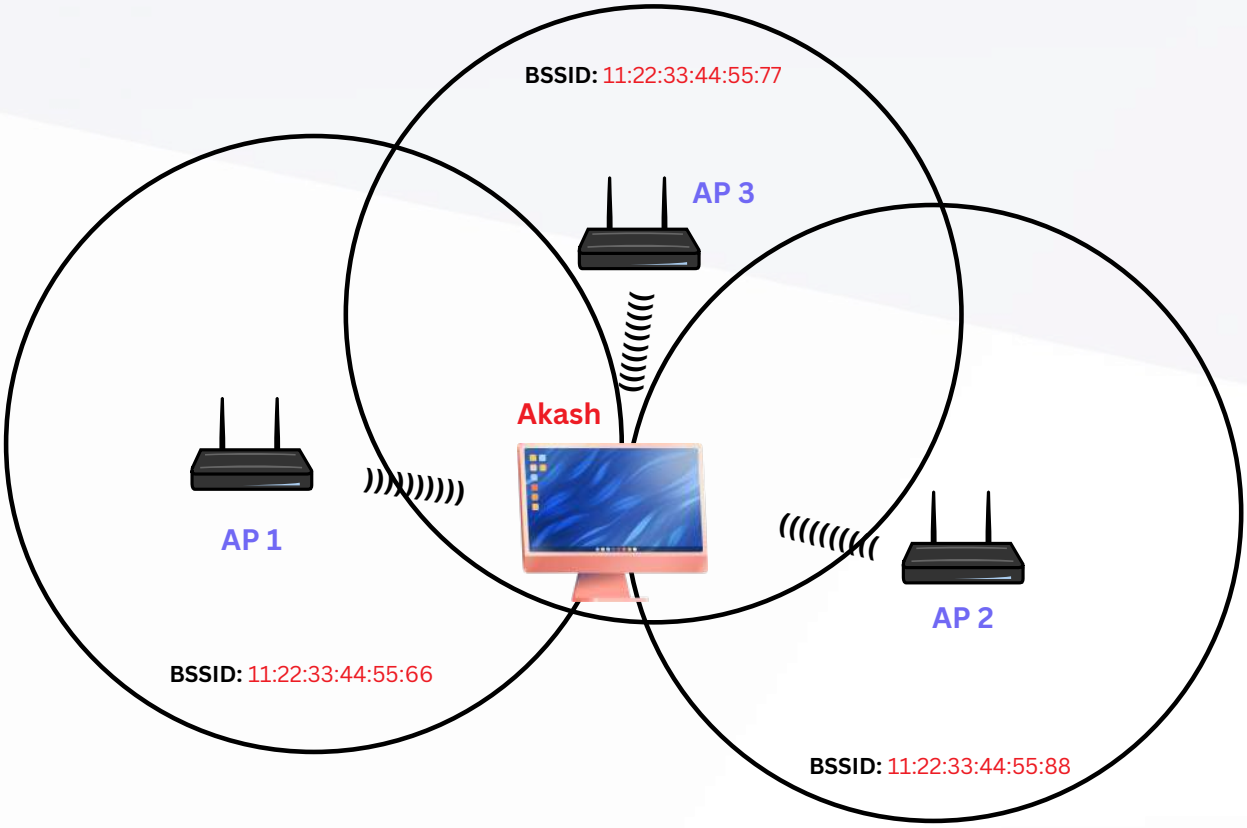
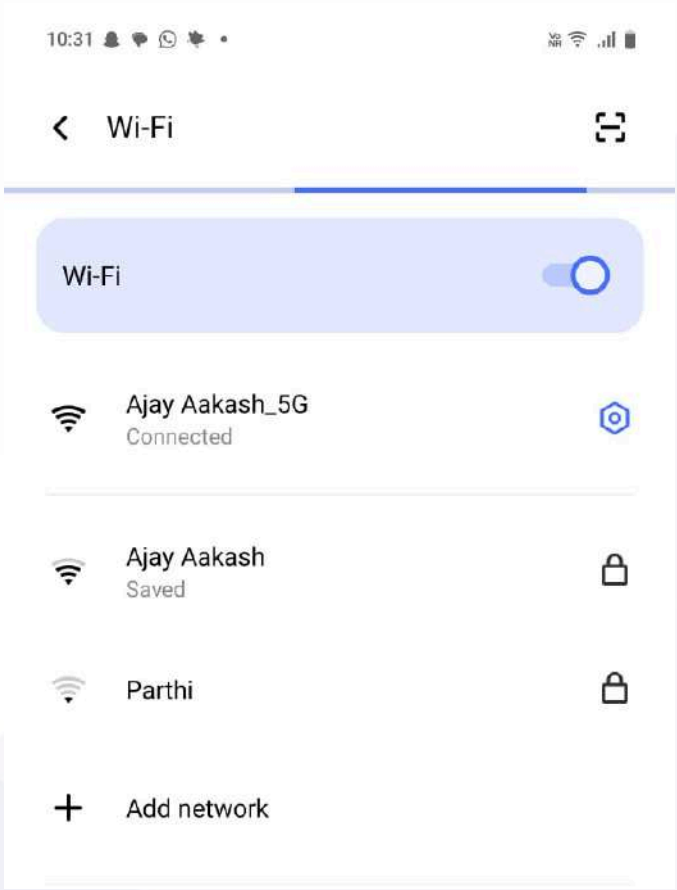


Illustration:



Scanning in Akash's device:



Qn 5:

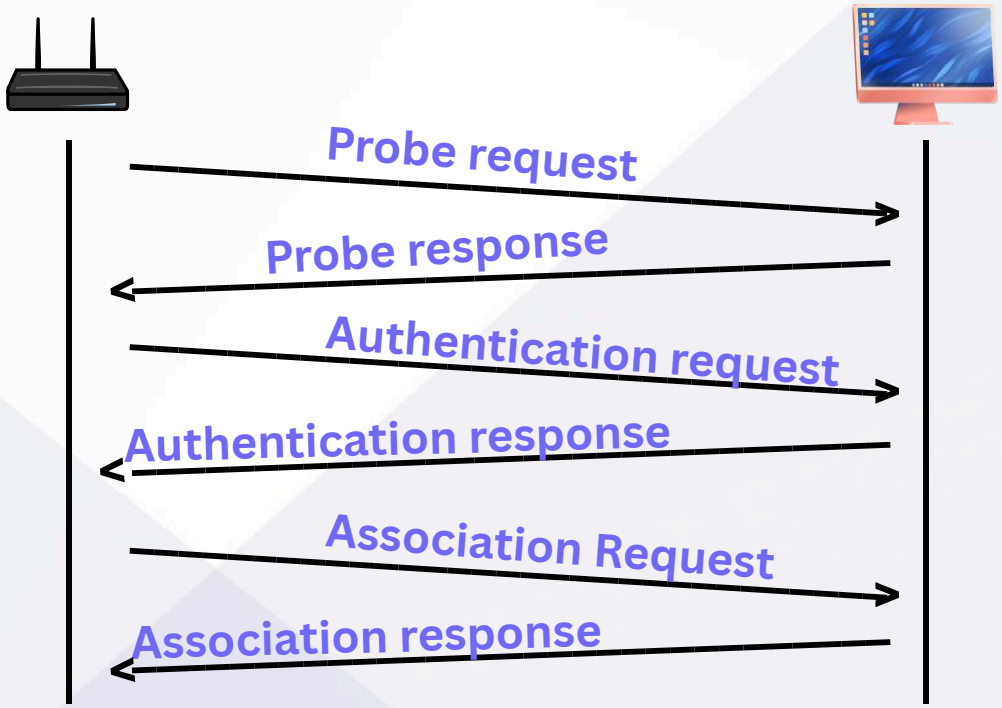
Brief about the client association process

Client Association Process:

- Client association is the handshake that lets a device join a Wi-Fi network
- It’s the moment a laptop or phone officially links to an access point
- The client sends an association request to the chosen access point
- The request includes supported data rates and security capabilities
- The access point checks the request and decides if the client fits
- If approved, the access point sends an association response with an AID
- The AID is a unique ID for the client within the network
- The process wraps up with the client ready to exchange data

Security & Authentication:

- Before association, authentication verifies the client’s identity
- This often involves WPA2 or WPA3 protocols
- Keys are exchanged to encrypt future communications



Qn 6:

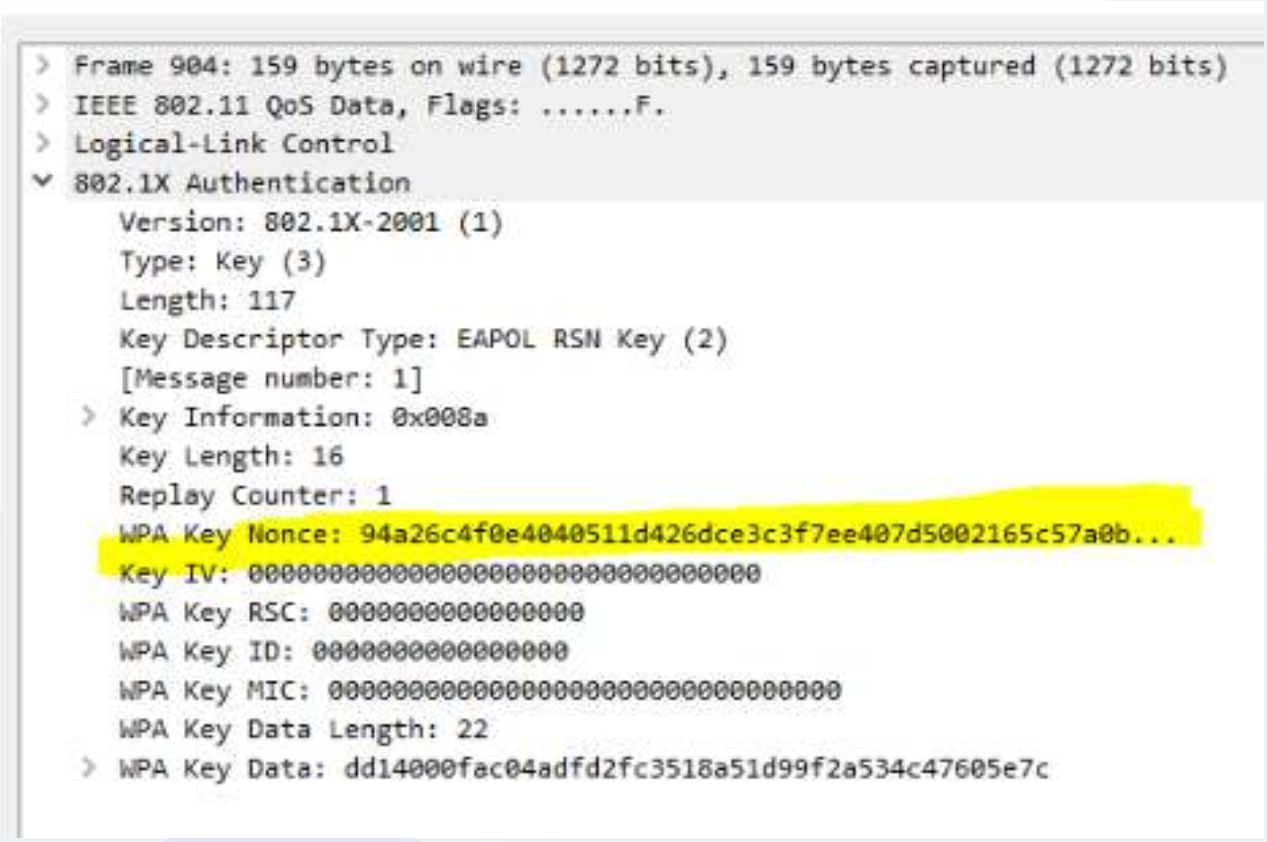
Explain each step involved in EAPOL 4-way handshake and the purpose of each key derived from the process

EAPOL 4-way Handshake:

- The EAPOL 4-way handshake is a security process to confirm a client and access point share the same key
- It happens after authentication to set up encryption for Wi-Fi
- EAPOL - **Extensible Authentication Protocol over LAN** (EAPOL)

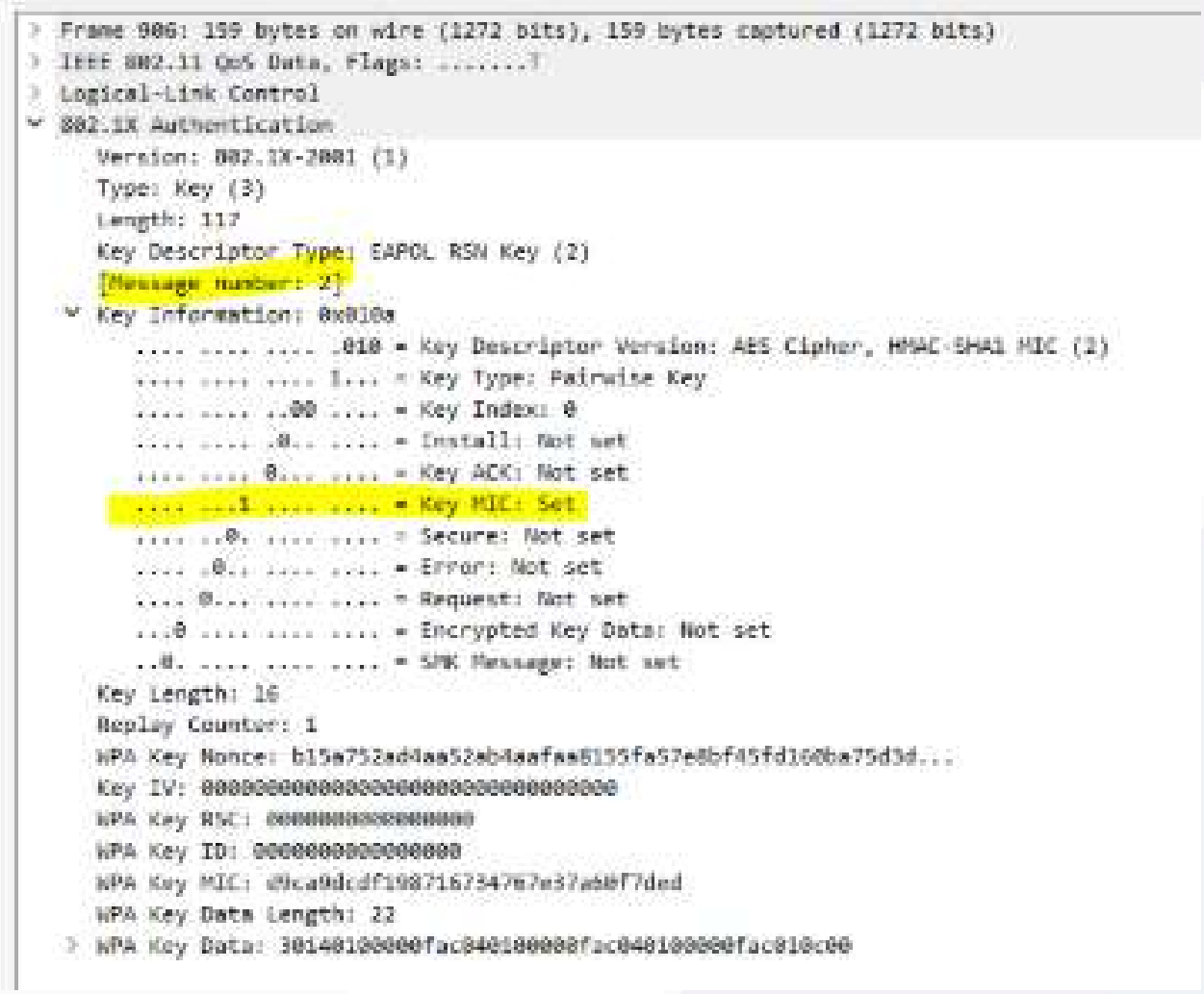
Step 1: Message 1 from AP

- The access point sends a nonce to the client
- This nonce is a random number used once to start the key exchange
- It includes the access point's MAC address for identification
- The message kicks off the handshake process
- It sets the stage for mutual authentication



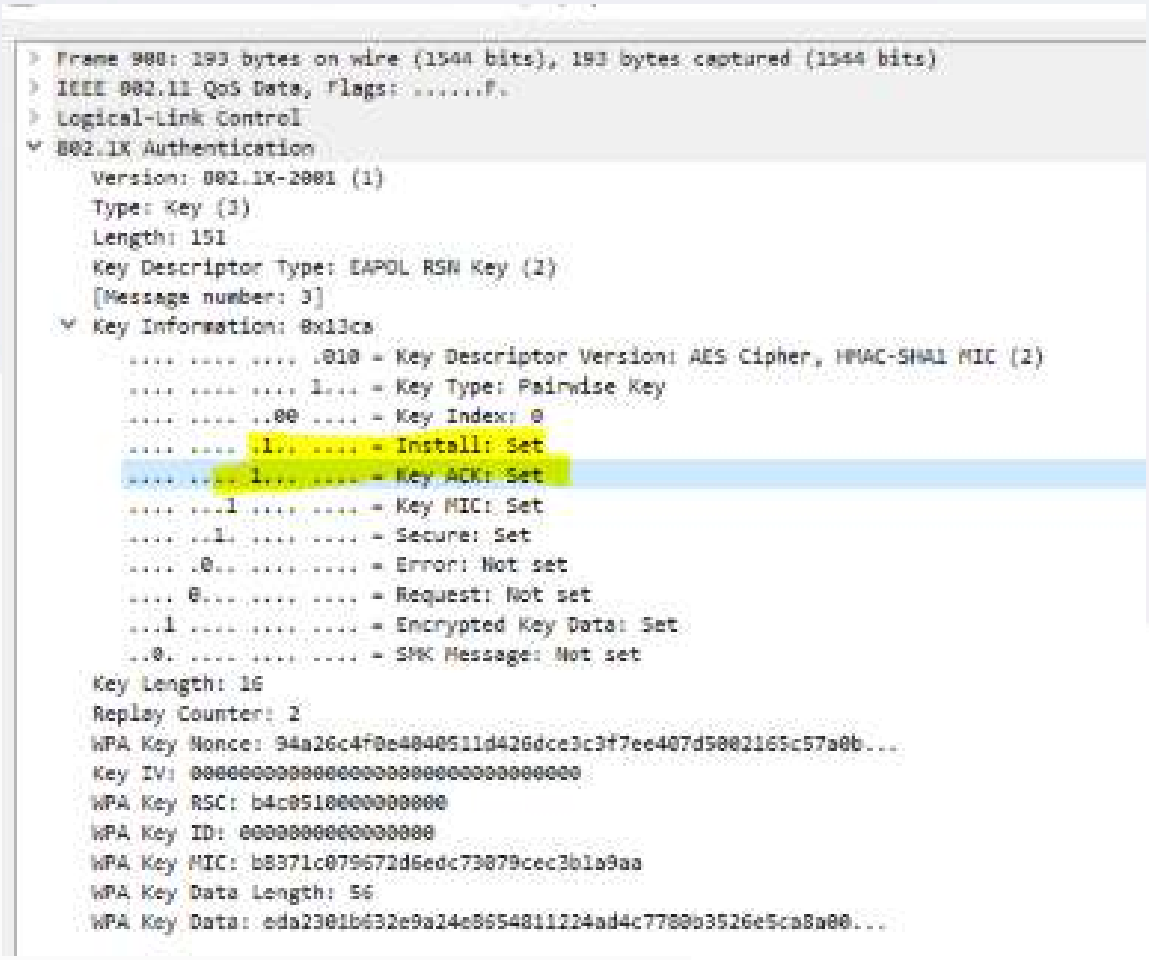
Step 2: Message 2 from Client

- The client responds with its own nonce and a message integrity code
- The MIC verifies the message hasn't been tampered with
- It includes the client's MAC address for verification
- The client also sends its group key handshake version
- This step proves the client holds the right credentials



Step 3: Message 3 from AP:

- The access point sends the group temporal key encrypted with the pairwise key
- It includes another MIC to ensure message integrity
- The access point confirms its identity with the client
- It signals the client to start using the new keys



Step 4: Message 4 from Client:

- The client acknowledges receipt with a final MIC
- It confirms the keys are installed and ready
- The client switches to the new encryption settings
- This completes the handshake process
- Both sides are now secure for data exchange

Keys:

- **Pairwise Master Key (PMK)** serves as the base key from the authentication phase
- **Pairwise Transient Key (PTK)** encrypts data between client and access point
- **Group Temporal Key (GTK)** secures multicast and broadcast traffic

Qn 7:

Describe the power saving scheme in MAC layer and explore on the types of Power saving mechanisms

Power Saving in MAC:

- The MAC layer includes a power saving scheme to help devices use less energy
- It's designed for battery-powered devices like phones or laptops
- The goal is to keep the device connected while saving power
- This scheme balances performance with energy efficiency
- It's a key feature for extending device battery life

How PS works:

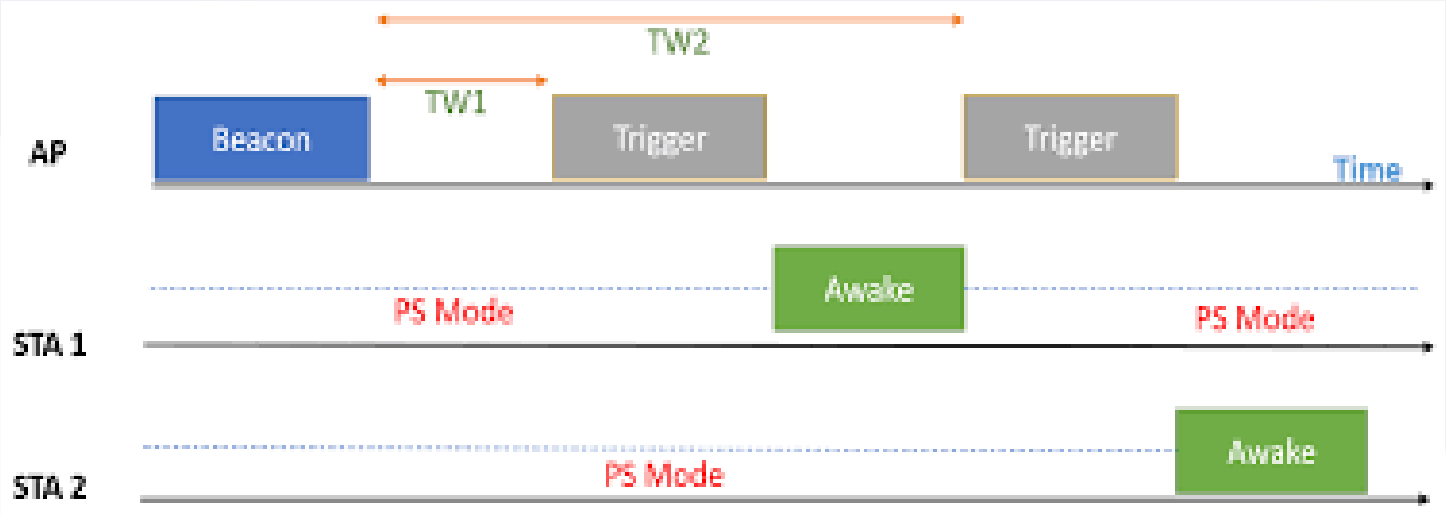
- Devices enter a sleep mode when not actively sending or receiving data
- The AP buffers data for sleeping devices
- Devices wake up at set intervals to check for buffered data
    - If there's data waiting, the device stays awake to receive it
    - If not, it goes back to sleep to save energy

Types:

- Power Saving Mode (PSM)
- Unscheduled Automatic Power Save Delivery (U-APSD)
- Targeted Wake Time (TWT)

1: Power Saving Mode (PSM):

- PSM lets a device tell the access point it's going to sleep
- The device sends a frame with a power management bit set to 1
- The AP then holds onto any data for that device
- The device wakes up periodically to listen for beacon frames
- Beacons include a Traffic Indication Map to show if data is waiting



2: Unscheduled Automatic Power Save Delivery (U-APSD)

- U-APSD allows devices to wake up on their own schedule
- The device triggers the AP to send buffered data
- It sends a special frame to request the data immediately
- This reduces wait time compared to PSM
- It’s great for real-time apps like voice or video calls
- U-APSD improves responsiveness while saving power

3: Target Wake Time (TWT)

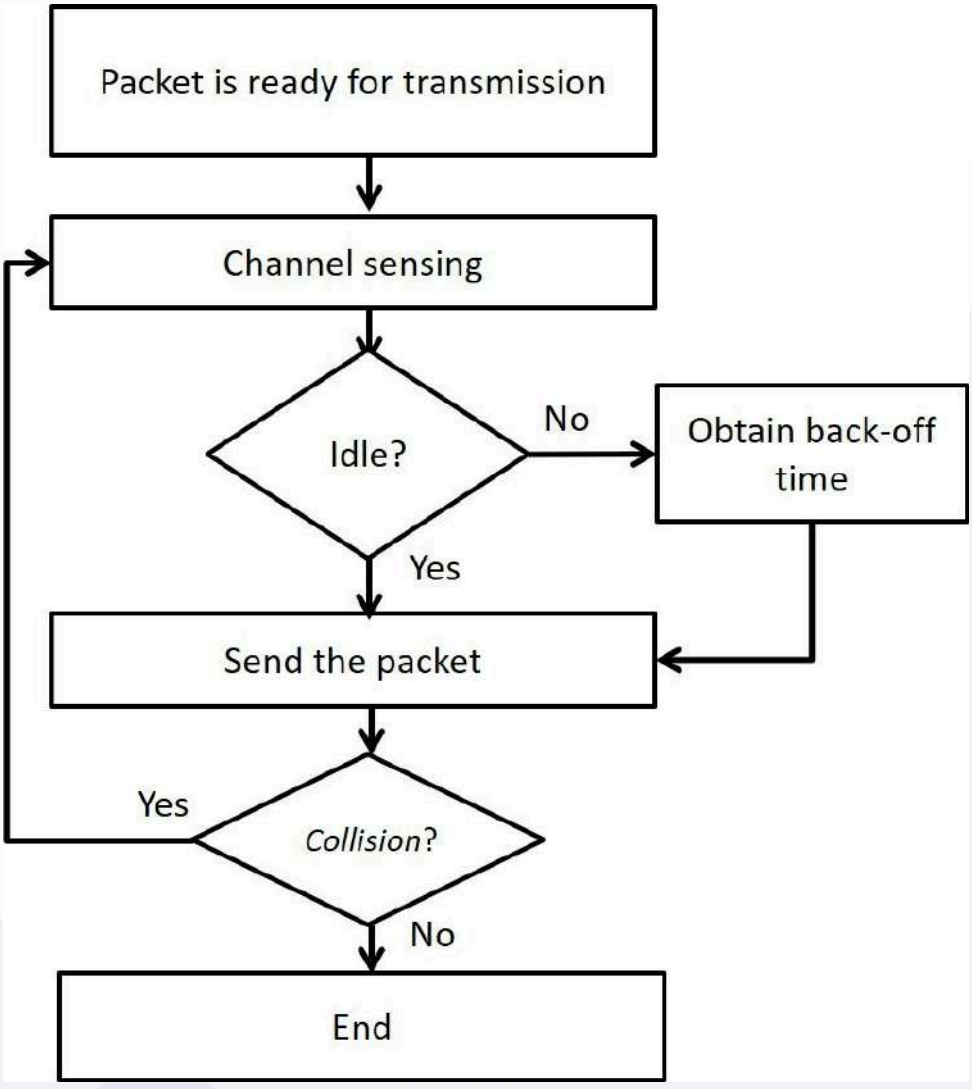
- TWT schedules specific times for devices to wake up
- The device AP agree on wake-up intervals
- This cuts down on unnecessary wake-ups and collisions
- It’s perfect for IoT devices that send small, periodic updates
- TWT also reduces network congestion in busy areas

Qn 8:

Describe the Medium Access Control methodologies

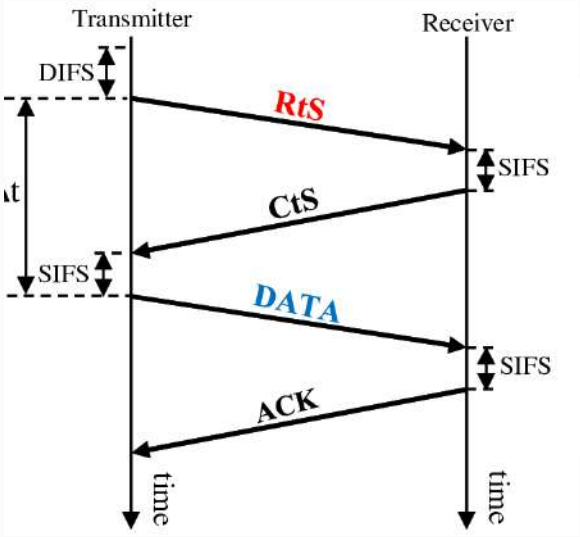
CSMA/CA:

- Carrier Sense Multiple Access with Collision Avoidance is the main method in Wi-Fi
- Devices listen to the channel before transmitting to check if it's busy
- If the channel is clear, they wait a random time before sending data
- This random wait reduces the chance of two devices starting at the same time
- If a collision still happens, devices back off and retry late



RTS/CTS:

- Request to Send and Clear to Send is an optional add-on to CSMA/CA
- A device sends an RTS frame to ask for permission to transmit
- The access point replies with a CTS frame to approve the request
- This clears the channel for that device, avoiding hidden node issues
- It's useful in crowded networks with many devices



Distributed Coordination Function (DCF):

- DCF is the foundation of CSMA/CA in Wi-Fi networks
- It uses a contention window to set random wait times for devices
- Each device picks a slot within this window to avoid clashes
- If the channel gets busy, the window size grows to reduce conflicts

Enhancements with EDCA:

- EDCA - **Enhanced Distributed Channel Access**
- EDCA improves on DCF for better performance
- It prioritizes traffic like voice or video over regular data
- Different queues are set up for different types of traffic
- High-priority queues get shorter wait times to go first

Qn 9:

Brief about the Block ACK mechanism and its advantages

Block ACK:

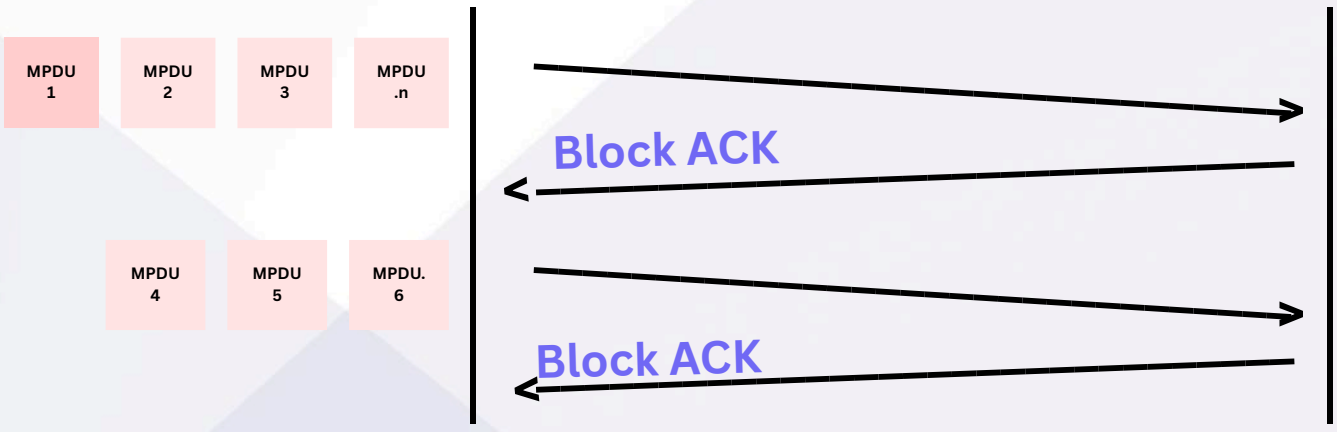
- Block ACK mechanism allows devices to confirm multiple frames at once
- It’s a Wi-Fi feature to make data transfer more efficient
- Instead of acknowledging each frame, it groups them together
- This reduces the back-and-forth chatter on the network
- It’s commonly used in modern Wi-Fi standards like 802.11n

How Block ACK works:

- The sender transmits a burst of frames in one go
- The receiver gets all frames and checks them for errors
- It sends a single Block ACK frame back to the sender
- The Block ACK lists which frames were received correctly
- If some frames fail, the sender retransmits only those
- This process happens quickly to keep data flowing

Advantages:

- Speed is increased
- Less number of ACK - so less chance of collision
- To improve overall throughput
- Mainly useful for video streaming applications

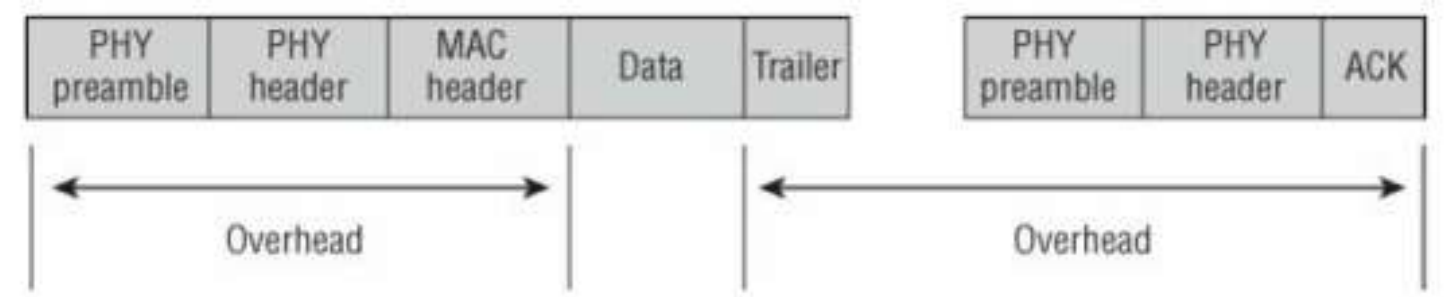


Qn 10:

Explain about A-MSDU, A-MPDU, and A-MSDU in A-MPDU

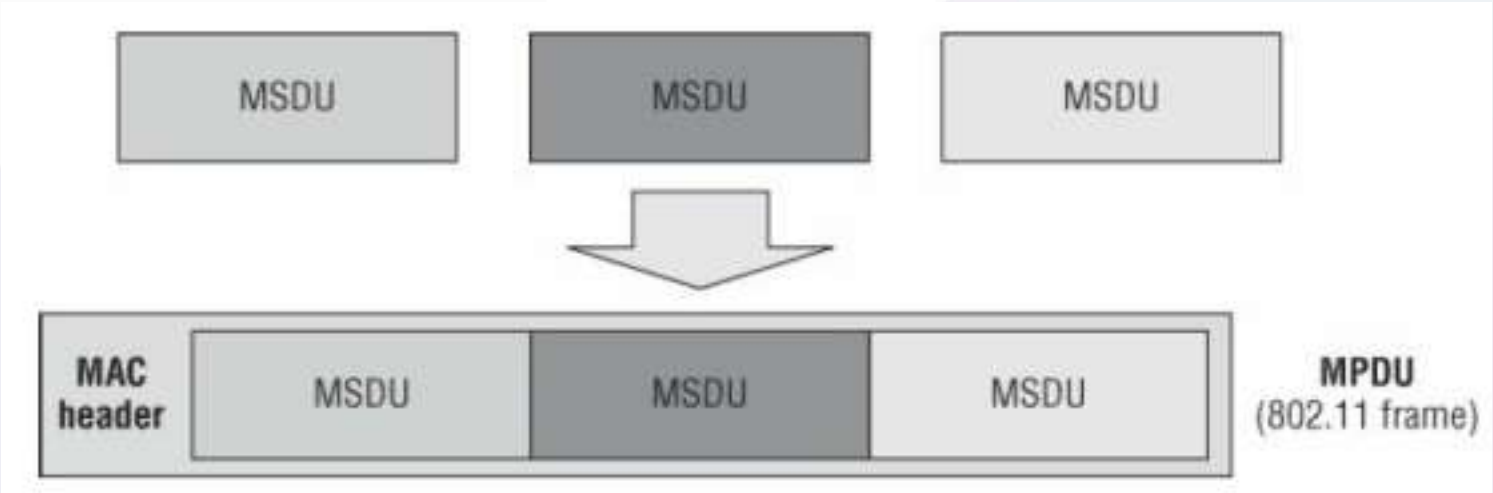
Overhead:

- Each frame will have separate header which will add Overhead
- So, combining them and having a single header will be efficient



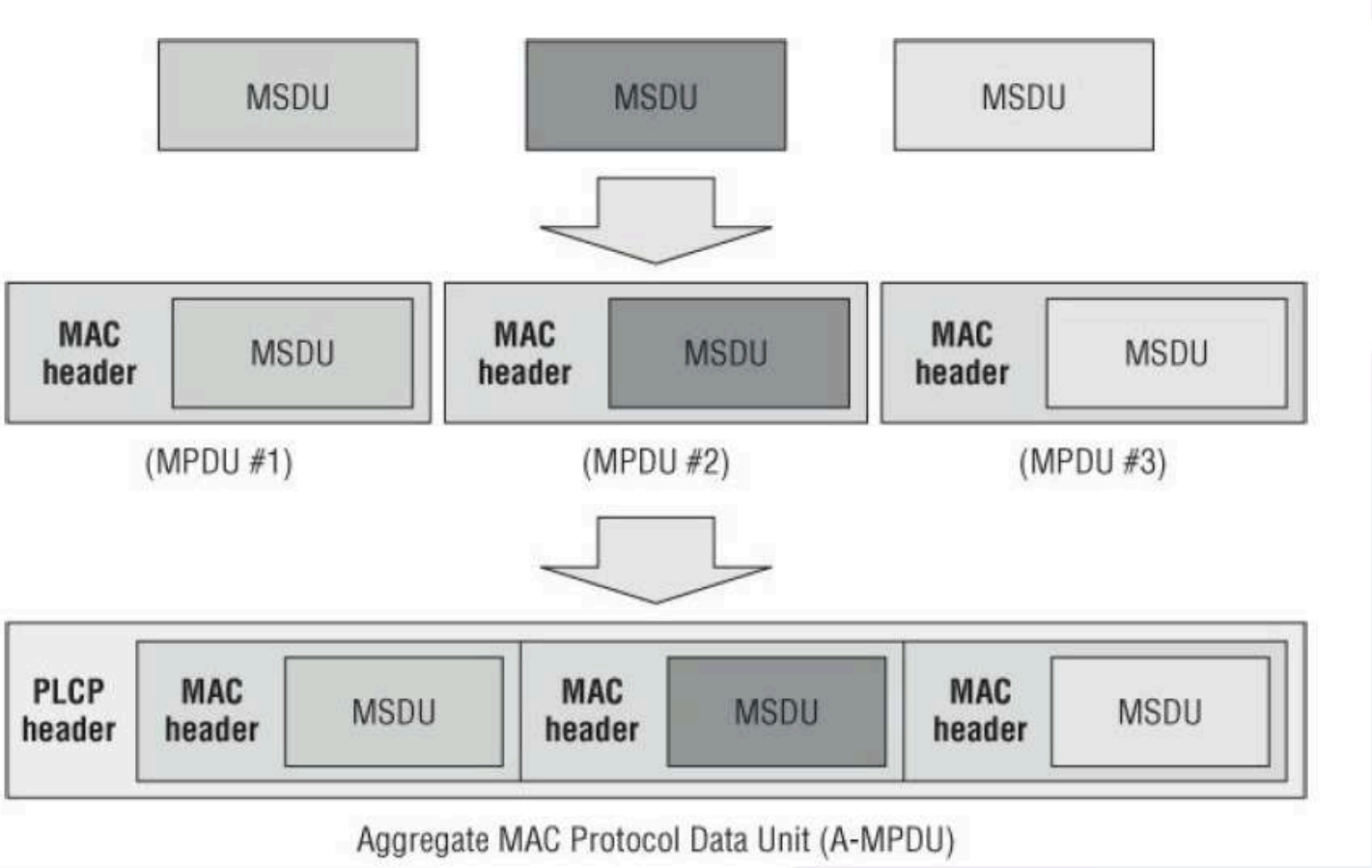
AMSDU:

- AMSDU - **Aggregated MAC Service Data Unit**
- It combines multiple data packets into one larger frame
- This happens before adding the MAC header
- Each packet shares a single header to save space
- It reduces overhead for small packets
- AMSDU is great for boosting efficiency



AMPDU:

- AMPDU - **Aggregated MAC Protocol Data Unit**
- It groups multiple frames that already have their own MAC headers
- Each frame gets its own error-checking field
- This allows individual frame retransmission if errors occur
- AMPDU supports higher throughput in noisy environments



AMSDU in AMPDU:

- A-MSDU in A-MPDU mixes both aggregation methods
- First, small packets are packed into an A-MSDU
- Then, multiple A-MSDUs are bundled into an A-MPDU
- This double aggregation maximizes data per transmission

THE END

AKASH S