WIFI Training Program

Module 4 – Assignment Questions

1. What is the significance of MAC layer and in which position it is placed in the OSI model
2. Describe the frame format of the 802.11 MAC header and explain the purpose of each field
3. Please list all the MAC layer functionalities in all Management, Control and Data plane
4. Explain the scanning process and its types in detail
5. Brief about the client association process
6. Explain each steps involved in EAPOL 4-way handshake and the purpose of each keys derived from the process
7. Describe the power saving scheme in MAC layer and explore on the types of Power saving mechanisms
8. Describe the Medium Access Control methodologies
9. Brief about the Block ACK mechanism and its advantages
10. Explain about A-MSDU, A-MPDU and A-MSDU in A-MPDU

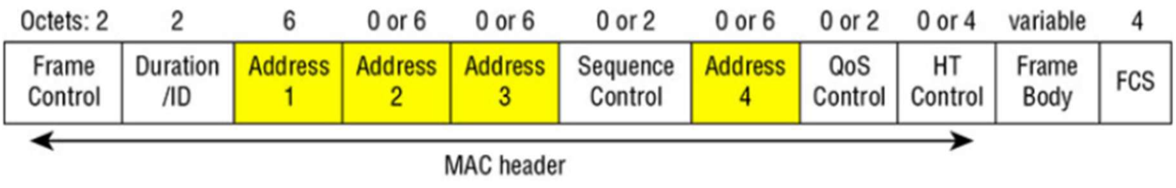
Q2) Describe the frame format of the 802.11 MAC header and explain the purpose of each field

he IEEE 802.11 MAC header is a crucial component of wireless frames. It contains control information required for delivering the data between wireless devices. The MAC header is located between the Physical Layer header and the frame body.

General Structure of the IEEE 802.11 MAC Header

The standard MAC header is typically 24 bytes in length, but it may extend up to 30 or more bytes depending on the type of frame and included optional fields (e.g., QoS control, HT control).

Field Name	**Size (Bytes)**	**Description**
Frame Control	2	Contains control information such as frame type, subtype, flags (To DS, From DS, Retry, etc.)
Duration/ID	2	Specifies the time (in microseconds) the channel is reserved or contains an association ID during PS-Poll frames
Address 1	6	Usually the receiver address (RA)
Address 2	6	Usually the transmitter address (TA)
Address 3	6	Varies based on frame type; can be the BSSID, source, or destination
Sequence Control	2	Contains sequence number and fragment number for frame reassembly
[Optional] Address 4	6	Used in wireless distribution systems (WDS) when both To DS and From DS bits are set
[Optional] QoS Control	2	Used in QoS data frames to identify traffic category and other parameters
[Optional] HT Control	4	Present in high-throughput (802.11n and later) frames to support MIMO and beamforming



Octets: 2	2	6	0 or 6	0 or 6	0 or 2	0 or 6	0 or 2	0 or 4	variable	4
Frame Control	Duration /ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QoS Control	HT Control	Frame Body	FCS

Q3) Please list all the MAC layer functionalities in all Management, Control and Data plane

MAC is located in layer – 2 and its significance is as follows,

MAC Layer Functionalities – Management Plane

These functionalities handle network setup, association, and maintenance.

Function	**Description**
Scanning	The station scans available channels to discover access points (APs). This can be done passively (listening for beacons) or actively (sending probe requests).
Client Association	The process of establishing a connection between a client (STA) and an AP. It includes authentication, association, and re-association.
Security Management	Handles encryption key exchange, authentication mechanisms, and protection of data. This includes WPA2/WPA3, EAPOL 4-way handshake, and related protocols.
QoS Management	Supports quality of service by prioritizing traffic types (voice, video, best-effort, background), enabling efficient multimedia and real-time application performance.
Power Management	Allows stations to enter low-power states when inactive and schedule wake-up times to conserve energy (e.g., TWT – Target Wake Time).
Load Balancing	Helps distribute clients across multiple APs or frequency bands to optimize performance and avoid congestion.

MAC Layer Functionalities – Control Plane

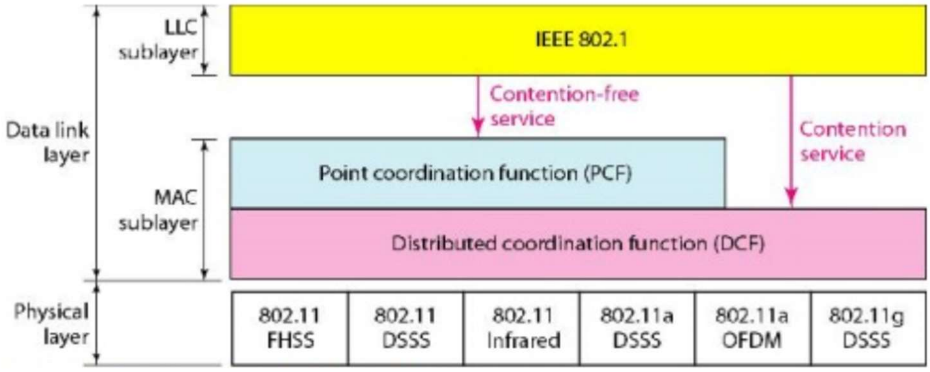
These functionalities are responsible for managing access to the wireless medium and regulating data flow.

Function	**Description**
Flow Control	Ensures that the sender does not overwhelm the receiver by managing the rate of data transmission.
Medium Access Control	Coordinates which device can access the medium to avoid collisions. In Wi-Fi, this includes CSMA/CA, RTS/CTS, interframe spaces, etc.

MAC Layer Functionalities – Data Plane

These functionalities handle the actual transmission and aggregation of user data.

Function	Description
AMSDU (Aggregate MSDU)	Aggregates multiple MAC Service Data Units into a single MAC frame to reduce overhead.
AMPDU (Aggregate MPDU)	Aggregates multiple MAC Protocol Data Units into a single transmission burst to improve throughput.
AMSDU in AMPDU	Combines both AMSDU and AMPDU techniques, allowing nested aggregation to further optimize performance.



Q4) Scanning Process and Its Types in IEEE 802.11

Passive Scanning

Definition:
In passive scanning, the STA listens to beacon frames that are periodically transmitted by APs on each channel.

Procedure:

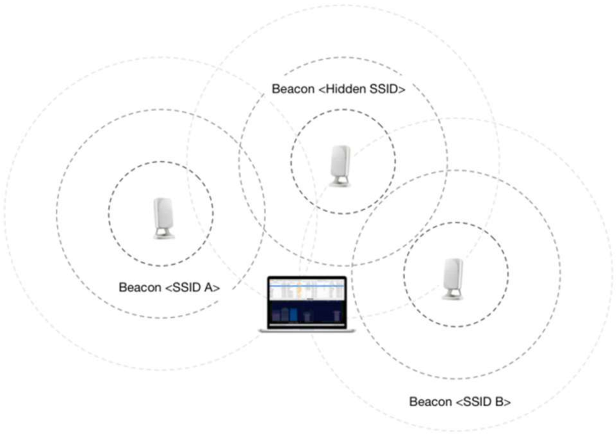
- The STA tunes its radio to a specific channel.
- It waits to receive beacon frames sent by APs (typically every 100 ms).
- It extracts information from the beacon such as:
  - SSID
  - BSSID (MAC address of the AP)
  - Supported rates
  - Channel
  - Security capabilities
- The STA repeats this on all channels defined in its regulatory domain.

Advantages:

- Low power consumption (STA is just listening).
- No active transmission required (useful in power-saving or restricted environments).

Disadvantages:

- Slower scanning (must wait for each AP to send a beacon).
- May miss APs with long beacon intervals or weak signals.



Passive Scan Mode

Active Scanning

Definition:
In active scanning, the STA actively sends probe request frames and waits for probe responses from APs.

Procedure:

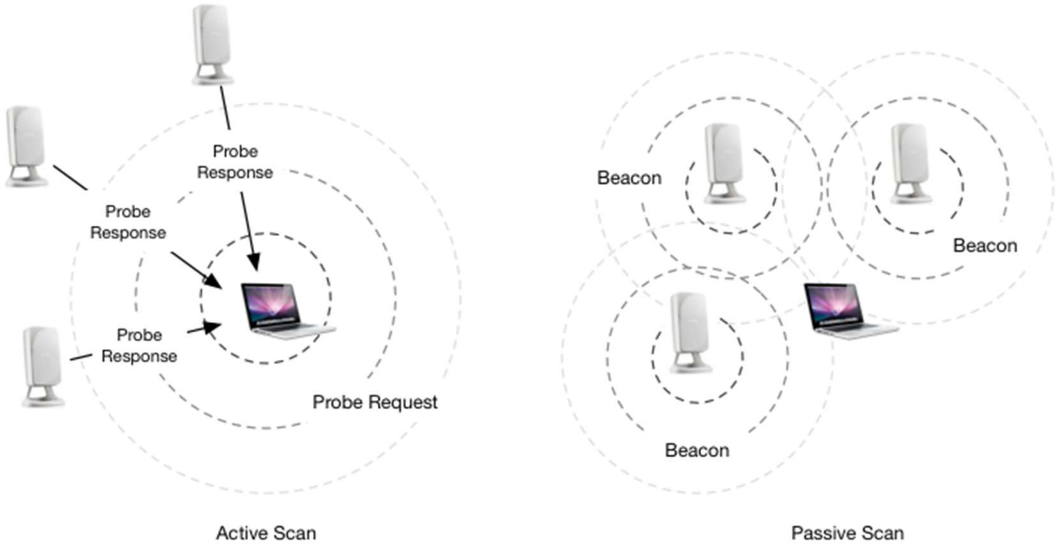
- The STA selects a channel and sends a broadcast (or directed) **probe request**.
- All APs on that channel respond with a **probe response** containing:
  - SSID
  - BSSID
  - Capabilities
  - Supported rates
  - Channel
  - Security features
- The STA collects responses and moves to the next channel.

Advantages:

- Faster discovery of APs (doesn't wait for periodic beacons).
- Can discover hidden SSIDs if probe requests are directed.

Disadvantages:

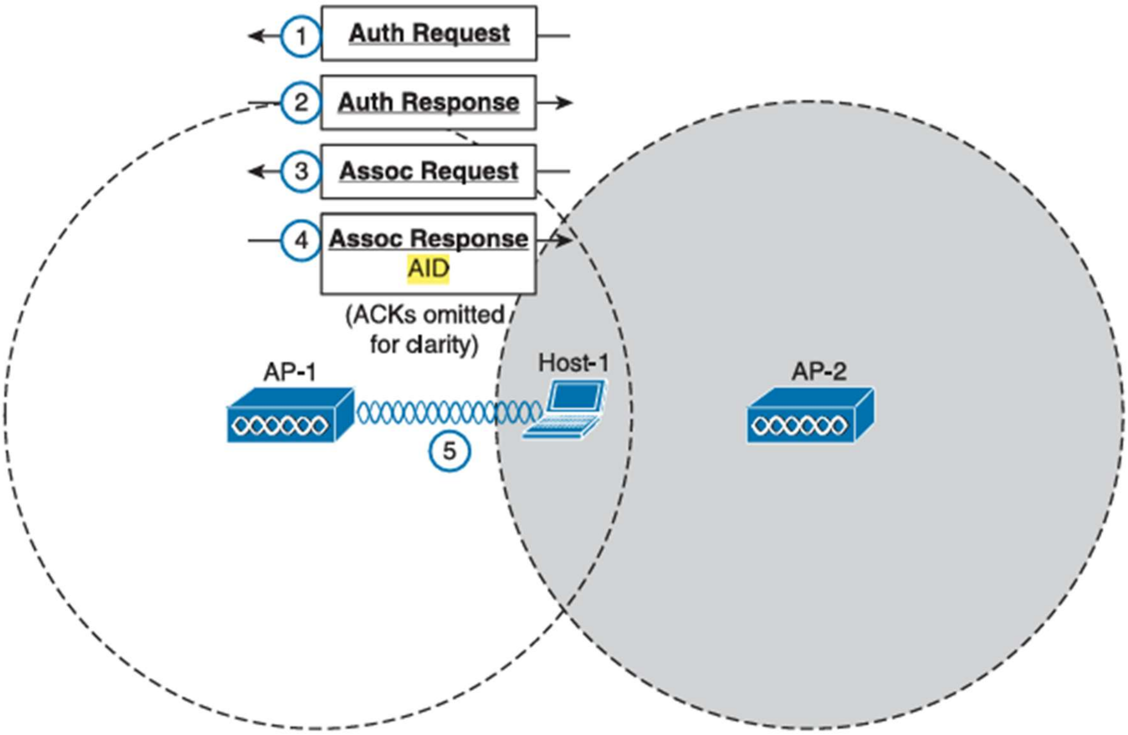
- More power-intensive (due to frame transmission).
- Generates additional traffic in the wireless medium.



Active Scan

Passive Scan

Q5) Brief about the client association process



Steps in the Client Association Process:

1. Scanning

The STA discovers available APs in its vicinity using either:

- **Passive scanning**: Listening for beacon frames.
- **Active scanning**: Sending probe requests and receiving probe responses.

→ Output: List of nearby APs with details like SSID, BSSID, signal strength, supported capabilities.

2. Authentication (Open or Shared Key)

Before joining the network, the STA must authenticate itself to the AP.

- **Open System Authentication** (most common):
  - Two-frame exchange with no real authentication (used with WPA2/WPA3).
- **Shared Key Authentication** (deprecated):
  - Uses WEP encryption (no longer secure or commonly used).

→ Output: If successful, STA is considered authenticated.

3. Association

After successful authentication, the STA sends an **Association Request frame** to the AP. This frame includes:

- STA capabilities (QoS, HT support, etc.)
- SSID
- Supported data rates

The AP responds with an **Association Response frame**:

- Status code (success/failure)
- Association ID (AID) assigned to the STA
- Supported capabilities of the AP

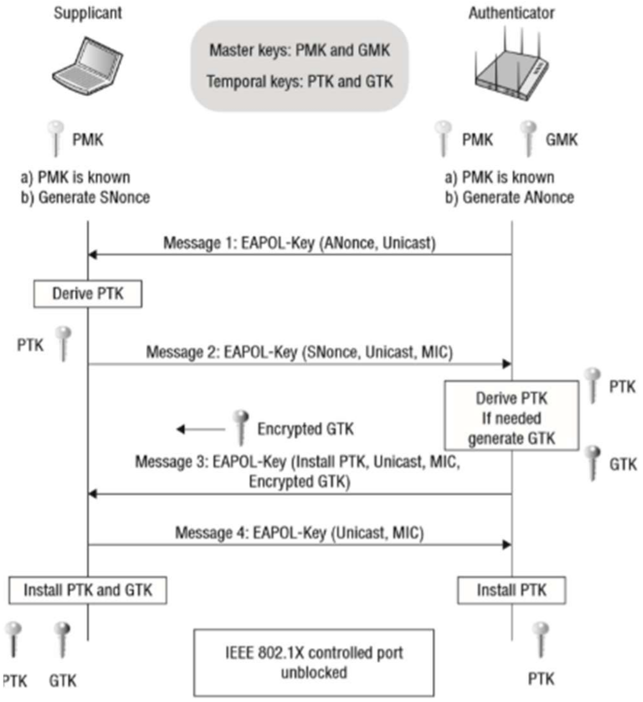
→ Output: STA becomes part of the Basic Service Set (BSS) and can start data communication.

```
 STA                   AP
|                      |
| -- Probe Request ---> |
| <-- Probe Response -- |
| -- Authentication -->  |
| <-- Auth Response ---  |
| -- Assoc Request ----> |
| <-- Assoc Response -- |
```

Key Points:

- The STA must complete both **authentication** and **association** to join a network.
- After association, encryption keys may be established via mechanisms like the **EAPOL 4-Way Handshake** (for WPA2/WPA3).
- Association can be **reinitiated** during roaming or if connection parameters change.

Q6) Explain each step involved in EAPOL 4-way handshake and the purpose of each keys derived from the process


Supplicant
Authenticator
Master keys: PMK and GMK
Temporal keys: PTK and GTK
PMK
PMK
GMK
a) PMK is known
b) Generate SNonce
a) PMK is known
b) Generate ANonce
Message 1: EAPOL-Key (ANonce, Unicast)
Derive PTK
PTK
Message 2: EAPOL-Key (SNonce, Unicast, MIC)
PTK
Derive PTK
If needed
generate GTK
Encrypted GTK
GTK
Message 3: EAPOL-Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key (Unicast, MIC)
Install PTK and GTK
Install PTK
PTK
GTK
IEEE 802.1X controlled port unblocked
PTK

The **EAPOL 4-Way Handshake** is a crucial part of the WPA2/WPA3 security protocol used in Wi-Fi networks. It occurs between a client station (STA) and an access point (AP) after the initial authentication phase (e.g., via 802.1X or PSK). The handshake ensures both parties share a secret encryption key and can establish a secure communication channel.

Keys Involved

Key	**Description**
PMK (Pairwise Master Key)	The master key derived during authentication (via PSK or 802.1X). Shared by both STA and AP.
PTK (Pairwise Transient Key)	Derived from PMK and used for unicast encryption between STA and AP.
GTK (Group Temporal Key)	Shared key used by AP for sending multicast/broadcast traffic.
ANonce / SNonce	Random numbers (nonces) generated by AP and STA, respectively.

Steps:

Message 1: AP → STA

- AP sends a **Nonce (ANonce)** and other parameters (e.g., replay counter).
- The STA now has all inputs needed to derive the PTK:
    - Inputs: PMK, ANonce, SNonce (its own), AP MAC, STA MAC.

Message 2: STA → AP

- STA generates its **SNonce** and computes the **PTK**.
- Sends the **SNonce** to the AP in an encrypted EAPOL frame.
- Optionally includes a Message Integrity Code (MIC) to prove knowledge of the PTK.

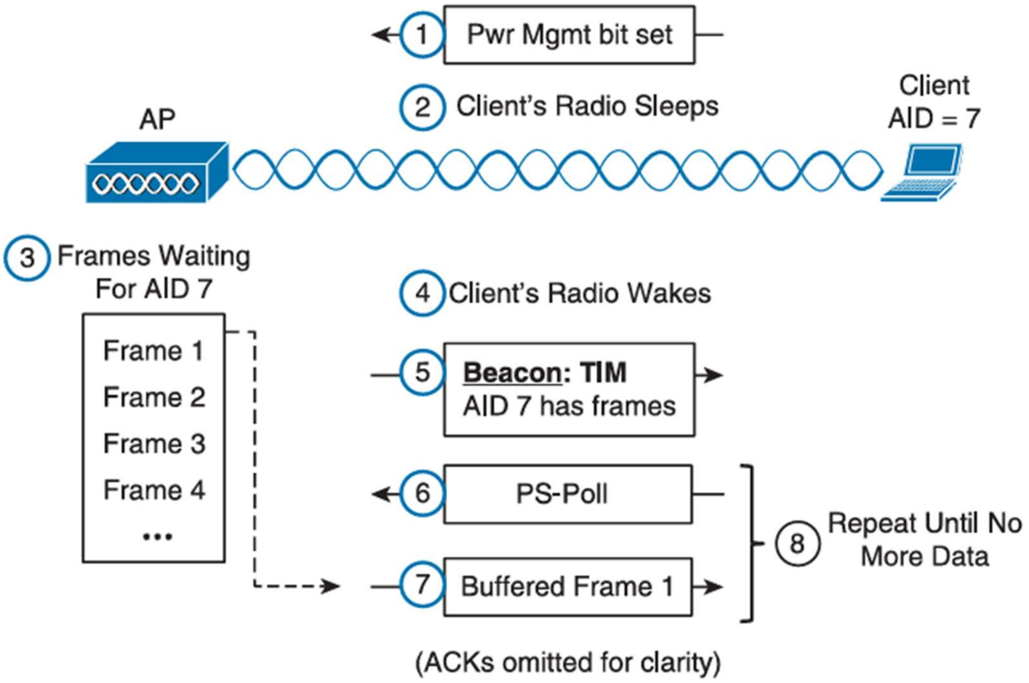
Message 3: AP → STA

- AP also derives the same PTK.
- Sends:
    - A message containing **GTK** (encrypted using PTK)
    - A **MIC** to validate authenticity
    - Installation instruction for keys (PTK and GTK)

Message 4: STA → AP

- STA confirms successful installation of keys by sending a final acknowledgment frame with a MIC.

Q7) Describe the power saving scheme in MAC layer and explore on the types of Power saving mechanisms



MAC-Level Power Save Mechanism (Legacy Power Save Mode)

1. Power Management Bit

Each frame from an STA contains a 1-bit Power Management flag:

- Set to 0: STA is in active mode.
- Set to 1: STA is in power-save mode (dozing when idle).

2. Beacon Monitoring

- AP periodically transmits beacon frames (typically every 100 ms).
- Beacon includes a Traffic Indication Map (TIM):
  - TIM indicates which STAs have buffered unicast data.
  - A DTIM (Delivery TIM) indicates upcoming multicast/broadcast traffic.

3. PS-Poll Frame

- If the STA sees its AID in the TIM bitmap, it sends a **PS-Poll** frame to the AP.
- The AP responds by delivering the buffered frame.
- Multiple frames may be sent, depending on the delivery process.

Power Saving Mechanism	Description
1. Legacy Power Save Mode	STA sleeps between beacon intervals, wakes to read TIM, and uses PS-Poll for data retrieval.
2. U-APSD (Unscheduled Automatic Power Save Delivery)	Used in QoS networks (802.11e); frames are delivered automatically during uplink transmission without explicit PS-Poll.
3. TWT (Target Wake Time) – 802.11ax	STA and AP negotiate specific wake-up times to reduce contention and save energy. Ideal for IoT.
4. rTWT (Restricted TWT) – 802.11be	Advanced scheduling: STAs get reserved access during restricted periods, optimizing power and latency.
5. Opportunistic Power Save (802.11n/ac)	The AP may opportunistically buffer and deliver frames when the STA is active, without formal negotiation.

Q8) Describe the Medium Access Control methodologies

The IEEE 802.11 standard defines multiple MAC coordination functions to manage how devices access the shared wireless medium. These methods ensure fair access, avoid collisions, and support Quality of Service (QoS).

Distributed Coordination Function (DCF)

Type: Contention-based
Standard: Mandatory in all 802.11 implementations
Basis: CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

Key Features:

- STAs listen before transmitting.
- If the medium is idle for a DIFS (Distributed Inter-Frame Space), transmission begins.
- If the medium is busy, the STA waits and selects a random backoff time.
- **RTS/CTS** (optional) is used to avoid collisions due to hidden terminals.

Frame Exchange Sequences:

- Basic: DATA → ACK
- With RTS/CTS: RTS → CTS → DATA → ACK

Advantages:

- Simple and decentralized
- Suitable for general data traffic

Limitations:

- No QoS guarantees
- Cannot efficiently prioritize delay-sensitive traffic (e.g., voice)

Point Coordination Function (PCF)

Type: Contention-free
Standard: Optional
Basis: Polling-based medium access (centralized control)

Key Features:

- AP acts as a Point Coordinator (PC).
- Operates during the Contention-Free Period (CFP) within a superframe.
- AP polls each STA in a predefined order.
- Eliminates contention and collisions.

Timing Structure:

- Superframe: [CFP] + [Contention Period (CP)]
- CFP starts with a Beacon frame.

Advantages:

- Supports time-sensitive applications (e.g., voice/video)
- Collision-free

Limitations:

- Poor scalability and limited support in real-world devices
- Inflexible and inefficient in mixed traffic scenarios

3. Enhanced Distributed Channel Access (EDCA)

Type: Contention-based with QoS support
Standard: Introduced in IEEE 802.11e
Basis: Extension of DCF with traffic differentiation

Key Features:

- Introduces Access Categories (ACs):
  - Voice (AC_VO)
  - Video (AC_VI)
  - Best Effort (AC_BE)
  - Background (AC_BK)
- Each AC has its own:
  - Arbitration Inter-Frame Space (AIFS)
  - Contention Window (CWmin, CWmax)
  - Transmission Opportunity (TXOP)
- Higher priority ACs use shorter AIFS and CW to access the medium faster.

Advantages:

- Provides QoS support
- Supports real-time traffic

Limitations:

- Still contention-based (no guaranteed delivery)
- Can lead to unfair access if not managed properly
-

Feature	**DCF**	**PCF**	**EDCA**
Access Type	Contention-based	Contention-free	Contention-based (QoS)
QoS Support	No	Limited	Yes
Central Coordinator	No	Yes (AP)	No
Real-Time Traffic Support	Poor	Moderate	Good
Deployment Status	Widely implemented	Rarely implemented	Widely used (QoS WLANs)

Q9) Brief about the Block ACK mechanism and its advantages (in IEEE 802.11)

What is Block ACK in IEEE 802.11?

Block Acknowledgment (Block ACK) is a mechanism introduced in IEEE 802.11e (and improved in 802.11n) to acknowledge multiple data frames with a single ACK, instead of sending one ACK for each frame.

It's used after transmitting a burst of frames, especially in high-throughput scenarios like video streaming or large file transfers.

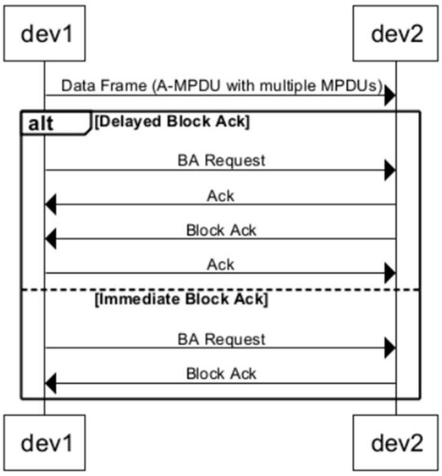
```
Sender (STA)          Receiver (STA)

   |                            |
   |---- Frame 1 -------------->|
   |---- Frame 2 -------------->|
   |---- Frame 3 -------------->|
   |      ...                   |
   |---- Frame N -------------->|
   |--- Block ACK Request -->|
   |←--Block ACK (bitmap) --|
```

Types of Block ACK

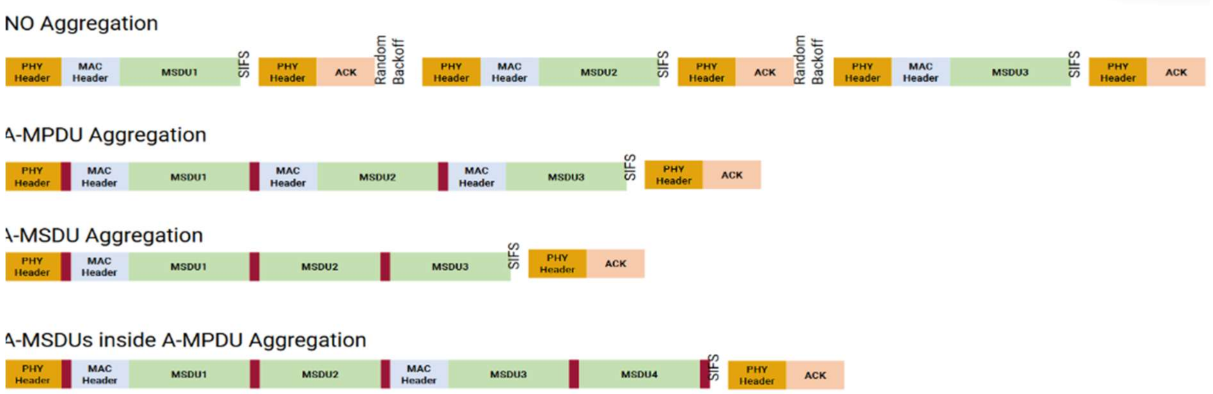
Type	**Description**
Immediate Block ACK	Receiver replies as soon as the Block ACK Request is received.
Delayed Block ACK	Receiver waits a short time before replying (less common).

Delayed vs Immediate Block Ack



Mechanism	Basic ACK	Block ACK
ACK Type	One per data frame	One for a block of frames
Overhead	High	Low
Throughput	Lower	Higher
Retransmission	Per frame	Selective
Use Case	Small or sporadic data	Burst or high-volume data

Q10) Explain about A-MSDU, A-MPDU and A-MSDU in A-MPDU



In Wi-Fi (IEEE 802.11), every data frame normally carries significant overhead (MAC headers, preambles, etc.). To transmit more data per unit time, IEEE 802.11n introduced:

- A-MSDU (Aggregated MAC Service Data Unit)
- A-MPDU (Aggregated MAC Protocol Data Unit)
- A-MSDU inside A-MPDU (Hybrid approach)
-

A-MSDU (Aggregated MSDU)

- Combines multiple MSDUs into a single MPDU.
- All payloads share a single MAC header.
- Suitable for traffic going to the same destination.

Structure: [MAC Header] [MSDU 1] [MSDU 2] [MSDU 3] ...

A-MPDU (Aggregated MPDU)

- Combines multiple MPDUs at the PHY layer.
- Each MPDU has its own MAC header and Frame Check Sequence (FCS).
- More resilient to errors.

Structure: [MPDU 1] [MPDU 2] [MPDU 3] ...

A-MSDU inside A-MPDU (Hybrid Aggregation)

- A hybrid scheme where each MPDU in an A-MPDU can contain an A-MSDU.
- Combines the efficiency of A-MSDU and the robustness of A-MPDU.

Structure: A-MPDU { MPDU 1 { A-MSDU { MSDU 1, MSDU 2 } } MPDU 2 { A-MSDU { MSDU 3, MSDU 4 } } ... }

Feature	**A-MSDU**	**A-MPDU**	**A-MSDU in A-MPDU**
Aggregation Layer	MAC	PHY	MAC and PHY
MAC Header per Unit	One	One per MPDU	One per MPDU
Retransmission Unit	Entire A-MSDU	Per MPDU	Per MPDU
Overhead	Low	Moderate	Moderate
Error Tolerance	Low	High	High
Destination Restriction	Same only	Can vary	Same per A-MSDU
Throughput	High	Higher	Highest

***Q1)* What is the significance of MAC layer and in which position it is placed in the OSI model**

The MAC (Medium Access Control) layer is a sub-layer of the Data Link Layer in the OSI model. It plays a critical role in managing how data is transmitted over a shared communication medium—especially in wireless networks like Wi-Fi.
Key Responsibilities of the MAC Layer:

- Access Control to the Medium: Determines when a device can transmit data over the channel. Uses techniques like CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) in wireless.
- Frame Delimiting and Addressing: Adds MAC addresses (unique hardware addresses) to frames to identify sender and receiver.
- Error Detection (Not Correction): Adds a CRC (Cyclic Redundancy Check) to detect errors in frames.
- Frame Construction and Parsing: Builds frames for data transmission and extracts data upon receipt.
- Acknowledgment and Retransmission: In wireless, often includes ACK frames to confirm successful delivery.
- Management and Control Frames Handling: Handles connection setup, authentication, and mobility (association, reassociation, etc.)