**Wifi Training Module 4 Assignment**

**Q1,3,4,5,6**

MAC LAYER IN WIFI :

1. Stands for Medium Access Control layer which plays crucial role by doing following functions:

1. Framing

2. Fragmentation

3. MAC addressing

4. Access Control

5. Error control

2. It is the part of Data Link Layer in OSI Model. It is the lower sublayer of Data link layer that works in vicinity with PHY layer.

3. Especially in Wifi (IEEE 802.11), it splits up the tasks into three planes. They are,

1. Management plane

2. Control plane

3. Data plane

4. Management Plane of MAC

1. It helps right from the establishment of WLAN and followed by authentication, association and maintenance of STA and AP in WLAN.

2. It does following functionalities:

a. Scanning - It is the process by which STA and AP knows (discovers) each other and further gets connected. There are two types in Scanning. They are:

1. Active Scanning - a process in which STA initiates the AP discovery by sending Probe requests either targeted towards particular SSID or as a broadcast message in identifying AP. In the probe request, all the capabilities of STA will be advertised to AP including Data rate, security schemes, Authentication mechanisms, Channel and Frequency in use etc. AP after receiving probe request, sends Probe response stating its Capabilities. Thus, final decision on association will be taken by STA only in this case.

Use case : During Roaming. Because, it might not listen to all channels available to get associated to any AP with same SSID (or even different - L3 roaming). Instead, it sends Probe request to current AP seeking help in getting list of neighboring APs and their capabilities and STA decides whether to accept the suggestion or not.

2. Passive Scanning - a process in which AP periodically broadcasts the Beacon frame in its BSS so that STA wants to get associated will listen to this frame stating APs capabilities and client will choose from the available APs and based on its requirement, it chooses one AP and sends authentication Request and further proceeds in getting associated with that AP.

Use case : In conventional Wifi Access, Beaconing is only used.

During Scanning, SSID (Service Set IDentifier - logical string used to identify the particular wireless service - not associated with single BSS might get extended to many BSS based on pre-configuration of VLAN. Basically, AP in any BSS maps SSID to VLAN. This SSID will be used to authorize the user what to do and not to do during authentication itself.), BSSID (Basic SSID - it is nothing but the MAC address of APs particular radio that forms BSS. Practically, each SSID in each BSS will have unique BSSID - helpful in roaming to identify AP), Data rate - This is given in the form of either DISABLED : will not be supported by APs or SUPPORTED : will be used if client is also ready to use or MANDATORY : Will be used by AP and forces client to do so , followed by channel setting, PHY setting; will be delivered by AP. Thus, all the possible capabilities of entities will be exchanged in this phase.

b. Authentication - It is the process by which security and encryption related settings (Open system authentication or shared key authentication) will be agreed and executed. Basically, in Wifi, WPA2 or WPA3 based authentication mechanisms are widely used. Happens after association.

Open Authentication is the one where there is no verification happens. Simply STA sends Auth Request and AP immediately accepts it by sending Auth Response. Prone to many security threats. Public wifi sources mainly used this. But nowadays, per session keys are developed and used in public Wifi.

In WPA2 - Pre shared key is used for encrypting messages. It follows EAPOL 4 way handshake for obtaining encryption key:

1. AP initiates by sending ANonce - 256 bits

2. STA calculates PMK from sent ANonce using PBKDF with MAC of both AP and Station and its own SNonce.

3. With PMK, STA calculates PTK using Pseudo Random Function with some common parameters.

4. STA extracts Message Integrity Code from PTK and sends both SNonce and MIC to AP (msg-2)

5. AP now calculates the same PTK using SNonce and verifies it with the computed MIC and obtained MAC.

6. AP now generates GTK (Group Transient Key) to encrypt optionally the broadcast and multicast messages with the help of PTK based encryption and sends to STA with MIC (msg-3)

7. STA install the keys and final confirmation with verified MIC is sent back (msg-4)

Based on this handshake, further communication (data payload) will be encrypted using PTK and GTK for security using AES-CCMP.

It is prone to Offline dictionary attacks (Password guessing), replay attack (KRACK), No forward secrecy, Evil Twin Attacks.

In WPA2 - Enterprise, 802.1X port based authentication is used with RADIUS Server. It treats STA as supplicant, AP as authenticator and has dedicated Server to authenticate. Since during association itself, negotiated capabilities are confirmed, AP begins this process by sending EAP Request identity to STA via captive portal asking credentials. AP as authenticator now forwards this request to RADIUS server once STA provides its credentials via EAP Response identity. Upon validation (there are many protocols to authenticate here), it sends Success/Rejection message via AP to STA. Thereby authentication or deauthentication happens. If successfully authenticated, after authorization (fixing limits to access network), accordingly the encryption key (PMK) will be delivered in secured manner which will then be used in 4 way handshake (instead of using common PMK).

common methods in RADIUS server authentication:

1. EAP-TLS (Extensible Authentication Protocol - Transport Layer Security): It is the advanced and widely used method in authentication by exchanging and verifying both STA and Server's certificates and then sending PMK

2. EAP-TTLS (Tunneled TLS) - Here server certificate is used to form encrypted tunnel and inside which authentication occurs using user password. Similarly PEAP (Protected EAP) and also relies on passwords.

In WPA3 - SAE (Simultaneous Authentication of Equals) which is based on Dragon FLY Password Authenticated Key Exchange type. It works by agreeing on some global parameters and chooses random scalar and performs Elliptic Key cryptography. It is also used in Mesh networks.

Here, at first, a Curve will be chosen (Finite cyclic group) and with the help of password, mac address, Password element is obtained which cannot be reverse engineered. with this, both parties chooses random scalar and exchanges commit elements (product of random scalar and element) now, both computes private secret key per session. it is ensured to be same because of properties. To confirm, both verifies common MIC and proceeds with 4 way handshake with the secret key to derive PTK and GTK

c. Association : It is done to generate AID for further communications. If any device wants to get out the network, it sends dissociation or de authentication frame. Even AP if finds STA to be rogue or malicious device, it sends de-association frame.

d. Management plane also ensures Power management for STAs, Load balancing by MLO (Active or simultaneous), VLAN Segmentation and roaming optimization.

Control plane :

1. RTS

2. CTS

3. ACK / BlockACK

4. PS-Poll frame

It mainly helps in controlling the access of the shared media by using RTS, CTS (which advertises NAV for virtual carrier sensing and also helps in avoiding Hidden and Exposed Node problem). ACK/BLOCKACK is helpful in ensuring whether packet reached recipient since wireless media collisions cannot be detected. PS-Poll frames are used by STAs in Power management scenario to retrieve buffered data from AP.

Data plane:

1. Conventional payload

2. QoS Data frame

3. QoS Null frame (for indicating power management and channel sounding)

**Q2.**

FRAME FORMAT FOR WIFI

1. Generally, for Data link layer in OSI, frame format follows common structure. That is,

MAC Header | Frame body | FCS

2. Frame body and FCS (Wifi follows CRC) remains the same but Frame header changes for wifi

3. Wifi frame format is given below:

Frame control (2) | Duration/ID (2) | Add-1 (6) | Add-2 (6) | Add-3 (6) | Seq No (2) | Add-3 (6) | QoS (2) | HT field (2) | Frame body (0-2304 with overhead for security) | FCS (4)

3. Frame control field in wifi contains the following:

1. Protocol - 00 for wifi

2. Type - Defines whether the frame is Management (00), Control (01), or Data (10)

3. Subtype - Identifies the specific type of frame (e.g., Beacon, RTS, CTS, Data)

4. To DS - Set if the frame is heading to the Distribution System (AP)

5. From DS - Set if the frame is coming from the Distribution System (AP)

6. More Fragments - Set if the frame is fragmented

7. Retry - Set if this is a retransmitted frame

8. Power Management - Indicates whether the STA is in power-saving mode

9. More Data - Indicates additional buffered data at the AP for power-saving STAs

10.Protected Frame - Set if the frame is encrypted (WEP, WPA, WPA2)

11.Order - Set for strictly ordered frames

To DS=0 and From DS=1: A1-Dest STA , A2-BSSID, A3-Actual sender in DS

To DS=1 and From DS=0: A1-BSSID , A2 - Source-STA , A3 - Actual destination in DS.

To DS=0 and From DS=0: Frame for AP, Frame for broadcast, DLS

To DS=1 and From DS=1: in Mesh networking

4. Duration/ID :

1. In conventional frames, it represents NAV (Network Allocation Vector) to reserve channel and to let other users know that channel will be reserved for that duration.

2. In power save poll frames, it contains Association ID

5. ADD-1: It represents the immediate destination or recipient

6. ADD-2: It represents the immediate source

7. ADD-3: it represents either actual destination or actual source

8. Seq No: In case of fragmentation, it represents which seq frames are being fragmented

9. ADD-4 : Used in the case of multi-hop routing.

10. Frame body - 0 to 2304 bytes with either layer-3 data or encrypted data or QoS data.

11. FCS - CRC-32 bits for frame integrity.

Q7

POWER SAVING IN WIFI MAC LAYER

1. Wi-Fi radios consume a lot of power, especially when constantly transmitting, receiving, or even just listening to the channel.

2. Power saving at the MAC layer allows devices to turn off their radio during idle times or schedule wake-up times to listen only when necessary.

3. Unlike cellular radios, Wi-Fi lacks a centralized controller, so each device must actively manage its power.

4. Apps and services expect constant internet access.

5. Even when idle, the device needs to stay associated to the AP.

6. In most of the real world cases, burst data transfer happens and not continuous thereby leaving space for idle periods so that STA can sleep.

7. Legacy Power Save Mode

1. Client may send QoS null frame to AP with power management bit set.

2. AP receives the frame and understands that STA is going to sleep.

3. AP starts buffering all the frames intended to it.

4. In every beacon frame, there is a field called TIM (Traffic Indication Map - Partial Virtual Bitmap) that contains fields for all associated clients.

5. If STA finds its AID field set, then it understands that it has buffered data.

6. It sends PS-Poll frame to AP to retrieve data.

7. AP starts replying with buffered frames and indicate if more data present.

8. Client after getting all buffered frames go to sleep again.

8. Unscheduled Automatic Power Save Delivery

1. Supports low latency applications.

2. APs push data once triggered without Ps-poll.

3. frames are here grouped as Service periods.

4. There are 4 AC like voice, video, background and best effort access categories.

5. In this mode, once STA informs for sleep mode, AP buffers data in terms of AC

6. STA after waking up sends trigger frame with appropriate AC and AP will send the appropriate Burst of frames.

7. Last frame will be marked as End of Service Period and then sleep immediately.

9. Target Wake Time

1. Client negotiates TWT agreement with AP. AP may reject or accept TWT agreement with any suggestions or changes.

2. Agreement includes wake interval (how much time after which it wakes up)

3. Wake duration is the time the STA is awake and listens. If AC got Delivery enabled, automatically AP senses wake time and sends. otherwise, STA will send QoS null frame to get data.

4. During wake time, any communication can happen between AP and STA.

10. WoWAN (Wake on WAN)

1. Similar technology in waking up but differs in the way that magic word will be transmitted by APs in case of any data transfer so that device will wake up from semi-sleep state

**Q8.**

MEDIUM ACCESS CONTROL TECHNIQUES

1. It is impossible to detect collisions in wireless environment. Therefore, best can be done is to avoid collision in the first place.

2. To coordinate access to the shared wireless medium, IEEE 802.11 defines two primary MAC coordination functions:

Distributed Coordination Function (DCF) – A contention-based access method using CSMA/CA.

Point Coordination Function (PCF) – A polling-based method used in infrastructure networks.

Now, there is another enhancement called EDCA (Enhanced Distributed Channel Access)

3. Distributed Coordination Function is the default MAC coordination function which works based on contention window and allows stations to use CSMA/CA.

1. At first, it does Virtual Carrier Sensing - a process in which all STAs with their NAV timer waits for its expiry. This NAV would have been advertised by RTS,CTS frame by other STA to transmit data in the shared media.

2. Once the channel is free by virtual sensing, It does physical sensing by sensing the energy of the live media via RSSI and compares it with CCA (Clear Channel Assessment threshold). If RSSI is lesser than CCA threshold, STA may proceed with its NAV advertisement via RTS and CTS and starts sending its payload.

3. If RSSI (First Signal detect happens which matches for wifi preamble and expects it to be 4 db more than noise floor and followed by energy detect which generally checks for the presence of similar signals from other technologies like oven, Bluetooth etc) is slightly comparable to CCA, but lesser than Overlapping BSS power detection threshold with different BSS color in HE signal field in PHY header, then also, it may proceed with its transmission.

4. However, in all other cases, it is advisable for STAs to defer transmission and wait for random contention window time and check again.

5. All transmissions expect ACK back to confirm the delivery of packets since, wireless media is unpredictable.

6. Once STA decides to begin transmission, it waits for DIFS (Distributed Inter Frame Space) time followed by Random Contention window value \* Slot time (fixed by frequency in use) (cw size is from 0 to 1023)

it first sends RTS stating its properties, length of information to be exchanged, duration for channel occupation , target recipient etc.

7. Target recipient upon receiving RTS will acknowledge by echoing it in the form of CTS.

8. Hidden node problem (two stations out of coverage to each other but has common station may transmit data to common station at same time leads to interference) can be avoided by using RTS,CTS pair. That is, a node which could not hear RTS but hear CTS being sent from common station should defer its transmission to that node.

9. Exposed node problem (just because another node is present in its coverage, it doesn't mean that a node should always defer its transmission rather it can check the Target AP and Target BSS and signal strength) can be avoided by the fact that RTS will be heard by the node but not CTS. so it understands that target is not in its reach so it can start transmission.

10. SIFS (Short Inter Frame Space) is for ACK, CTS will be considered.

11. EIFS (Extended IFS) for persistent collisions which leads to increased contention window size.

POINT COORDINATION FUNCTION :

1. Operates only in infrastructure mode where AP as centralized controller eliminates contention and reserves the entire medium.

2. AP starts polling stations in round robin fashion without considering QoS.

3. AP periodically sends CF-poll frame to stations asking and granting permission to transmit

4. Stations respond with data or indicate they have nothing to send.

5. AP here uses PIFS (PCF IFS) to gain priority over medium using PCF.

EDCA:

1. It is the simple extension of DCF by considering QoS.
2. It provides Arbitration IFS like DIFS which is short for high priority tasks. Similarly, contention window is ensured to be minimum for higher priority tasks.
3. Moreover, high priority tasks will get more Transmission opportunity than lower priority tasks that is more duration.

**Q9,Q10.**

BLOCK ACK

1. In traditional Wi-Fi , every frame sent by a sender was immediately acknowledged by the receiver using an ACK frame. This was inefficient, especially when Data rates are high, Large numbers of small packets are sent, Latency and overhead are critical.

2. To address this, Block ACK was introduced in IEEE 802.11e.

3. Instead of sending an ACK for every frame, the receiver buffers multiple data frames from the sender and sends a single Block ACK frame that acknowledges multiple MPDUs at once.

4. There are implicit and explicit block ACK possible. In explicit block ACK, prior setup agreement should be made and to be negotiated by using Add Block ACK Agreement (ADDBA) request frame by sender which include starting seq number, buffer size, timeout for ack, traffic identifier (related to QoS that may have different block ACK params depending on traffic streams).

5. works well with A-MPDU with any seq number with agreed block size.

6. Receiver after receiving buffered frames either immediately or after processing frames, sends block ACK with particular sequence number and bitmap stating which frames it lost.

7. Thereby retransmitting the selective missed frames in aggregated blocks instead of sending whole aggregated block.

8. After sometime, if block ACK scheme is not needed, it should terminate by sending DELBA.

MAC AGGREGATION

1. It is the efficient concept by which redundancy can be reduced in frame transmission and also enhances block ack.

2. It increases throughput and reduces congestion , interframe spaces and also promotes time sensitive networking.

3. In single transmission, under single header, multiple frames can be sent using wifi protocol.

4. In case of no aggregation, each frame will have both PHY and MAC header and after each frame, SIFS will be considered.

4. There are three types of MAC AGGREGATION. They are

1. A-MPDU aggregation - Here, under single PHY hdr, multiple frames with MAC headers for each frame will be sent as single entity therefore BLOCK ack after single SIFS can be expected.

2. A-MSDU Aggregation - Under single PHY and MAC headers, multiple frames will be embedded. though looks efficient, it might be difficult to organize and retransmit incase of any errors.

1. A-MSDU inside A-MPDU aggregation - it is the mix of above two types by which under single PHY hdr, frames will be grouped such that each group contains one MAC header making it easier to track and organize.