MODULE 4 ASSIGNMENT

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

MAC layer corresponds to the second layer of the OSI model which plays a vital role in managing access to the medium(wireless in this case), ensuring there is no collision and is responsible for converting message into MAC frame before sending it to the physical layer and at the opposite side, it ensures that message is reconstructed and is sent to L3. On a broader context, it manages three planes namely Management Plane, Control Plane and Data Plane.

2. Describe the frame format of the 802.11 MAC header and explain the purpose of each fields.

Below is the frame format for 802.11 MAC header which consists of various fields and sub fields each adding information to the packet.

MAC HEADER	FRAME BODY	FRAME CHECK SEQUENCE

MAC HEADER :

It consists of 9 fields which incorporate information like Destination Address, Data, CRC and most important of all, Frame Control which by itself consists of various information like the protocol version, type of function(management/data or control), subtype, security standard, power management and many more.

FRAME BODY :

Frame body consists of the actual data that is being transmitted over the Wireless Network.

FCS :

Frame Check Sequence is responsible to check the integrity of the message and whether it has been received without any transmission errors.

3. Please list all the MAC layer functionalities in all Management, Control and Data plane.

MANAGEMENT PLANE:

The management plane is responsible for establishing and maintaining connection between wireless devices and help stations and access points Associate and maintaining connectivity. The various functionalities of Management Plane are :

- Advertise Capabilities
- Connection Management
- Security Management
- Mobility Management
- Load Management
- Power Management
- QoS Management
- Channel Management
- Multiple Access Management

CONTROL PLANE:
Once connection has been established, the control plane ensures that the connectivity between the devices is secure and the transmission of data between them are smooth. The main functionalities of the Control Plane are:

- Flow Control
- Power Save Control
- Medium Access Control

DATA PLANE:
Data Plane is responsible for actual transfer of data between the wireless devices connected. Its primary functionality is Data Transmission and Frame Aggregation.

4. Explain the scanning process and its types in detail

ACTIVE SCANNING:
This is the type of scanning in which the Station that needs to connect to a wireless network, sends out a Probe Request as a broadcast message in all the channels. When an AP receives a Probe Request, it sends out a Probe Response which contains all the capabilities of the Access Point. The Client receives this Response message from one or more AP(s) and decides which AP to connect to and later sends out Authentication Request and other subsequent frames for association.

PASSIVE SCANNING:
This is the type of scanning in which an AP periodically sends out a Beacon frame which consists of the capabilities of the AP. The station which intends to connect to the wireless network, listens to the Beacon frame it receives from all the APs and decides upon which AP to connect to.

5. Brief about the client association process.
The first step of Client Association Process is scanning which is explained above. Once the station chooses which AP to connect to, it sends Probe Request and receives Probe Response from the AP. Once it receives the probe response, it checks the compatibility between AP and Station and sends out a Authentication Request. The AP responds with an Authentication

Response which marks end of Authentication and start of Association. The Station and AP exchange Association requests and responses before Station starts to exchange data with AP.

6. Explain each steps involved in EAPOL 4-way handshake and the purpose of each keys derived from the process

The EAPOL 4-way handshake is a secure method of establishing a connection between the client and the Access Point. The process involves 4 major steps:

- Message 1 : Where AP initiates the handshake by sending out frames containing ANonce, a random number. This is a unicast message and contains the SSID of the AP.
- Message 2 : The client responds to the AP by sending SNonce, a random number generated by the client and MIC which is used to check the integrity of the message. The AP will use ANonce and SNonce to generate Pairwise Temporal Key.
- Message 3 : The AP sends the calculated PTK along with GTK as PMK (Primary Master Keys) to the client.
- Message 4 : The client sends back a final message to acknowledge that the process is complete.

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

Power Management is one of the important functionalities of MAC layer so much so that it the MAC layer frame format contains a bit in the Frame Control field of the MAC header which is used to denote Power Management. If that bit is set to 1, it signals the station is actively power-saving by switching some transceivers. The power management bit along with Traffic Indication Map in beacon frames is used to manage traffic.

8. Describe the Medium Access Control methodologies

Point Co-ordination Function:

The PCF allows users to transmit by granting access to the Stations by polling them. By reserving the medium, AP ensures that Stations cannot transmit data unless polled by the AP. The stations are polled in a Round Robin method.

Distributed Co-ordination Function:

DCF is a hybrid methodology which uses PCF with distributed control. In this method, everyone including the Access Point are considered as participants contending for the wireless medium. It operates based on CSMA/CA mechanism where data is transmitted when a participant senses a medium to be idle. If a collision takes place, the station waits for particular amount of time called `backoff` before retransmitting the same signal.

Enhanced Distribution Channel Access:

EDCA is QoS enhanced DCF where in traffic priority is given to stations contending for medium access. By taking various parameters into consideration, traffic is transmitted into separate queues in the Radio Hardware.

9. Brief about the Block ACK mechanism and its advantages

Block ACK is a mechanism where acknowledgement to multiple frames are given at a time. This is a very efficient mechanism that is popularly used. Block ACK is used during aggregation. The transmitter initiates the process by sending Add Block Ack(ADDBA) to find out if receiver supports Block ACK and it receives an acknowledgement from the receiver. After transmitting the data, the transmitter asks for Block ACK with a request and it sends an acknowledgement. This session can be deleted by sending Delete Block Ack(DELBA) by the transmitter. The two types of Block ACK are Immediate BLOCK ACK and Delayed BLOCK ACK.

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

A-MSDU stands for Aggregate MAC Service Data Unit which is aggregation of two or more MSDU. MSDUs are data packet which are received by the MAC layer from the layers above it.

A-MPDU stands for Aggregate MAC Protocol Data Unit which is aggregation of two or more MPDU. MPDUs are data packets which are received by the physical layer from the MAC layer. Multiple MPDUs are aggregated together which is transmitted with a PHY header by the radio.

A-MSDU in A-MPDU refers to a scenario where multiple A-MSDUs are bundled together to create an A-MPDU. This approach can be beneficial for scenarios where there are many smaller MSDUs to transmit, allowing for further aggregation and overhead reduction.