MCC VIVA

1. Need of specialized MAC
   - It is to avoid a collision in wireless communication as it can damage the data.
   - Collision detection is very difficult in wireless scenarios because the transmission power in the area of the transmitting antenna is many orders of magnitude higher than the receiving power.
   - The signal in case of wireless networks decrease in their strength as it travels larger distances.

2. Tunneling
   - Tunneling is a method used to transfer a payload of one protocol using an internetwork transportation medium of another protocol.
   - The data that need to be transferred are typically frames/packets belonging to a certain protocol (different to the protocol used to send data).

3. Encapsulation
   - Because the transmitted payload belongs to a different protocol, it cannot be sent as it is created.
   - Encapsulation is the process of encapsulating the payload with an additional header so that it can be sent (tunneled) through the intermediate network correctly.
   - After the transmission, the encapsulated payload needs to be de-encapsulated at the routing end point and can be forwarded to the final destination.

4. Multiplexing
   - Multiplexing is the process of combining multiple signals into one signal, over a shared medium.

5. Types of multiplexing
   A. Analog Multiplexing: The analog multiplexing techniques involve signals which are analog in nature. The analog signals are multiplexed according to their frequency (FDM) or wavelength (WDM).

   - Frequency Division Multiplexing (FDM)
     a. It is the most used technique.
     b. It uses various frequencies to combine streams of data, for sending them on a communication medium, as a single signal.

   - Wavelength Division Multiplexing (WDM)
     a. In this, many data streams of different wavelengths are transmitted in the light spectrum.
     b. If the wavelength increases, the frequency of the signal decreases.

   B. Digital Multiplexing: The term digital represents the discrete bits of information. Hence the available data is in the form of frames or packets, which are discrete.

   - Time Division Multiplexing (TDM):
     a. In TDM, the time frame is divided into slots.
     b. This technique is used to transmit a signal over a single communication channel, with allotting one slot for each message.

- Code Division Multiple Access (CDMA):
    a. It is an example of multiple access where amnyl transmitters use a single channel to send information simultaneously.
    b. Every user uses the full available spectrum instead of getting allotted by separate frequency.
    c. CDMA is much recommended for voice and data communications.

- Space Division Multiple Access (SDMA):
    a. It is a technique which is MIMO (multiple-input multiple-output) architecture.
    b. It is used mostly in wireless and satellite communication.
    c. All users can communicate at the same time using the same channel.

6. Frequency reuse:
- In this scheme, allocation and reuse of channels throughout a coverage region is done.
- Each cellular base station is allocated a group of radio channels or Frequency sub-bands to be used within a small geographic area known as a cell.
- The process of selecting and allocating the frequency sub-bands for all of the cellular base stations within a system is called Frequency reuse or Frequency Planning.

7. Mobile IP Protocol:
- Mobile IP is a communication protocol (created by extending Internet Protocol, IP) that allows the users to move from one network to another with the same IP address.
- It ensures that the communication will continue without user's sessions or connections being dropped.
- Components of Mobile IP

a. Mobile Node (MN):
It is the hand-held communication device that the user carries e.g. Cell phone.
b. Home Network:
It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).
c. Home Agent (HA):
It is a router in home network to which the mobile node was originally connected
d. Home Address:
It is the permanent IP address assigned to the mobile node (within its home network).
e. Foreign Network:
It is the current network to which the mobile node is visiting (away from its home network).
f. Foreign Agent (FA):
It is a router in foreign network to which a mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers it to the mobile node.
g. Correspondent Node (CN):
It is a device on the internet communicating to the mobile node.
h. Care of Address (COA):
It is the temporary address used by a mobile node while it is moving away from its home network.

8. Architecture of GSM:

- The GSM architecture consists of three major interconnected subsystems that interact with themselves and with users through a certain network interface.
- The subsystems are Base Station Subsystem (BSS), Network Switching Subsystem (NSS) and Operational Support Subsystem (OSS). Mobile Station (MS) is also a subsystem but it is considered as a part of BSS.

- BSS stands for Base Station Subsystem. BSS handles traffic and signaling between a mobile phone and the network switching subsystem. BSS has two components BTS and BSC.
- NSS stands for Network and Switching Subsystem. NSS is the core network of GSM. That carried out call and mobility management functions for mobile phones present in the network. NSS have different components like VLR, HLR and EIR.
- OSS stands for Operating Subsystem. OSS is a functional entity which the network operator monitors and controls the system. OMC is part of OSS.

9. Difference between GSM and GPRS

1.	GSM stands for Global Systems for Mobile.	GPRS stands for General Packet Radio Service.
2.	GSM is a cellular standard for mobile phone communications to cater to voice services and data delivery using digital modulation where SMS has a profound effect on society.	GPRS is an up-gradation of GSM features over the basic features to obtain much higher data speeds and simple wireless access to packet data networks than standard GSM.
3.	System generation is 2G.	System generation is 2.5G.
4.	The frequency bands used in the GSM system are 900 and 1800 MHz.	The frequency bands used in the system are 850, 900, 1800 and 1900 MHZ.
5.	The type of connection is a circuit-switched network.	Here the type of connection is a packet-switched network.
6.	It provides data rates of 9.6 kbps.	It provides data rates of 14.4 to 115.2 kbps.
7.	In GSM billing is based on the duration of the connection.	In GPRS billing is based on the features amount of data transferred.
8.	It does not allow direct connection to the internet.	It allows direct connection to the internet.
9.	It is based on system TDMA.	It is based on system GSM.
10.	In GSM, single time slot is allotted to a single user.	In GPRS, multiple time slots can be allotted to a single user.
11.	It takes long time to connect.	It provides faster connection.
12.	In this location area concept is used.	In this routing area concept is used.
13.	SMS (Short Messaging Service) is one of the popular features.	MMS (Multimedia Messaging Service) is one of the popular features.

10. WLAN

- A wireless local-area network (WLAN) is a group of colocated computers or other devices that form a network based on radio transmissions rather than wired connections.
- A Wi-Fi network is a type of WLAN; anyone connected to Wi-Fi while reading this webpage is using a WLAN

11. Types of WLAN:
    1. Infrastructure based wireless network:
        - Infrastructure mode was designed to deal with security and scalability issues.
        - In this mode, wireless clients can communicate with each other.
    2. Ad hoc mode
        - It is based on the Independent Basic Service Set (IBSS).
        - In IBSS, clients can set up connections directly to other clients without an intermediate AP.
        - This allows you to set up peer-to-peer network connections.
        - The main problem is that it is difficult to secure since each device you need to connect to will require authentication.

12. Threats in WLAN:
- The three most common WLAN security threats include:
    1. denial of service attacks - where the intruder floods the network with messages affecting the availability of the network resources
    2. spoofing and session hijacking - where the attacker gains access to network data and resources by assuming the identity of a valid user
    3. eavesdropping - where unauthorised third parties intercept the data being transmitted over the secure network

13. Mobile TCP
- M-TCP (mobile TCP)1 approach has the same goals as Indirect TCP and snooping TCP.
- It is to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems.
- M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover.
- M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.

14. Internet Protocol:
- The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
- Data traversing the Internet is divided into smaller pieces, called packets.
- IP information is attached to each packet, and this information helps routers to send packets to the right place.
- Every device or domain that connects to the Internet is assigned an IP address, and as packets are directed to the IP address attached to them, data arrives where it is needed.

15. TCP
- Transmission Control Protocol (TCP) is a standard that defines how to establish and maintain a network conversation by which applications can exchange data.

- TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. Together, TCP and IP are the basic rules that define the internet.

16. Antenna
    - It is a device which converts electromagnetic radiation in space into electrical currents in conductors or vice versa, depending on whether it is being used for receiving or transmitting.
    - The radiation pattern of an antenna describes the relative strength of the radiated field in various directions from the antenna.

17. Types of antenna
    - Isotropic antenna: Theoretical antenna which radiates its power uniformly in all directions. It is an ideal antenna which radiates equally in all directions.
    - Omnidirectional Antenna: This type of antenna is useful for broadcasting a signal to all points of the compass or when listening for signals from all points.

    a. Dipole:
        - The dipole radiation pattern is 360 degrees in the horizontal plane and approximately 75 degrees in the vertical plane.
        - Most commonly used is Hertzian Dipole.
        - It consists of two collinears conductors of equal length.
    b. Monopole:
        - Also known as marconi antenna.
        - This type of antenna is efficient for mounting on the rooftop of a car.
    c. Directional Antenna:
        - It is an antenna which radiates or receives greater power in specific directions.
        - This allows increased performance and reduced interference from unwanted sources.
        - These antennas should be directed in the direction of the transmitter or receiver.
        - Ex: parabolic and yagi antenna.
    d. Sectorized Antenna:
        - Several directional antennas can be combined on a single pole to construct a sectorized antenna.
    e. Antenna Arrays:
        - It is a configuration of multiple antennas arranged to achieve a given radiation pattern.

18. General Packet Radio Service:
    - It is a packet oriented wireless data communication service for mobile communications on 2G and 3G cellular communication systems.
    - It is non-voice, high speed packet switching technology intended for GSM networks.
      It can be used to provide connections on the basis of internet protocols that support a wide variety of enterprises as well as commercial applications.

19. Difference between 3G and 4G

S.NO	3G Technology	4G Technology
1.	It stands for 3rd generation technology.	While it stands for 4th generation technology.
2.	Maximum upload rate of 3G technology is 5 Mbps.	While the maximum upload rate of 4G technology is 500 Mbps.
3.	Maximum download rate of 3G technology is 21 Mbps.	While the maximum download rate of 4G technology is 1 Gbps.
4.	It uses packet switching technique.	While it uses packet switching technique as well as message switching technique.
5.	The frequency range of 3G technology is from 1.8 GHz to 2.5 GHz.	While it's frequency range is from 2 GHz to 8 GHz.
6.	It lenient horizontally.	While it lenient horizontally as well as vertically.
7.	It is a **wide area cell based** network architecture.	While it is the **integration of Wireless LAN as well as Wide Area cell based** network architecture.
8.	There is turbo codes are used for error correction in 3G technology.	4G technology uses concatenated codes for error correction.

20. User Mobile Profile:
    - It is a combination of historic records and predictive patterns of mobile terminals,
    - It serves as fundamental information for mobility management and enhancement of quality of service (QoS) in wireless multimedia networks.

21. Properties of electromagnetic signals:
    - Radio waves are transmitted easily through air. They do not cause damage if absorbed by the human body, and they can be reflected to change their direction.

22. VLR:
    - A visitor location register (VLR) is a server in a cellular network that supports roaming functions for users outside the coverage area of their own HLR.
    - The VLR uses Signaling System 7 to obtain information about the user from the HLR.
    - Then establishes a temporary record on the VLR while the user is within the VLR coverage area, ensuring mobility management and call-handling functions.

23. HLR:

- Home Location Register (HLR) is a database that contains data regarding authorized subscribers using a global system for mobile communication (GSM) core network.
- The home location register stores information ranging from phone numbers to current location of the subscriber.

24. Cell Breathing:
    - It is a mechanism which allows overloaded cells to offload subscriber traffic to neighbouring cells by changing the geographic size of their service area.
    - Heavily loaded cells decrease in size while neighbouring cells increase their service area to compensate.
    - Thus, some traffic is handed off from the overloaded cell to neighbouring cells, resulting in load balancing

25. Routing protocol:
    - Routing Protocols are the set of defined rules used by the routers to communicate between source & destination.
    - They do not move the information to the source to a destination, but only update the routing table that contains the information.
    - There are mainly two types of Network Routing Protocols: Static and Dynamic

26. Static Routing Protocol:
    - These are used when an administrator manually assigns the path from source to the destination network.
    - It offers more security to the network.

27. Dynamic Routing Protocol:
    - Dynamic routing helps routers to add information to their routing tables from connected routers automatically.
    - These types of protocols also send out topology updates whenever the network changes' topological structure.

28. Hidden Terminal Problem:
    - It is a problem in wireless LANs (wireless local area networks).
    - It is a transmission problem that arises when two or more stations who are out of range of each other transmit simultaneously to a common recipient.
    - This is prevalent in decentralised systems where there aren't any entities for controlling transmissions.
    - This occurs when a station is visible from a wireless access point (AP), but is hidden from other stations that communicate with the AP.

29. Handover or Handoff
    - Handover or hand off is a process in telecommunication and mobile communication.
    - In this, cellular transmission (voice or data) is transferred from one base station (cell site) to another without losing connectivity to the cellular transmission.
    - Handover is a core element in deploying mobile transmission as it creates data sessions or connects phone calls between mobile devices which are constantly on the move.

30. 5G and its disadvantages:

- 5G is the fifth generation of cellular technology.
- It is designed to increase speed, reduce latency, and improve flexibility of wireless services.
- 5G technology has a theoretical peak speed of 20 Gbps, while the peak speed of 4G is only 1 Gbps.
- Disadvantages of 5G:
    a. Many of the old devices would not be compatible with 5G, hence, all of them need to be replaced with new one — an expensive deal.
    b. Developing infrastructure requires a high cost.
    c. Security and privacy issues yet to be solved.

31. LTE
- LTE stands for Long Term Evolution and is sometimes referred to as 4G LTE.
- It's a standard for wireless data transmission and it is much faster than 3G.
- It provides much higher data speed, low latency and great performance.

32. Wifi Security:
- Wireless network security primarily protects a wireless network from unauthorized and malicious access attempts.
- Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default.

33. Bluetooth and types of bluetooth network
- Bluetooth is a wireless technology, used for transferring data from one device to another device.
- The distance between the two devices is very short from the fixed, mobile device and building personal area network.
    a. Piconet:
        - Piconet is a type of bluetooth network that contains one primary node called master node and seven active secondary nodes called slave nodes.
        - Thus, we can say that there are a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take part in communication unless it gets converted to the active state.
    b. Scatternet:
        - It is formed by using various piconets.
        - A slave that is present in one piconet can act as master or we can say primary in other piconet.
        - This kind of node can receive a message from a master in one piconet and deliver the message to its slave into the other piconet where it is acting as a slave.
        - This type of node is referred to as bridge node. A station cannot be master in two piconets.

32. Difference between WEP and WPA

S.No.	WEP	WPA
01.	WEP stands for Wired Equivalent Privacy.	WPA stands for Wi-Fi Protected Access.
02.	It is a security protocol for wireless networks which provides data confidentiality comparable to a traditional wired network.	It is a security protocol which is used in securing wireless networks and designed to replace the WEP protocol.
03.	Wired Equivalent Privacy (WEP) was introduced in 1999 means before WPA.	Wi-Fi Protected Access (WPA) was developed by the Wi-Fi Alliance in 2003 means after WEP.
04.	It provides wireless security through the use of an encryption key.	It provides wireless security through the use of a password.
05.	Data Privacy (Encryption) method is Rivest Cipher 4 (RC4).	Data Privacy (Encryption) method is Rivest Cipher 4 (RC4) and Temporal Key Integrity Protocol (TKIP).
06.	Authentication method in WEP is Open system authentication or shared key authentication.	Authentication method in WPA is WPA-PSK and WPA-Enterprise.
07.	Data integrity is provided through CRC 32.	Data integrity is provided through Message integrity code.
08.	It uses 40 bit key and 24 bit random number.	WPA key is 256 bit key.
09.	Key management is not provided in WEP.	Key management is provided through 4 way handshaking mechanism.
10.	In WEP no protection against reply attacks.	In WPA sequence counter is implemented for reply protection.