ASSIGNMENT-3

UNIT 3:

1. Compare: GSM and GPRS.

GSM	GPRS
The frequency bands used in the system are 900 MHz and 1800 MHz that helps to identify the communication channels and manage the protocols associated	There are 850, 900, 1800 and 1900 MHz to manage the system frequency and to support the communication. 850 and 1900 MHz is used in America and other frequencies in Europe, Asia, Africa and other middle east
GSM is good at controlling circuit switching traffic and manages all the circuit in the network to control the traffic of mobile devices	GPRS is good at handling packets and even the data is transferred in the form of packets. Hence, traffic is also controlled as packets and manage the packets in the network of GPRS
The location are concept is used so that the mobiles are traced and communicated with a location within the GSM network	The routing area concept is used as the data is transferred as packets and these are used in the communication of the mobile devices
It takes a long time to connect with any network through GSM an=s it has circuit switching and manages it through the symmetric mode of transmission. The data transmission is monitored and managed through circuits in the network	A network connection is done faster in the system as packet data is used in GPRS. Data transmission through packets makes the system to manage the data and send messages in the asymmetric mode of transmission. The maximum speed is 114 Kbps
Internet service is not provided in GSM and this makes communication harder in the system. Communication has to be done through messages or calls.	Internet services are provided in GPRS and this is done with wireless systems. Hence the internet can be used even in remote areas and communication is done through emails or other messaging services with the internet
GSM does not have GPRS incorporated in the system and hence it need not manage other services when GSM is in use. This makes communication simple	GPRS incorporates GSM in the network but the communication is made simply by allowing GSM services even when the user is using GPRS services. Thus, GPRS modifies the GSM network
GSM is used in almost all countries and remote areas. Hence, GSM provides its service to the fullest to the user.	GPRS services cannot be offered in all the countries ad remote areas. This makes GPRS confined to development areas with a proper network connection
Single time slots are allowed per user in the system	Multiple time slots are allowed to the user in the system and this makes the user use different applications at a time.

2. Give different Tele-services provided by GSM.

Ans: GSM offers three basic types of services:

- Telephony services or teleservices
- Data services or bearer services
- Supplementary services

Tele-services

- The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

Voice Calls-

- The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.

Videotext and Facsmile-

- Another group of teleservices includes Videotext access, Teletex transmission, Facsmile alternate speech and Facsmile Group 3, Automatic Facsmile Group, 3 etc.

Short Text Messages-

- Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

Bearer Services

- Data services or Bearer Services are used through a GSM phone. To receive and send data is the essential building block leading to widespread mobile Internet access and mobile data transfer. GSM currently has a data transfer rate of 9.6k. New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

Supplementary Services

- Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others.

3. What kind of changes need in GSM to convert it into GPRS explain that? Explain application of GPRS?

Ans: The GPRS network architecture reuses the GSM network nodes such as MSC/VLR. HLR, and BSS. New network nodes have been introduced for the transport of packet data. These nodes are-

1. Gateway GPRS support nodes(GGSN)
2. Service GPRS support nodes(SGSN)

- The subnetwork formed by the SGSNs and the GGSNs is called the GPRS core network. In order to reuse the GSM node, new interfaces have been defined between the GSM network nodes and the different elements of the GPRS core network.

GPRS network has following elements:

1. SGSN:
   The SGSN is the node that is serving the MS; it is responsible for GMM. It delivers packets to the MSs and communicate with HLR to obtain the GPRS subscriber profile. It manages the registration of the new mobile subscriber in order to keep a record of their LA for routing purposes. The SGSN can be connected to one or several BSSs
2. GGSN:
   The GGSN provides interworking with external packet data networks (PDNs). It may be linked to the one or several data network. It is connected with SGSN via an IP-based GPRS backbone network. The GGSN is a router that forwards incoming packets from the external PDN to the SGSN of the addressed MS. It also forwards the outgoing packets to the external PDN. The PDN is external data network to which the connected the GPRS network. An example of a PDN is the internet network.
3. HLR:
   The HLR is a database that contain,among other things, packet domain subscription data in routing information
4. Mobile switching center/visitor location register (MSC/VLR):
   The MSC coordinates the setting up of calls to and from GSm users and manages GSM mobility. The MSC is not only directly involved in the GPRS network. It forwards circuit-switched paging for the GPRS-attached MSs to the SGSN when the Gs interface is present.
5. BSS:
   The BSS ensures the radio connection between the mobile and the network. It is responsible for radio access management. The BSS is composed of two elements: the BTS and the BSC. The BTS integrates all the radio transmission and radio reception boards. The BSC is responsible for the management of the radio channels. The BSC has switching capabilities that are used for circuit-switched calls and can also be used for GPRS traffic
6. EIR:
   The EIR is a database that contains terminal identities.

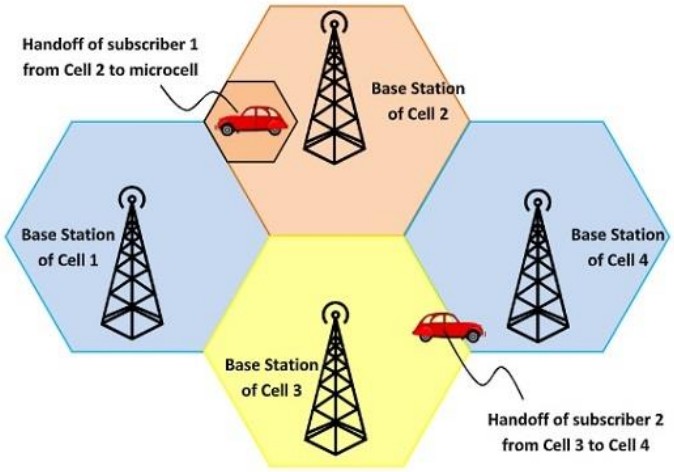
Application of GPRS:

1. Communication: E-mail, fax, unified messaging and internet/intranet access etc.
2. Value-added services: information services and games etc.
3. E-commerce: retail, ticket purchasing, banking and financial trading, etc.
4. Location based application: navigation, traffic conditions, airline/rail schedules and location finder, etc
5. Vertical application: freight delivery, fleet management, and sales-force automation
6. Advertising: it may be location sensitive. Foe ex: a user entering a mall can receive advertisements specific to the stores in that mall.

4. What are the needs of Mobile IP? Explain handoff operation in Mobile IP.

Ans: Mobile IP (Internet Protocol) enables the transfer of information to and from mobile computers, such as laptops and wireless communications. The mobile computer can change its location to a foreign network and still access and communicate with and through the mobile computer's home network.

In cellular communications, the handoff is the process of transferring an active call or data session from one cell in a cellular network or from one channel to another.Handoff is necessary for preventing loss of interruption of service to a caller or a data session user. Handoff is also called handover.



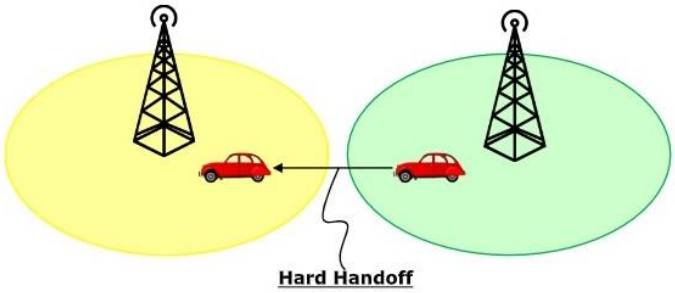
Handoffs are triggered in any of the following situations –

- If a subscriber who is in a call or a data session moves out of coverage of one cell and enters coverage area of another cell, a handoff is triggered for a continuum of service. The tasks that were being performed by the first cell are delineating to the latter cell.
- Each cell has a pre-defined capacity, i.e. it can handle only a specific number of subscribers. If the number of users using a particular cell reaches its maximum capacity, then a handoff occurs. Some of the calls are transferred to adjoining cells, provided that the subscriber is in the overlapping coverage area of both the cells.
- Cells are often sub-divided into microcells. A handoff may occur when there is a transfer of duties from the large cell to the smaller cell and vice versa. For example, there is a traveling user moving within the jurisdiction of a large cell. If the traveler stops, then the jurisdiction is transferred to a microcell to relieve the load on the large cell.
- Handoffs may also occur when there is an interference of calls using the same frequency for communication.

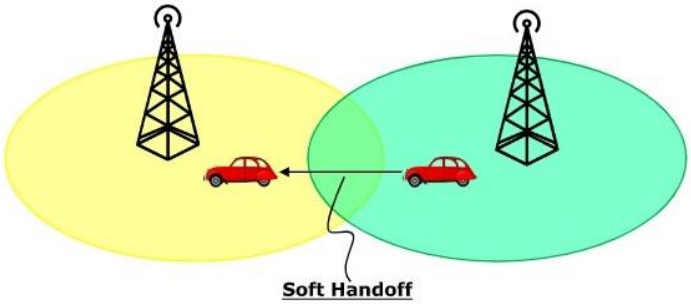
There are two types of handoffs –

1. Hard handoff- In a hard handoff, an actual break in the connection occurs while switching from one cell to another. The radio links from the mobile station to the

existing cell is broken before establishing a link with the next cell. It is generally an inter-frequency handoff. It is a “break before make” policy.



2. Soft handoff- In soft handoff, at least one of the links is kept when radio links are added and removed to the mobile station. This ensures that during the handoff, no break occurs. This is generally adopted in co-located sites. It is a “make before break” policy.

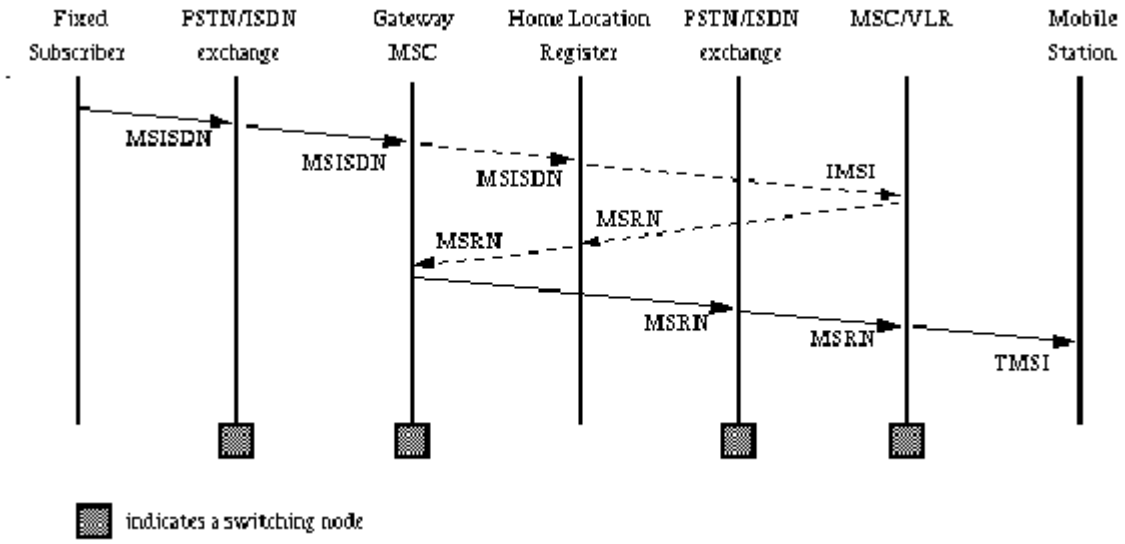


5. Explain GSM call routing.

Ans: In a mobile system the endpoints of the connection may not be fixed. A GSM subscriber may roam nationally as well as internationally. The number dialed to reach a specific Mobile Station is called the Mobile Subscriber ISDN (MSISDN).

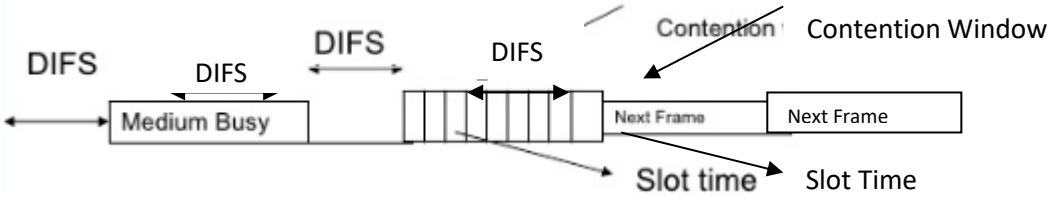
The process of locating a MS when calling it, is complex. A incoming call i directed to a Gateway MSC (GMSC), which is a MSC with added functionality to get the HLR database for routing information. The information returned to the GMSC is the Mobile Station Roaming Number (MSRN), which is a temporary number that identifies the MSC servicing the MS.

In figure, the typical routing scenario is shown. The scenario starts with the GMSC asking the HLR for a MSRN. The HLR typically only stores the address of the subscribers current VLR, therefore the HLR needs to inquire this VLR for a MSRN. The VLR allocates a MSRN from an associated pool to the call and creates a binding between the called subscribers IMSI and the MSRN. This MSRN is returned to the HLR and the inquiring GMSC. The GMSC can now route the call to the MSC servicing the called MS. The MSC uses the MSRN to look up the IMSI of the MS and uses this to page the MS.



6.Explain DFWMAC-DCF using CSMA/CA.

Ans: A mobile device waits for DIFS and if the medium is free after DIFS, it accesses the medium. So the medium is busy.



- Once the above device releases the resources in the medium, it waits for DIFS. The contention period starts. A few devices start their random back off timer and the countdown of the timers start.
- Whichever device that completes the timer back off time first will get the access to the medium.
- As soon as the device senses that the medium is busy, it loses the chance for this cycle and has to try after DIFS duration.
- Now the back off time is initialised for the rest of the devices and they start all over again after DIFS.
- **Short interframe spacing (SIFS):**
- Highest priority, acknowledgements, polling responses
- **PCF interframe spacing (PIFS):**
- Medium priority, time bounded service
- **DCF interframe spacing (DIFS):**
- Asynchronous data service within contention period- lowest priority
- Issue with the Above Scheme:
- A node will not have a Priority once it has lost the chance. Irrespective of the amount of wait in the last cycle, it has to start all over again.

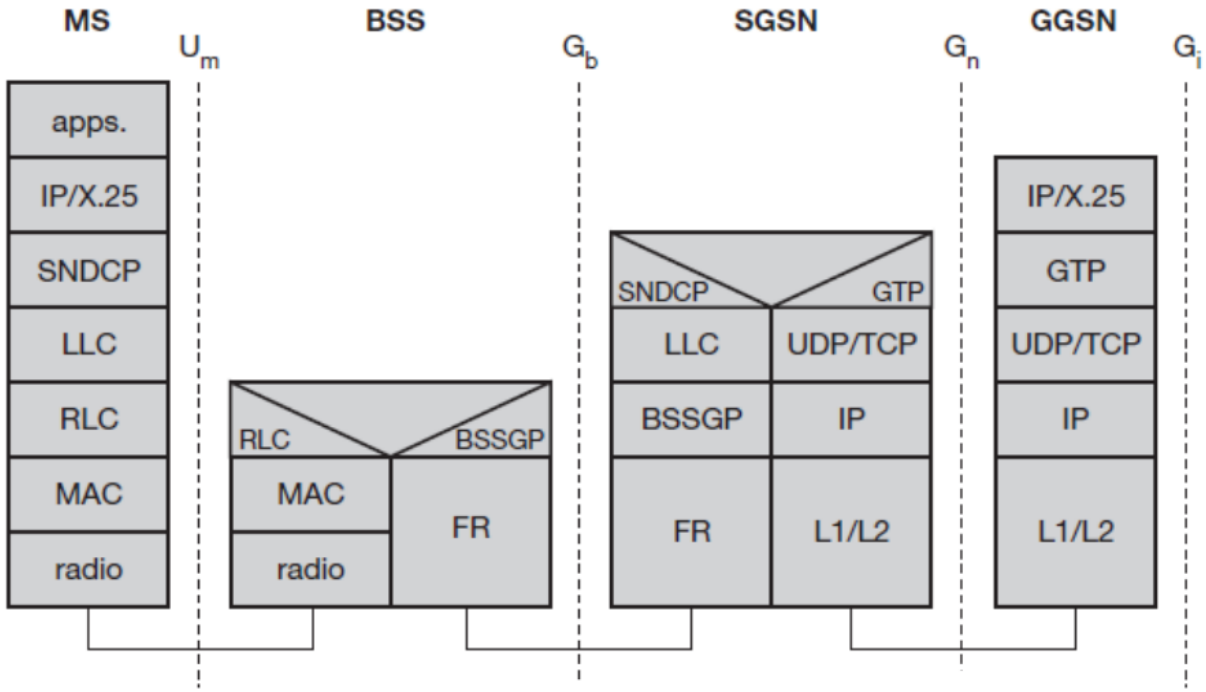
7. Differentiate GSM and CDMA.

Parameter	GSM	CDMA
Full form	Global System for Mobile communication.	Code Division Multiple Access.
Technology used	FDMA (Frequency division multiple access) and TDMA (Time division multiple access).	CDMA (Code division multiple access).
Availability	GSM is globally widely used and available.	CDMA is available in fewer countries and carriers.
Data speed rate	42Mbps in HSPA (3G).	3.6Mbps in CDMA.
Features	GSM supports transmitting data and voice both at once.	CDMA does not support this feature.
Customer Information	Stored in a SIM card.	Stored in a headset or phone.
Handoff	Hard handoff	Soft handoff
Multiple Access Technique	TDMA	CDMA
Type of System	Band limited	Power limited
Frequency reuse	Max 3.	Max 1.
Carrier Frequency	200 KHz	1.25 MHz
Spread Spectrum	Not applicable	Applicable
System Capacity	Less	4-5 times greater than GSM

2
2

8. Draw and explain the GPRS transmission plane protocol model.

Ans: The GPRS protocol stack for user data transmission is shown in Fig. Um (air interface), Gb, and Gn are the interfaces located between MS and BSS, BSS and SGSN, and SGSN and GGSN respectively. Here, we only describe the protocols implemented in the developed model. SNDCP protocol encapsulates the IP packets in GPRS specific packet formats. LLC layer provides a reliable logical link to the data units from the higher layer. This logical link is independent of the underlying radio interface protocols. LLC layer provides either acknowledged or unacknowledged data transmission. GTP tunnels user data between the two GSNs in the GPRS backbone network. BSSGP layer conveys routing and QoS-related information between the BSS and the SGSN. RLC layer provides a reliable radio link for data transfer between the MS and the BSS. MAC layer controls the multiplexing of signalling and data messages from various GPRS users. GSM RF (Radio Frequency) layer controls the physical channel management, modulation, demodulation, transmission, power control, and channel coding/decoding.



- The flow of GPRS protocol stack and end-to-end message from MS to the GGSN is displayed in the below diagram. GTP is the protocol used between the SGSN and GGSN using the Gn interface. This is a Layer 3 tunnelling protocol.
- The process that takes place in the application looks like a normal IP sub-network for the users both inside and outside the network. The vital thing that needs attention is, the application communicates via standard IP, that is carried through the GPRS network and out through the gateway GPRS. The packets that are mobile between the GGSN and the SGSN use the GPRS tunnelling protocol, this way the IP addresses located on the external side of the GPRS network do not have deal with the internal backbone. UDP and IP are run by GTP.
- The air interface provides radio channel connection between an MS and BTS. GPRS employs distinct frequencies in uplink (radio link from MS to BTS) and downlink (radio link from BTS to MS) directions. It employs a combination of frequency division and time division multiple access (FDMA and TDMA) schemes to allocate radio resources (physical channels). A physical channel in GPRS is defined as a radio frequency channel and time slot pair. GPRS employs a 52-frame multiframe structure: each multiframe consists of 52 TDMA frames and four TDMA frames constitute a radio block. Each TDMA frame consists of eight time slots. The Protocol Data Units (PDUs) exchanged between the RLC/MAC entities in the MS and the BTS are called RLC/MAC blocks. Each PDU is transmitted in the same time slot over four continuous TDMA frames (in one radio block). In order to provide higher throughputs, an MS supporting GPRS may transmit or receive in several time slots of a TDMA frame. This capability is indicated by the multislot class of the MS. GPRS shares physical channels with GSM.
- Sub Network Dependent Convergence Protocol (SNDCP) and Logical Link Control (LLC) combination used in between the SGSN and the MS. The SNDCP flattens data to reduce the load on the radio channel. A safe logical link by encrypting packets is

provided by LLC and the same LLC link is used as long as a mobile is under a single SGSN.

- In case, the mobile moves to a new routing area that lies under a different SGSN; then, the old LLC link is removed and a new link is established with the new Serving GSN X.25. Services are provided by running X.25 on top of TCP/IP in the internal backbone.

UNIT 4:

1. What are the advantages of WLAN?

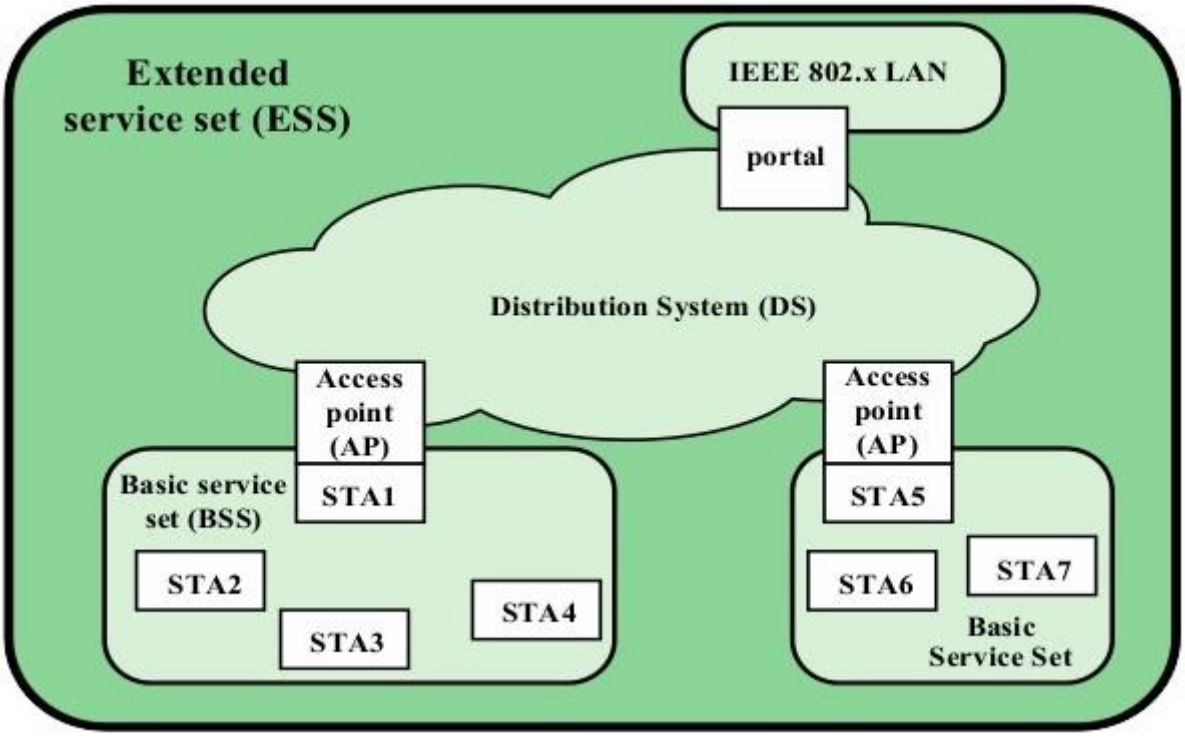
Ans: The advantages of WLAN are as follows:

- **Mobility**: WLAN offers wire-free access within operating range.
- **Low Implementation Costs**: WLAN is easy to setup, relocate, change and low cost.
- **Installation Speed and Simplicity**: Fast and simple installation of WLAN.
- **Network Expansion**: Easy expansion of WLAN possible.
- **Higher Flexibility**: Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls.
- **Planning**: Wireless ad hoc networks allow for communication without planning. Wired networks need wiring plans.
- **Robustness**: Wireless networks can survive disasters; if the wireless devices survive people can still communicate.

2. Draw and Explain the IEEE 802.11 Architecture in Details.

Ans: IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

- The IEEE developed an international standard for WLANs. The 802.11 standard focuses on the bottom two layers of the OSI model, the physical layer (PHY) and data link layer (DLL).
- The objective of the IEEE 802.11 standard was to define a medium access control (MAC) sub layer, MAC management protocols and services, and three PHYs for wireless connectivity of fixed, portable, and moving devices within a local area.
- The three physical layers are an IR baseband PHY, an FHSS radio in the 2.4GHz band, and a DSSS radio in the 2.4GHz.
- The smallest building block of a wireless LAN is a basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same shared wireless medium.
- A BSS may isolate or it may connect to a backbone distribution system (DS) through an access point (AP).



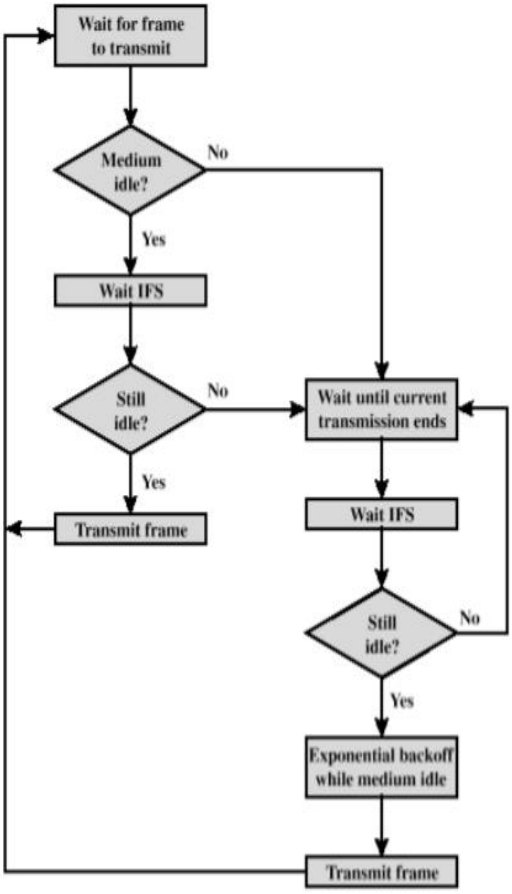
- The components of IEEE 802.11 architecture are as follows
- **Stations (STA)** − Stations comprise all devices and equipments that are connected to the wireless LAN. A station can be of two types:
- **Wireless Access Points (WAP)** − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
- **Client.** − Clients are workstations, computers, laptops, printers, smart phones, etc.
- Each station has a wireless network interface controller.
- **Basic Service Set (BSS)** −A basic service set is a group of stations communicating at physical layer level. BSS can be of two categories depending upon mode of operation:
- **Infrastructure BSS** − Here, the devices communicate with other devices through access points.
- **Independent BSS** − Here, the devices communicate in peer-to-peer basis in an ad hoc manner.
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.
- The AP functions as a bridge and a relay point. In a BSS, client stations do not communicate directly with one another.
- Rather, if one station in the BSS wants to communicate with another station in the same BSS, the MAC frame first sent from the originating station to the AP, and then from the AP to the destination station.
- Similarly, a MAC frame from a station in the BSS to a remote station sent from the local station to the AP and then relayed by the AP over the DS on its way to the destination station.
- The BSS generally corresponds to what referred to as a cell in the literature. The DS can a switch, a wired network, or a wireless network.
- When all the stations in the BSS mobile stations, with no connection to other BSSs, the BSS called an independent BSS (IBSS).

- **An IBSS is typically an ad hoc network. In an IBSS, the stations all communicate directly, and no AP involved.**
- A simple configuration is shown in Figure, in which each station belongs to a single BSS; that is, each station is within wireless range only of other stations within the same BSS.
- It is also possible for two BSSs to overlap geographically so that a single station could participate in more than one BSS.
- Further, the association between a station and a BSS dynamic. Stations may turn off, come within range, and go out of range.
- An extended service set (ESS) consists of two or more basic service sets interconnected by a distribution system.
- Typically, the distribution system a wired backbone LAN but can any communications network. The extended service set appears as a single logical LAN to the logical link control (LLC) level.
- The figure indicates that an access point (AP) implemented as part of a station; the AP the logic within a station that provides access to the DS by providing DS services in addition to acting as a station.
- To integrate the IEEE 802.11 architecture with a traditional wired LAN, a portal used. The portal logic implemented in a device, such as a bridge or a router. That part of the wired LAN and that attached to the DS.

3. Discuss with suitable diagram distributed coordination function with IEEE 802.11medium access control logic.

Ans: Distributed Coordination Function

- DCF makes use of simple CSMA algorithm.
    a) If a station has MAC frame to transmit, it listens to the medium.
    b) If the medium is idle, station may transmit.
    c) Otherwise it must wait until current transmission is complete.
- DCF does not include a Collision detection function.
- To ensure smooth and fair functioning of this algorithm, DCF includes a set of delays that amounts to a priority scheme.
- Let us consider a single delay known as an Inter Frame Space (IFS).



- Different Space(IFS) Usage
  1) **SIFS (Short IFS)**: The shortest IFS, used for immediate response actions.
  2) **PIFS (Point Coordination Function IFS)**: A mid-length IFS, used by centralized controller in the PCF Scheme.
  3) **DIFS (Distributed Coordination Function IFS)**: The longest IFS, used as a minimum delay for asynchronous frames.

4. List all and explain any five IEEE 802.11 services.

Ans: Services are divided into two sections:

1) Station Services(SS)
2) Distribution System Services(DSS)

There are five services provided by the DSS.

1) Association
2) Reassociation
3) Disassociation
4) Distribution
5) Integration

Station services are:

1) Authentication
2) Deauthentication
3) Privacy
4) MAC Service Data Unit(MSDU) Delivery

Distribution System Services:

- Distribution system services, as defined by 802.11, provide functionality across a distribution system. Access points provide distribution system services.

(1)Association:

- Each station must initially invoke the association service with an access point before it can send information through a distribution system. The association maps a station to the distribution system via an access point.
- Each station can associate with only a single access point, but each access point can associate with multiple stations. Association is also a first step to providing the capability for a station to be between BSSs.

(2)Disassociation:

- A station or access point may invoke the disassociation service to terminate an existing association.
- This service is a notification , therefore, neither party may refuse termination.
- Stations should disassociate when leaving the network. An access point, for example, may disassociate all its stations if being removed for maintenance.

(3)Distribution:

- A station uses the distribution service every time it sends MAC frames across a distribution system.
- The 802.11 standard does not specify how the distribution system delivers the data. The distribution service provides the distribution system with only enough information to determine the proper destination BSS.

Station Services:

- The 802.11 standard defines services for providing functions among stations. A station may be within any wireless element on the network, such as a handheld PC or handheld scanner.
- In addition, all access points implement station services. To provide the necessary functionality, these stations need to send and receive MSDUs and implement adequate levels of security.

(1)Deauthentication:

- When a station wants to disassociate from another station, it invokes the deauthentication service. Deauthentication is a notification and cannot be refused.

- A station performs deauthentication by sending an authentication management frame to advice of the termination of authentication.

(2)Privacy:

- With a wireless network, all stations and other devices can hear data traffic taking places within range on the network, seriously affecting the security level of a wireless link.
- IEEE 802.11 counters this problem by offering a privacy service option that raises the security level of the 802.11 network to that of a wired network.

5. Compare: WiMAX and Wi–Fi.

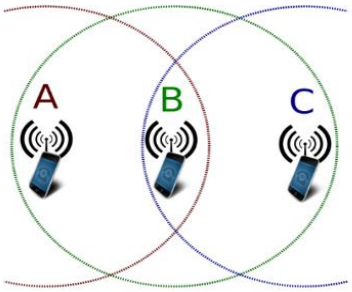
	WiMAX	**Wi-Fi**
	WiMax is for the WAN.	Wi-Fi is for a LAN.
Official Release:	WiMAX came into the picture in the year 2004.	Wi-Fi was officially launched in the year 1997.
IEEE Standards:	WiMAX is standardized under 802.16y family of wireless networking where y refers to various WiMAX versions.	Wi-Fi has been defined under IEEE 802.11x standards where x is various Wi-Fi versions.
Versions of the Standard:	WiMAX has a number of different versions: 802.16a, 802.16d and 802.16e are some popular WiMAX versions.	Wi-Fi has several versions of it such as 802.11b, 802.11g, and 802.11n.
Range:	An ideal WiMAX network can reach about 80-90 kilometers in terms of range.	An ideal Wi-Fi based network reaches around 100meters as it a maximum range.
Data transfer Rates:	WiMAX networks have a flexible bandwidth option which ranges from 1.25MHz to 20MHz.	Wi-Fi networks have a channel bandwidth of 20MHz.
Encryption Techniques:	WiMAX include Triple Data Encryption Algorithm and Advanced Encryption Standards.	Wi-Fi includes Advanced Encryption Standard (AES)and RC4.
Authentication:	WiMAX uses X.509 or PKMv2 as authentication algorithms.	Wi-Fi uses Extensible Authentication Protocol (EAP). Wired Equivalent Privacy (WEP), security algorithms depending on the Wi-Fi version.
Operating Frequency Band:	WiMAX technology provides two types of wireless services- Line of sight service with operating frequency band up to 66 GHz, whereas, for non-line of sight service, the operating frequency is between 2 to 11 GHz.	Wi-Fi operates in the unlicensed 2.4 GHz and 5 GHz bands.

Communication Type:	WiMAX supports full duplex communication with 256 FFT OFDM along with single carrier and 2048 FFTOFDM technology.	Wi-Fi supports half duplex communication with 52 FFT OFDM technology.
Mobility:	WiMAX provides both fixed and mobile versions. The fixed version (802.16e and 802.16d) is used for residential as well as business areas, whereas the mobile version is seen to replace existing mobile network technologies like GSM or CDMA.	Wi-Fi currently provides the fixed version, the mobile version being in development.

6. Discuss hidden and exposed terminals.

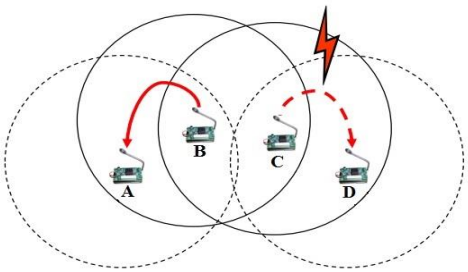
Ans: **Hidden Terminal Problem:**

- A wireless network with lack of centralized control entity, sharing of wireless bandwidth among network access nodes i.e. medium access control (MAC) nodes must be organized in decentralized manner.
- The hidden terminal problem occurs when a terminal is visible from a wireless access point (APs), but not from other nodes communicating with AP. This situation leads the difficulties in medium access control sub-layer over wireless networking.
- In a formal way hidden terminals are nodes in a wireless network that are out of range of other node or a collection of nodes.
- Consider the scenario of wireless networking with three wireless devices(e.g. mobile The transmission range of access point A reaches at B, but not at access point C, similarly transmission range of access point C reaches B, but not at A. These nodes are known as hidden terminals. The problem occurs when nodes A and C start to send data packets simultaneously to the access point B. Because the access points A and c are out of range of each other and resultant they cannot detect a collision while transmitting, Carrier sense multiple access with collision detection (CSMA/CD) does not work, and collisions occur, which then corrupt the data received by the access point B due to the hidden terminal problem.
- The hidden terminal analogy is determined as follows
    - Terminal C wants to send data to B, terminal C senses a "free" medium (CS fails) and starts transmitting.
    - Collision at B occurs, A cannot detect this collision (CD fails) and continues with its transmission at B
    - Terminal A is "hidden" from C and vice versa
- Some other technology that can be employed to solve hidden node problem are: Increase Transmitting Power from the Nodes. With the enhancement of the transmission power of access point can solve the hidden terminal problem by allowing the cell around each mode to increase in size, encompassing all of the nodes.
- Use Omni directional antennas: Since nodes using directional antennas are nearly invisible to nodes that are not positioned in the direction the antenna is aimed at, directional antennas should be used only for very small networks.



Exposed Terminal Problem:

- In wireless networks, when a node is prevented from sending packets to other nodes because of a neighboring transmitter is known as the exposed node problem
- Consider the wireless network having four nodes labeled A,B,C and D, where the two receivers are out of range of each other, yet the two transmitters (B,C) in the middle are in range of each other.
- Here, if a transmission between A and B is taking place, node C is prevented from transmitting to D as it concludes after carrier sense that it will interfere with the transmission by its neighbor node B.However note that node D could still receive the transmission of C without interference because it is out of range from B. Therefore, implementing directional antenna at a physical layer in each node could reduce the probability of signal interference, because the signal is propagated in a narrow band.
- The exposed terminal analogy is described as follows:
    - B sends to A , C wants to send to another terminal D not A or B
    - C senses the carrier and detects that the carrier is busy
    - C postpones its transmission until it detects the medium as being idle again
    - But A is outside radio range of C, waiting is not necessary
    - C is "exposed" to B



Hidden Vs Exposed Terminal Problem

- In the case of hidden terminal problem, unsuccessful transmissions result from collisions between transmissions originated by a node such as node A which cannot hear the ongoing transmissions to its corresponding node B. The probability of such a collision is proportional to the total number of terminal hidden from node A
- In the case of exposed terminal, unsuccessful transmissions result from nodes such as node A being prevented from transmitting because their corresponding node is unable to send a CTS. Again such unsuccessful transmissions are proportional to the number of exposed terminals. Both these events lead to degradation of node's throughput.