END TERM EXAMINATION [DEC. 2016]
SEVENTH SEMESTER [B.TECH.]
WIRELESS COMMUNICATION (ETEC-405)

Time : 3 hrs. **M.M. : 75**

Note: Attempt any five questions including Q. no. 1 which is compulsory.

Q.1. (*a*) What are the two major parts of a typical PCS network architecture? **(3)**

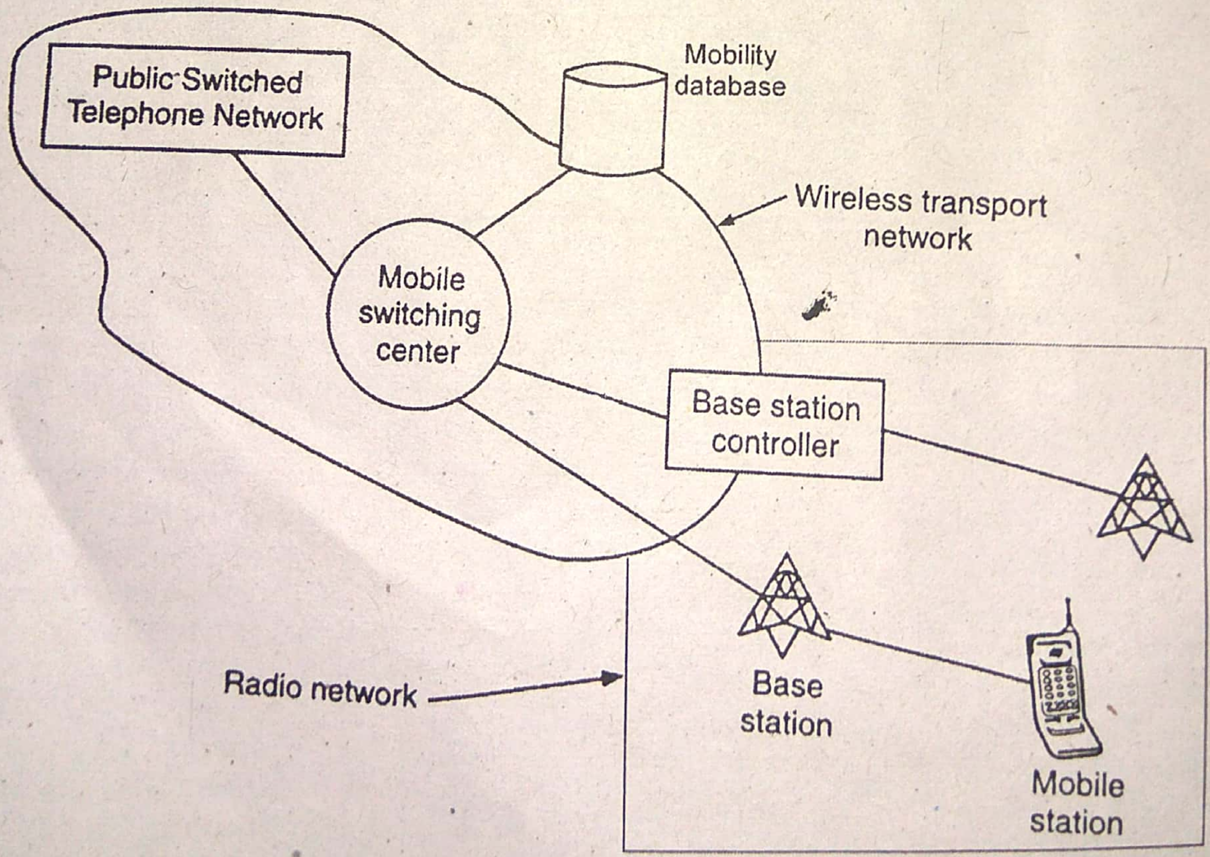
Ans. The PCS architecture consist of two part

i. Radio network

ii. Wireless transport network

Radio Network: PCS users carry mobile stations (MS) to communicate with a BS in a PCS network. MS is also referred to as handset or mobile phone. The radio coverage of a base station is called cell. In GSM network, each cell is controlled by BSC which are connected to MS through BS. The BSC are connected to MSC by landlines.

Wireline Transport Network: An MSC is a telephone exchange configured specially for mobile applications. It interfaces the MS (via BS) with PSTN. MSCs are also connected with mobility database to track the location of MS and roaming management. The databases are HLR and VLR. HLR contains the authentication information like IMSI (International Mobile Subscriber Identity), identification information like name, address of the subscriber, billing information like prepaid or postpaid, operator selection, denial of service to a susbscriber etc. VLR gives information about the location area of the subscriber while on roaming and power off status of the handset.



Q.1. (*b*) What are the differences between the second generation mobile technology and third generation mobile technology? **(3)**

Ans. Difference between 2G and 3G Technology

• **Cost:** The license fee to be paid for 3G network is much higher as compared to 2G networks. The network construction and maintenance of 3G is much costlier than 2G networks. Also from the customers point of view the expenditure for 3G network will be excessively high if they make use of the various applications of 3G.

• **Data Transmission:** The main **difference between 2G and 3G** networks is seen by the mobile users who download data and browse the Internet on the mobile phones. They find much faster download speeds, faster access to the data and applications in 3G networks as compared to 2G networks. 2G networks are less compatible with the functions of smart phone. The speed of data transmission in 2G network is less than 50,000 bits per sec while in 3G it can be more than 4 million bits per sec.

• **Function:** The main function of 2G technology is the transmission of information via voice signals while that of 3G technologies is data transfer via video conferencing, MMS etc.

• **Features:** The features like mobile TV, video transfers and GPS systems are the additional features of 3G technology that are not available with 2G technologies.

• **Frequencies:** 2G technology uses a broad range of frequencies in both upper and lower bands, under which the transmission depends on conditions such as weather. A drawback of 3G is that it is simply not available in certain regions.

• **Implication:** 3G technology offers a high level of security as compared to 2G technology because 3G networks permit validation measures when communicating with other devices.

• **Making Calls:** Calls can be made easily on both 2G and 3G networks with no real noticeable differences except that in 3G network video calls can also be made. The transmission of text messages and photos is available in both the networks but 2G networks have data limit and the speed of the data transmission is also very slow as compared to 3G.

•**Speed:** The downloading and uploading speeds available in 2G technologies are up to 236 Kbps. While in 3G technology the downloading and uploading speeds are up to 21 Mbps and 5.7 Mbps respectively

Q.1. (c) What are the main parts of the GSM SMS protocol stock? (3)

Ans. The CM layer is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management. Each of these services are treated as individual layer within the CM layer.

Q.1. (d) What is EDGE? Explain. (3)

Ans. EDGE (enhanced data for global evolution) EDGE (also known as Enhanced GPRS or EGPRS) is a data system used on top of GSM networks. It provides nearly three times faster speeds than the outdated GPRS system. The theoretical maximum speed is 473 kbps for 8 timeslots but it is typically limited to 135 kbps in order to conserve spectrum resources. Both phone and network must support EDGE, otherwise the phone will revert automatically GPRS.EEDGE meets the requirements for a 3G network but is usually classified as 2.75G.

1. Q. (e) What is Wi-Max Technology? Explain (3)

Ans. WiMAX (Worldwide Interoperability for Microwave Access) is a family of wireless communication standards based on the IEEE 802.16 set of standards, which provide multiple physical layer (PHY) and Media Access Control (MAC) options. WiMAX was initially designed to provide 30 to 40 megabit-per-second data rates, with the 2011 update providing up to 1 Gbit/s for fixed stations.

The bandwidth and range of WiMAX make it suitable for the following potential applications:

- Providing portable mobile broadband connectivity across cities and countries through various devices.
- Providing a wireless alternative to cable and digital subscriber line (DSL) for "last mile" broadband access.
- Providing data, telecommunications (VoIP) and IPTV services (triple play).
- Providing Internet connectivity as part of a business continuity plan.
- Smart grids and metering

Q.2. (*a*) How do TDMA, FDMA and CDMA works? Complete these three technologies **(8)**

Ans. TDMA : TDMA is a digital technique that divides a single channel or band into time slots. Each time slot is used to transmit one byte or another digital segment of each signal in sequential serial data format. This technique works well with slow voice data signals, but it's also useful for compressed video and other high-speed data.

FDMA: FDMA is the process of dividing one channel or bandwidth into multiple individual bands, each for use by a single user *(Fig. 1)*. Each individual band or channel is wide enough to accommodate the signal spectra of the transmissions to be propagated. The data to be transmitted is modulated on to each subcarrier, and all of them are linearly mixed together.

CDMA: CDMA is another pure digital technique. It is also known as spread spectrum because it takes the digitized version of an analog signal and spreads it out over a wider bandwidth at a lower power level. This method is called direct sequence spread spectrum (DSSS) as well .

Frequency division multiple access (FDMA):

It is a technology by which the total bandwidth available to the system is divided into frequencies. This division is done between non overlapping frequencies that are then assigned to each communicating pair (2 phones)

FDMA is used mainly for analog transmission. Its not that this technology is not capable of carrying digital information, but just that it is not considered to be an efficient method for digital transmission. Because just imagine if the frequencies to handle the customers gets over? What if more capacity is required? The only option would be to drill down the existing frequencies to a much narrower amount which will not be very competent. In FDMA all users share the satellite simultaneously but each user transmits at single frequency.

To understand this technology better, just imagine how FM radio works. All the radios have their own frequency bands and they send their signals at the carefully allocated unique frequencies within the available bands.

Code division multiple access (CDMA):

Unlike FDMA, CDMA separates calls by code. Every bit of a conversation is been tagged with a specific and unique code. The system gets a call, it allocates a unique code to that particular conversation, now the data is split into small parts and is tagged with the unique code given to the conversation of which they are part of. Now, this data in small pieces is sent over a number of the discrete frequencies available for use at any time in the specified range. The system then at the endreassembles the conversation from the coded bits and deliver itJ Does it make sense?

Just think about how you recollect your luggage at the end of the flight journey. When you check in, a tag with a code is given to you which is also given to your luggageJ And at the destination, you collects your luggage on the basis of thatJ I know you will say that you recognize your bag, but then I have a habit of always matching the codes of my bag and the one on the tag given to me and that is how I become sure of not picking up the wrong lunguageJ

Time division multiple access (TDMA):

Unlike FDMA and CDMA, In TDMA the division of calls happens on time basis. The system first digitizes the calls, and then combines those conversations into a unified digital stream on a single radio channel. Now it divides each cellular channel into three time slots that means three calls get put on a single frequency and then, a time slot is assigned to each call during the conversation, a regular space in a digital stream. The users transmit in rapid succession, one after the other, each using its own time slot. This allows multiple stations to share the same transmission medium (e.g. radio frequency channel) while using only a part of its channel capacity.

This technology enables three different users to use one frequency at the same time.

Here there is no need for three separate frequencies like in FDMA. As in FDMA, instead of monopolizing a single radio channel for a single call, TDMA efficiently carries three calls at the same timeJ

BTW, this technology is the one used in our GSM system

Q.2. (*b*) What is mobility management? Explain. **(7)**

Ans. Mobility management is one of the major functions of a GSM or a UMTS network that allows mobile phones to work. The aim of mobility management is to track where the subscribers are, allowing calls, SMS and other mobile phone services to be delivered to them.

Location update procedure

The location update procedure allows a mobile device to inform the cellular network, whenever it moves from one location area to the next. Mobiles are responsible for detecting location area codes (LAC). When a mobile finds that the location area code is different from its last update, it performs another update by sending to the network, a location update request, together with its previous location, and its Temporary Mobile Subscriber Identity (TMSI).

The mobile station also stores the current LAC in the SIM card, concatenating it to a list of recently used LACs. This is done to avoid unnecessary IMSI attachment procedures in case the mobile station has been forced to switch off (by removing the battery, for example) without having a chance to notify the network with an IMSI detach and then switched on right after it has been turned off. Considering the fact that the mobile station is still associated with the Mobile Switching Center/Visitor Location Register (MSC/VLR) of the current location area, there is no need for any kind of IMSI attachment procedures to be done. There are several reasons why a mobile may provide updated location information to the network. Whenever a mobile is switched on or off, the network may require it to perform an IMSI attach or IMSI detach location update procedure. Also, each mobile is required to regularly report its location at a set time interval using a *periodic location update* procedure. Whenever a mobile moves from one location area to the next while not on a call, a *random location* update is required. This is also required of a stationary mobile that reselects coverage from a cell in a different location area, because of signal fade. Thus, a subscriber has reliable access to the network and may be reached with a call, while enjoying the freedom of mobility within the whole coverage area.

When a subscriber is paged in an attempt to deliver a call or SMS and the subscriber does not reply to that page then the subscriber is marked as absent in both the MSC/

VLR and the Home Location Register (HLR) (Mobile not reachable flag MNRF is set). The next time the mobile performs a location update, the HLR is updated and the mobile not reachable flag is cleared.

Q.3. (*a*) What is hand off? What is roaming? How do you perform hand off during roaming?

Ans. Roaming is one of the fundamental mobility management procedures of all cellular networks. Roaming is defined as the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services, including home data services, when travelling outside the geographical coverage area of the home network, by means of using a visited network. This can be done by using a communication terminal or else just by using the subscriber identity in the visited network. Roaming is technically supported by a mobility management, authentication, authorization and billing procedures.

Handoff : In cellular telecommunications, the terms **handover** or **handoff** refer to the process of transferring an ongoing call or data session from one channel connected to the core network to another channel. In satellite communications it is the process of transferring satellite control responsibility from one earth station to another without loss or interruption of service.

The most basic form of handover is when a phone call in progress is redirected from its current cell (called *source*) to a new cell (called *target*).[1] In terrestrial networks the source and the target cells may be served from two different cell sites or from one and the same cell site (in the latter case the two cells are usually referred to as two *sectors* on that cell site). Such a handover, in which the source and the target are different cells (even if they are on the same cell site) is called *inter-cell*handover. The purpose of inter-cell handover is to maintain the call as the subscriber is moving out of the area covered by the source cell and entering the area of the target cell.

A special case is possible, in which the source and the target are one and the same cell and only the used channel is changed during the handover. Such a handover, in which the cell is not changed, is called *intra-cell* handover. The purpose of intra-cell handover is to change one channel, which may be interfered or fading with a new clearer or less fading channel.

In addition to the above classification of *inter-cell* and *intra-cell* classification of handovers, they also can be divided into hard and soft handovers

Hard handover: Is one in which the channel in the source cell is released and only then the channel in the target cell is engaged. Thus the connection to the source is broken before or 'as' the connection to the target is made—for this reason such handovers are also known as *break-before-make*. Hard handovers are intended to be instantaneous in order to minimize the disruption to the call. A hard handover is perceived by network engineers as an event during the call. It requires the least processing by the network providing service. When the mobile is between base stations, then the mobile can switch with any of the base stations, so the base stations bounce the link with the mobile back and forth. This is called 'ping-ponging'.

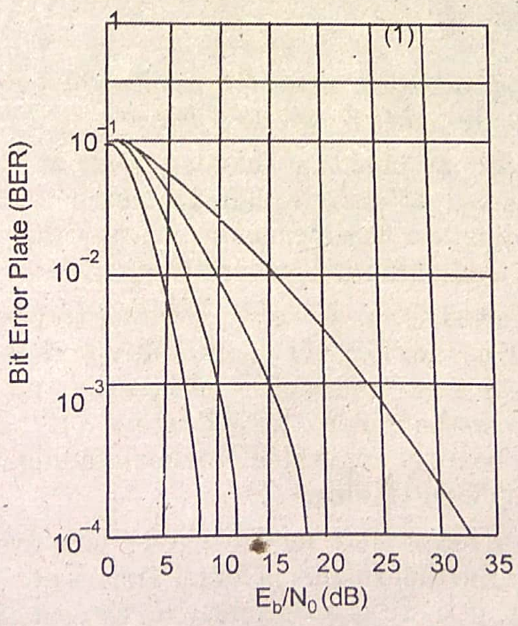
Soft handover: Is one in which the channel in the source cell is retained and used for a while in parallel with the channel in the target cell. In this case the connection to the target is established before the connection to the source is broken, hence this handover is called *make-before-break*. The interval, during which the two connections are used in parallel, may be brief or substantial. For this reason the soft handover is perceived by network engineers as a state of the call, rather than a brief event. Soft handovers may involve using connections to more than two cells: connections to three, four or more cells can be maintained by one phone at the same time. When a call is in a state of soft handover, the signal of the best of all used channels can be used for the call at a given moment or all the signals can be combined to produce a clearer copy of the signal. The latter is more advantageous, and when such combining is performed both in the downlink (forward link) and the uplink (reverse link) the handover is termed as *softer*. Softer handovers are possible when the cells involved in the handovers have a single cell site.

Handover can also be classified on the basis of handover techniques used. Broadly they can be classified into three types:

1. Network controlled handover
2. Mobile phone assisted handover
3. Mobile controlled handover

Q.3. (*b*) Discuss about BER performance in fading channels. **(7)**

Ans. One of the major distinctions between the wire -line and wireless communication lies in the physical properties of wireless channels which include propagation losses, multipath, fading, and so on. Different transmission media have different properties and are modeled differently. Different channel models ; flat and frequency selective fading fast and slow fading ,AWGN, Rayleigh and Rician fading channels. In the performance analysis of a wireless communication system. defining bit error rate (BER; no of bit errors per bit transfered) is very important. Rician fading. wireless channel can be characterized by a parameter K (Rician factor) which is defined as the ratio of the dominant (line of-light) path to the scattered path (multipath). When k = 0, the channel is Raylight channel (the power in dominant path is zero). When K = ∞; the channel is AWGN channel (the power in scattered path is zero). For any finite value of K, the channel is Rician channel.



k = 16; (5)

The theoretical BER vs E_b/N_0 Ratio curve for various Fading conditions (1) Frequency selective fading of fast fading distortion; (2) Flat fading and slow fading rayleigh limit K = 0; (3) Rician fading k = 4; (4) Rician fading (5) Additive white gaussian noise k = ∞.

BER performance as a function of $\frac{E_b}{N_0}$ is plotted in Fig. for various fading channel models. It can be observed that as $\frac{E_b}{N_0}$ ratio increases, the bit-error rate drops. Following conclusions can be obtained from the graph about different fading channel models.

With a reasonably high $\frac{E_b}{N_0}$ ratio, an AWGN wireless channel exhibits fairly good performance.

- A Rician fading channel model exhibit provides good performance with larger values of K.
- The Rayleigh fading channel model provides relatively poor performance.The situation is same for slow as well as flat fading.
- Finally, in aces fast fading and frequency selective fading channel in an urban environment, fading effects worse than the so-called worst case of Rayleigh fading. In such cases, BER performance remains poor even if we increase $\frac{E_b}{N_0}$ ratio.

Q.4. (*a*) What is distance dependent fading? What is rayleight fading? What is shadow fading?

Ans. Distance dependent fading: The strength of received signal varies with distances is known as distance dependent fading. There are two type of distance dependent fading:

(1) long distance

(2) short distance

Rayleigh fading is a statistical model for the effect of a propagation environment on a radio signal, such as that used by wireless devices.

Rayleigh fading models assume that the magnitude of a signal that has passed through such a transmission medium (also called a communications channel) will vary randomly, or fade, according to a Rayleigh distribution — the radial component of the sum of two uncorrelated Gaussian random variables.

Rayleigh fading is viewed as a reasonable model for tropospheric and ionospheric signal propagation as well as the effect of heavily built-up urban environments on radio signals. Rayleigh fading is most applicable when there is no dominant propagation along a line of sight between the transmitter and receiver. If there is a dominant line of sight, Rician fading may be more applicable. Rayleigh fading is a special case of two-wave with diffuse power (TWDP) fading.

Rayleigh fading is a reasonable model when there are many objects in the environment that scatter the radio signal before it arrives at the receiver. The central limit theorem holds that, if there is sufficiently much scatter, the channel impulse responsewill be well-modelled as a Gaussian process irrespective of the distribution of the individual components. If there is no dominant component to the scatter, then such a process will have zero mean and phase evenly distributed between 0 and 2π radians. The envelope of the channel response will therefore be Rayleigh distributed colling this random variable.

R, it will have a probability density function

Shadow fading :Shadowing from obstacles affecting the wave propagation, sometimes referred to as **shadow fading**.

Q.4. (b) How does IS-95 CDMA works? Explain **(7)**

Ans. The IS-95 standard describes a Code Division Multiple Access (CDMA) system in which the audio band data signal is multiplied by a high rate spreading signal. This spreading signal is formed from a pseudo-noise code sequence, which is then multiplied by a Walsh code for maximum orthogonality to (ie. to have low cross-correlation with) the other codes in use in that cell. Typically, CDMA pseudo-noise sequences are very long, thereby giving excellent crosscorrelation characteristics. (IS-95 uses a 242-1 chip period, derived from a 42 bit mask.) The IS-95 system can be thought of as having many layers of protection against interference. It allows many users to co-exist, with minimal mutual interference. They can be described by the signal conditioning sequence that occurs on forward and reverse channels (**Figure 1 and Figure 2, respectively**). The forward channel carries information from the base station to the mobile unit; the reverse channel carries information from the mobile unit to the base station. The transmission channels are shown; the reception of each channel follows the reverse sequence. The forward channels are between 869 and 894 MHz, while the reverse channels are between 824 and 849 Mhz. Within these bands, four sub-bands are available for CDMA, of widths 1, 0.1, 9 and 10 MHz;

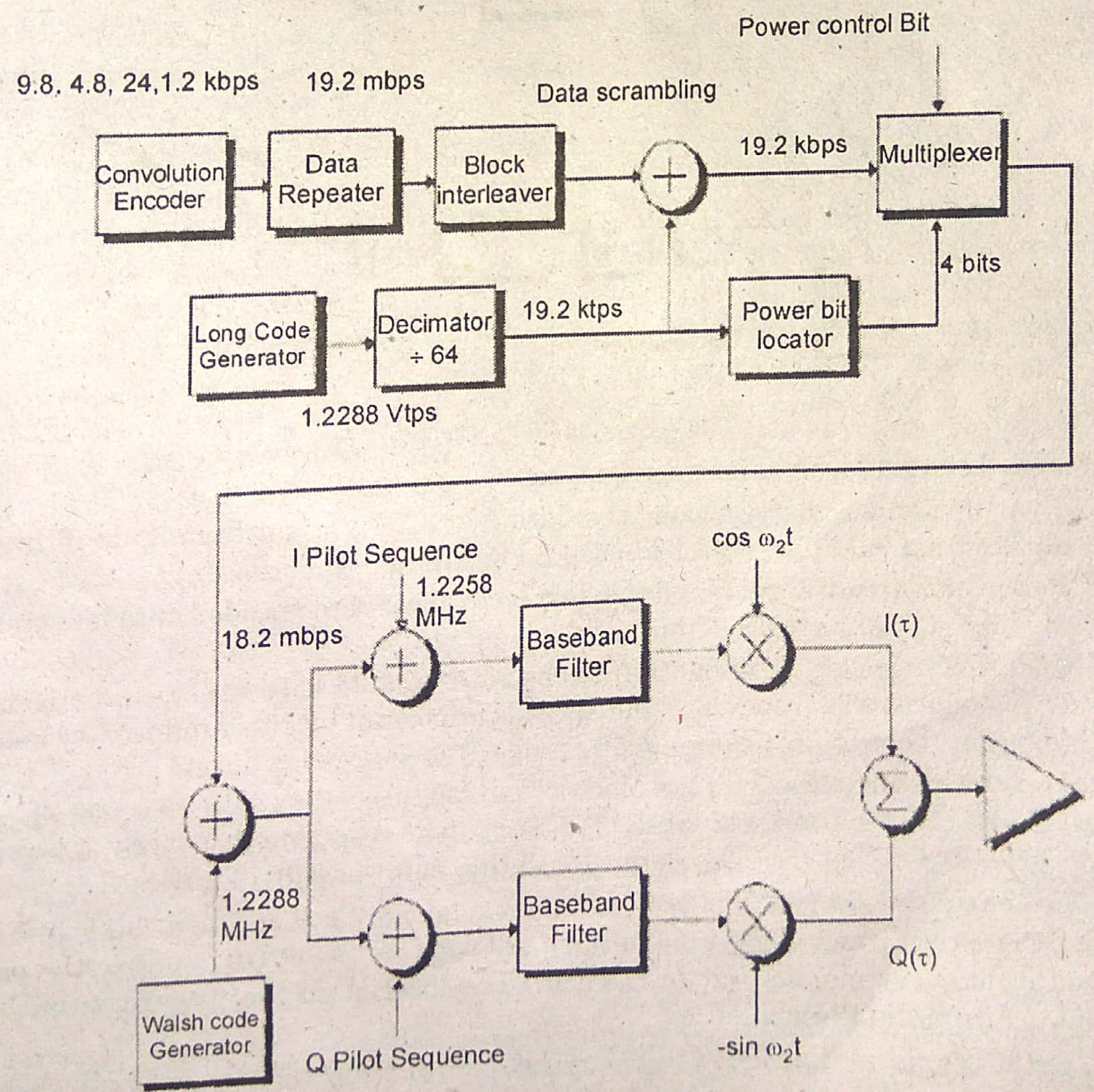


Figure: Forward CDMA channel

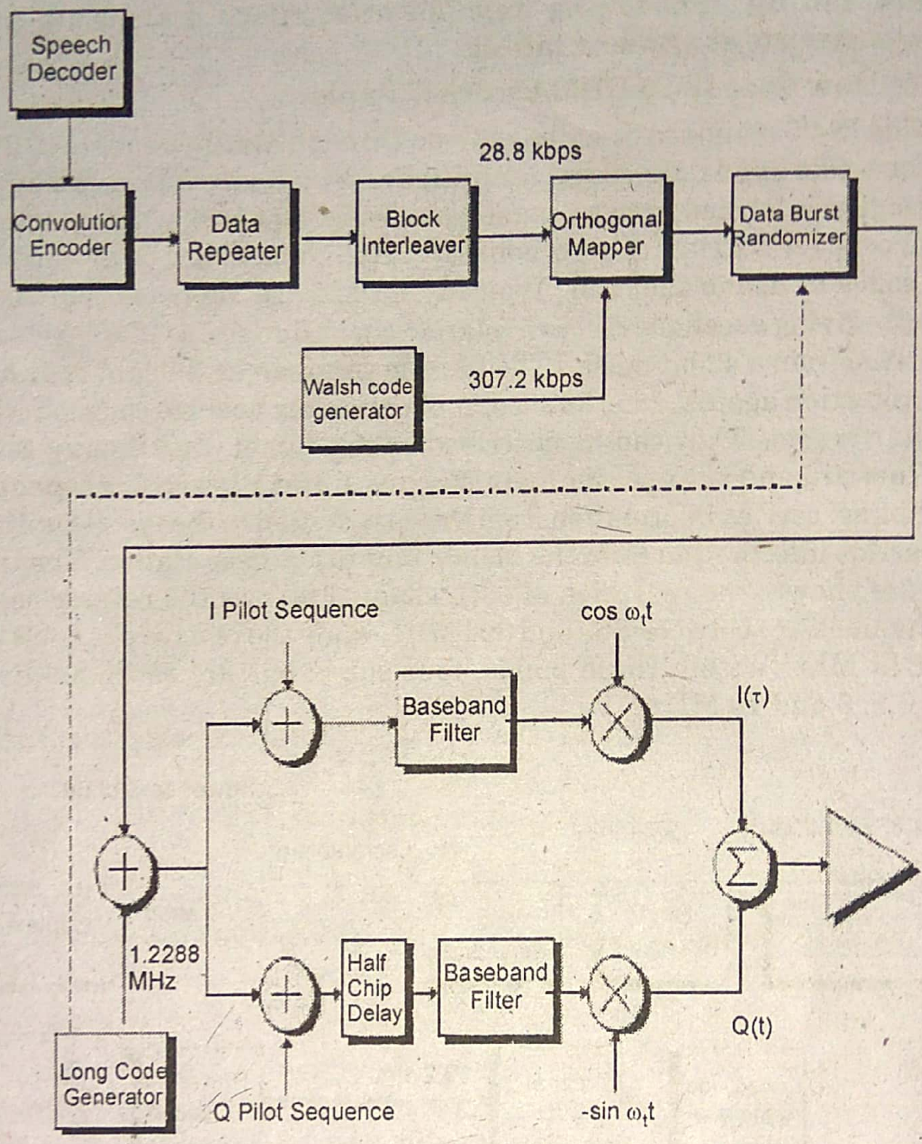


Fig.2. Reverse CDMA Channel

Forward channel transmission sequence:

1. Convolution encoder Encodes the data from one stream to two, doubling the nominal rate from 9.6 kpbs to 19.2 kbps, 4.8 kbps data to 9.6 kbps, etc.

2. Repetition circuit Repeats coded symbols, so lower rate encoded data is increased from 9.6, 4.8 or 2.4 kbps to 19.2 kbps.

3. Block Interleaver Reads data into the rows of a 24 x 16 array, and out of the columns; introduces a 20 msec delay, but spreads important bits (as produced by modern speech encoders) over time as proof against deep fades or noise bursts.

4. Data scrambling The data are Modulo 2 added to every 64th bit of a pseudo-noise (PN) sequence created from a 42 bit shift register. (The resulting 242-1 bits repeat once per century after initiation.) The data rate at this point is still 19.2 kbps.

5. Power control Every 1.25 msec, or 24 data symbols, a power control bit is inserted, in order to instruct the mobile unit to raise or lower its power (to equalize the power received from every mobile unit in the cell.) The location of the power control bit is determined from the PN sequence.

6. Orthogonal covering The 19.2 kbps data are spread with a 1.2288 Mbps Walsh function, so that each one bit data symbol is spread by 64 Walsh chips. The Walsh function provides 64 mutually orthogonal binary sequences, each of length 64.

7. Quadrature spreading The data are split into two bit streams, which are Modulo 2 added to two different but well defined "Pilot" pseudo-noise sequences generated from 15 bit shift registers. The code repeats 75 times every 2 seconds, or at 26.7 msec intervals.

8. Quadrature modulation The binary I and Q outputs are mapped onto four phases of a quadrature modulator, at $\pm\pi/4$ and $\pm3\pi/4$, using quadrature phase shift keying (QPSK).

9. RF modulation The baseband quadrature data are raised to the forward cellular radio band, 869 to 894 MHz.

The IS-95 channel occupies 1.25 MHz within this band, the rest of which is occupied by other cellular services such as AMPS.

Reverse channel transmission sequence:

1. Speech encoder Produces nominal 9600 bps data stream, dynamically reduced to 4800, 2400, or 1200 bps during pauses and gaps in speech; quiet periods correspond to 1200 bps data.

2. Convolution encoder Encodes the data from one stream to three, tripling the data rate from 9.6 kpbs to 28.8 kbps,4.8 kbps data to 14.4 kbps, etc.

3. Repetition circuit Repeats coded symbols, so lower rate encoded data is increased from 9.6, 4.8 or 2.4 kbps to 19.2 kbps.

4. Block Interleaver Reads data into the columns of a 32 x 18 array, and out of the rows; introduces a 20 msec delay, but spreads important bits over time as proof against deep fades or noise bursts.

5. Orthogonal mapping The 28.8 kbps data are split into sequential sets of six bits each, which are mapped to one of 64 Walsh functions. The data rate is therefore raised to 28.8 k x 64 chips/ 6 bits = 307.2 kpbs.

6. Burst Randomizing The Walsh symbols are broken into groups of six, each group being 1.25 msec in duration.

These are collected into frames of 16 power groups, or 1.25 msec x 16 = 20 msec. At 9600 bps, all 16 groups are transmitted; at 4800 bps, 8 randomly selected groups are transmitted; at 2400 bps, 4 groups; at 1200 bps, 2 groups. The transmitted groups are chosen randomly, according to a formula based on 14 bits of the PN sequence of the second last group in the previous frame.

7. Direct sequence spreading The data are Modulo 2 added to every bit of a pseudo-noise (PN) sequence created from a 42 bit shift register. The PN sequence is generated at 1.2288 MHz, so each Walsh chip is spread by four long code PN chips.

8. Quadrature spreading The data are split into two bit streams, which are Modulo 2 added to two different but well defined "Pilot" pseudo-noise sequences generated from 15 bit shift registers.

9. Quadrature modulation The binary I and Q outputs are mapped onto four phases of a quadrature modulator, at $\pm\pi/4$ and $\pm3\pi/4$, using offset quadrature phase shift keying (OQPSK). (The Q channel is shifted by half a chip for improved spectral shaping.)

10. RF modulation The baseband quadrature data are raised to the reverse cellular radio band, 824 to 849 MHz.

The IS-95 channel occupies 1.25 MHz within this band, the rest of which is occupied by other cellular services such as AMPS.

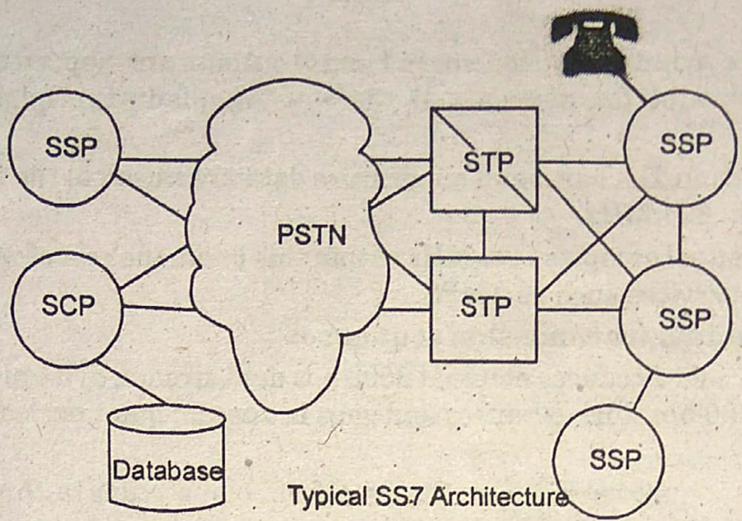
Q.5. (*a*) Why is SS7 classified as a common channel signaling protocol? What are the main elements in the SS7 architecture. Describe them. **(8)**

Ans. SS7 Architecture consists of three different entities:

1. SSP (Service Switching Point)

2. STP (Signal Transfer Point)

3. SCP (Service Control Point)



Typical SS7 Architecture

1. Service Switching Point (SSP)

- SSPs are switches in SS7 network.
- SSPs convert a dialed number from a subscriber line to SS7 signaling messages.
- SSPs setup, manage and release voice circuits required to make a call.
- SSPs send messages using the ISDN User Part (ISUP) and Transaction Capabilities Application Part (TCAP) protocols
- SSP's function is to use a global title to determine how to connect a call using its routing table.

2. Signal Transfer Point (STP)

- An STP is a router and/or a gateway in the SS7 network.
- Messages are not originated by an STP..
- If an originating SSP does not know the address of a destination SSP, the STP must provide it using Global Title Translation.
- Gateway STPs serve as the interface into another network and they can provide protocol conversion.
- STPs also provide traffic and usage measurements.

3. SCP (Service Control Point)

An SCP is usually a computer used as a front end to a database system. It is an interface to application-specific databases. The address of an SCP is a *point code*, and the address of the database it interfaces with is a *subsystem number*. The database is an application entity which is accessed via the TCAP protocol. It accepts a query for information from a subsystem at another node. SCP is used by STP to perform a function called global title translation

Q.5. (*b*) Show how to integrate the registration and the authentication procedures in GSM. **(7)**

Ans. Home Location Register (HLR): This database contains all the administrative information about each subscriber along with their last known location. In this way, the GSM network is able to route calls to the relevant base station for the MS. When a user switches on their phone, the phone registers with the network and from this it is possible to determine which BTS it communicates with so that incoming calls can be routed appropriately. Even when the phone is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position.

There is one HLR per network, although it may be distributed across various sub-centres to for operational reasons.

• **Visitor Location Register (VLR):** This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided. The VLR can be implemented as a separate entity, but it is commonly realised as an integral part of the MSC, rather than a separate entity. In this way access is made faster and more convenient.

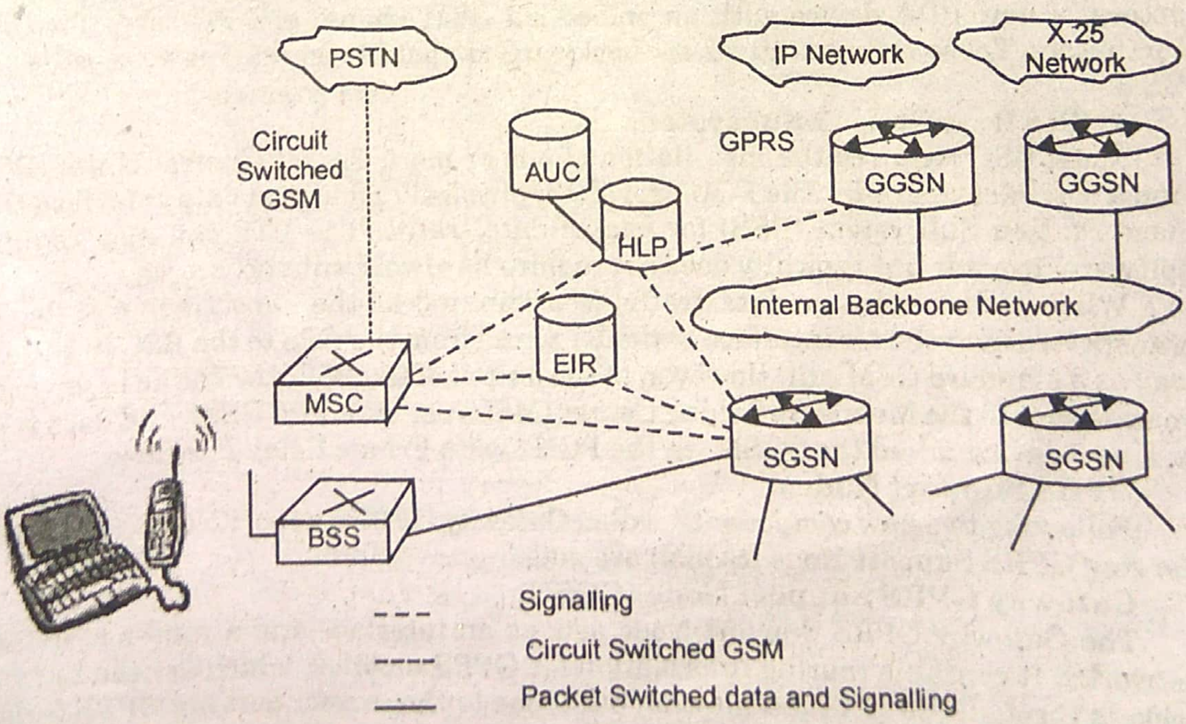
• **Equipment Identity Register (EIR):** The EIR is the entity that decides whether a given mobile equipment may be allowed onto the network. Each mobile equipment has a number known as the International Mobile Equipment Identity. This number, as mentioned above, is installed in the equipment and is checked by the network during registration. Dependent upon the information held in the EIR, the mobile may be allocated one of three states - allowed onto the network, barred access, or monitored in case its problems.

• **Authentication Centre (AuC):** The AuC is a protected database that contains the secret key also contained in the user's SIM card. It is used for authentication and for ciphering on the radio channel.

Q.6. (*a*) Describe the GPRS architecture and protocols. How many of them already exist in GSM? (8)

Ans. GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission. This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.

Following is the GPRS Architecture diagram:



GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GSM Network Element	Modification or Upgrade Required for GPRS
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data. A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers. These mobile stations are backward compatible for making voice calls using GSM.

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call. However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node. The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

Q.6. (*b*) Compare W.CDMA and CDMA 2000.

Ans.

Parameter	WCDMA	CMDA2000
Carrier Spacing : spacing between CDMA operators to obtain channel protection	5 MHz	3.75 MHz
Chip Rate : number of DSSS pulses per second; a chip is a pulse of DSSS code	4.096 MHz	3.68 MHz
Spreading Factor : SF=(Chip Rate)/(Data Rate)	Higher	Lower
Power Control Frequency : the output power of the transmitter is controlled by itself at this frequency	1500 Hz	800 Hz
Frame Duration : the time duration of a frame;between beginning and end of the frame.	10 ms	20 ms (also uses 5, 30, 40 ms frames)
Base Stations : base stations may or may not need synchronous timings	Asynchronous	Synchronous
Forward Link Pilot : The pilot is a channel modulated only by the PN (Pseudo Noise) spreading codes	TDM, Dedicated pilot	CDM, Common Pilot
Antenna Beam Forming : used for directional signal transmission & reception	DM, Dedicated pilot	Auxiliary pilot

Q.7. (*a*) Write short note on quality of service in 3G.

Ans. The Internet was originally designed for nonreal-time data services such as interactive burst or interactive bulk transfer. In these applications, there are no requirements on the maximum amount of delays that a packet may encounter during its transit to the destination. Similarly, bandwidths required by an end user are never specified. As such, the network accepts all incoming packets without using any admission control mechanism, forwards them using a simple, first-come-first-served algorithm, and delivers them on a best-effort basis. Thus, issues concerning the *quality of service* (QoS) delivered to an end user are rather straightforward. The QoS in present-day mobile IP is also minimal because, once again, data is delivered using the best-effort scheme. With the emergence of real-time multimedia services as envisaged by *third-generation* (3G) wireless systems, new QoS requirements are imposed on the networks. For example, with interactive video conferencing or streaming video and audio, the network must be able to deliver these services to the destination on a timely basis. Because flow control or retransmission is not possible for these applications, the bit error rate or packet loss ratio must be kept below a certain level; otherwise, the QoS may suffer. For instance, if the bit error rate is too high, the video in an MPEG application may never synchronize at a receiver.

Q.7. (*b*) What is mobile IP? Discuss **(7)**

Ans. Mobile IP (or MIP) is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address. Mobile IP for IPv4 is described in IETF RFC 5944, and extensions are defined in IETF RFC 4721. **Mobile IPv6**, the IP mobility implementation for the next generation of the Internet Protocol, IPv6, is described in RFC 6275. The Mobile IP allows for location-independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet. While away from its home network, a mobile node is associated with a *care-of* address which identifies its current location and its home address is associated with the local endpoint of a tunnel to its *home agent*. Mobile IP specifies how a mobile node registers with its home agent and how the home agent routes datagrams to the mobile node through the *tunnel*.

Q.8. Describe four major technologies for WLL System. What are the advantage and disadvantage of these approaches? **(15)**

Ans. 1. Wireless local loop is used for wireless communication links which deliver plain old telephone services or broadband services to customers. This is an ideal application which provides telephone services remotely and is mostly used in developing countries where cable infrastructure is either expensive or speed is not fast. This wireless link can be a part of the connection between the subscribers and switch.

This system is based on radio networks which provide services like telephone in remote areas. Different types of wireless local loop include Broadband Wireless Access, Radio in the Loop, Fixed Radio Access andFixed Wireless Access.

1. HNS Terminal Earth Station Quantum System
2. lucent Wireless Subscriber System
3. HNS E-TDMA
4. The PACS WLL System

In comparison to the alternative of deploying copper lines, WLL technology offers a number of key advantages:

- **Faster deployment:** WLL systems can be deployed in weeks or months as compared to the months or years need for the deployment of aboveground or underground copper wire. Even with higher costs per subscriber that may be associated with the WLL terminal and base station equipment, the faster rate of deployment can permit a higher return on investment.

- **Lower deployment costs:** The deployment of WLL technology involves considerably less heavy construction than does the laying of copper lines. The lower construction costs may be more than offset by the additional equipment costs associated with WLL technology, but, in urban areas especially, the process of routing cable to individual households is also much more time consuming than deploying wireless base stations, which are shared by many subscribers. Wireline networks also take more time to deploy than WLL networks because they require government right of way authorization to dig trenches through public streets.

- **Lower network maintenance, management, and operating costs:** Especially in areas where the deployment of copper lines has the potential to be haphazardly performed, wireless equipment can be less failure prone than copper wire and can be less vulnerable to sabotage, theft, or damage due to the elements or other parties. In some WLL systems, network management, including fault-finding and system reconfiguration, can be conducted from a centralized location to fully administer the WLL network between the telephone network interface and the subscriber terminal. The overall result is reduced lifetime network costs.

• **Lower network extension costs:** Wireless local loop technology intrinsically offers flexibility to meet uncertain levels of penetration and subscriber growth rates. Once the WLL infrastructure is in place, each incremental subscriber can be installed at very little cost. WLL systems that are designed to be modular and scalable can furthermore allow the pace of network deployment to closely match demand, minimizing the costs associated with underutilized plant. Such systems are flexible enough to meet uncertain levels of penetration and rates of growth.

• **High bandwidth is available providing:**

- Video;
- High-speed Internet access; and
- Telephony services.

Disadvantages:

• The technology is more costly due to the need for research and development

Moreover, some network operators fear technological obsolescence , that if a commitment is made to a specific WLL technology today, then within a few years it may be surpassed by technologies currently under development.

• The technology has not been tested over a long term of time for reliability and repair costs

The disadvantages of a wireless local loop solution, lie in the fact that much of the technology particularly on the digital side, is relatively untried.

• Certain technologies are not available in all areas, which leaves people with the unsupported technology disconnected

The capital cost of WLL technology, even when it compares favorably to the deployment of copper lines, remains outside the reach of many government or private network operators.

• Wireless technology requires that data be sent over open space, which makes it susceptible to interception and decreases the security of the transmission

• Customer accessibility is still low in the US

Where traditionally most of the innovations in new technology comes from.

• **Market investment is slow in the US**

Due to the low penetration of American companies in the market.

Q.9. Write short note on:

(a) Bluetooth.

Ans. Bluetooth is a wireless technology standard for exchanging data over short distances (using short-wavelength UHF radio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables.

Bluetooth operates at frequencies between 2402 and 2480 MHz, or 2400 and 2483.5 MHz including guard bands 2 MHz wide at the bottom end and 3.5 MHz wide at the top. This is in the globally unlicensed (but not unregulated) industrial, scientific and medical (ISM) 2.4 GHz short-range radio frequency band. Bluetooth uses a radio technology called frequency-hopping spread spectrum. Bluetooth divides transmitted data into packets, and transmits each packet on one of 79 designated Bluetooth channels. Each channel has a bandwidth of 1 MHz. It usually performs 800 hops per second, with Adaptive Frequency-Hopping (AFH) enabled. Bluetooth low energy uses 2 MHz spacing, which accommodates 40 channels. Gaussian frequency-shift keying (GFSK) modulation was the only modulation scheme available. Since the introduction of Bluetooth 2.0+EDR, π/4-DQPSK (differential quadrature phase shift keying) and 8DPSK modulation may also be used between compatible devices. Devices functioning with GFSK are said to be operating in basic rate (BR) mode where an instantaneous bit rate of 1 Mbit/s is possible. The term Enhanced Data Rate (EDR) is used to describe π/4-DPSK and 8DPSK schemes, each giving 2 and 3 Mbit/s respectively. The combination of these (BR and EDR) modes in Bluetooth radio technology is classified as a "BR/EDR radioA master BR/EDR Bluetooth device can communicate with a maximum of seven devices in a piconet (an ad-hoc computer network using Bluetooth technology), though not all devices reach this maximum. The devices can switch roles, by agreement, and the slave can become the master (for example, a headset initiating a connection to a phone necessarily begins as master—as initiator of the connection—but may subsequently operate as slave).

Q.9. (*b*) Mobile adhoc networks

Ans. • A **mobile ad hoc network** (**MANET**), also known as wireless ad hoc network or **ad hoc wireless network**, is a continuously self-configuring, infrastructure-less network of mobile devices connected wirelessly.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

MANETs are a kind of wireless ad hoc network (WANET) that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer, self-forming, self-healing network. MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz)

Types of **mobile ad hoc network** (**MANET**)

• Vehicular ad hoc networks (VANETs) are used for communication between vehicles and roadside equipment. Intelligent vehicular ad hoc networks (InVANETs) are a kind of artificial intelligence that helps vehicles to behave in intelligent manners during vehicle-to-vehicle collisions, accidents.

• Smart phone ad hoc networks (SPANs) leverage the existing hardware (primarily Bluetooth and Wi-Fi) in commercially available smart phones to create peer-to-peer networks without relying on cellular carrier networks, wireless access points, or traditional network infrastructure. SPANs differ from traditional hub and spoke networks, such as Wi-Fi Direct, in that they support multi-hop relays and there is no notion of a group leader so peers can join and leave at will without destroying the network.

• Internet-based mobile ad-hoc networks (iMANETs) is a type of wireless ad hoc network that supports Internet protocols such as TCP/UDP and IP. The network uses a network-layer routing protocol to link mobile nodes and establish routes distributedly and automatically.

• Hub-Spoke MANET - Multiple sub-MANETs may be connected in a classic Hub-Spoke VPN to create a geographically distributed MANET. In such type of networks normal ad hoc routing algorithms does not apply directly. One implementation of this is Persistent System's CloudRelay.

• Military or tactical MANETs are used by military units with emphasis on data rate, real-time requirement, fast re-routing during mobility, data security, radio range, and integration with existing systems. Common radio waveforms include the US Army's JTRS SRW.