L. J Institutes of Engineering and Technology

Remedial MSE Important Questions

SEM: 7
Subject Name: Mobile Computing and Wireless Communication
Subject Code: 3170710

1 **Define channel capacity. Write Shannon and Nyquist capacity formula in detail. State the key factors that affect channel capacity.**

Answer:
channel capacity: The maximum rate at which data can be transmitted over a given communication path, or channel, under given conditions is referred to as the **channel capacity.**

There are four concepts here that we are trying to relate to one another:

1. **Data rate:** It is defined as the number of bits transmitted by the transmitter per second. This is the rate, in bits per second (bps), at which data can be communicated.
   This capability depends on following factors.
   1. The amount of energy put into transmitting each signal.
   2. Distance to be travelled.
   3. Noise
   4. Channel Bandwidth
2. **Channel Bandwidth:** This is the bandwidth of the transmitted signal as constrained by the transmitter and the nature of the transmission medium, expressed in cycles per second, or Hertz. The Bandwidth of the communication medium should be large enough to transmit the digital signal reliably. An inadequate bandwidth will distort the signal and introduce errors into the received signal.
3. **Noise: T**he average level of noise over the communications path.
4. **Error rate:** This is the rate at which errors occur, percentage of time when bits are flipped. Where an error is the reception of a 1 when a 0 was transmitted or the reception of a 0 when a 1 was transmitted.

Nyquist Theorem:

→ Let us consider the case of a channel that is noise free. In this environment, the limitation on data rate is simply the bandwidth of the signal.

→ A formulation of this limitation, due to Nyquist, states that if the rate of signal transmission is 2B, then a signal with frequencies no greater than B is sufficient to carry the signal rate.

→ The converse is also true: Given a bandwidth of B, the highest signal rate that can be carried is 2B. This limitation is due to the effect of inter symbol interference, such as is produced by delay distortion.

→ If the signals to be transmitted are binary (take on only two values), then the data rate that can be supported by B Hz is 2B bps. As an example, consider a voice channel being used, via modem, to transmit digital data. Assume a bandwidth of 3100 Hz. Then the capacity, C, of the channel is 2B = 6200 bps.

→ Signals with more than two levels can be used; that is, each signal element can represent more than one bit.

→ With multilevel signaling, the Nyquist formulation becomes

$$C = 2B \log_2 M$$

→ Where M is the number of discrete signal elements or voltage levels. Thus, for M = 8, a value used with some modems, a bandwidth of B = 3100 Hz yields a capacity C = 18,600 bps.

→ So, for a given bandwidth, the data rate can be increased by increasing the number of different signal elements.

Shannon Theorem:

→ Nyquist's formula indicates that, all other things being equal, doubling the bandwidth doubles the data rate. Now consider the relationship among data rate, noise, and error rate. The presence of noise can corrupt one or more bits. If the data rate is increased, then the bits become "shorter" in time, so that more bits are affected by a given pattern of noise. Thus, at a given noise level, the higher the data rate, the higher the error rate.

→ For a given level of noise, we would expect that a greater signal strength would improve the ability to receive data correctly in the presence of noise.

→ **SNR:** the signal-to-noise ratio (SNR, or *S/N)*, which is the ratio of the power in a signal to the power contained in the noise that is present at a particular point in the transmission.

→ Typically, this ratio is measured at a receiver, because it is at this point that an attempt is made to process the signal and eliminate the unwanted noise. For convenience, this ratio is often reported in decibels:

$$\mathrm{SNR}_{\mathrm{dB}} = 10 \log_{\mathrm{lO}} (\text{Signal power / Noise power})$$

→ A high SNR will mean a high-quality signal.

→ The signal-to-noise ratio is important in the of digital data transmission because it sets the upper bound on the achievable data rate.

→ Shannon's result is that the maximum channel capacity, in bits per second, obeys the equation

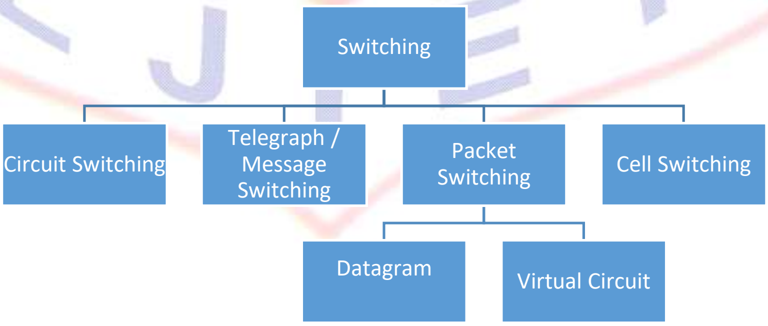
$$C = B \log_2(1 + \mathrm{SNR})$$

→ Where C is the capacity of the channel in bits per second and *B* is the bandwidth of the channel in Hertz.

Note also that, because noise is assumed to be white, the wider the bandwidth, the more noise is admitted to the system. Thus, as *B* increases, SNR decreases.

2 **Describe the Switching Techniques. Explain the Circuit Switching and Packet Switching in detail.**

→ Information may be switched as it travels from sender to receiver over multiple path through various communication channel.



Circuit Switching:

→ **Circuit switching** is a technique that directly connects the sender and the receiver in an **unbroken path**.

→ Used in Public telephone networks and is the basis for private network built on leased - basis. Telephone switching equipment, for example, establishes a path that connects the caller's telephone to the receiver's telephone by making a physical connection.

→ It is Used for voice terrify

→ Less efficient in digital data

→ Dedicated path is established

→ Connection is transparent (Once connection is established, it appears to attach devices as if there were a direct connection)

→ On each physical link, a logical channel is dedicated to channel.

→ There are three phases of circuit switching:

1. Circuit Establishment
2. Data Transfer
3. Circuit Disconnect

→ Connection should established before terms begins. Nodes must have switching capacity and channel capacity to establish connection.

→ Switches must have intelligence to work out routing.

→ Circuit switching uses any of two following:

- Space division switching technique
- Time division switching technique

Application:

→ Developed for voice traffic

→ Private Branch Exchange (PBX) (Inter connection of telephones within a building or office)

Advantages:

→ Dedicated transmission so guaranteed data rates.

→ No delay in data flow

→ Real time transfer of voice signal

Disadvantages:

→ Can not use channel for another data transfer even if the channel is free.

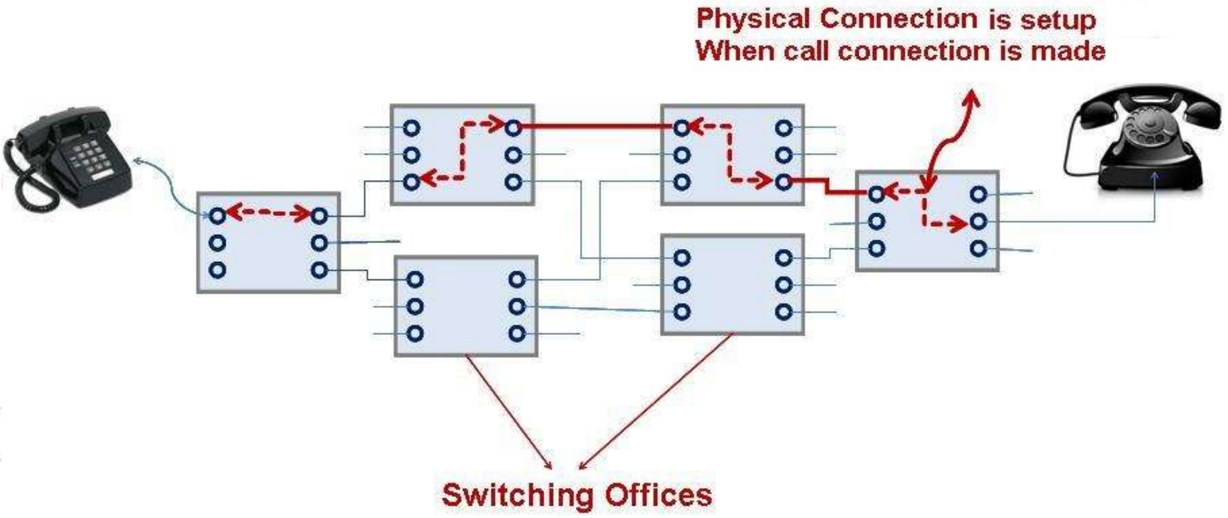
→ Require more bandwidth

→ Takes long time to establish connection

→ High cost

→ Not reliable (Call can be lost)

→ Can not use reliably for Digital data.



Packet Switching:

→ Packet switching can be seen as a solution that tries to combine the advantages of message and circuit switching and to minimize the disadvantages of both.

→ With message switching there is no need to establish a dedicated path between two stations.

→ There are two methods of packet switching: **Datagram and virtual circuit**.

- → In both packet switching methods, a message is broken into small parts, called packets.
- → Since packets have a strictly defined maximum length, they can be **stored in main memory instead of disk**; therefore access delay and cost are minimized.
- → Also the transmission speeds, between nodes, are optimized
- → At each node packets are received, stored briefly (buffered) and past on to the next node.
- → Store and forward mechanism
- → Each packet contains some portion of the user data plus control info needed for proper functioning of the network
- → Examples of packet switching networks are X.25, Frame Relay, ATM and IP.
- → Station breaks long message into packets. Packets sent one at a time to the network.
- → Packets handled in two ways:

1. Datagram

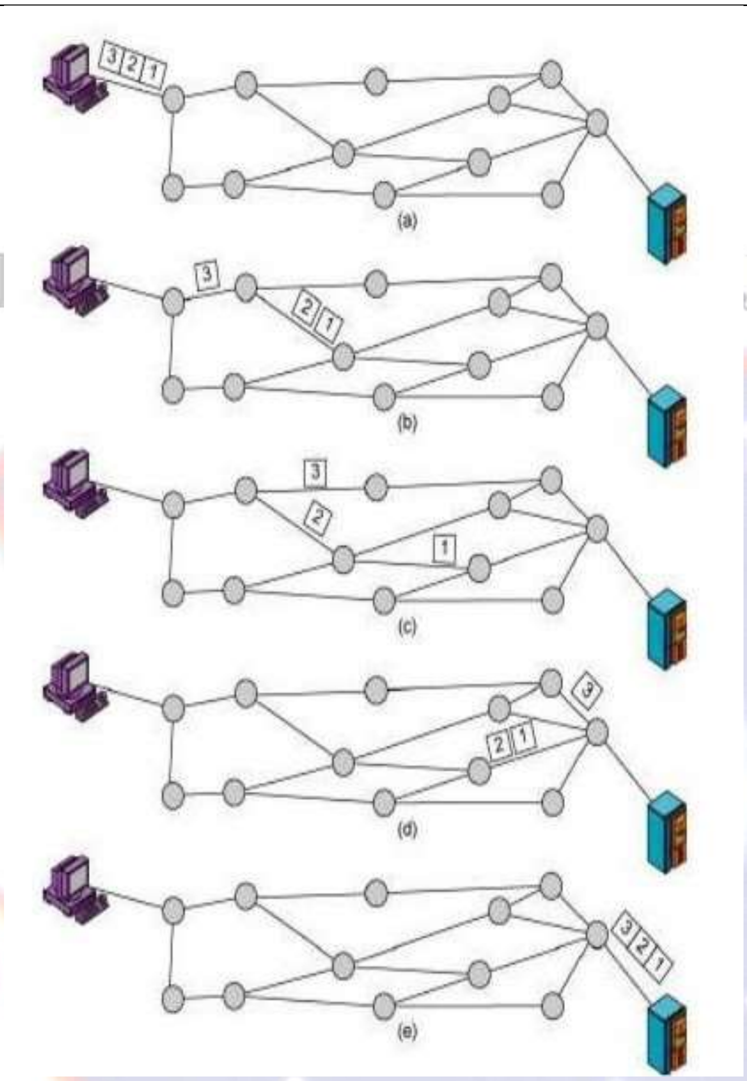
- → Each packet treated independently.
- → Packets can take any practical route
- → Packets may arrive out of order
- → Packets may go missing
- → Up to receiver to re-order packets and recover from missing packets
- → Datagram packet switching generally corresponds to the network layer. The packets are called as **Datagrams.**
- → Switching device are routers.
- → It is connection less network because the switch does not keep any information about the connection state.
- → No connection set up or tear down.

2. Virtual circuit

- → First establish virtual path between sender and receiver then sends all the data packets through that path only.
- → Call request and call accept packets establish connection (handshake)
- → Each packet contains a Virtual Circuit Identifier (VCI) instead of destination address
- → No routing decisions required for each packet
- → Clear request to drop circuit
- → Not a dedicated path

Advantages:

- → Packet switching is cost effective, because switching devices do not need massive amount of secondary storage.
- → Packet switching offers improved delay characteristics, because there are no long messages in the queue (maximum packet size is fixed).
- → Packet can be rerouted if there is any problem, such as, busy or disabled links.
- → The advantage of packet switching is that many network users can share the same channel at the same time. Packet switching can maximize link efficiency by making optimal use of link bandwidth.



Disadvantages:

→ Protocols for packet switching are typically more complex.

→ It can add some initial costs in implementation.

→ If packet is lost, sender needs to retransmit the data. Another disadvantage is that packet-switched systems still can't deliver the same quality as dedicated circuits in applications requiring very little delay - like voice conversations or moving images.

3 **Explain the differences between 1G, 2G, 2.5G and 3G mobile communications.**

	1G	**2G**	**2.5G**	**3G**
Year of introduction	1980	1993	1997	2001
Location of First Commerce	USA	Finland	Finland	Japan
Technology	AMPS (Advance Mobile Phone System) , NMT (Nordiac Mobile Telephone) , NIT (Nippen Telegraph and Telelphone) , ETACS (Enhanced	IS-95 (Interim Standard – 95), GSM (Global System Mobile), IS-136 (Interim Standard –	GPRS (General Packet Radio Service), EDGE (Enhanced Data rate for GSM	IMT-2000 (International Mobile Telephone), WCDMA (Wideband Code Division Multiple Access), TD-

	Total Access Communication System)	136), PDC (Pacific Digital Cellular)	Evolution), HSCSD (High Speed Circuit Switched Data)	SCDMA (Time Division Synchronous Code Division Multiple Access), UMTS (Universal Mobile Telecommunication Service)
Type of Switching	Circuit Switching	Circuit switching for voice and packet switching for data	Packet	Packet
Multiple Access	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA
Data Rates	2.4-14.4 kbps	14.4 kbps	20-40 kbps 171.2 kbps for gprs	3.1 mbps
Supports	Voice only	Data, voice and SMS	Data, Voice, SMS, MMS	Data and Voice
Internet	No internet	Narrowband	Narrowband	Broadband
Operating frequency	800 MHz	GSM 900-1800 MHz CDMA 800 MHZ	GPRS 850-1900 MHz	2100 MHz
Carrier Frequency	30 KHz	200 KHz	200 KHz	5MHz
Bandwidth	Analog	25 MHz	25 MHz	25 MHz
Handoff	Horizontal	Horizontal	Horizontal	Horizontal and Vertical
Advantages	Network Elements are simple and easy to use	SIM and Internet Starts	Supports SMS and MMS, High speed internet	High security International Roaming
Disadvantage	1) Limited capacity 2) Susceptible to noise 3) Frequent call drop 4) Poor battery life 5) Poor handoff	1) Slow Data rate 2) Low Network range	Low Network range	1) High Power Consumption 2) High cost of spectrum licenses
Application	Voice calls	Voice calls , SMS,FAX	Voice call, SMS, MMS, VPN	Voice call, SMS, MMS, VPN, Mobile TV, GPS, Video conferencing, VoIP

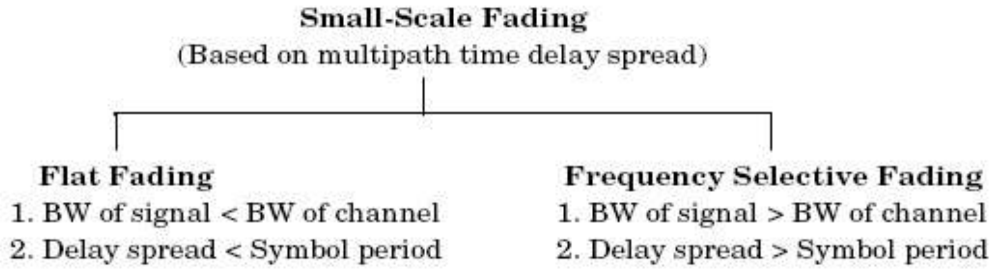
4 What is fading? Differentiate

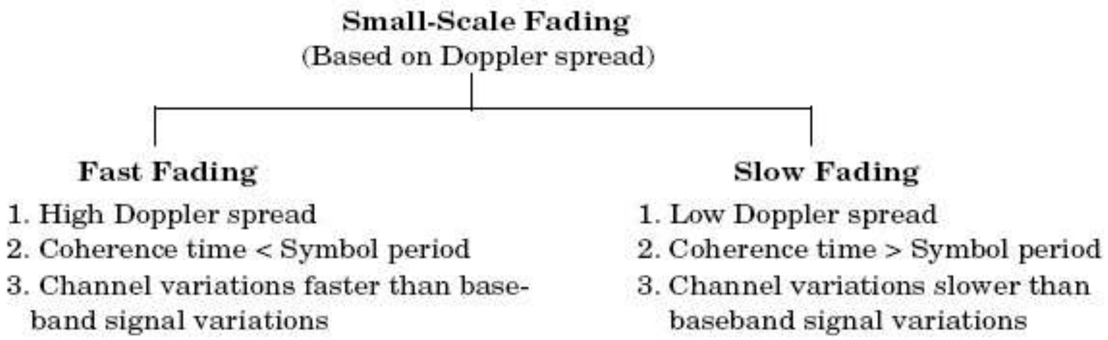
i. Fast and slow fading

ii.Flat and selective fading.

Answer:

- Fading is used to explain the quick changes or fluctuations in the amplitude, frequency or phase of the signal over a short period of time.
- Due to effect of multipath signal the multipath signal combines at receiver will vary in amplitude and phase depending upon the distributions of intensity, relative propagation time of waves and bandwidth of transmitted signal.
- Fading: In wireless communication, It is variation of the attenuation of a signal with various variables like time, geographical position and radio frequency.
- Fading is of two types:
  1. Small scale fading: Short distance
  2. Large scale fading: Long distance


Small-Scale Fading
(Based on multipath time delay spread)
Flat Fading
1. BW of signal < BW of channel
2. Delay spread < Symbol period
Frequency Selective Fading
1. BW of signal > BW of channel
2. Delay spread > Symbol period


Small-Scale Fading
(Based on Doppler spread)
Fast Fading
1. High Doppler spread
2. Coherence time < Symbol period
3. Channel variations faster than base-band signal variations
Slow Fading
1. Low Doppler spread
2. Coherence time > Symbol period
3. Channel variations slower than baseband signal variations

5 Define : Blocking, Reflection, Refraction, Diffraction, Scattering, Multipath Propagation, Antenna gain.

1. **Blocking or shadowing:** An extreme form of attenuation is blocking or shadowing of radio signals due to large obstacles. The higher the frequency of a signal, the more it behaves like light. Even small obstacles like a simple wall, a truck on the street, or trees in an alley may block the signal.
2. **Reflection:** If an object is large compared to the wavelength of the signal, e.g., huge buildings, mountains, or the surface of the earth, the signal is reflected. The reflected signal is not as strong as the original, as objects can absorb some of the signal's power. Reflection helps transmitting signals as soon as no LOS exists. This is the standard case for radio transmission in cities or mountain areas. Signals transmitted from a sender may bounce off the walls of buildings several times before they reach the receiver. The more often the signal is reflected, the weaker it becomes
3. **Refraction:** This effect occurs because the velocity of the electromagnetic waves depends on the density of the medium through which it travels. Only in vacuum does it equal c. As the figure shows, waves that travel into a denser medium are bent towards the medium. This is the reason for LOS radio waves being bent towards the earth the density of the atmosphere is higher closer to the ground.
4. **Diffraction:** this effect is very similar to scattering. Radio waves will be deflected at an edge and propagate in different directions. The result of scattering and diffraction are patterns with varying signal strengths depending on the location of the receiver.
5. **Scattering:** If the size of an obstacle is in the order of the wavelength or less, then waves can be scattered. An incoming signal is scattered into several weaker outgoing signals.

6. **Multipath Propagation:** Radio waves emitted by the sender can either travel along a straight line, or they may be reflected at a large building, or scattered at smaller obstacles.

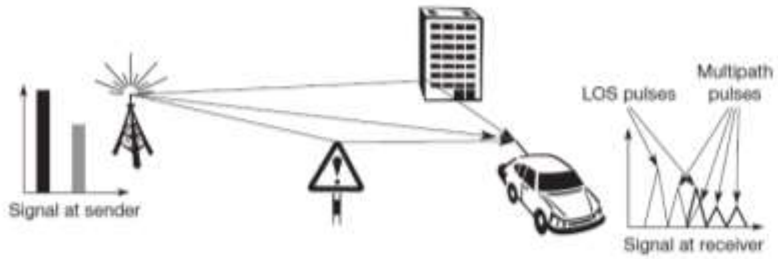


Figure 2.14 Multi-path propagation and intersymbol interference

- This simplified figure only shows three possible paths for the signal. In reality, many more paths are possible.
- As there is no direct LOS (line of sight), multiple reflections from different objects causes the radio waves to travel along different paths of varying lengths resulting in fading. The interaction between these waves causes multipath propagation at a particular location.
- As distance between transmitter and receiver increases the strength of the waves decreases.
- Due to the finite speed of light, signals travelling along different paths with different lengths arrive at the receiver at different times. This effect (caused by multi-path propagation) is called delay spread: the original signal is spread due to different delays of parts of the signal.
- This delay spread is a typical effect of radio transmission, because no wire guides the waves along a single path as in the case of wired networks.
- Notice that this effect has nothing to do with possible movements of the sender or receiver.
- Typical values for delay spread are approximately 3 μs in cities, up to 12 μs can be observed.
- For a real situation with hundreds of different paths, this implies that a single impulse will result in many weaker impulses at the receiver. Each path has a different attenuation and, the received pulses have different power.
- Some of the received pulses will be too weak even to be detected.
- At the receiver, both impulses interfere, i.e., they overlap in time. Now consider that each impulse should represent a symbol, and that one or several symbols could represent a bit. The energy intended for one symbol now spills over to the adjacent symbol, an effect which is called **inter symbol interference (ISI).**
- The higher the symbol rate to be transmitted, the worse the effects of ISI will be, as the original symbols are moved closer and closer to each other. ISI limits the bandwidth of a radio channel with multi-path propagation (which is the standard case).

7. Antenna Gain:

Antenna gain also called as directive gain

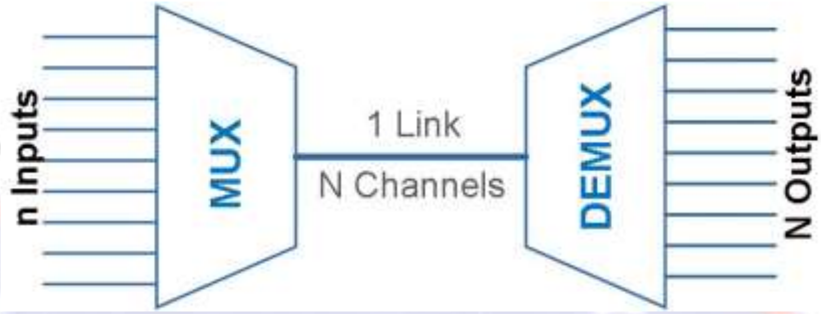
The ratio of the power density radiated in that direction by an isotropic antenna to that by a directional antenna.

Directive gain =Power density in Isotropic / Power density in directional

6 **Define the term Multiplexing. Explain the SDM, CDM , FDM and TDM with one example each.**

- In both local and swide area communications, it is almost always the case that the capacity of the transmission medium exceeds the capacity required for the transmission of a single signal. To make efficient use of the transmission system, it is desirable to carry multiple signals on a single medium. This is referred to as *multiplexing.*
- Figure depicts the multiplexing function in its simplest form. There are *n* inputs to a multiplexer.
- The multiplexer is connected by a single data link to a demultiplexer.
- The link is able to carry *n* separate channels of data. The multiplexer combines (multiplexes) data from the *n* input lines and transmits over a higher capacity data link.

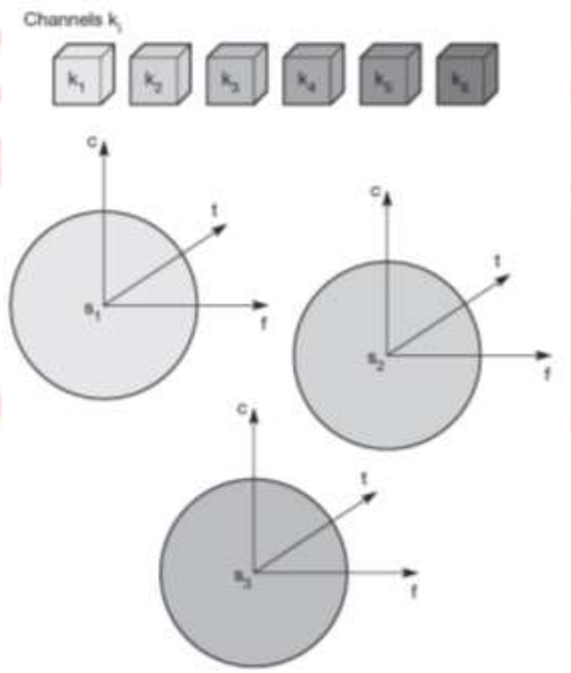
- The demultiplexer accepts the multiplexed data stream, separates (demultiplexes) the data according to channel, and delivers them to the appropriate output lines.
- In short, Multiplexing is combining the all input signal into a single composite signal and transmit it over the communication medium.



- This can be carried out in four dimension:

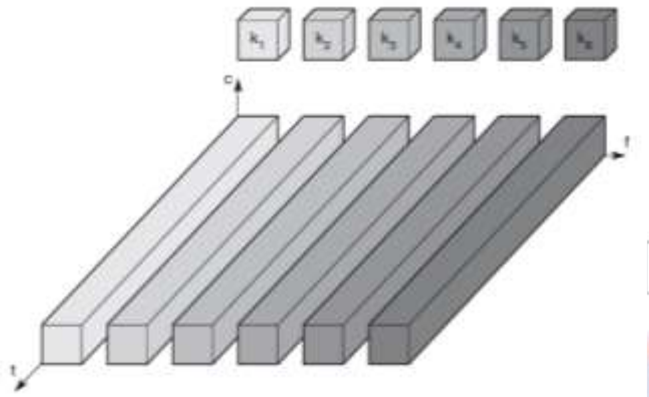
1. **Space Division Multiplexing (SDM):** In SDM the space is divided into different carrier signal for transmission. For example, the figure shows 3 channels Ki and introduces a three dimensional coordinate system.

→ 3 dimensions are code (C), time (T), frequency (F)
→ Space dimensions are represented via circles.
→ Channel K1 and K3, can be mapped onto the three spaces S1 to S3, which clearly separates the channels and prevent the interference ranges from overlapping.
→ The space between the interference ranges is called guard spaces.
→ Example, on Highway, driver has own lane



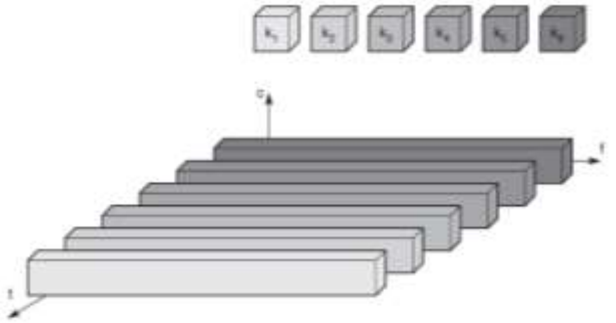
2. **Frequency Division Multiplexing (FDM):** In FDM, it subdivide the frequency dimensions into several non-overlapping frequency bands

→ Each channel Ki allocated its own frequency band as indicated.
→ Sender using a certain frequency band can use this band continuously.
→ Guard space (adjacent channel interference, avoid frequency band over lapping)
→ Example, Radio station within the same region, where each radio station has its own frequency.
→ No need complex co-ordination between sender and receiver. Receiver only has to tune into the specific sender.



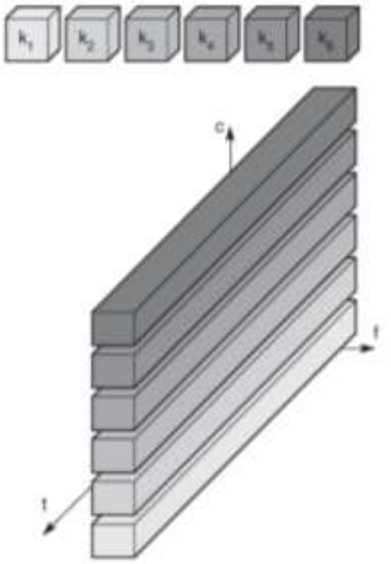
3. **Time Division Multiplexing (TDM):** In TDM, Channel Ki is given the whole bandwidth for a certain amount of time.

→ All senders are at the same frequency but at different point in time.
→ Guard space is represented by time gaps.
→ Synchronization between sender and receiver is necessary. So all needs precise clock.
→ In receiver tunning needs adjusting frequency at exactly the right point in time.



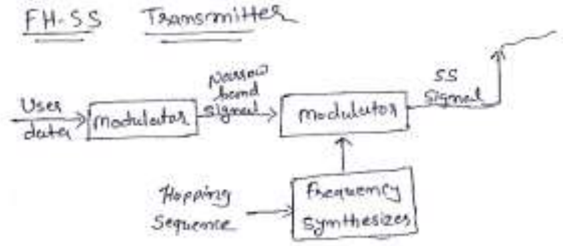
4. **Code Division Multiplexing (CDM):** In CDM, each user is assigned separate code for transmission.

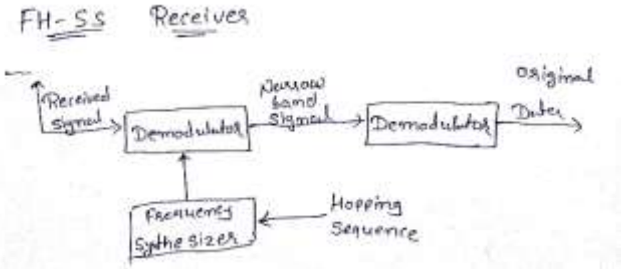
→ It is more secure
→ Guard space is represented by orthogonal code.
→ Communication is done over separate language.



7 Define FHSS. Discuss advantages and applications of FHSS.

→ **Frequency Hopping (FH):** Frequency hopping is a form of spreading in which the center frequency of a conventional carrier is altered many times within a fixed time period (like one second) in accordance with a pseudo-random list of channels.

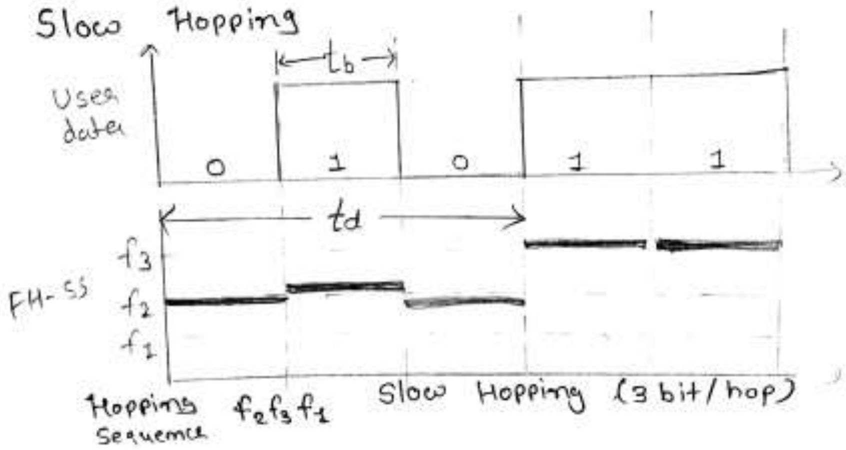




→

- In FH-SS system, the total available bandwidth is split into many channels of smaller bandwidth plus guard spaces between the channels.
- Transmitter and receiver stays on one of these channels for a certain time and then hop to another channel.
- The pattern of channel usage is called as the hopping sequence and the time spend on a channel with a certain frequency is called the Dwell time.
- FH-SS comes in two variants depending on the rate of frequency hopping.
  1. Slow frequency hopping
  2. Fast frequency hopping

- **Slow Frequency hopping:**
  - → In slow FH the symbol rate R_S of the MFSK signal is an integer multiple of the hop rate R_h
  - → That means several symbols are transmitted corresponding to each frequency hop
  - → Each frequency hope Implies several symbols
  - → Frequency hopping takes place slowly.
  - → In figure shows five user bits with a bit period T_b. performing slow hopping the transmitted uses the frequency f2 for transmitting the first three bits during the dwell time $T_{d.}$
  - → Then, the transmitter hops to the next frequency f3
  - → It is typically cheaper and have relaxed tolerances, but they are not as immune to narrowband interference as fast hopping system.
  - → Slow FH is an option for GSM.



- **Fast Frequency hopping:**

→ Fast FH is used for defeating a smart jammer who tries to interfere the transmission**.**

→ The transmitter changes the frequency several times during the transmission of a single bit.

→ In fast FH-SS system, there are multiple hops for each M-ary symbol.

→ Hence, each hop is a “chip”

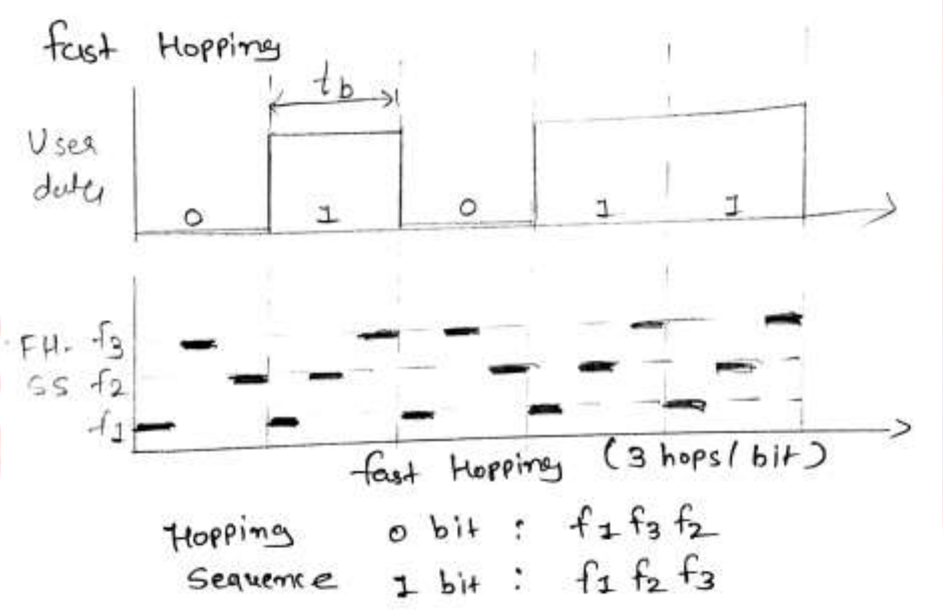
→ In figure the transmitter hops three times during a bit period.

→ Fast hopping systems are more complex to implement Transmitter and receiver have to stay synchronized within smaller tolerance to perform hopping at more or less the same points in time.

→ Much better at overcoming the effects of narrow band interference and frequency selective fading.

→ Much better at overcoming the effects of narrowband interference and frequency selective fading.

→ Frequency synthesizer is used to synchronize transmitter and receiver with same hopping sequence applied.

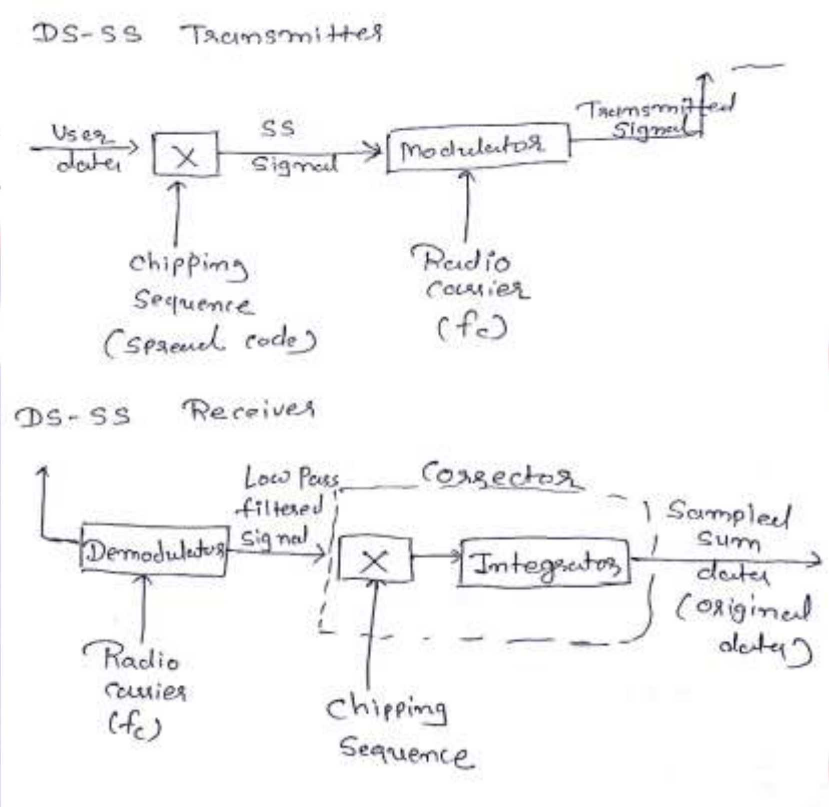


→

8 **Explain Direct sequence spread spectrum with example.**

- The most important advantage of spread spectrum modulation is that it provides protection against externally generated interfering signals. Such signals are called as a jamming signal.
- The information bearing signal is made to occupy a bandwidth which is much larger than the minimum bandwidth required for its transmission.
- This will make the signal to appear like a noise and blends into the background.
- Every user assigned a special code that code is used to encode signal
- XOR technique is used to combine data stream with chip-sequence code (Spread Code)
- These chip sequence codes produced by transmitter are already known to receiver. And receiver dispread the signal.
- The receiver will use the same chip-sequence to reconstruct the information signal.
- To get the original signal we need to XOR the signal.
- The DSSS receiver is more complex than the transmitter.
- The pseudorandom sequence at the sender and receiver have to be precisely synchronized because the receiver calculates the product of a chip with the incoming signals.
- During a bit period, which also has to be derived via synchronization, an integrator adds all the products.
- Calculating the products of chips and signal and adding the products in an integrator is also called correlation and the device is called corrector.

- Finally, in each bit period a decision unit samples the sums generated by the integrator and decides if this sum represents a binary 1 or a 0.



Features of DSSS:

1. It provides good security against potential jamming or interpretation
2. Extreamly effective against narrowband signal.
3. Very effective against broadband interference.

Application:

1. Jamming signal
2. Military communication
3. Cordless phone
4. Digital cellular telephony
5. Satellite navigation
6. WLAN
7. Bluetooth

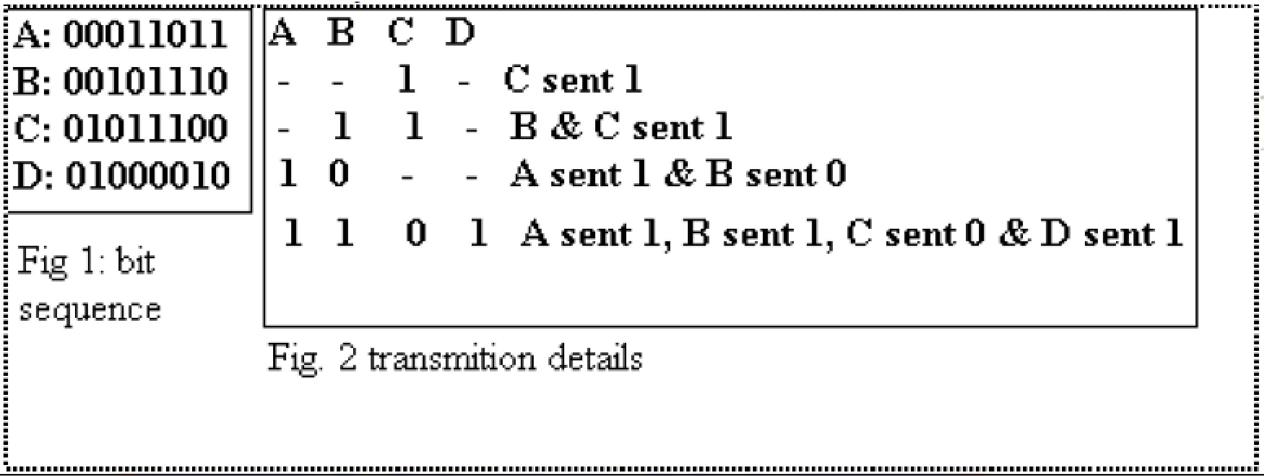
Disadvantages:

1. Increased bandwidth
2. Need for broad PN sequence.

Synchronization is affected by the variable distance between the transmitter and receiver.

9 In a CDMA network, assume there are four stations A, B, C, and D with their chip sequences, shown in Fig. 1. Fig. 2 shows four cases of four stations transmitting at the same time. Show the

transmitted sequences S1 to S4 and how DSSS does the recovery at receiver.



A: 00011011
B: 00101110
C: 01011100
D: 01000010

Fig 1: bit sequence

A	B	C	D	
-	-	1	-	C sent 1
-	1	1	-	B & C sent 1
1	0	-	-	A sent 1 & B sent 0
1	1	0	1	A sent 1, B sent 1, C sent 0 & D sent 1

Fig. 2 transmition details

Transmitter Side :

station-1 only C Transmits '1'

$C = (01011100)$

$S_1 = C = (-1, +1, -1, +1, +1, +1, -1, -1)$

station-2 B sent 1 and C sent 1

$B = (-1, -1, +, -1, +1, +1, +1, -1)$

$C = (-1, +1, -1, +1, +1, +1, -1, -1)$

$S_2 = B + C$

$= C$

station-3 A sent 1, B sent 0

$A = (-1, -1, -1, +1, +1, -1, +1, +1)$

$\overline{B} = (+1, +1, -1, +1, -1, -1, -1, +1)$

$S_3 = A + \overline{B}$

$S_3 = (0, 0, -2, +2, 0, -2, 0, +2)$

station-4 A sent 1, B sent 1, C sent 0 and D sent 1

$A = (-1, -1, -1, +1, +1, -1, +1, +1)$

$B = (-1, -1, +1, -1, +1, +1, +1, -1)$

$\overline{C} = (+1, -1, +1, -1, -1, -1, +1, +1)$

$D = (-1, +1, -1, -1, -1, -1, +1, -1)$

$S_4 = A + B + \overline{C} + D$

$S_4 = (-2, -2, 0, -2, 0, -2, +4, 0)$

Receiver Side:

station-1

$S_1 = C = (-1, +1, -1, +1, +1, +1, -1, -1)$

$S_1 \cdot C = (-1, +1, -1, +1, +1, +1, -1, -1)$

$\cdot\ (-1, +1, -1, +1, +1, +1, -1, -1)$

$= (+1, +1, +1, +1, +1, +1, +1, +1)$

$= 8/8 = 1 \rightarrow$ '1' bit.

station-2

$S_2 - (-2, 0, 0, 0, +2, +2, 0, -2)$

for B $S_2 \cdot B = (-2, 0, 0, 0, +2, +2, 0, -2)$

$\cdot\ (-1, -1, +1, -1, +1, +1, +1, -1)$

$= (+2, +0, +0, +0, +0, +2, +2, +0, +2)$

$= (+2 + 0 + 0 + 0 + 0 + 2 + 2 + 0 + 2)$

$= 8/8 = +1$

$\Rightarrow$ '1' bit sent.

station-3 $S_3 = (0, 0, -2, +2, 0, -2, 0, +2)$

for A $S_3 \cdot A = (0, 0, -2, +2, 0, -2, 0, +2)$

$\cdot\ (-1, -1, -1, +1, +1, -1, +1, +1)$

$= (0, 0, +2, +2, 0, +2, 0, +2)$

$= (0 + 0 + 2 + 2 + 0 + 2 + 0 + 2)$

$= 8/8 \Rightarrow$ bit '1' sent

for B $S_3 \cdot B = (0, 0, -2, +2, 0, -2, 0, +2)$

$\cdot\ (-1, -1, +1, -1, +1, +1, +1, -1)$

$= (+0, +0, -2, -2, +0, -2, +0, -2)$

$= (0 + 0 - 2 - 2 + 0 - 2 + 0 - 2)$

$= -8/8 = -1 \Rightarrow$ bit '0' sent.

Station-4

$S_4 = (-2, -2, 0, -2, 0, -2, +4, 0)$

for A $S_4 \cdot A = (-2, -2, 0, -2, 0, -2, +4, 0) \cdot$

$(-1, -1, -1, +1, +1, -1, +1, +1)$

$= +2 + 2 + 0 - 2 + 0 + 2 + 4 + 0$

$= 8/8 \Rightarrow$ bit '1' sent

$S_4 \cdot B = (-2, -2, 0, -2, 0, -2, +4, 0) \cdot$

$(-1, -1, +1, -1, +1, +1, +1, -1)$

$= +2 + 2 + 0 + 2 + 0 - 2 + 4 + 0$

$= 8/8 \Rightarrow$ bit '1' sent

$S_4 \cdot C = (-2, -2, 0, -2, 0, -2, +4, 0) \cdot$

$(-1, +1, -1, +1, +1, +1, -1, -1)$

$= +2 - 2 + 0 - 2 + 0 - 2 - 4 + 0$

$= -8/8 = -1 \Rightarrow$ bit '0' sent

$S_4 \cdot D = (-2, -2, 0, -2, 0, -2, +4, 0) \cdot$

$(-1, +1, -1, -1, -1, -1, +1, -1)$

$= +2 - 2 + 0 + 2 + 0 + 2 + 4 + 0$

$= 8/8 = 1 \Rightarrow$ bit '1' sent

10 Describe Error Control Coding with detail explanation of Error Detection and Error Correction.

The most important two techniques for error are as follow:

1. **Error Detection:** In this receiver can request for the retransmission of the complete or a part of message if it finds some error in the received signal message.

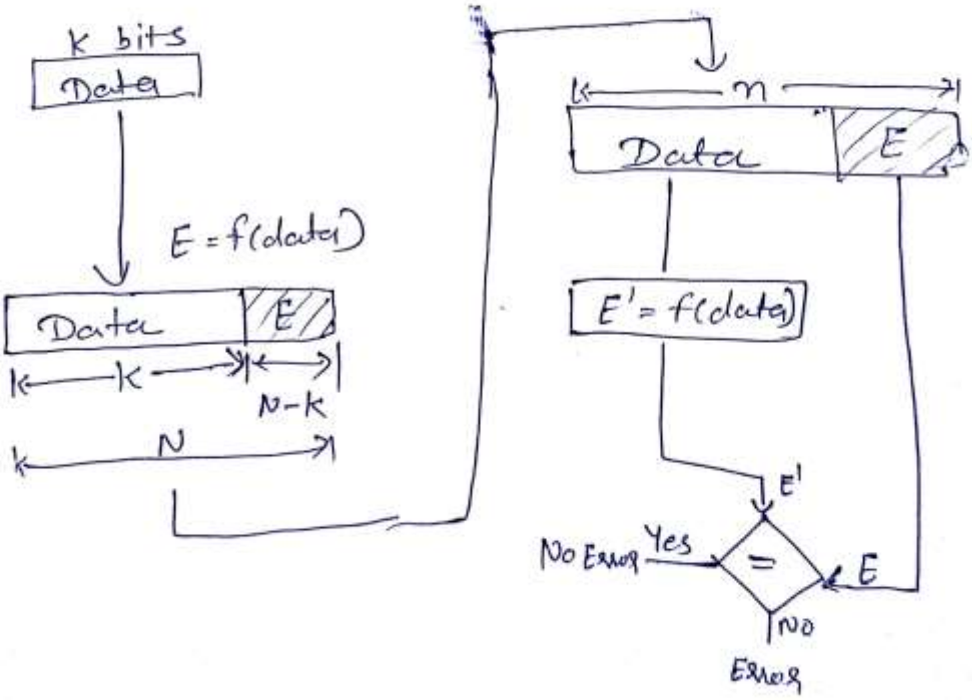
→ This required additional feedback channel to send request for retransmission.
→ Error detection technique operates on the following principle.
→ For a given frame of bits, the transmitter adds additional bits that constitute error-detection code.
→ This code is calculated as a function of the other transmitted bits.
→ For a data block of K bits, the error detection algorithm yields. Error detection code of N-K bits where (N-K) < K.
→ This error detection code also referred to as the check bits, and this is appended to the data block to produce a frame of n bits, which is then transmitted.
→ At receiver side it separates the incoming frame into the K bit of data and N-K bits of error detection code.
→ Now, receiver will performs the error detection calculation on the data bits and compare this value with the value of incoming error detection code.
→ A detected error occurs if and only if there is a mismatch.
→ Basic approach used for error detection is the use of redundancy bits, where additional bits are added to facilitate detection of errors.
→
→ Some popular techniques for error detection are:

1. Parity check : Blocks of data from the source are subjected to a check bit or parity bit generator form, where a parity of :

1 is added to the block if it contains odd number of 1's, and
0 is added if it contains even number of 1's
This scheme makes the total number of 1's even, that is why it is called even parity checking.

2. Checksum: In checksum error detection scheme, the data is divided into k segments each of m bits.
In the sender's end the segments are added using 1's complement arithmetic to get the sum. The sum is complemented to get the checksum.
The checksum segment is sent along with the data segments.
At the receiver's end, all received segments are added using 1's complement arithmetic to get the sum. The sum is complemented.
If the result is zero, the received data is accepted; otherwise discarded.

3. Cyclic redundancy : Unlike checksum scheme, which is based on addition, CRC is based on binary division.
In CRC, a sequence of redundant bits, called cyclic redundancy check bits, are appended to the end of data unit so that the resulting data unit becomes exactly divisible by a second, predetermined binary number.
At the destination, the incoming data unit is divided by the same number. If at this step there is no remainder, the data unit is assumed to be correct and is therefore accepted.
A remainder indicates that the data unit has been damaged in transit and therefore must be rejected.



Error Correction: In this at receiver side the error is corrected. So there is no such feedback path and request for retransmission. Error is corrected. Some of the technique is known as hamming code and convolutional code.

There are two error correction technique:

1. Hamming Code
2. Convolution code

11 Explain the following Multiple Access Techniques used to access the channel by mobile subscriber.

- Frequency Division Multiple access.
- Time Division Multiple access.
- Code Division Multiple access.

Ans:

Multiple Access System:

- In this kind of system multiple users can transmit by single channel.
- The multiple access technique is used in the multiuser environment for applications such as satellite communication and wireless mobile communication.
- Multiple access techniques are classified below:
  1. Frequency Division Multiple Access (FDMA)
  2. Time Division Multiple Access (TDMA)
  3. Space Division Multiple Access (SDMA)
  4. Code Division Multiple Access (CDMA)

- **Frequency division multiple access (FDMA)**
- In wireless communication, the individual users are allocated individual channels. The channels or the frequency band is unique for each subscriber.
- The entire allowed radio spectrum is divided into many slices of the frequency bands and each band or channel is allocated to users.

Features of FDMA:

- It comprises all algorithms allocating frequencies to transmission channels according to the frequency division multiplexing (FDM).

- Allocation can either be fixed (as for radio stations or the general planning and regulation of frequencies) or dynamic (i.e., demand driven).
- Complexity of FDMA is less
- It have narrow bandwidth as each channel supports only one circuit per carrier.
- The symbol time is large in comparison to the delay spread
- ISI (Inter symbol Interference) is low.
- Cost of cell site is higher in comparison to the TDMA system.
- It is a continuous transmission method. So few bits are required for overhead purpose.
- FDM is often used for simultaneous access to the medium by base station and mobile station in cellular network.

Advantages of FDMA:

1. All stations can operate continuously all 24 hours without having to wait for their turn to come.
2. No synchronization is necessary
3. The complexity of system is low.

Disadvantages of FDMA:

1. Intermodulation frequencies can cause adjacent channel interference.
2. As result of non linearities, intermodulation product are generated.
3. Cell site cost is high
4. Bandwidth is narrow.
5. Carrier only one circuit at a time.

TDMA:

- Compared to FDMA, time division multiple access (TDMA) offers a much more flexible scheme, which comprises all technologies that allocate certain time slots for communication, i.e., controlling TDM. Now tuning in to a certain frequency is not necessary, i.e., the receiver can stay at the same frequency the whole time.
- Each user to allocate a time slot in which the user can access the channel.
- In each slot only one user is allowed to transmit or receive.
- Using only one frequency, and thus very simple receivers and transmitters, many different algorithms exist to control medium access. Listening to different frequencies at the same time is quite difficult, but listening to many channels separated in time at the same frequency is simple.
- The TDMA system transmit data in burst and buffer method. Means, the transmission from different users in interfaced into a repeating frame structure.

Features of TDMA:

- TDMA uses different time slots for transmission and reception. So duplexer not required.
- As the transmission rates are high adaptive equalization is necessary.
- TDMA shares a single carrier frequency with several users where each user makes use of non-overlapping time slots.
- The number of time slots depends on parameters like bandwidth, modulation method etc.
- Bandwidth is supplied on demand to different users by assigned priority.
- It can be turned off when not in use.
- Guard time needs to be minimized.
- Handoff process is simple.
- Due to burst transmission high synchronization over head is needed in TDMA systems.

CDMA:

- Codes with certain characteristics can be applied to the transmission to enable the use of code division multiplexing (CDM).

- Code division multiple access (CDMA) systems use exactly these codes to separate different users in code space and to enable access to a shared medium without interference.
- The main problem is how to find “good” codes and how to separate the signal from noise generated by other signals and the environment.
- The code directly controls the chipping sequence. But what is a good code for CDMA? A code for a certain user should have a good autocorre-lation2 and should be orthogonal to other codes. Orthogonal in code space has the same meaning as in standard space (i.e., the three dimensional space).
- Think of a system of coordinates and vectors starting at the origin, i.e., in (0, 0, 0).3 Two vectors are called orthogonal if their inner product is 0, as is the case for the two vectors (2, 5, 0) and (0, 0, 17): (2, 5, 0)*(0, 0, 17) = 0 + 0 + 0 = 0.
- But also vectors like (3, –2, 4) and (–2, 3, 3) are orthogonal: (3, –2, 4)*(–2, 3, 3) = –6 – 6 + 12 = 0.
- By contrast, the vectors (1,2,3) and (4,2, –6) are not orthogonal (the inner product is –10), and (1, 2, 3) and (4, 2, –3) are “almost” orthogonal, with their inner product being –1 (which is “close” to zero).
- This description is not precise in a mathematical sense. However, it is useful to remember these simplified definitions when looking at the following examples where the original code sequences may be distorted due to noise.
- Orthogonality cannot be guaranteed for initially orthogonal codes.
- Now let us translate this into code space and explain what we mean by a good autocorrelation. The Barker code (+1, –1, +1, +1, –1, +1, +1, +1, –1, –1, –1),

Features:

- Soft handoff is done.
- CDMA uses co channel cells
- CDMA system users share the same frequency.
- CDMA has a soft capacity limit.
- Multipath fading can be reduced.
- In CDMA more than one user is allowed to share a channel or sub channel with the help of DS-SS.
- Each user is assigned a unique code.
- At receiver the signal is recovered by using the same code sequence.
- In CDMA the user access the channel in random manner. Hence overlap possible (near, far, hidden, exposed)

Advantages of CDMA:

1. Biggest advantage over TDMA/FDMA provide secure communication.
2. In CDMA Multiplexer the frequency hopping phenomenon can be used.

Disadvantages of CDMA:

1. A problem of self-jamming can be occur.
2. Near and far problem occur in CDMA receiver if an unwanted user uses a high transmitted power.

12 Explain functional architecture of GSM system. And also give different tele-services provided by GSM.

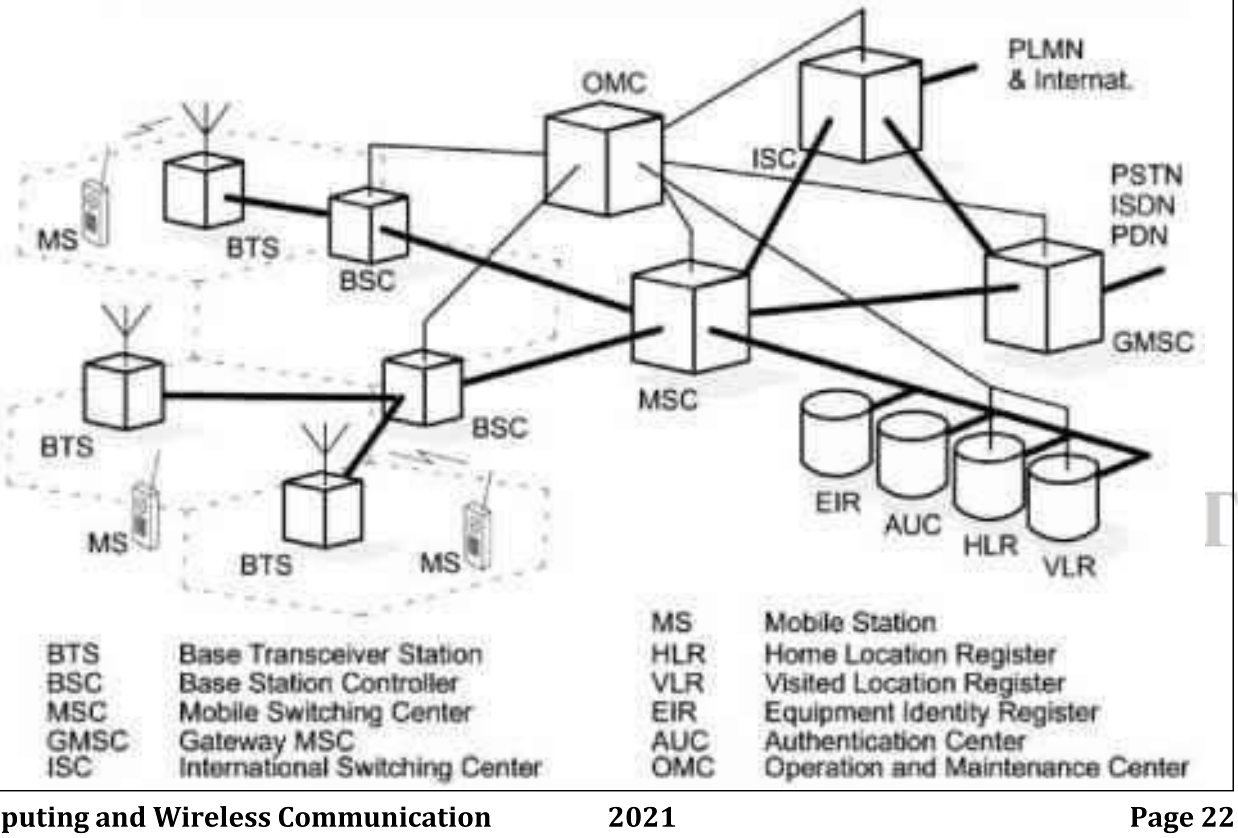
GSM Architecture

- In System, It consists at the minimum one administrative region assigned to one MSC (Mobile Switching Centre).
- Administrative region is commonly known as PLMN (Public Land Mobile Network).
- Each administrative region is subdivided into one or many Location Area (LA).

- One LA consists of many cell groups and each cell group is assigned to one BSC (Base Station Controller).
- For each LA, there will be at least one BSC while cells in one BSC can belong to different LAs.

Radio subsystem (RSS): As the name implies, the radio subsystem (RSS) comprises all radio specific entities, i.e., the mobile stations (MS) and the base station subsystem (BSS). Figure shows the connection between the RSS and the NSS via the A interface (solid lines) and the connection to the OSS via the O interface (dashed lines).

- **Base station subsystem (BSS):** A GSM network comprises many BSSs, each controlled by a base station controller (BSC). The BSS performs all functions necessary to maintain radio connections to an MS, coding/decoding of voice, and rate adaptation to/from the wireless network part. Besides a BSC, the BSS contains several BTSs.
- **Base transceiver station (BTS):** A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS can form a radio cell or, using sectorized antennas, several cells, and is connected to MS via the Um interface (ISDN U interface for mobile use), and to the BSC via the Abis interface. The Um interface contains all the mechanisms necessary for wireless transmission (TDMA, FDMA etc.)
- **Base station controller (BSC):** The BSC basically manages the BTSs. It reserves radio frequencies, handles the handover from one BTS to another within the BSS, and performs paging of the MS. The BSC also multiplexes the radio channels onto the fixed network connections at the A interface.
- **Mobile station (MS):** The MS comprises all user equipment and software needed for communication with a GSM network. An MS consists of user independent hard- and software and of the subscriber identity module (SIM), which stores all user-specific data that is relevant to GSM. While an MS can be identified via the international mobile equipment identity (IMEI), a user can personalize any MS using his or her SIM, i.e., user-specific mechanisms like charging and authentication are based on the SIM, not on the device itself. Device-specific mechanisms, e.g., theft protection, use the device specific IMEI. Without the SIM, only emergency calls are possible. The SIM card contains many identifiers and tables, such as card-type, serial number, a list of subscribed services, a personal identity number (PIN), a PIN unblocking key (PUK), an authentication key Ki, and the international mobile subscriber identity (IMSI).



		MS	Mobile Station
BTS	Base Transceiver Station	HLR	Home Location Register
BSC	Base Station Controller	VLR	Visited Location Register
MSC	Mobile Switching Center	EIR	Equipment Identity Register
GMSC	Gateway MSC	AUC	Authentication Center
ISC	International Switching Center	OMC	Operation and Maintenance Center

- **Network and switching subsystem (NSS):** The “heart” of the GSM system is formed by the network and switching subsystem (NSS). The NSS connects the wireless network with standard public networks, performs handovers between different BSSs, comprises functions for worldwide localization of users and supports charging, accounting, and roaming of users between different providers in different countries. The NSS consists of the following switches and databases:
  - **Mobile services switching center (MSC):** MSCs are high-performance digital ISDN switches. They set up connections to other MSCs and to the BSCs via the A interface, and form the fixed backbone network of a GSM system. Typically, an MSC manages several BSCs in a geographical region. A gateway MSC (GMSC) has additional connections to other fixed networks, such as PSTN and ISDN. Using additional interworking functions (IWF), an MSC can also connect to public data networks (PDN) such as X.25. An MSC handles all signaling needed for connection setup, connection release and handover of connections to other MSCs. The standard signaling system No. 7 (SS7) is used for this purpose. SS7 covers all aspects of control signaling for digital networks (reliable routing and delivery of control messages, establishing and monitoring of calls). Features of SS7 are number portability, free phone/toll/collect/credit calls, call forwarding, three-way calling etc. An MSC also performs all functions needed for supplementary services such as call forwarding, multi-party calls, reverse charging etc.
  - **Home location register (HLR):** The HLR is the most important database in a GSM system as it stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN), subscribed services (e.g., call forwarding, roaming restrictions, GPRS), and the international mobile subscriber identity (IMSI). Dynamic information is also needed, e.g., the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC. As soon as an MS leaves its current LA, the information in the HLR is updated. This information is necessary to localize a user in the worldwide GSM network. All these user-specific information elements only exist once for each user in a single HLR, which also supports charging and accounting. HLRs can manage data for several million customers and contain highly specialized data bases which must fulfill certain real-time requirements to answer requests within certain time-bounds.
  - **Visitor location register (VLR):** The VLR associated to each MSC is a dynamic database which stores all important information needed for the MS users currently in the LA that is associated to the MSC (e.g., IMSI, MSISDN, HLR address). If a new MS comes into an LA the VLR is responsible for, it copies all relevant information for this user from the HLR. This hierarchy of VLR and HLR avoids frequent HLR updates and long-distance signaling of user information.

- **Operation subsystem (OSS):** The third part of a GSM system, the operation subsystem (OSS), contains the necessary functions for network operation and maintenance. The OSS possesses network entities of its own and accesses other entities via SS7 signaling. The following entities have been defined:
  - **Operation and maintenance center (OMC):** The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). Typical OMC management functions are traffic monitoring, status reports of network entities, subscriber and security management, or accounting and billing. OMCs use the concept of telecommunication management network (TMN) as standardized by the ITU-T.
  - **Authentication center (AuC):** As the radio interface and mobile stations are particularly vulnerable, a separate AuC has been defined to protect user identity and data transmission. The AuC contains the algorithms for authentication as well as the keys for encryption and generates the values needed for user authentication in the HLR. The AuC may, in fact, be situated in a special protected part of the HLR.

- **Equipment identity register (EIR):** The EIR is a database for all IMEIs, i.e., it stores all device identifications registered for this network. As MSs are mobile, they can be easily stolen. With a valid SIM, anyone could use the stolen MS. The EIR has a blacklist of stolen (or locked) devices. In theory an MS is useless as soon as the owner has reported a theft. Unfortunately, the blacklists of different providers are not usually synchronized and the illegal use of a device in another operator's network is possible (the reader may speculate as to why this is the case). The EIR also contains a list of valid IMEIs (white list), and a list of malfunctioning devices (gray list).

There are three types of services:

1. Bearer services: It permits transparent and non-transparent, synchronous and asynchronous data transmission.

Transparent service: only use the functions of the physical layer to transmit data. Data transmission has constant delay and throughput if no transmission error occurs.The only mechanism to increase transmission quality is the use of Forward Error Correction (FEC), which codes redundancy into the data stream and help to reconstruct the original data in case of error.

Non Transparent bearer services: It uses layer 2 and 3 to implement error correction and flow control. This uses transparent services, adding a radio link protocol (RLP). Ex, PSTN, ISDN, packet switched PDN (x.25). Data transmission can be synchronous and asynchronous full duplex.

2. **Tele services:**

1. **Telephony:** high quality digital voice transmission, offering at least the typical bandwidth of 3.1 KHz of analog.
   Special coder/decoder are used for voice transmission, while other codes are used for the transmission of analog data for communication with traditional computer modems. Example, fax machines.
2. **Emergency number:** this service is mandatory for all providers and free of charge.
   It should be highest priority connection, possibly pre-empting other connection, and will automatically be set up with the closest emergency center.

3. SMS (Short message service): which offers transmission of messages of up to 160 characters. The SMS do not use the standard GSM but exploit unused capacity in signaling channel. Sending and receiving of message is possible during data or voice transmission. Example, email headers or stock quotes. It can transfer, logos, ringtones, and horoscopes. SMS is used for updating mobile phone software or for implementing so called push services.

4. Enhanced message services (EMS): It offers a large message size (760 characters), formatted text, and transmission of animated pictures, small images and ring tones.

5. Multimedia message services (MMS): It offers transmission of larger pictures (GIF, JPG, and WBMP), short video clips and comes with mobile phones that integrate small cameras.

6. Group 3 fax: fax is transmitted a digital data over the analog telephone network according to the ITU-T standard. T.4 and T.30 using modems. A transparent fax services is used 1) fax data and 2) fax signaling

3. Supplementary services: This services offers various enhancement for the standard telephony services and may vary from provider to provider. Typical supplementary services are user identification, call radiation or forwarding of outgoing calls

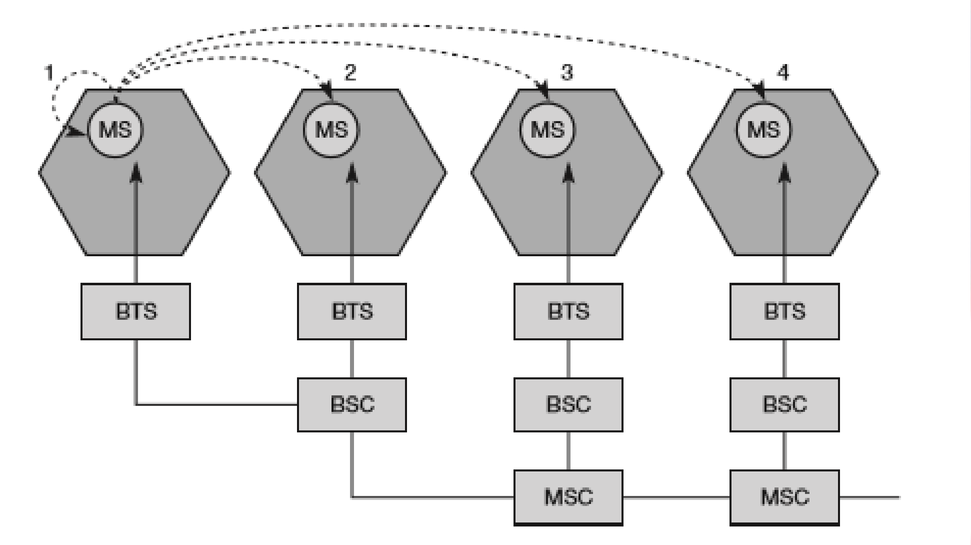
13 How is Mobility Management done in GSM? List the various handovers carried out in GSM and explain any one of them in detail.

Answer:

- → The process of handover or handoff within any cellular system is of great importance.
- → It is a critical process and if performed incorrectly handover can result in the loss of the call.
- → Dropped calls are particularly annoying to users and if the number of dropped calls rises, customer dissatisfaction increases and they are likely to change to another network.

- There are two basic reasons for a handover (about 40 have been identified in the standard):
  - The mobile station moves out of the range of a BTS or a certain antenna of a BTS respectively. The received signal level decreases continuously until it falls below the minimal requirements for communication. The error rate may grow due to interference, the distance to the BTS may be too high (max. 35 km) etc. – all these effects may diminish the quality of the radio link and make radio transmission impossible in the near future.
  - The wired infrastructure (MSC, BSC) may decide that the traffic in one cell is too high and shift some MS to other cells with a lower load (if possible). Handover may be due to load balancing.

Types of GSM handover



- → Within the GSM system there are four types of handover that can be performed for GSM only systems:
  - ○ **Intra-BTS handover:** This form of GSM handover occurs if it is required to change the frequency or slot being used by a mobile because of interference, or other reasons.
  - ○ In this form of GSM handover, the mobile remains attached to the same base station transceiver, but change the channel or slot.
  - ○ **Inter-BTS Intra BSC handover:** This GSM handover or GSM handoff occurs when the mobile is moved out of the coverage area of one BTS but into another controlled by the same BSC.
  - ○ In this instance the BSC is able to perform the handover and it assigns a new channel and slot to the mobile, before releasing the old BTS from communicating with the mobile.
  - ○ **Inter-BSC handover:** When the mobile is moved out of the range of cells

controlled by one BSC, a more involved form of handover has to be performed, handing over not only from one BTS to another but one BSC to another.

- For this the handover is controlled by the MSC.
- **Inter-MSC handover:** This form of handover occurs when changing between networks. The two MSCs involved negotiate to control the handover.

Example: Figure shows the typical behavior of the received signal level while an MS moves away from one BTS (BTSold) closer to another one (BTSnew). In this case, the handover decision does not depend on the actual value of the received signal level, but on the average value. Therefore, the BSC collects all values (bit error rate and signal levels from uplink and downlink) from BTS and MS and calculates average values. These values are then compared to thresholds, i.e., the handover margin (HO_MARGIN)

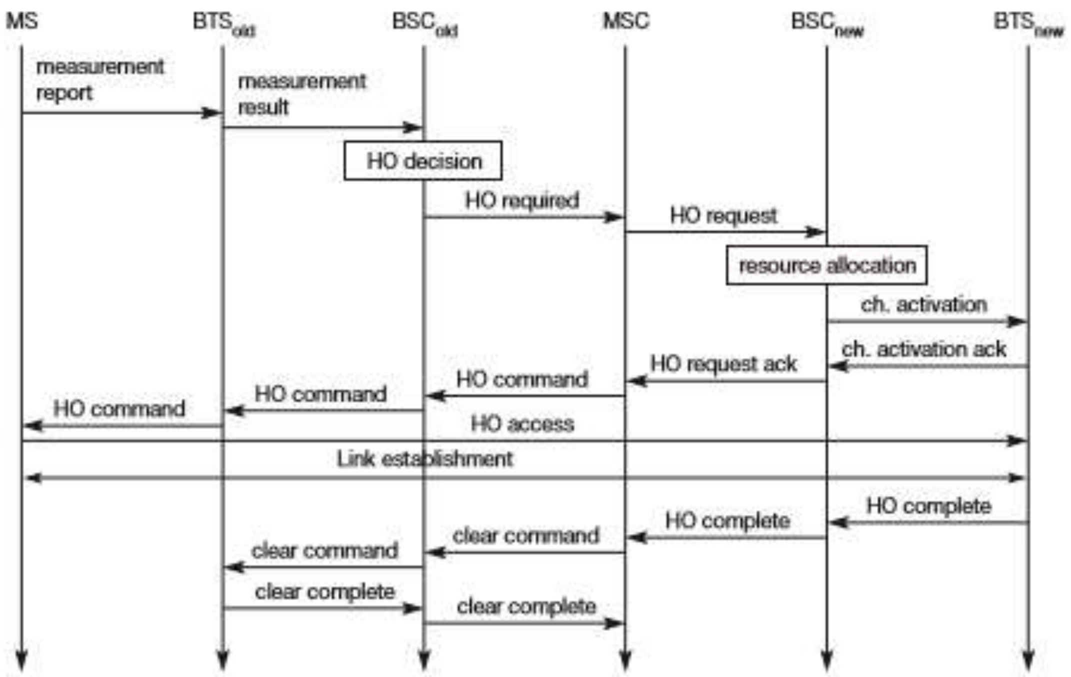


Figure shows the typical signal flow during an inter-BSC, intra-MSC handover.

- The MS sends its periodic measurements reports, the BTSold forwards these reports to the BSCold together with its own measurements. Based on these values and, e.g., on current traffic conditions, the BSCold may decide to perform a handover and sends the message HO_required to the MSC.

- The task of the MSC then comprises the request of the resources needed for the handover from the new BSC, BSCnew. This BSC checks if enough resources (typically frequencies or time slots) are available and activates a physical channel at the BTSnew to prepare for the arrival of the MS.

- The BTSnew acknowledges the successful channel activation, BSCnew acknowledges the handover request. The MSC then issues a handover command that is forwarded to the MS. The MS now breaks its old radio link and accesses the new BTS. The next steps include the establishment of the link (this includes layer two link establishment and handover complete messages from the MS).

- Basically, the MS has then finished the handover, but it is important to release the resources at the old BSC and BTS and to signal the successful handover using the handover and clear complete messages as shown. More sophisticated handover mechanisms are needed for seamless handovers between different systems.

14 Explain mobile originated call and mobile terminated call procedure.

- All these numbers are needed to find a subscriber and to maintain the connection with a mobile station. The interesting case is the mobile terminated call (MTC), i.e., a situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station).
- Figure 4.8 shows the basic steps needed to connect the calling station with the mobile user.
- In step,

1. a user dials the phone number of a GSM subscriber.
2. The fixed network (PSTN) notices (looking at the destination code) that the number belongs to a user in the GSM network and forwards the call setup to the Gateway MSC
3. The GMSC identifies the HLR for the subscriber (which is coded in the phone number) and signals the call setup to the HLR
4. The HLR now checks whether the number exists and whether the user has subscribed to the requested services, and requests an MSRN from the current VLR
5. After receiving the MSRN
6. the HLR can determine the MSC responsible for the MS and forwards this information to the GMSC
7. The GMSC can now forward the call setup request to the MSC indicated.
8. From this point on, the MSC is responsible for all further steps. First, it requests the current status of the MS from the VLR.
9. If the MS is available, the MSC initiates paging in all cells it is responsible for (i.e. the location area, LA.
10. as searching for the right cell would be too time consuming (but this approach puts some load on the signaling channels so optimizations exist). The BTSs of all BSSs transmit this paging signal to the MS
11. If the MS answers (12 and 13), the VLR has to perform security checks (set up encryption etc.). The VLR then signals to the MSC to set up a connection to the MS

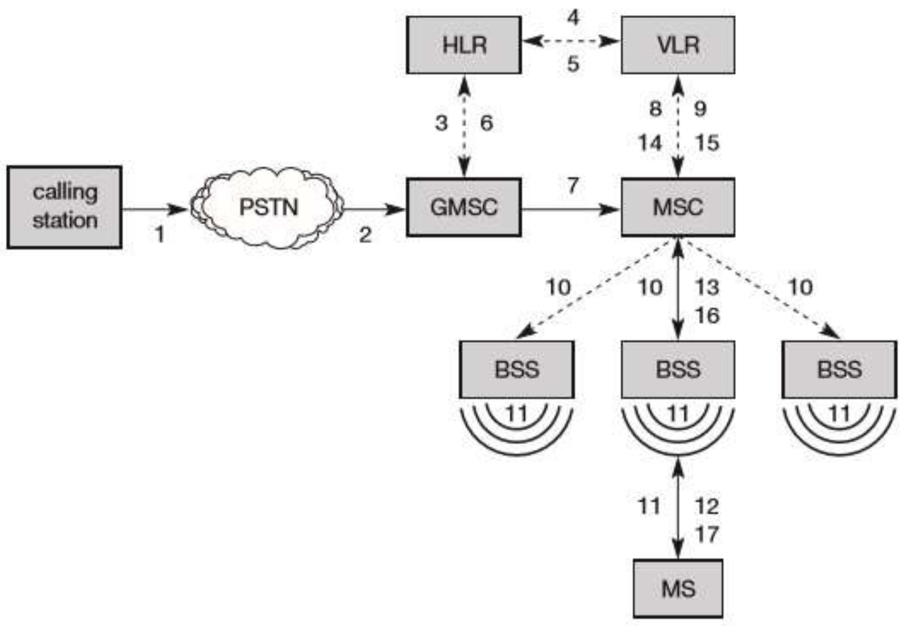


Figure 4.8
Mobile terminated call (MTC)

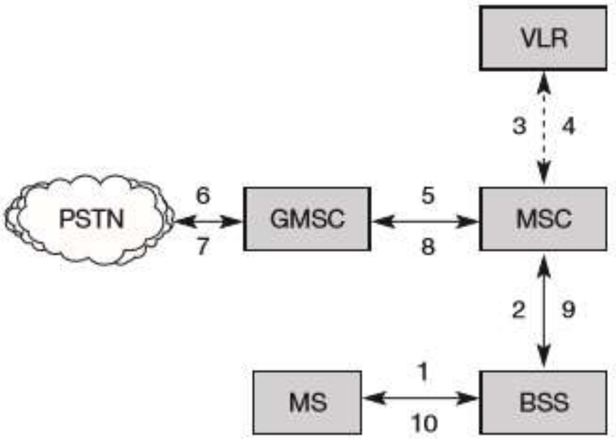


Figure 4.9
Mobile originated call (MOC)

mobile originated call (MOC):

- It is much simpler to perform a mobile originated call (MOC) compared to a MTC (see Figure 4.9).
    1. The MS transmits a request for a new connection.
    2. the BSS forwards this request to the MSC
    3. The MSC then checks if this user is allowed to set up a call with the requested service (3 and 4) and checks the availability of resources through the GSM network and into the PSTN.
    4. If all resources are available, the MSC sets up a connection between the MS and the fixed network.

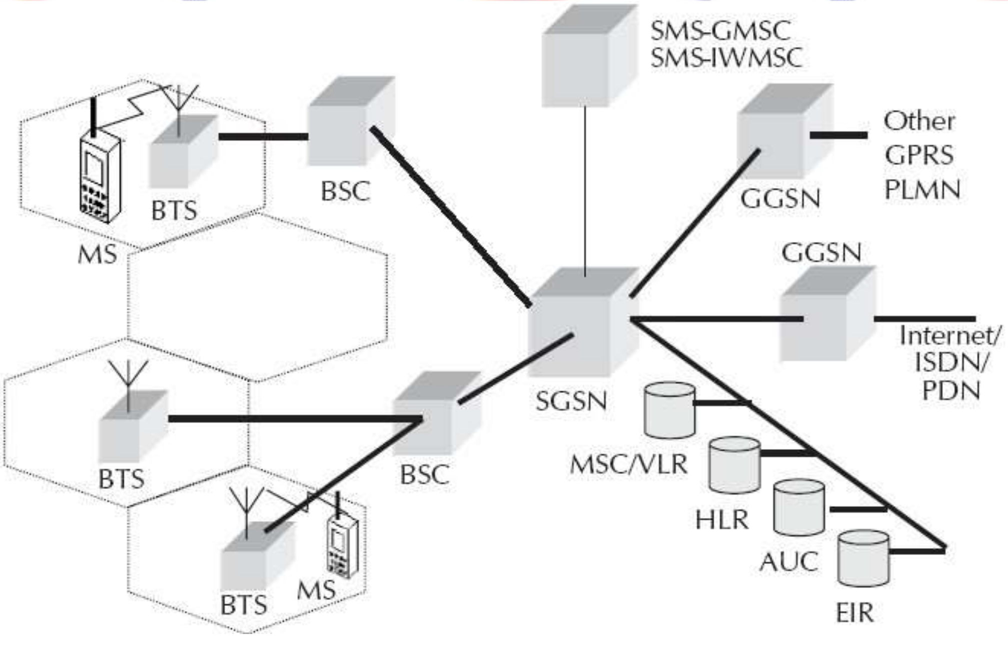
- In addition to the steps mentioned above, other messages are exchanged between an MS and BTS during connection setup (in either direction).
- These messages can be quite often heard in radios or badly shielded loudspeakers as crackling noise before the phone rings.

15 Draw GPRS System Architecture. Discuss GPRS network enhancement over GSM.

GPRS architecture:

→ GPRS uses the GSM architecture for voice.

→ GPRS support nodes are responsible for the delivery and routing of data packets between the mobile stations and the external packet data networks (PDN).



AUC	**Authentication Center**	**MS**	**Mobile Station**
BSC	**Base Station Controller**	**MSC**	**Mobile Switching Center**
BTS	**Base Transceiver Station**	**PDN**	**Packet Data Network**
EIR	**Equipment Identity Register**	**PLMN**	**Public Land Mobile Network**
GGSN	**Gateway GPRS Support Node**	**SMSC**	**Short Message Service Center**
GPRS	**General Packet Radio Service**	**SMS-GMSC**	**SMS Gateway MSC**
HLR	**Home Location Register**	**SMS-IWMSC**	**SMS Inter-Working MSC**
ISDN	**Integrated System Digital Network**	**SGSN**	**Serving GPRS Support Node**

→ There are 2 types of support nodes which are given below:

Serving GPRS Support Node (SGSN)

→ A SGSN is at the same hierarchical level as the MSC. Whatever functions MSC does for the voice, SGSN does the same for packet data.

→ SGSN's tasks include packet switching, routing and transfer, mobility management, logical link management, and authentication and charging functions.

→ SGSN processes registration of new mobile subscribers and keeps a record of their location inside a given service area.

→ The location register of the SGSN stores location information and uses profiles of all GPRS users registered with the SGSN.

→ SGSN sends queries to HLR to obtain profile data of GPRS subscribers. The SGSN is connected to the base station system with Frame Relay.

Gateway GPRS Support Node (GGSN)

→ A GGSN acts as an interface between the GPRS backbone network and the external packet data network.

→ GGSN's function is similar to that of a router in a LAN. GGSN maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations.

→ It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like internet or X.25, PDP sends these packets out on the corresponding packet data network.

→ The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register.

→ GGSN also performs authentication and charging functions related to data transfer.

Some existing GSM network elements must be enhanced in order to support packet data. These are as following

→ Some Nodes of GSM Network needs to be upgraded to support the GPRS system.

Base Station System (BSS)

→ BSS system needs enhancements to recognize and send packet data.

→ This includes BTS upgrade to allow transportation of user data to the SGSN.

→ Also, the BTS needs to be upgraded to support packet data transportation between the BTS and the MS (Mobile Station) over the radio.

Home Location Register (HLR)

→ HLR needs enhancement to register GPRS user profiles and respond to queries originating from GSNs regarding these profiles.

Mobile Station (MS)

→ The mobile station or the mobile phone for GPRS is different from that of GSM.

SMS Nodes

→ SMS-GMSCs and SMS-IWMSCs are upgraded to support SMS transmission via the SGSN.0

→ Optionally, the MSC/VLR can be enhanced for more efficient coordination of GPRS and non- GPRS services and functionality.

→ GPRS uses two frequency bands at 45 MHz apart; viz., 890-915 MHz for uplink (MS to BTS), and 935-960 MHz for downlink (BTS to MS).

Uplink: 890 to 915 Mhz
Downlink: 935 to 960 Mhz

16 Discuss GPRS specific applications, Billing and Limitation of GPRS.

GPRS-Specific Applications:

- **Chat:** chat is a very popular service in Internet and GSM (over SMS). Groups of like-minded people. use chat services as a means to communicate and discuss matters of interest. Generally, people use different chat services; one, through Internet and the other, using SMS (offered by mobile operator)

- **Multimedia Services:** Multimedia objects like photographs, pictures, postcards, greet ng cards and presentations, static web pages can be sent and received over the mobile network. There are many phones available in the marketplace where a digital camera is integrated with the phone. These pictures can be sent as an electronic object or a printed one. Sending moving images in a mobile environment has several vertical market applications including monitoring parking lots or building sites for intruders or thieves. This can also be used by law enforcement agents, journalists, and insurance agents for sending images of accident site. Doctors can use these applications to send pictures of patients from a health center for expert help.

- **Virtual Private Network:** GPRS network can be used to offer VPN services. Many Bank ATM machines use VSAT (Very Small Aperture Terminal) to connect the ATM system with the banks server. As the bandwidth in GPRS is higher, many banks in India are migrating from VSAT to GPRS-based networks. This is expected to reduce the transaction time by about 25%

- **Personal Information Management:** Personal diary, address book, appointments, engagements etc. are very useful for a mobile individual. Some of these are kept in the phone some in the organizer and some in the Intranet. UsingJ2ME and WTAI (Wireless Telephony Application Interface) the address book, the diary of the phone can be integrated with the diary at the home office. GPRS and other bearer technology will help achieve this.

- **Job Sheet Dispatch:** GPRS can be used to assign and communicate job sheets from office-based staff to mobile field staff. Customers typically telephone a call center whose staff takes the call and categorize it. Those calls requiring a visit by field sales or service representative can then be escalated to those mobile workers. Job dispatch applications can optionally be combined with vehicle positioning applications so that the ne available suitable personnel can be deployed to serve a customer

- **Unified Messaging:** Unified messaging uses a single mailbox for all messages, including voice mail, fax, e-mail, SMS, MMS, and pager messages. With the various mailbox in one place, unified messaging systems then allow for a variety of access methods to recover messages of different types. Some will use text-to-voice systems to read e-mail and, less commonly, faxes over a normal phone line, while most will allow the interrogation of the contents of the various mailboxes through data access, such as the Internet. Others may be configured to alert the user on the terminal type of their choice when messages are received

- **Vehicle Positioning:** This application integrates GPS (Global Positioning System) that tell people where they are. GPS is a free-to-use global network of 24 satellites run by the US Department of Defence. Anyone with a GPS receiver can receive their satellite position and thereby find out where they are. Vehicle-positioning applications can be used to deliver several services including remote vehicle diagnostics, ad hoc stolen vehicle tracking and new rental car fleet tariffs. In India this application is becoming popular in logistics industry

- **Location-based Services and Telematics:** Location-based services provide the ability to link push or pull information services with a user's location. Examples include hotel and restaurant finders, roadside assistance, and city-specific news and information. All systems developed for Intelligent Transportation System (ITS) are built around GPRS and GPS technology. Location can be determined either through GPS or cell id from the operator. This technology also has vertical applications such as workforce management and vehicle tracking.

Billing:
Tariffing of data in wireless network has always been a challenges.

→ For voice networks tariffs are generally based on distance and time means that user pay more for long distance calls. They also pay more if they keep the circuit busy by talking for a longer period of time. So charging is fundamental part of the architecture.

→ On other hand, in data services charging with circuit busy does not have any meaning. Also, charging a customer by the distance traversed by a packet does not make any sense.

→ It is Believed that the optimal GPRS pricing model will be based on two variables, Time and Packet.

→ Network operators will levy a nominal per packet charge during peak time plus a flat rate. There will be no per packet charge during non-peak times.

→ Time and packet related charging will encourage application such as Remote monitoring, meter reading and chat to use GPRS at night when spare network capacity is available.

→ Simultaneously, nominal per packet charge during the day will help to allocate scarce radio resources, and charge radio heavy application such as file and image transfer more than application with lower data intensity.

→ It has the advantage of automatically adjusting customer charging according to their application usage.

→ **Minimum charging information that must be collected are:**

- Destination and source addresses
- Usage of radio interface
- Usage of external Packet Data Networks
- Usage of the packet data protocol addresses
- Usage of general GPRS resources and location of the Mobile Station

→ A GPRS network needs to be able to count packets to charging customers for the volume of packets they send and receive.

→ Various business models exist for charging customers as billing of services can be based on the transmitted data volume, the type of service, the chosen QoS profile, etc.

→ GPRS call records are generated in the GPRS Service Nodes. Packet counts are passed to a Charging Gateway that generates Call Detail Records that are sent to the billing system.

→ The Charging for GPRS services dependent on following parameters:

1. **Duration:** the duration of a PDP context session.
2. **Time:** date time of the day, day of week, (low tariffs for happy hours at night).
3. **Volume:** the amount of data bites sent and received.
4. **Location:** the location of the subscribers
5. **Flat rate:** a fixed monthly change a rental.
6. **Free Charge:** data subscribed should be free from charge.
7. **Quality of Service:** More charge for high network priority and data rate.
8. **SMS:** Specific CDRs will be generated by SGSN for SMS.
9. **Reverse charging:** the subscriber sending the data is charged. The subscriber receiving the data is not charged for the data received.

Limitation of GPRS

→ A GPRS is a new enabling mobile data service which offers a major improvement in spectrum efficiency, capability and functionality compared with today's non-voice mobile services.

→ However, it is important to note that there are some limitations with GPRS, which can be summarized as:

Limited Cell Capacity for All Users

→ GPRS does impact a network's existing cell capacity.

→ There are only limited radio resources that can be deployed for different uses - use for one purpose precludes simultaneous use for another.

→ For example, voice and GPRS calls both use the same network resources. If tariffing and billing are not done properly, this may have impact on revenue.

Speeds Much Lower in Reality

→ Achieving the theoretical maximum GPRS data transmission speed of 171.2 kbps would require a single user taking over all eight timeslots without any error protection.

→ Clearly, it is unlikely that a network operator will allow all timeslots to be used by a single GPRS user.

→ Additionally, the initial GPRS terminals are expected be severely limited - supporting only one, two or three timeslots.

→ The bandwidth available to a GPRS user will therefore be severely limited.

→ The reality is that mobile networks are always likely to have lower data transmission speeds than fixed networks.

Transit Delays

→ GPRS packets are sent in all different directions to reach the same destination.

→ This opens up the potential for one or some of those packets to be lost or corrupted during the data transmission over the radio link.

→ The GPRS standards recognize this inherent feature of wireless packet technologies and incorporate data integrity and retransmission strategies.

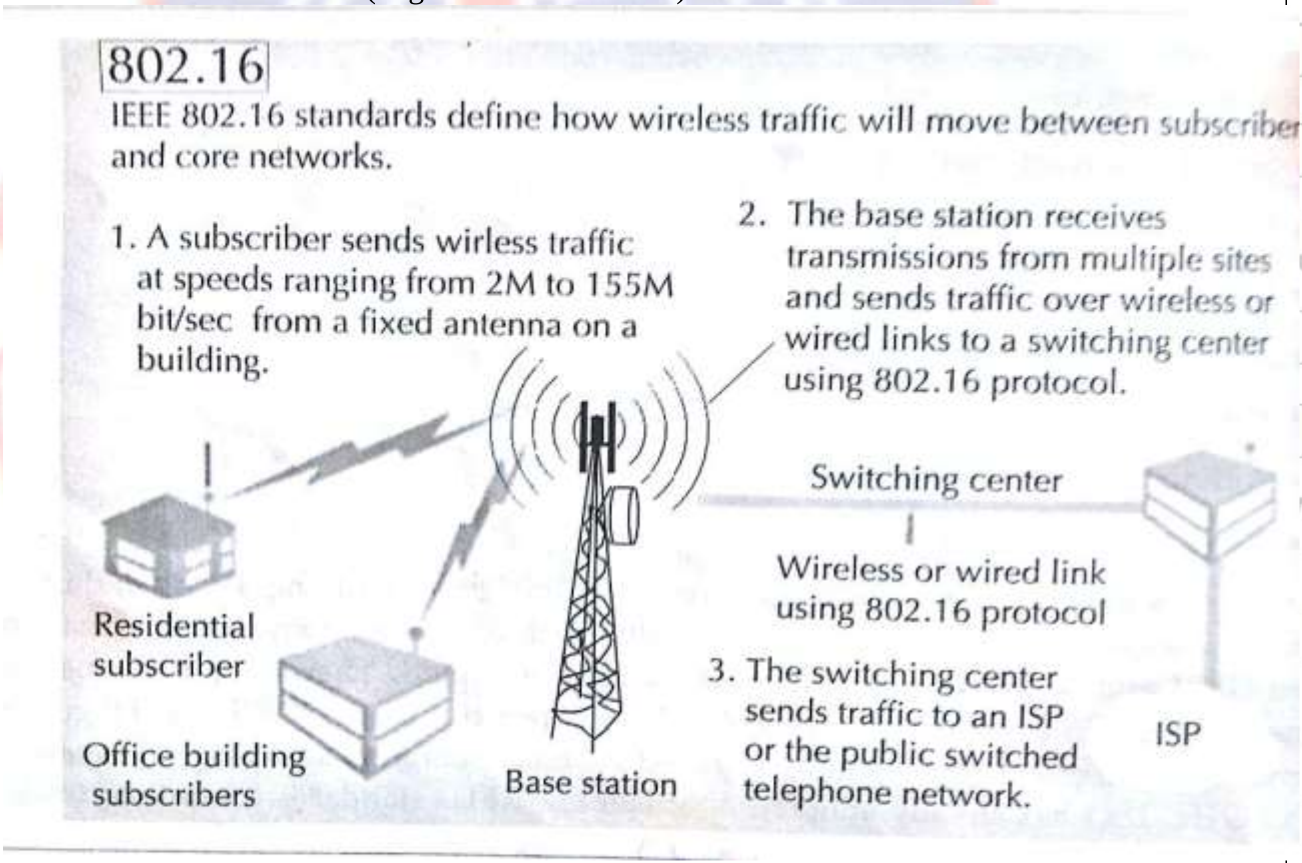
→ However, the result is that potential transit delays can occur.

Support of GPRS Mobile Terminate Connection for a Mobile Server not Supported:

→ As of date a GPRS terminal can only act as a client device. There are many services for which the server needs to be mobile.example could be a mobile healthcare center for rural population. For such application the server needs to be on the mobile network and user needs to be connect to the server. Using GPRS network, such communication is not possible.

17 Explain architecture of IEEE 802.16 standard

- The World is moving towards a convergence of voice, data, and video. This convergence will demand interoperability and high data rate. Keeping this in mind, the IEEE 802 Committee set up the 802.16 working group in 1999 to develop wireless broadband or wirelessMAN (wireless metropolitan area network) standards.
- Wireless MAN offers an alternative to high bandwidth wireline access networks like fiber optic, cable modems and DSL (Digital Subscriber Line).


802.16
IEEE 802.16 standards define how wireless traffic will move between subscriber and core networks.
1. A subscriber sends wirless traffic at speeds ranging from 2M to 155M bit/sec from a fixed antenna on a building.
2. The base station receives transmissions from multiple sites and sends traffic over wireless or wired links to a switching center using 802.16 protocol.
Switching center
Wireless or wired link using 802.16 protocol
Residential subscriber
Office building subscribers
Base station
3. The switching center sends traffic to an ISP or the public switched telephone network.
ISP

- The release of wirelessMAN (IEEE 802.16) standards in April 2002 has paved the way for the entry of broadband wireless access as a new bearer to link homes and businesses with core telecommunications network access to buildings through exterior antennas communicating with radio base stations.
- The technology is expected to provide less expensive access with more ubiquitous broadband access with integrated data, voice and video services.
- One of the most attractive aspects of wireless broadband technology is that networks can be created in just weeks by developing a small number of base stations on building or poles to create high-capacity wireless access systems.

- In a wired set up, one physical wire will connect the device with the network. Also, we need to keep many wires reserved for future growth. Therefore, the initial investment in wired infrastructure is very high. Wireless network can grow as the demand increases.
- At any point in time the numbers of active users are always a fraction of the number of subscribers. In a wireless environment the number of channels is always low compared to the number of subscribers. This makes wireless technologies very attractive to the service providers.

- IEEE 802.16 standardizes the air interface and related functions associated with WLL. Three working Groups have been chartered to produce following standards.
    - IEEE 802.16.1-Air interface for 10 to 66 GHz.
    - IEEE 802.16.2-Cpexistence of broadband wireless access systems.
    - IEEE 802.16.3-Air interface for licensed frequencies, 2 to 11 GHz.
    - Extensive radio spectrum is available in frequency bands from 10 to 66 GHz worldwide. In a business scenario, 802.16 can serve as a backbone for 802.11 networks. Other possibilities are using 802.16 within the enterprise along with 802.11a, b or g.

- IEEE 802.16 standards are concerned with the air interface between a subscriber's transceiver station and a base transceiver station. The 802.16 standards are organized into three-layer architecture.
    - The physical layer: This layer specifies the frequency band, the modulation scheme, error-correction techniques, synchronization between transmitter and receiver, data rate and the multiplexing structure.
    - The MAC (Media Access Control) layer: This layer is responsible for transmitting data in frames and controlling access to the shared wireless medium through media access control (MAC) layer. The MAC protocol defines how and when a base station or subscriber station may initiate transmission on the channel.
    - Above the MAC layer is a convergence layer that provides functions specific to the service being provided. For IEEE 802.16.1, bearer services include digital audio/video multicast, digital telephony, ATM, Internet access, wireless trunks in telephone network and frame relay.

18 How does the Mobile IP work? Explain its architecture.

How Mobile IP works / Architecture of Mobile IP:

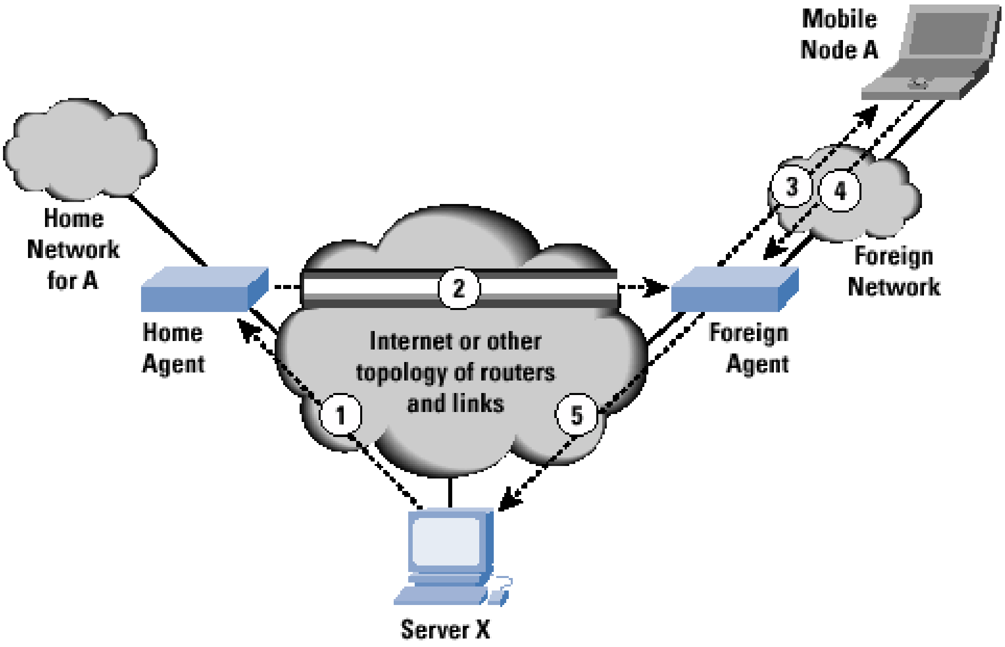
- As the user moves, the point of attachment will change from one subnet to another subnet resulting in a change of IP address. This will force the connection to terminate. Therefore, the technology for allowable mobility while a data connection is alive is known as "Mobile IP".
- The Term 'Mobile' in 'Mobile IP' signifies that, while a user is connected to applications across the Internet and user's point of attachment changes dynamically, all connections are maintained despite the change in underlying network properties.
- This is similar to the handoff/roaming situation in cellular system.
- In cellular network, when a user is mobile, the point of attachment changes. However, in spite of such changes the user is able to continue the conversation.

How Does Mobile IP Works?

- Internet Protocol (IP) routes packets from a source endpoint to a destination endpoint through various routers.
- An IP address of a host can be considered to be a combination of network address and node address
- The network portion of an IP address is used by routers to deliver the packet to the last router in change to which the target computer is attached. This last router then uses the host portion of the IP address to deliver the other IP packet to the destination computer.

- In additional to IP addresses of the host for meaning full communication we need the TCP or UDP port of the application.
- A TCP connection is identified by a quadruplet that contains the IP addresses and port number of the sender and point along with the IP address and port number of the receiving end point.
- To ensured that an active TCP connection is not terminated while the user is mobile, it is essential that all of this four identifier remain constant.
- The TCP ports are application specific and generally constant.
- However, the IP address change from subnet to subnet. Therefore, to fix this problem mobile IP allows the mobile node to use two IP addresses. Which are given bellow.
  1. Home address
  2. Care-of address
- The home address is static and known to everybody as the identity of the host.
- The Care-of address changes at each new point of attachment and can be thought of as the mobile nodes location specific address.
- When the mobile node is roaming and is attached to a foreign network, the home agent receives all the packets for the mobile node and arranges to forward them to the mobile nodes current point of attachment.
- The network node that is responsible for forwarding and managing this transparency is known as the home agent.
- Whenever the mobile node moves, it registered its new care-of address with its home agent.
- The home agent forward the packet to the foreign network using the care-of address.
- The delivery requires that the packet header is modified so that the care-of address becomes the destination IP address.
- This new header encapsulates the original packet, causing the mobile nodes home address to have no impact on the encapsulated packets routing. This phenomenon is called tunneling.

Figure shows in general terms how mobile IP deals with the problem of dynamic IP address.



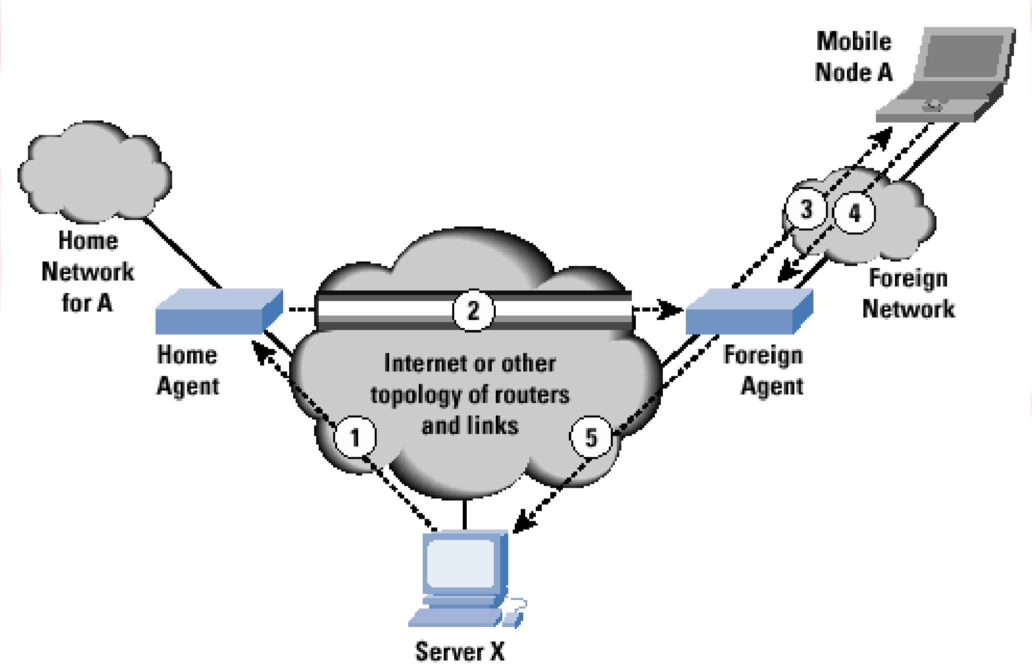
- Let us take an example of IP datagrams being exchanged over a TCP connection between the mobile node (A) and another host (Server X), this following steps occurs
- **Step 1:** Server X wants to transmit an IP datagram to node A. the home address of A is advertised and known to X. X does not know whether A is in the home network or some ware else. Therefore, X send the packet to A with A's home address as the destination IP address in the IP header. The IP datagram is routed A's home network.

- **Step 2:** at A’s home network, the incoming IP datagram is intercepted by the home agent. The home agent discovers that A is in a foreign network. A care-of address has been allocated to A by this foreign network and available with home agent. The home agent encapsulates the entire datagram inside a new IP datagram, with A’s care-of address in the IP header. This new datagram with the care-of address as the destination address is retransmitted by the home agent.
- **Step 3:** at the foreign network the IP datagram is intercepted by the foreign agent. The foreign agent is the counter part of the home agent in the foreign network. The foreign agent strips off the outer IP header, and delivers the original datagram to A.
- **Step 4:** A intends to response to this massage and sends traffic to X. in this example X is not mobile, therefore X has a fixed IP address. For routing A’s IP datagram to X, each datagram is send to some router in the foreign. Typically, this router is the foreign agent. A uses X’s IP address as the destination address.

The mobile IP needs to support three basic capabilities,

1. **Discovery:** a mobile node uses discovery procedure to identifies prospective home agents and foreign agents.
2. **Registration:** a mobile node uses a registration procedure to inform its home agent of its care-of address.
3. **Tunnelling:** tunnelling procedure is used to forward IP datagram from a home address to a care-of address.

19 What is a mobile IP? Explain discovery, registration and tunnelling with mobile IP.



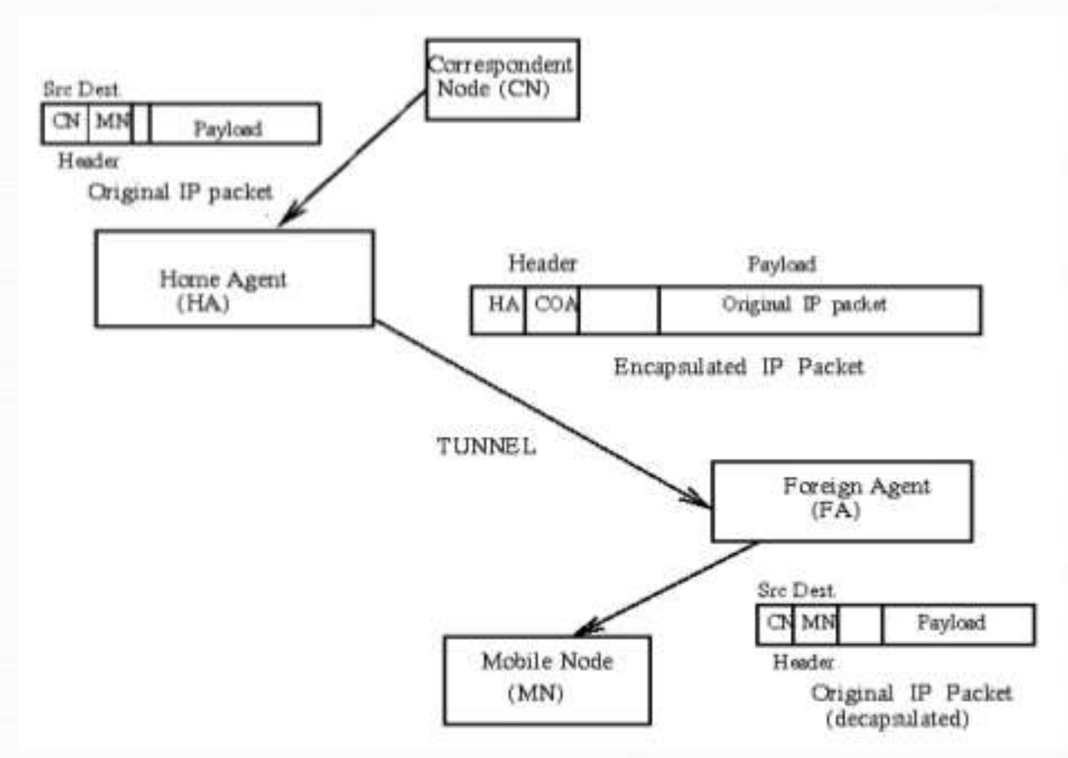
- **Discovery:**
  - This procedure is used to identify the home agents and foreign agents.
  - It the router detects any new mobile node, it sends a router advertisement message for knowing the point of attachment to internet.
  - The discovery procedure is on top of existing router discovery
  - The discovery procedure can be used to determine whether a node is home network or foreign network
  - A router advertisement message is periodically sent to compare the address of the network part of the IP with router IP address assigned by the home network. If the data matches, mobile node is in the home network otherwise the mobile node is in foreign network

- **Registration:**
  - Once a mobile node gets a care of address from the foreign agent, it needs to be registered with the home agent using the care-of-address.
  - With the care-of address information the mobile node issues a registration request to the home agent.
  - The home agent responds by updating the routing table and sending a registration replay to the mobile node.

Authentication:

- Authentication is a necessary step for registration. Every mobile node needs to be authenticated
- With the help of HMAC-MD5 hashing algorithm and 128 bit secrete key a digital signature is generated
- The digital signature is unique. The home agent along with the mobile node share a common key for authentication so that it is unknown to hackers
- The home agent contains a binding for the mobile node referred to as the triplet. It comprises the registration lifetime, home address and care of address
- Following is the list of registration steps
  - **Step 1:** The mobile node sends a request for registration to the foreign agent. The mobile node request for forwarding service from the foreign agent.
  - **Step II:** The registration request is relayed by the of foreign agent to the mobile nodes home agent.
  - **Step III:** The registration request is accepted/rejected by the home agent. The home agent sends a registration reply to the foreign agent.
  - **Step IV:** The reply message is relayed by the foreign node to the mobile node that requested registration.
- The mobile node can behave as its own foreign agent with a co-located care of address. This address is IP address got from mobile that relates to the foreign network. Registration is done directly with the home agent when the mobile node uses a co-located care of address

- **Tunnelling and Encapsulations:**



Tunnelling:

- A tunnel creates a virtual pipe so that data packets can travel from the start to the end of the tunnel. Tunnelling is done through IP within IP encapsulation.

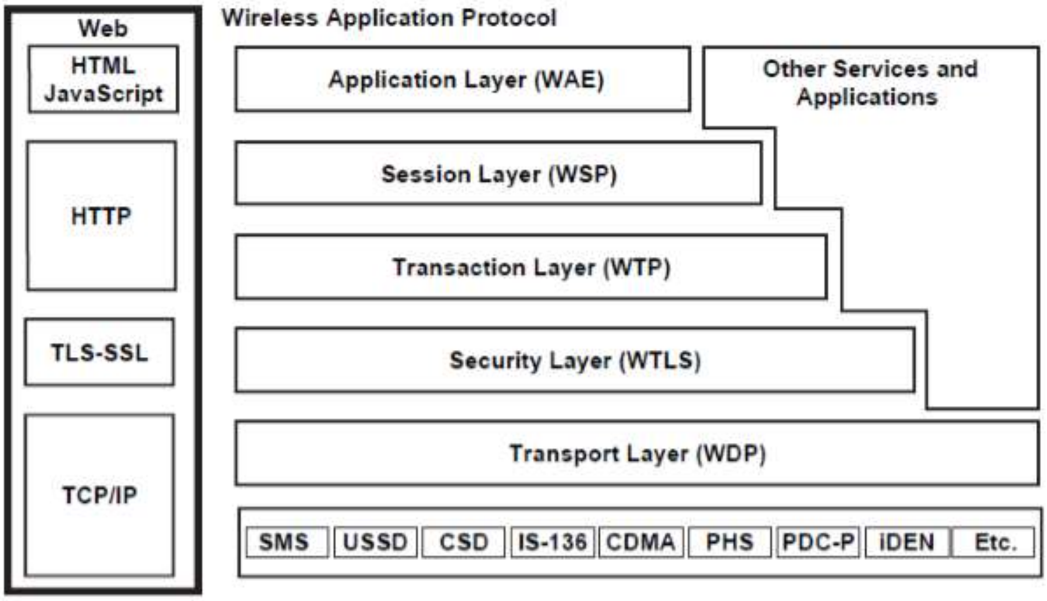
Encapsulation:

- Encapsulation is a method where the data packet comprises a packet header and data and then a new packet is created by combining them. A reverse method is following for encapsulation.
- Using IP-within IP, the home agent, adds a new IP header called tunnel header.
- The new tunnel header uses the mobile node's care-of address as the tunnel destination IP address.
- The tunnel header uses 4 as the protocol number, indicating that the next protocol header is again an IP header.
- In IP-within-IP, the entire original IP header is preserved as the first part of the payload of the tunnel header.
- The foreign agent after receiving the packet, drops the tunnel header and delivers the rest to the mobile node.

20 Describe the WAP protocol stack. What are the functions of different layers in this protocol stack?

WAP Architecture

- It provides a scalable and extensible environment for application development of mobile
- This is achieved using layered design of protocol stack. The layers resemble the layers of OSI model.
- Each layer is accessible by layers above as well as by other services and applications through a set of well-defined interface.
- External applications may access session, transaction, security and transport layers directly.



Wireless Application **Environment**

- WAE is the uppermost layer in the WAP stack. It is general purpose environment based on combination of WWW and mobile telephony technologies.
- Its primary objective is to achieve interoperable environment that allows operators and service providers to build applications that can reach wide variety of wireless platforms.
- It uses URL and URI for addressing. Language used is WML and WML script. WML script can be used for validation of user input.

User Agent

- Technically user agent significant who works on behalf of the users.
- In WWW and WAE context, user agent is the user facing browser software.
- In WAE this is generally referred to as micro-browser.
- WAE allows the integration of domain-specific user agents as well.

User Agent Profile (UAProf)

- The UAProf specification allows WAP to notify the content server about the device capability.
- UAProf is also referred to as Capability and preference information (CPI).
- CPI is passed from the WAP client to the origin server through intermediate network points.

Wireless Markup language (WML)

- WML is tag-based document manipulation language. It shares the heritage with HTML of W3C and HDML of Unwired planet.
- WML is designed to specify presentation and user interaction on mobile phones and other wireless devices.
- WML implements a deck and card metaphor.

WMLScript

- WMLScript is an extended subset of JavaScript and forms a standard means for adding procedural logic to WML decks.
- WMLScript is used to do client side processing. Therefore, it can be used very effectively to add intelligence to the client and enhance the user interface.

Wireless Telephony Application

- WTA provides a means to create telephony services using WAP. It uses WTA Interface (WTAI) which can be evoked from WML and for WML script.
- The Repository makes it possible to store WTA services in device which can be accessed without accessing the network. The access can be based on any event like call disconnect, call answer etc.
- Sometimes, there can be notification to user based on which WTA services are accessed by users. The notification is called WTA service indication.

Wireless Session Protocol.

- WSP provides reliable, organized exchange of content between client and server.
- The core of WSP design is binary form of HTTP. All methods defined by HTTP 1.1 are supported.
- Capability negotiation is used to agree on common level of protocol functionality as well as to agree on a set of extended request methods so that full compatibility to HTTP applications can be retained.
- An idle session can be suspended to free network resources and can be resumed without overload of full-blown session establishment.
- WSP also supports asynchronous requests. Hence, multiple requests will improve utilization of air time.

Wireless Transaction Protocol

- WTP is defined as light-weight transaction-oriented protocol suitable for implementation in thin clients.
- Each transaction has unique identifiers, acknowledgements, duplicates removal and retransmission.

- Class 1 and Class 2 enable user to confirm every received message, however, in class 0, there is no acknowledgement.
- WTP has no security mechanisms and no explicit connection set-up or tear-down phases.

Wireless Transport Layer Security

- WTLS is security protocol based on industry standard transport layer security (TLS). It provides transport layer security between a WAP client and the WAP Gateway/ Proxy.
- The goals of WTLS are data integrity, privacy, authentication, Denial-of-service protection.
- It has features like datagram support, optimized handshake and dynamic key refreshing.

Wireless Datagram Protocol

- WDP provides application addressing by port numbers, optional segmentation and reassembly, optional error detection.
- It supports simultaneous communication instances from higher layer over a single underlying WDP bearer service. The port number identifies higher level entity above WDP.
- The adaptation layer of WDP maps WDP functions directly on to a bearer based on its specific characteristics.
- On the GSM SMS, datagram functionality is provided by WDP.

Optimal WAP Bearers

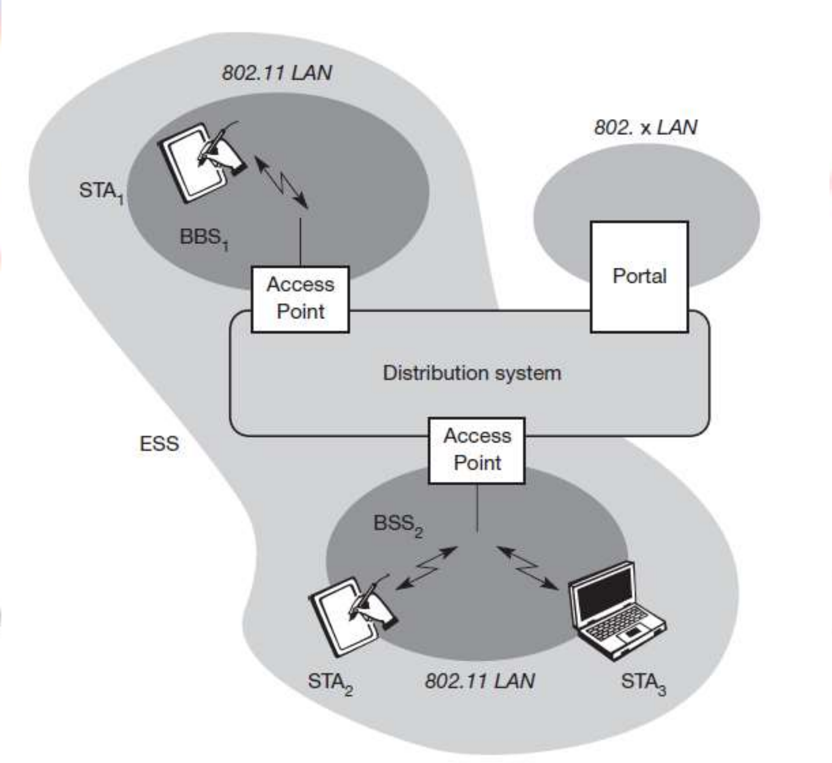
- The WAP is designed to operate over a variety of different service like SMS,' Circuit Switched Data (CSD)', GPRS,' Unstructured Supplementary Services Data(USSD)'.

21 Explain IEEE 802.11 architecture and services.

Architecture:

- Wireless networks can exhibit two different basic system architectures infrastructure-based or ad-hoc.

Infrastructure based:

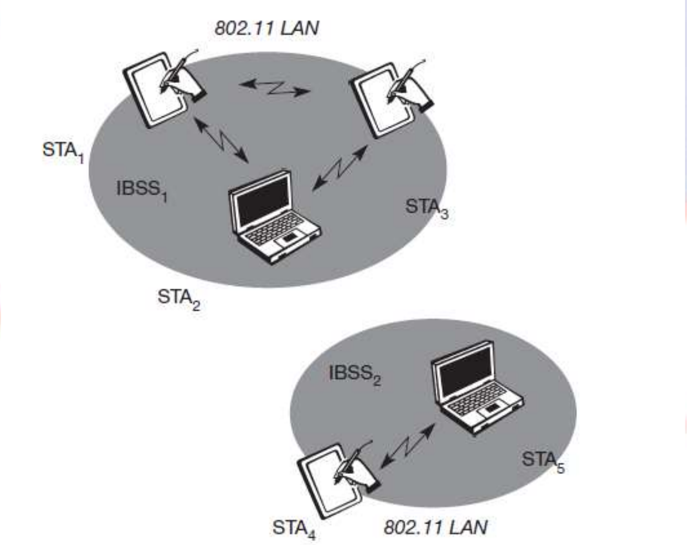


- Figure 1 shows the components of an infrastructure and a wireless part as specified for IEEE 802.11. Several nodes, called stations (STAi), are connected to access points (AP).

- Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.
- The stations and the AP which are within the same radio coverage form a basic service set (BSSi). The example shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system. A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area.
- This network is now called an extended service set (ESS) and has its own identifier, the ESSID. The ESSID is the 'name' of a network and is used to separate different networks. Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN.
- The distribution system connects the wireless networks via the APs with a portal, which forms the interworking unit to other LANs.
- The architecture of the distribution system is not specified further in IEEE 802.11. It could consist of bridged IEEE LANs, wireless links, or any other networks.
- However, distribution system services are defined in the standard (although, many products today cannot interoperate and needs the additional standard IEEE 802.11f to specify an inter access point protocol).
- Stations can select an AP and associate with it. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs. APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service.

Ad-hoc based:

- In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) as shown in Figure 2.

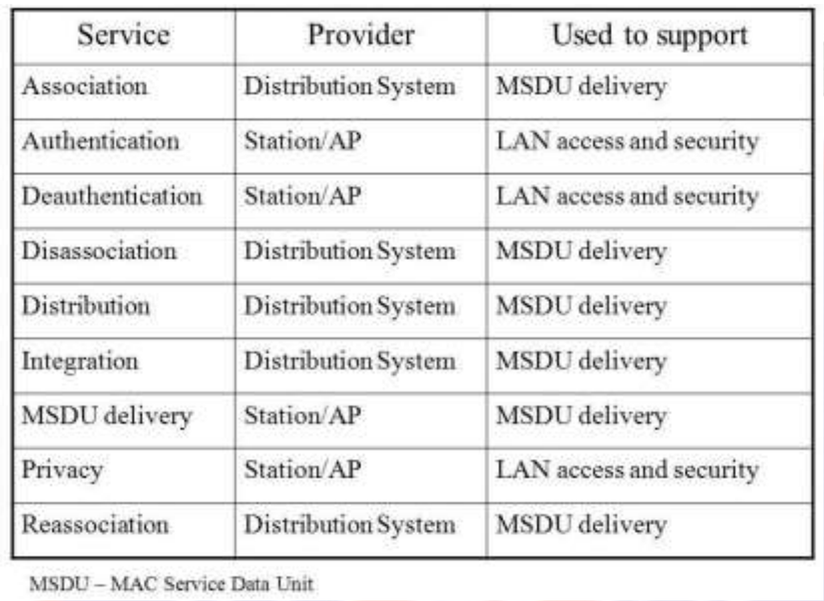


- In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2.
- This means for example that STA3 can communicate directly with STA2 but not with STA5. Several IBSSs can either be formed via the distance between the IBSSs (see Figure) or by using different carrier frequencies (then the IBSSs could overlap physically).
- IEEE 802.11 does not specify any special nodes that support routing, forwarding of data or exchange of topology information as, e.g., HIPERLAN 1 or Bluetooth.

IEEE 802.11 Servicess:

IEEE 802.11 defines nine services that need to be provided by the wireless LAN to provide functionality equivalent to that which is inherent to wired LANs.

IEEE 802.11 Services



Service	Provider	Used to support
Association	Distribution System	MSDU delivery
Authentication	Station/AP	LAN access and security
Deauthentication	Station/AP	LAN access and security
Disassociation	Distribution System	MSDU delivery
Distribution	Distribution System	MSDU delivery
Integration	Distribution System	MSDU delivery
MSDU delivery	Station/AP	MSDU delivery
Privacy	Station/AP	LAN access and security
Reassociation	Distribution System	MSDU delivery

MSDU – MAC Service Data Unit

Association Related Services:

- → The primary purpose of the MAC layer is to transfer MSDUs between MAC entities; this purpose is fulfilled by the distribution service.
- → For that service to function, it requires information about stations within the ESS, which is provided by the association-related services.
- → Before the distribution service can deliver data to or accept data from a station, that station must be associated. Before looking at the concept of association, we need to describe the concept of mobility.
- → The standard defines three transition types based on mobility:
    - o **No transition:** A station of this type is either stationary or moves only within the direct communication range of the communicating stations of a single BSS.
    - o **BSS transition:** This is defined as a station movement from one BSS to another BSS within the same ESS. In this case, delivery of data to the station requires that the addressing capability be able to recognize the new location of the station.
    - o **ESS transition:** This is defined as a station movement from a BSS in one ESS to a BSS within another ESS.
    - o This case is supported only in the sense that the station can move. Maintenance of upper-layer connections supported by 802.11 cannot be guaranteed. In fact, disruption of service is likely to occur.
- → To deliver a message within a DS, the distribution service needs to know where the destination station is located.
- → Specifically, the DS needs to know the identity of the AP to which the message should be delivered in order for that message to reach the destination station.
- → To meet this requirement, a station must maintain an association with the AP within its current BSS. Three services relate to this requirement:
    - o **Association**: Establishes an initial association between a station and an AP Before a station can transmit or receive frames on a wireless LAN, its identity and address

must be known.

- For this purpose, a station must establish an association with an AP within a particular BSS. The AP can then communicate this information to other APs within the ESS to facilitate routing and delivery of addressed frames.
- **Reassociation**: Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another.
- **Disassociation**: A notification from either a station or an AP that an existing association is terminated.
- A station should give this notification before leaving an ESS or shutting down. However, the MAC management facility protects itself against stations that disappear without notification.

Access and Privacy Services:

→ There are two characteristics of a wired LAN that are not inherent in a wireless LAN.

1. In order to transmit over a wired LAN, a station must be physically connected to the LAN. On the other hand, with a wireless LAN, any station within radio range of the other devices on the LAN can transmit. In a sense, there is a form of authentication with a wired LAN, in that it requires some positive and presumably observable action to connect a station to a wired LAN.
2. Similarly, in order to receive a· transmission from a station that is part of a wired LAN, the receiving station must also be attached to the wired LAN. On the other hand, with a wireless LAN, any station within radio range can receive. Thus, a wired LAN provides a degree of privacy, limiting reception of data to stations connected to the LAN.

→ IEEE 802.11 defines three services that provide a wireless LAN with these two features:

Authentication:

→ Used to establish the identity of stations to each other. In a wired LAN, it is generally assumed that access to a physical connection conveys authority to connect to the LAN.

→ This is not a valid assumption for a wireless LAN, in which connectivity is achieved simply by having an attached antenna that is properly tuned.

→ The authentication service is used by stations to establish their identity with stations they wish to communicate with IEEE 802.11 supports several authentication schemes and allows for expansion of the functionality of these schemes.

→ The standard does not mandate any particular authentication scheme, which could range from relatively unsecure handshaking to public key encryption schemes.

→ However, IEEE 802.11 requires mutually acceptable, successful authentication before a station can establish an association with an AP.

Deauthentication:

→ This service is invoked whenever an existing authentication is to be terminated.

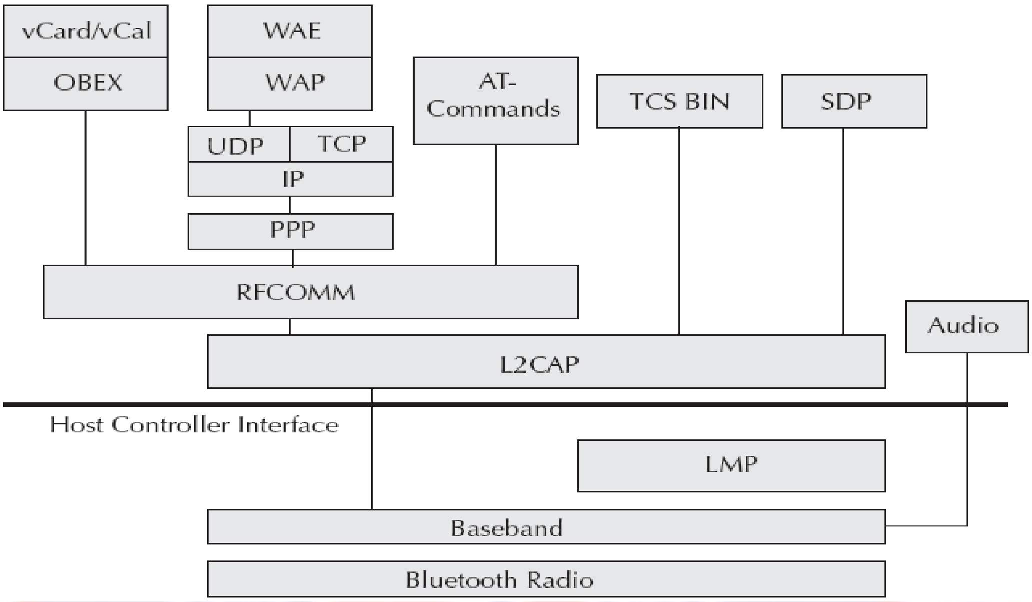
Privacy:

Used to prevent the contents of messages from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

22 Explain Bluetooth Protocol Stack.

Bluetooth Protocol Architecture:

- Bluetooth uses spread spectrum technologies at the Physical Layer while using both direct sequence and frequency hopping spread spectrum technologies.
- It uses connectionless (ACL–Asynchronous Connectionless Link) and connection-oriented (SCO– Synchronous Connection-oriented Link) links.
- Bluetooth protocol stack can be divided into four basic layers according to their functions.



Bluetooth Core Protocols:

- This comprises of baseband, Link Manager Protocol (LMP), Logical Link Control and Adaption Protocol (L2CAP), and Service Discovery Protocol (SDP).
- **Baseband**: It enables the physical RF link between Bluetooth units forming a piconet.
- This layer uses inquiry and paging procedures to synchronize the transmission with different Bluetooth devices. Using SCO and ACL link different packets can be multiplexed over the same.
- **Link Manager Protocol:** When two Bluetooth devices come within each other's range, link managers of either device discover each other.
- **Service Discovery Protocol (SDP):** It enables a Bluetooth device to join a piconet. Using SDP a device inquires what services are available in a piconet and how to access them.
- SDP uses a client-server model where the server has a list of services defined through service records.
- In Bluetooth device there is only one SDP server. If a device provides multiple services, one SDP server acts on behalf of all of them.
- **Logical Link Control and Adaption Protocol (L2CAP):** This layer is responsible for segmentation of large packets and the reassembly of fragmented packets.
- L2CAP is also responsible for multiplexing of Bluetooth packets from different applications.

Cable Replacement Protocol:

- This protocol has only one member which is Radio Frequency Communication (RFCOMM).

- **RFCOMM:** It is a serial line communication protocol and is based on ETSI 07.10 specification.
- The “cable replacement” protocol emulates RS-232 control and data signals over Bluetooth Baseband Protocol.

Telephony Control Protocol:

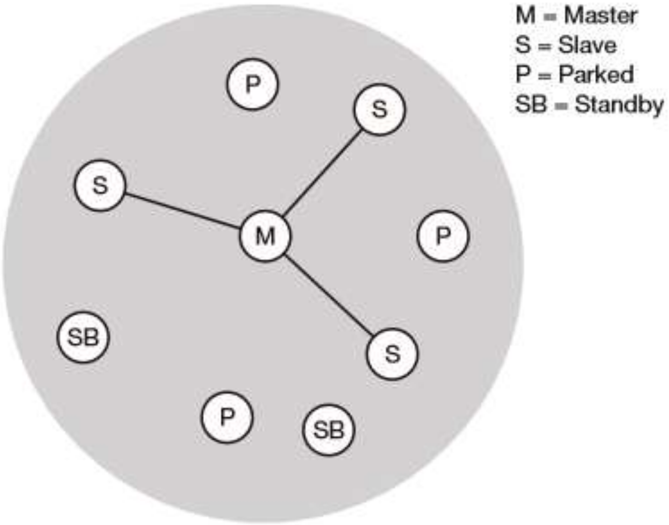
- It comprises of two protocol stacks, viz., Telephony Control Specification Binary (TCS BIN), and the AT-commands.
- **Telephony Control Specification Binary (TCS BIN):** It is a bit-oriented protocol. It defines all the call control signaling protocol for set up of speech and data calls between Bluetooth devices.
- It also defines mobility management procedures for handling groups of Bluetooth TCS devices. It is based on the ITU-T Recommendation Q.931.
- **AT-Commands:** It defines a set of AT-commands by which a mobile phone can be used and controlled as a modem for fax and data transfers.
- AT commands are used from a computer or DTE to control a modem or DC. They are based on ITU-T Recommendation V.250 and GSM 07.07.

Adopted Protocols:

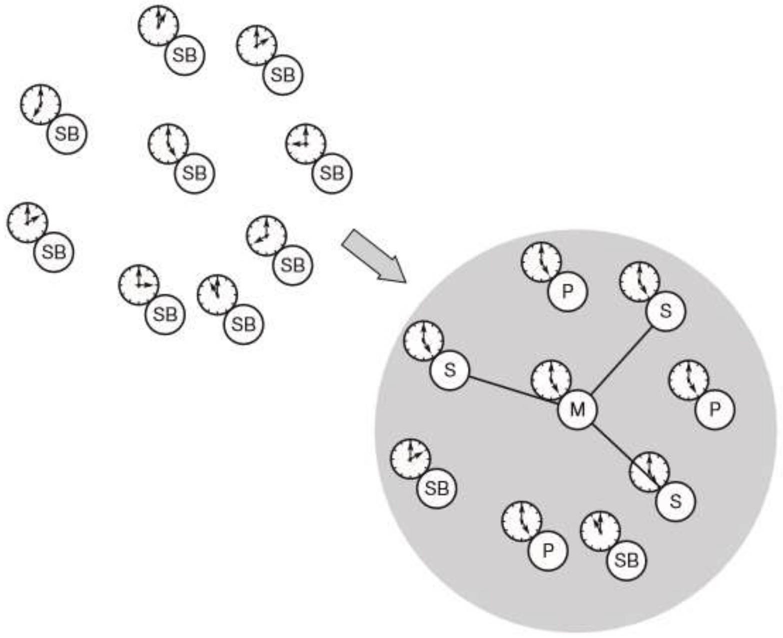
- This has many protocols stacks like Point-to-Point Protocol (PPP), TCP/IP Protocol, OBEX (Object Exchange Protocol), Wireless Application Protocol (WAP), vCard, vCalender, Infrared Mobile Communication (IrMC), etc.
- **PPP Bluetooth:** This offers PPP over RFCOMM to accomplish point-to-point connections. Point-to-Point Protocol is the means of taking IP packets to/from the PPP layer and placing them onto the LAN.
- **TCP/IP:** This protocol is used for communication across the Internet. TCP/IP stacks are used in numerous devices including printers, handheld computers, and mobile handsets.
- TCP/IP/PPP is used for the all Internet bridge usage scenarios.
- **OBEX Protocol:** OBEX is a session protocol developed by the Infrared Data Association (IrDA) to exchange objects.
- OBEX provides the functionality of HTTP in a much lighter fashion. It defines a folder listing object, which can be used to browse the contents of folders on remote devices.
- **Content Formats:** vCard and vCalender specifications define the format of an electronic business card and personal calendar entries developed by the Versit consortium.
- These content formats are used to exchange messages and notes. They are defined in the IrMC specification.
- LMP then engages itself in peer-to-peer message exchange. These messages perform various security functions starting from authentication to encryption.
- It also controls the power modes, connection state, and duty cycles of Bluetooth devices in a piconet.

23 What is piconet and scatternet? Explain. How many maximum numbers of devices can communicate within one piconet?

- **Piconet:** A very important term in the context of Bluetooth is a piconet. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence.



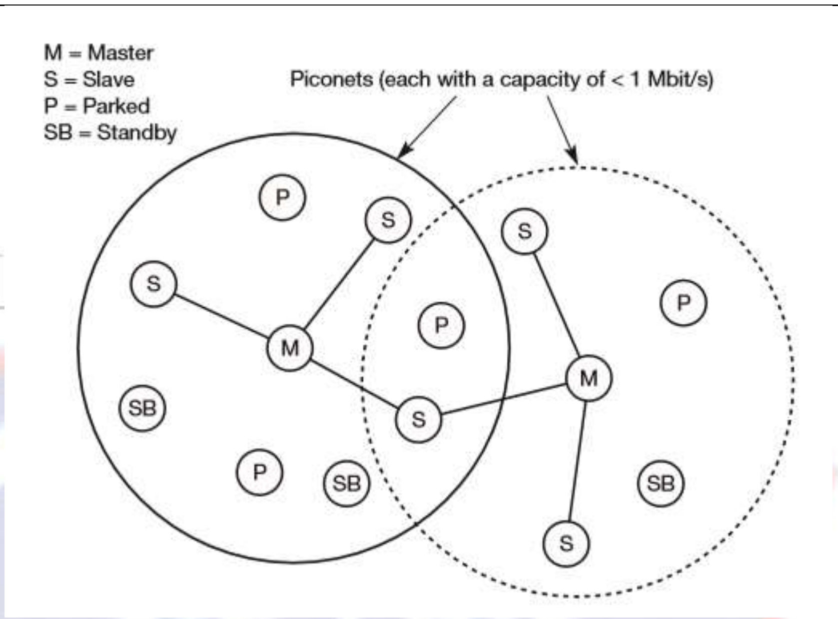
- Figure shows a collection of devices with different roles. One device in the piconet can act as master (M), all other devices connected to the master must act as slaves (S).
- The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Each piconet has a unique hopping pattern. If a device wants to participate it has to synchronize to this.
- Two additional types of devices are shown:
  - parked devices (P) can not actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds.
  - Devices in stand-by (SB) do not participate in the piconet.
- Each piconet has exactly one master and up to seven simultaneous slaves.
- More than 200 devices can be parked.
- The reason for the upper limit of eight active devices, is the 3-bit address used in Bluetooth.
- If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.
- Figure gives an overview of the formation of a piconet.
- As all active devices have to use the same hopping sequence they must be synchronized.
- The first step involves a master sending its clock and device ID.
- All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave.
- There is no distinction between terminals and base stations, any two or more devices can form a piconet.
- The unit establishing the piconet automatically becomes the master, all other devices will be slaves.
- The hopping pattern is determined by the device ID, a 48-bit worldwide unique identifier.
- The phase in the hopping pattern is determined by the master’s clock. After adjusting the internal clock according to the master a device may participate in the piconet.



- All active devices are assigned a 3-bit active member address (AMA).
- All parked devices use an 8-bit parked member address (PMA).
- Devices in stand-by do not need an address.
- All users within one piconet have the same hopping sequence and share the same 1 MHz channel.
- As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate). (Only having one piconet available within the 80 MHz in total is not very efficient.) This led to the idea of forming groups of piconets called scatternet.

Scatternet: Scatternet is a group of Piconet. Only those units that really must exchange data share the same piconet, so that many piconets with overlapping coverage can exist simultaneously.

- In the example, the scatternet consists of two piconets, in which one device participates in two different piconets.
- Both piconets use a different hopping sequence, always determined by the master of the piconet.
- Bluetooth applies FH-CDMA for separation of piconets.
- In an average sense, all piconets can share the total of 80 MHz bandwidth available. Adding more piconets leads to a graceful performance degradation of a single piconet because more and more collisions may occur.
- A collision occurs if two or more piconets use the same carrier frequency at the same time.
- This will probably happen as the hopping sequences are not coordinated.
- If a device wants to participate in more than one piconet, it has to synchronize to the hopping sequence of the piconet it wants to take part in.



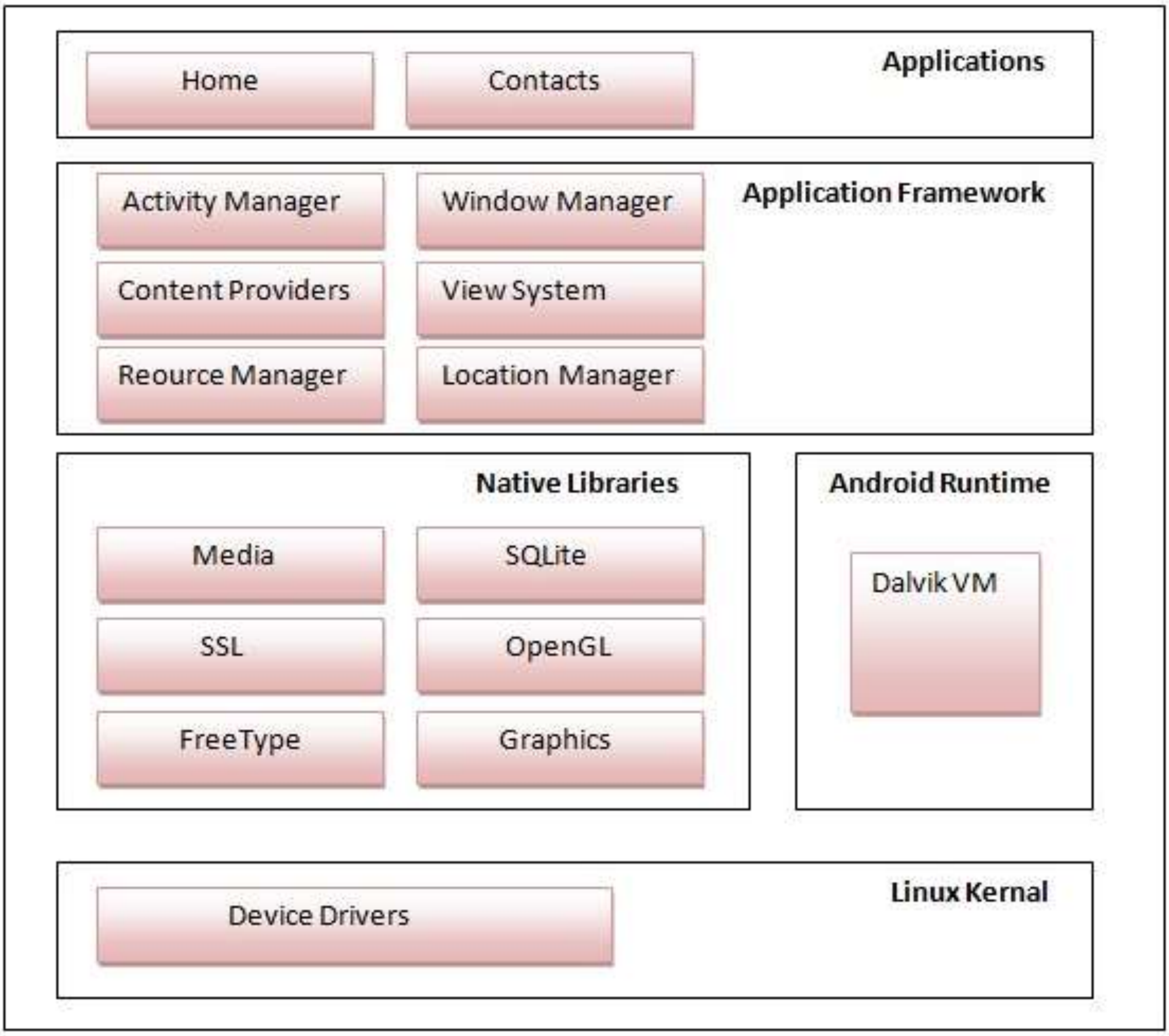
- If a device acts as slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join.
- After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet.
- To enable synchronization, a slave has to know the identity of the master that determines the hopping sequence of a piconet.
- Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time.

The remaining devices in the piconet continue to communicate as usual.

24 Draw Android Architecture. Also explain Android Application Framework in brief

android architecture or **Android software stack** is categorized into five parts:

1. linux kernel
2. native libraries (middleware),
3. Android Runtime
4. Application Framework
5. Applications



1) Linux kernel

It is the heart of android architecture that exists at the root of android architecture. **Linux kernel** is responsible for device drivers, power management, memory management, device management and resource access.

2) Native Libraries

On the top of linux kernel, their are Native libraries such as WebKit, OpenGL, FreeType, SQLite, Media, C runtime library (libc) etc.

The WebKit library is responsible for browser support, SQLite is for database, FreeType for font support, Media for playing and recording audio and video formats.

- Provides access to the application model and is the cornerstone of all Android applications.
- **android.content** − Facilitates content access, publishing and messaging between applications and application components.
- **android.database** − Used to access data published by content providers and includes SQLite database management classes.
- **android.opengl** − A Java interface to the OpenGL ES 3D graphics rendering API.
- **android.os** − Provides applications with access to standard operating system services including messages, system services and inter-process communication.
- **android.text** − Used to render and manipulate text on a device display.
- **android.view** − The fundamental building blocks of application user interfaces.

- **android.widget** − A rich collection of pre-built user interface components such as buttons, labels, list views, layout managers, radio buttons etc.
- **android.webkit** − A set of classes intended to allow web-browsing capabilities to be built into applications.

3) Android Runtime

In android runtime, there are core libraries and DVM (Dalvik Virtual Machine) which is responsible to run android application. DVM is like JVM but it is optimized for mobile devices. It consumes less memory and provides fast performance.

4) Android Framework

On the top of Native libraries and android runtime, there is android framework. Android framework includes **Android API's** such as UI (User Interface), telephony, resources, locations, Content Providers (data) and package managers. It provides a lot of classes and interfaces for android application development.

The Android framework includes the following key services −

- **Activity Manager** − Controls all aspects of the application lifecycle and activity stack.
- **Content Providers** − Allows applications to publish and share data with other applications.
- **Resource Manager** − Provides access to non-code embedded resources such as strings, color settings and user interface layouts.
- **Notifications Manager** − Allows applications to display alerts and notifications to the user.
- **View System** − An extensible set of views used to create application user interfaces.

5) Applications

On the top of android framework, there are applications. All applications such as home, contact, settings, games, browsers are using android framework that uses android runtime and libraries. Android runtime and native libraries are using linux kernal.

25 What are the common layouts available in Android? Elaborate any five layouts.

The basic building block for user interface is a **View** object which is created from the View class and occupies a rectangular area on the screen and is responsible for drawing and event handling. View is the base class for widgets, which are used to create interactive UI components like buttons, text fields, etc.

The **ViewGroup** is a subclass of **View** and provides invisible container that hold other Views or other ViewGroups and define their layout properties.

At third level we have different layouts which are subclasses of ViewGroup class and a typical layout defines the visual structure for an Android user interface and can be created either at run time using **View/ViewGroup**objects or you can declare your layout using simple XML file **main_layout.xml** which is located in the res/layout folder of your project.

Android Layout Types

There are number of Layouts provided by Android which you will use in almost all the Android applications to provide different view, look and feel.

Sr.No	Layout & Description
1	**Linear Layout** LinearLayout is a view group that aligns all children in a single direction, vertically or horizontally.
2	**Relative Layout** RelativeLayout is a view group that displays child views in relative positions.
3	**Table Layout** TableLayout is a view that groups views into rows and columns.
4	**Absolute Layout** AbsoluteLayout enables you to specify the exact location of its children.
5	**Frame Layout** The FrameLayout is a placeholder on screen that you can use to display a single view.
6	**List View** ListView is a view group that displays a list of scrollable items.
7	**Grid View** GridView is a ViewGroup that displays items in a two-dimensional, scrollable grid.

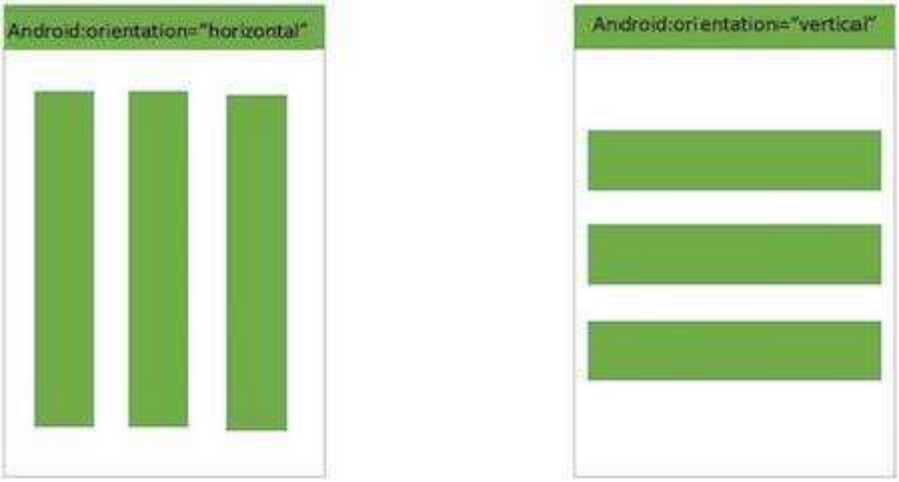
Layout Attributes

Each layout has a set of attributes which define the visual properties of that layout. There are few common attributes among all the layouts and there are other attributes which are specific to that layout. Following are common attributes and will be applied to all the layouts:

Sr.No	Attribute & Description
1	**android:id** This is the ID which uniquely identifies the view.
2	**android:layout_width**

	This is the width of the layout.
3	**android:layout_height** This is the height of the layout
4	**android:layout_marginTop** This is the extra space on the top side of the layout.
5	**android:layout_marginBottom** This is the extra space on the bottom side of the layout.
6	**android:layout_marginLeft** This is the extra space on the left side of the layout.
7	**android:layout_marginRight** This is the extra space on the right side of the layout.
8	**android:layout_gravity** This specifies how child Views are positioned.
9	**android:layout_weight** This specifies how much of the extra space in the layout should be allocated to the View.
10	**android:layout_x** This specifies the x-coordinate of the layout.
11	**android:layout_y** This specifies the y-coordinate of the layout.
12	**android:layout_width** This is the width of the layout.
13	**android:layout_width** This is the width of the layout.
14	**android:paddingLeft** This is the left padding filled for the layout.
15	**android:paddingRight** This is the right padding filled for the layout.
16	**android:paddingTop** This is the top padding filled for the layout.
17	**android:paddingBottom** This is the bottom padding filled for the layout.

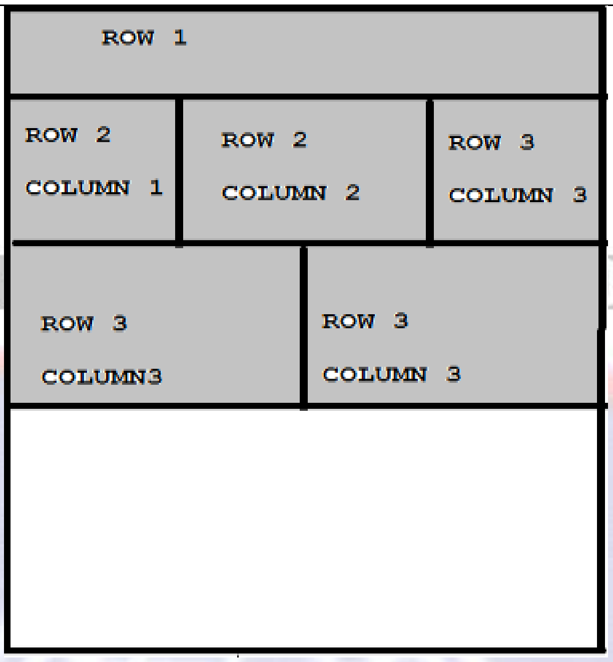
Linear Layout


Android:orientation="horizontal"
Android:orientation="vertical"

A Layout that arranges its children in a single column or a single row.

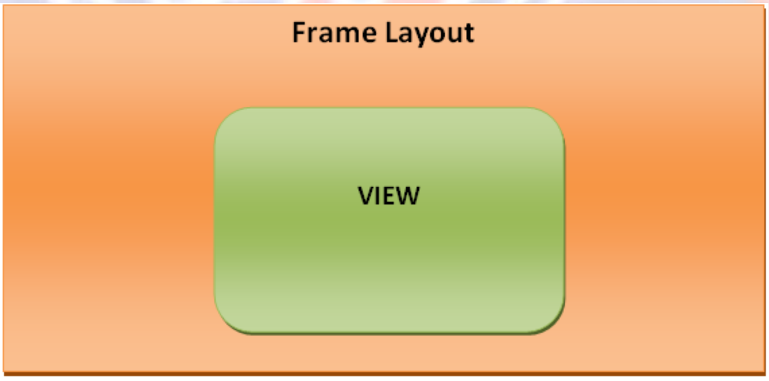
- **Relative Layout**
  - RelativeLayout is a view group that displays child views in relative positions. The position of each view can be specified as relative to sibling elements (such as to the left-of or below another view) or in positions relative to the parent RelativeLayout area (such as aligned to the bottom, left or center).

- **ScrollView**
  - **ScrollView** is a special kind of layout, designed to hold view larger than its actual size. When the Views size goes beyond the ScrollView size, it automatically adds scroll bars and can be scrolled vertically.
  - ScrollView can hold only one direct child. This means that, if you have complex layout with more view controls, you must enclosethem inside anotherstandard layout like LinearLayout, TableLayout or RelativeLayout.
- **Table Layout**
  - Android TableLayout going to be arranged groups of views into rows and columns. You will use the <TableRow> element to build a row in the table. Each row has zero or more cells; each cell can hold one View object.



- **FrameLayout**

  Frame Layout is designed to block out an area on the screen to display a single item. Generally, FrameLayout should be used to hold a single child view, because it can be difficult to organize child views in a way that's scalable to different screen sizes without the children overlapping each other.


Frame Layout
VIEW