1.1 Personal Communication Services (PCS) :

Definition :

- PCS is a wireless phone service which is similar to a cellular system, providing services such as wireless access and personal mobility via small terminal, allowing communication at any place any time and in any form.
- PCS provides advanced coverage and it delivers services at more personal level. PCS is also called as digital cellular service. PCS is 2G wireless technology.
- PCS has ability to connect to PSTN, WiFi, WiMax etc.
- The main goal of personal communication service / personal communication networks is to provide wireless communication coverage everywhere for different types of communication requirements of PCS users to access the telephone networks.
- PCS is incorporated with mobile and fixed network, to provide an universal access.
- PCS manages their individual call services according to their service by providing unlimited accessibility.

1.1.1 PCS Architecture : I-Scheme : S-22

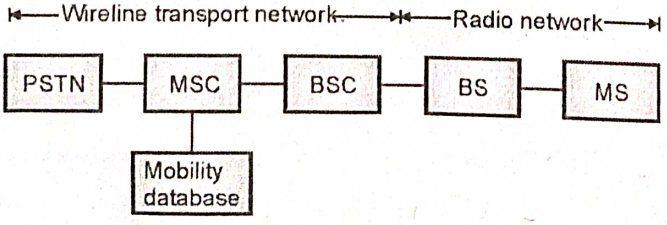
- In the telecommunication industry, a PCS technology has grown very rapidly. The most popular telephony systems are cellular telephony and cordless and low tier PCS telephony.
- The architecture of a PCS system is as shown in Fig. 1.1.1. It consists of two parts such as :
  1. Radio network.
  2. Wireline transport network.

1. Radio network :

- In a PCS network, PCS users carry MSs (Mobile Stations) to communicate with the BSC (base station).
- MS can be a handset, subscriber unit or mobile phone. A cell is the radio coverage of a base station.
- Through the dedicated microwave links or land links, the base station will reach the wireline transport network.
- In GSM network, through base station, BSC (Base Station Controller) controls every cell that is connected to mobile station.
- BSCs are connected to MSC with the help of landlines.

2. Wireline transport network :

- In a PCS network MSC (Mobile Station Controller) acts as a special switch which is connected to the base station.
- The MSC is connected to the PSTN to provide the services between the PCS users and wireline users.
- MSCs are connected to the mobility database to keep the track of location of mobile station.
- The mobility databases are HLR (Home Location Register) and VLR (Visitor Location Register).
- HLR includes the authentication information such as IMSI (International Mobile Subscriber Identity), identification information such as address, name of the subscriber, operator selection, billing information, denial of service to a subscribe etc.
- VLR includes data about the location area of subscriber in case of power off status of the handset or in roaming.



Where,
PSTN - Public switched telephone network
MSC - Mobile switching center
BSC - Base station controller
BSC - Base station
BSC - Mobile station

(G-2618) **Fig. 1.1.1 : PCS architecture**

1.2 Global System for Mobile (GSM) :

Definition :

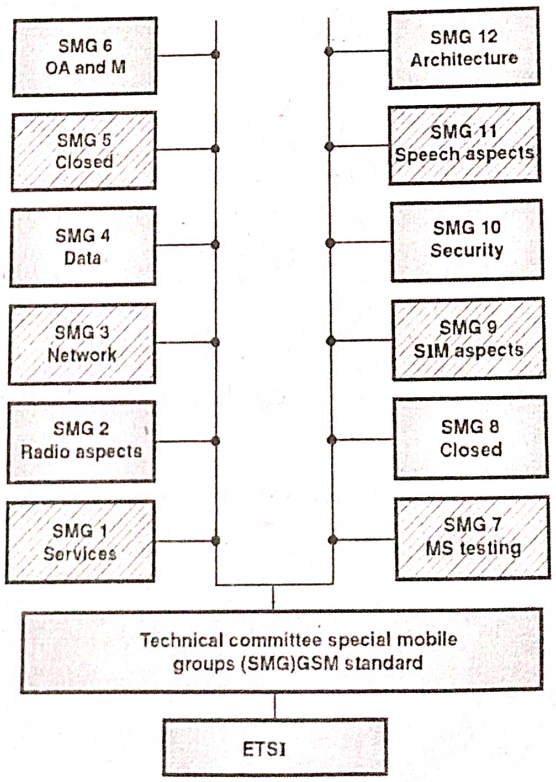
- The Global System for Mobile Communications **(GSM)** is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for second-generation (2G) digital cellular networks used by mobile devices such as mobile phones and tablets.
- Various mobile systems developed over the years are GSM, NA-TDMA, CDMA, PDC etc.
- The only multiple access technique in analog cellular systems is FDMA (frequency division multiple access) but the digital cellular systems can use either TDMA or CDMA for them.
- The long form of **GSM** is global system for mobile communications, it is a digital mobile system and it uses **TDMA** for multiple access.
- We know that in TDMA each user is allowed to use the radio channel only for a fixed duration of time.
- During this time slot, the user is allowed to utilize the entire bandwidth of the channel. Therefore the data is transmitted in the form of bursts.
- A European group called CEPT began to develop the GSM-TDMA system in 1982. The first GSM system was implemented in Germany in 1992. It was named as D_2.
- GSM is a second generation cellular system standard. It was developed in order to solve the fragmentation problems of the first generation cellular systems.
- GSM is the world's first cellular system to specify the digital modulations.

1.2.1 GSM : The European TDMA Digital Cellular Standard :

- Global System for Mobile is world's first cellular system based on digital modulation. It is a second generation system (2G) developed in Europe.
- It was first deployed in Finland in December 1991. By the mid-2010s, it achieved over 90% market share, and started operating in over 193 countries.
- The 2G networks were developed as a replacement for first generation (1G) analog cellular networks.
- The GSM standard originally described a digital, circuit-switched network optimized for full duplex voice telephony.
- A GSM system has maximum 200 full duplex channels per cell.
- Each cell has different uplink and downlink frequency. It uses a combination of FDM, TDM and slotted ALOHA to handle the channel access.

1.2.2 GSM Standardization and Service Aspects :

- The Global System for Mobile (GSM) provides its subscribers a high quality, clear digital wireless phone service along with improved call security and privacy.
- This 2G cellular system uses digital modulation and network level architecture and services. The commercial services of GSM started in mid-1991.
- The Special Mobile Group (SMG) looks after the GSM standardization under ETSI (European Telecommunication standards institute).
- The technical subcommittee's of the special mobile group (SMG) makes all the updates or revisions in this standard.
- Fig. 1.2.1 shows the GSM standardization in ETSI.



(G-1891) Fig. 1.2.1 : GSM standardization in ETSI

- GSM was widely accepted in a number of non-European countries as well such as Asia, South America and Australia, because of its advantages.
- GSM has been designed to handle both voice and data traffic. The voice waveform is digitally encoded before transmission.
- Over the years the GSM standard is enhanced to support more and more services and capabilities such as HSCSD (high speed circuit switched data, EDGE, GPRS etc.
- The frequency bands used for the GSM transmission are 900 MHz, 1800 MHz and 1900 MHz.

1.2.3 Features of GSM :

S-15, W-15, S-16, W-17, S-18, W-18

MSBTE Questions

Q. 1 State any four features of GSM.

(S-15, W-15, S-16, W-17, S-18, 4 Marks)

Q. 2 List the features and services of GSM.

(W-18, 4 Marks)

Some of the important features of GSM are as follows :

1. GSM can support more subscribers in the given spectrum.
2. The short messaging service (SMS) is provided by the GSM standard, that allows its subscribers to transmit and receive character text messages.
3. GSM has a subscriber identity module (SIM), which is a memory device that stores all the important information like subscriber's identification number.
4. Each subscriber is allotted a four digit personal ID number, the activates service from any GSM phone. The SIMs are smart cards or plug-in modules. Each subscriber needs to insert his SIMs into a mobile phone, to receive GSM calls to the number irrespective of the location.
5. The GSM system provides the on-the-air privacy by encrypting the digital bit stream sent by the GSM transmitter.
6. The same GSM phone can be used in different networks.
7. The data transmission and reception rate supported across GSM networks is 9600 bps.
8. GSM also supports FAX transmission and reception at 9.6 kbps.
9. The size of GSM handsets is much smaller.
10. GSM supports the facilities like call forwarding, call on hold, conferencing, Calling Number Identification Presentation (CLIP) and international roaming.
11. GSM is compatible with ISDN for supplementary services.

- Following are the two most important GSM features :
  1. Subscriber Identity Module (SIM).
  2. On air privacy.

1. Subscriber Identity Module (SIM) :

- The SIM card of a GSM phone is nothing but a memory device that stores some very important information like, identification number of the subscriber, the type of network and the countries in which the services can be provided to the subscriber.
- In addition it also stores the unique privacy key for the subscriber for decrypting the encrypted received messages and other important information.
- A SIM is required to activate service for any GSM phone.
- Without a SIM all GSM mobile phone cannot operate.

2. On air privacy :

- On-air privacy is the second important feature of GSM. On-air privacy indicates that the GSM system ensures some kind of privacy of the transmitted signal.
- The analog FM cellular system calls can be easily monitored because no on air privacy is provided.
- However the GSM transmitters use encryption to encode the signals before transmitting them which makes them a lot safer and hard to monitor.

1.2.4 GSM Services : S-16, W-16, S-17, W-18, S-19

MSBTE Questions

Q. 1 Describe user services provided in GSM.

(S-16, W-16, S-17, S-19, 4 Marks)

Q. 2 List the features and services of GSM.

(W-18, 4 Marks)

- **GSM services** are of following two types and they are as per the ISDN guidelines :
  1. Teleservices.
  2. Data services.

- **Teleservices** are the services corresponding to the standard mobile telephony and the traffic originated from either teleservices or data services.
- **Data services** are the GSM services corresponding to the communication between computers and packet switched traffic.

User services :

- The user services are of the following three categories :
  1. Telephone services.
  2. Bearer services or data services.
  3. Supplementary ISDN services.

1. Telephone services :

The following services are called as telephone services :

1. Emergency calling.
2. FAX
3. Videotext.
4. Teletext.

2. Bearer or data services :

These services correspond to the transfer of data between computers and packet switched traffic as mentioned earlier.

3. Supplementary ISDN services :

- The following services, that are digital in nature are known as supplementary ISDN services :
  1. Call diversion.
  2. Closed user group.
  3. Caller identification
  4. SMS (upto 160 words)
- The first generation analog mobile networks cannot provide all these services. SMS (short message services) is an example of supplementary services.

Service model :

- Fig. 1.2.2 shows the reference model for GSM services.
- As shown in Fig. 1.2.2, a **Mobile Station (MS)** is connected to the **GSM-PLMN** (Public Land Mobile Network) via the Um interface. GSM-PLMN is the infrastructure required for the GSM.
- The **PLMN** is connected to the transit networks such as **PSTN** (Public Switched Telephone Network) or **ISDN** (Integrated Services Digital Network).
- An additional network called source / destination network may be connected before connecting another **terminal TE.**

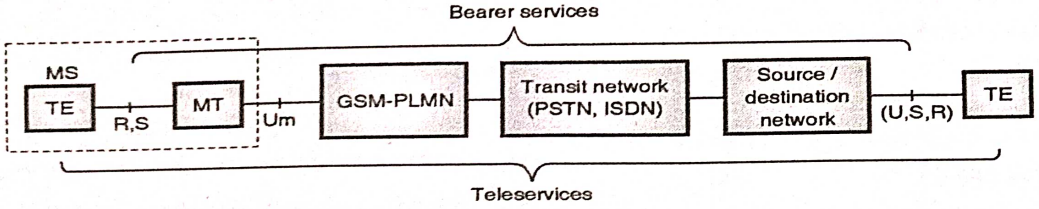
Bearer services :

- Bearer services are basically the **data services** which correspond to the communication between a computer and packet switched traffic.
- As shown in Fig. 1.2.2, **bearer services** are defined as all those services that enable the transmission of data between **interfaces and networks** (From S to S as shown).
- In the classical GSM model, the bearer services are **connection oriented** and use circuit or packet switching.

Mobile Terminal (MT) :

- Within the mobile station (MS), the job of the mobile terminal (MT) is to perform all the network specific tasks such as coding, TDMA, FDMA etc.
- In addition, the MT also offers an interface for data transmission (S) to the terminal TE.
- Further interfaces such as (R) may be needed depending on the capabilities of TE.

MS : A Mobile station, MT : Mobile Termination
PLMN : Public Land Mobile Network
TE : Terminal



(G-2454) **Fig. 1.2.2 : Reference model of GSM services**

Teleservices :

- Teleservices correspond to the standard mobile telephony and the traffic originated from either teleservices or data services.
- As shown in Fig. 1.2.2, these services are specified **end to end** i.e. from one terminal (TE) to the other terminal.

1.2.5 Bearer Services :

- In GSM, there are different mechanisms for the data transmission. The **bearer services** permit the data transmission of transparent and non-transparent, synchronous or asynchronous types.
- Bearer services are of two types :

1. Transparent bearer services.
2. Non-transparent bearer services.

1. Transparent bearer services :

- These services use the functions of only the **physical layer** for the data transmission.
- The delay and the throughput of the data transmission is constant if there is no transmission error.
- The transmission quality can be improved only by using the Forward Error Correction (FEC).
- The data rates of 2.4, 4.8 or 9.6 kbps are possible depending on the FEC.
- These services do not try to recover the lost data irrespective of the cause.

2. Non-transparent bearer services :

- These services use the functions of the first three layers of the OSI model i.e. physical, data link layer and network layer.
- These services use protocols in the DLL and network layer to add error correction and flow control.
- Due to this, a special mechanism of **selective reject** gets added to facilitate retransmission of lost or erroneous data.
- This reduces the error rate remarkably. But delay and throughput do not remain constant. They depend on the transmission quality.

Features of bearer services :

- The important features of bearer services are as follows :

1. Full duplex data transmission.
2. Synchronous transmission data rates : 1.2, 2.4, 4.8 and 9.6 kbps.
3. A synchronous transmission data rates : 300 to 9600 kbps.

1.2.6 Teleservices :

- Basically the standard mobile telephony and the mobile originated or base originated traffic comes under the teleservices.
- The teleservices are as follows :

1. Digital telephony.
2. Emergency number.
3. SMS.
4. EMS.
5. MMS.
6. Group 3 FAX.

1. Digital telephony :

- The main service of GSM is to provide a high quality digital voice transmission, with a minimum bandwidth of 3.1 kHz.
- Special codecs (combination of coder and decoder) are used for transmission of voice digitally.

2. Emergency number :

- With this GSM service the same emergency number can be used throughout a country. This is a mandatory but free service with the highest connection priority.
- If this number is dialled, then the call with the nearest emergency center is set up automatically.

3. Short Message Service (SMS) :

- With this service the user can send messages upto 160 characters. SMS messages are not transmitted over the standard data channels of GSM.
- Instead they are sent over the unused capacity of signaling channels.
- Hence SMS sending and receiving is possible even when the voice or data is being transmitted.
- SMS can transfer logos, ring tones, horoscopes alongwith the text messages. It is also possible to update the software of a mobile phone via SMS.

4. Enhanced Message Service (EMS) :

- EMS is the successor of SMS which offers a message size of upto 760 characters.

- It is possible to send text, ring tones, small images, animated pictures in a standard way using EMS.
- But EMS service never took off commercially.

5. **Multimedia Message Service (MMS) :**

- With this service, it is possible to transmit large pictures (GIF, JPEG) and short video clips.
- MSS is integral part of mobile phones with an inbuilt camera.

6. **Group 3 FAX :**

- This is one more non-voice teleservice in which fax data is transmitted as digital data over the network of analog telephone lines.
- The fax data and signaling information is sent over the transparent bearer service.

1.2.7 Supplementary Services :

- The supplementary services provide various enhancements for the standard telephony services.
- Some of the typical supplementary services are as follows :

1. **Conference Call :** This service allows a mobile subscriber to start a conference call i.e. a simultaneous conversation takes place between three or more mobile subscribers.
2. **Call Waiting :** During a conversation this service informs a mobile subscriber about an incoming call. The user can answer, reject, or ignore the incoming call while conversation.
3. **Call Hold :** This service allows a user to put an incoming call on hold and after a while call can be resumed.
4. **Call Forwarding :** To divert calls from the original recipient to another number call forwarding service is used. The user himself can set up this service on his/her mobile.
5. **Call Barring :** To restrict some type of calls such as outgoing calls like ISD or incoming calls from unwanted numbers call barring service is useful.
6. **Caller Identification :** On your mobile screen, this service displays the telephone number of the person who is calling. It displays telephone number of a person to whom you are connected.
7. **Suggestion of Charge :** This service informs the user about the cost of the services used by them.
8. **Closed User Groups :** This service is intended for the group of subscribers who want to call only each other in the group.

1.3 GSM System Architecture :

S-15, W-15, W-16, S-17, W-17, S-18, W-18, S-19

MSBTE Questions

Q. 1 Explain GSM architecture in detail with neat sketch.

(S-15, W-15, 6 Marks, S-17, S-18, W-18, S-19, 8 Marks)

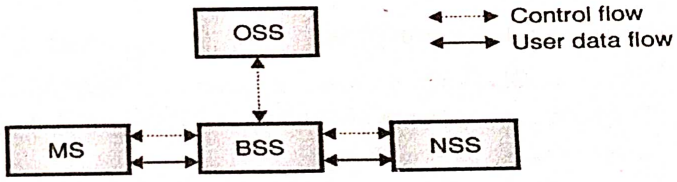
Q. 2 With neat labelled diagram describe GSM architecture. List subsystems involved in it.

(W-16, 6 Marks, W-17, 8 Marks)

Block diagram :

- Fig. 1.3.1 shows the architecture of a GSM system. It shows that the GSM system consists of many subsystems such as :

1. Mobile station (MS).
2. Base station subsystem (BSS).
3. The network and switching subsystem (NSS).
4. Operating subsystem (OSS).



(D-895) Fig. 1.3.1 : GSM architecture

Mobile station (MS) :

This equipment is used to support the connections of the external terminals such as a PC or FAX.

Base station subsystem (BSS) :

- The BSS and MS are connected to each other via a radio interface. It is also connected to NSS in the same way.
- GSM operation is based on the open system inter connection (OSI) model.

Network and switching subsystem (NSS) :

- NSS as shown in Fig. 1.3.2 uses an intelligent network (IN). A signalling NSS is one of the main switching function of GSM.
- The primary job of NSS is the management of the communication between GSM users and other communication users.

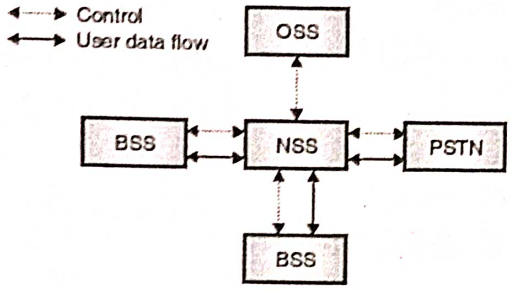
Operation subsystem (OSS) :

- The OSS takes care of the following areas of operation :

1. Network operation and maintenance.
2. Charing and billing.
3. Management of mobile equipment.

Modulation :

- The GSM uses the Gaussian minimum shift keying (GMSK) as its modulation technique.



(D-896) **Fig. 1.3.2 : NSS external environment**

1.3.1 GSM Frequency Spectrum :

GSM specifications with FDMA :

- The multiple access scheme used for GSM is a combination of FDMA and TDMA. If FDMA is used then following are its specifications :

1. Number of channels : 124
2. Frequency slot / channel : 200 kHz.
3. Uplink frequency band : 935-960 MHz.
4. Downlink frequency band : 890-915 MHz.
5. Duplex separation : 45 MHz.

GSM specifications with TDMA :

- The specifications with a TDMA GSM system are :

1. Channel width : 200 kHz.
2. Number of time slots : 8 per frame.
3. Frame duration : 4.615 mS.
4. Time slot duration burst period : 0.577 mS

1.3.2 Detail GSM Architecture :

S-15, W-16, S-17, W-17, S-18, W-18, S-19

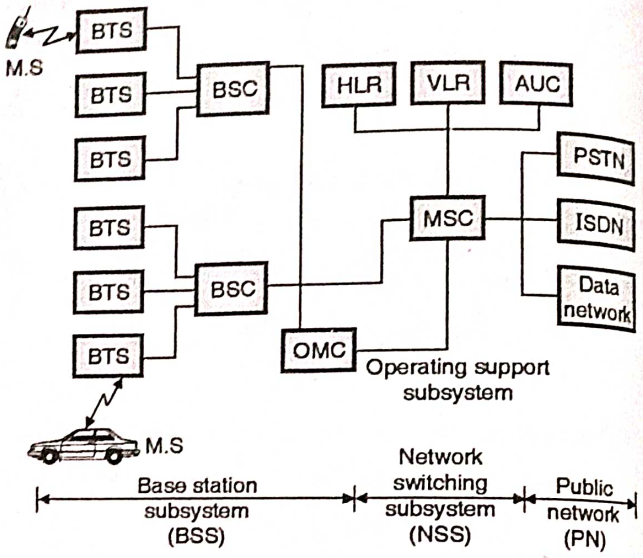
MSBTE Questions

Q. 1 Explain GSM architecture in detail with neat sketch. **(S-15, S-17, S-18, W-18, S-19, 8 Marks)**

Q. 2 With neat labelled diagram describe GSM architecture. List subsystems involved in it. **(W-16, 6 Marks, W-17, 8 Marks)**

Block diagram :

- The detail architecture of a GSM system is shown in Fig. 1.3.3.



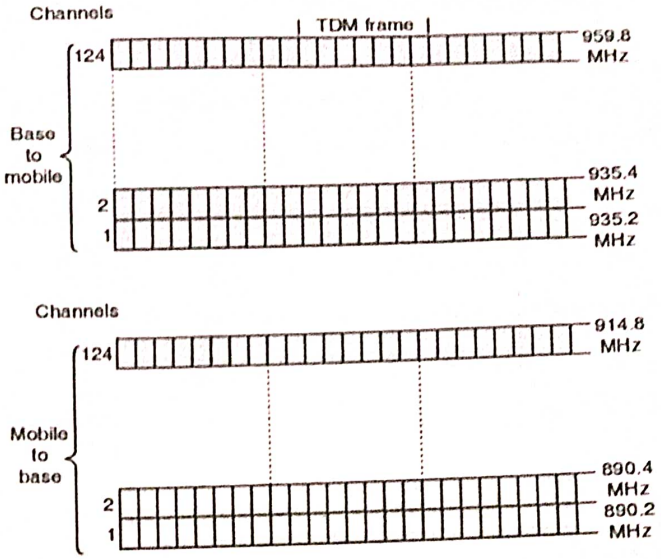
(B-2206) **Fig. 1.3.3 : GSM system architecture**

- The BTS and BSC both are part of the Base Station Subsystem (BSS).
- Each BSS is made of many BSCs (Base Station Controllers) and all BSCs are connected to a single MSC.
- Each BSC has hundreds of BTSs. (Bus Transceiver Stations) connected to it. These BTSs are controlled by the corresponding BSCs.
- The BTSs are connected to BSCs either physically or via microwave links or dedicated leased lines.
- The interface between BTS to BSC is called as **Abis interface.** This interface is expected to carry the voice data (traffic) and maintenance data.
- The BSCs are physically connected to MSC (Mobile Switching Center) via dedicated / leased lines or microwave link. This interface is known as the **A interface.**

- The NSS contains three different databases, called Home Location Register (HLR), Visitor Location Register (VLR) and Authentication Center (AUC).
- The **HLR** is a database containing the subscriber information and location information of each user, who is staying in the same city as MSC.
- Each subscriber is assigned a unique International Mobile Subscriber Identity (IMSI) and this number will identify each user.
- **VLR database** is used to temporarily store the IMSI and customer information for each roaming subscriber.
- **AUC** is the strongly protected database which takes care of authentication and handles the encryption keys for all the subscribers in HLR and VLR.
- The OSS supports one or more Operation Maintenance Centers (OMC). The OMC is used for monitoring and maintaining the performance of each MS, BS, BSC and MSC used in a GSM system.

1.4 GSM Radio Aspects :

- GSM originally used two 25 MHz cellular bands but now it is used in many bands. The two 25 MHz bands are as follows :
- The 890-915 MHz band is for the subscriber-to-base transmissions called as the **reverse link or uplink.**
- And the 935-960 MHz band was for base to subscriber transmissions called as the **forward link or downlink.**
- A GSM system has up to a maximum of 200 full–duplex channels per cell.
- Each channel consists of a downlink frequency (935.2 MHz to 959.8 MHz) i.e. from base station to mobile station and an uplink frequency (890.2 MHz to 914.8 MHz) i.e. from mobile station to base station.
- Each frequency band is 200 kHz (0.2 MHz) wide. Both the uplink and downlink frequency bands consist of 124 channels as shown in Fig. 1.4.1.
- As shown in the Fig. 1.4.1, each frequency channel supports eight separate connections using TDM.
- Each TDM slot has a specific structure as shown in Fig. 1.4.1. Each TDM slot consists of 148 bit data frame.
- Each data frame starts and ends with 3 zero bits, for frame delineation purpose. It also contains two 57 bit information fields, each having a control bit that indicates whether the information field is for voice or data.

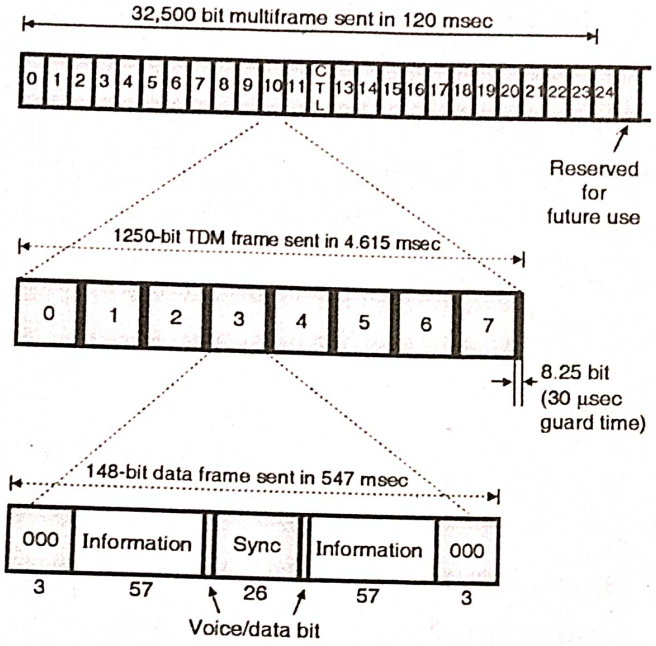


(G-1000) Fig. 1.4.1 : GSM frequency band allocation

- Between the information fields is a 26-bit sync field which is used by the receiver to synchronize to the sender's frame boundaries.
- As shown in the Fig. 1.4.2 eight data frames make up a TDM frame and 26 TDM frames make up a 120 m sec multi-frame, of the 26 TDM frames in a multi-frame, slot 12 is used for control and slot 25 is reserved for future use.
- The broadcast control channel is a continuous stream of output from the base station containing its identity and the channel status.
- All mobile station monitor their signal strength to see when they have moved into a new cell.
- The dedicated control channel is used for location updating, registration and call setup. Each base station maintains a database of mobile stations currently under its jurisdiction and the information needed to maintain this database is sent on the dedicated control channel.
- The GSM has a common control channel which is split up into 3 logical subchannels.

1. **Paging channel :** The base station uses this channel for announcing the incoming calls. Each mobile station checks it continuously to know about the calls it is supposed to reply.

2. **Random access channel :** It uses a slotted ALOHA system and enables a mobile station to request and book a slot on the dedicated control channel. The mobile station can use this slot to set up a call.
3. **Access grant channel :** The slot assigned to an M.S. is announced on this channel.



(G-1001) Fig. 1.4.2 : GSM TDM structure

GSM air interface :

Table 1.4.1 summarizes the GSM air interface specifications.

Table 1.4.1 : GSM air interface specifications

Sr. No.	Parameter	Value
1.	Reverse channel frequency	890 – 915 MHz
2.	Forward channel frequency	935-960 MHz
3.	ARFCN number	0-124 and 975-1023
4.	Frequency spacing	45 MHz
5.	Frame period	4.615 mS.
6.	Users per frame	8
7.	Modulation Data Rate	270.83 kbps
8.	Time slot period	576.9 µS
9.	Modulation	GMSK
10.	Interleaving	40 mS

1.5 GSM Channel Types :

S-15, S-16, S-17, W-18

MSBTE Questions

Q. 1 Explain GSM channel types. **(S-15, S-16, W-18, 4 Marks)**

Q. 2 Draw and explain GSM channels. **(S-17, 6 Marks)**

Types :

- GSM channels are of two types :

1. GSM traffic channels (TCHs).
2. Control channels (CCHs).

- The traffic channels (TCHs) are supposed to carry speech or data signals that are encoded into digital form.
- Their functions and formats on forward as well as reverse links are the same.
- The base station uses the control channels to communicate the signaling and synchronization commands to the mobile station.
- The control channels (CCH) defined for the forward links and those defined for the reverse links are entirely different.
- The traffic channels can be further classified into six different types whereas control channel can be of more than six types.

1.5.1 GSM Traffic Channels (TCHs) :

W-15, S-17, W-17, S-18, S-19

MSBTE Questions

Q. 1 Describe GSM traffic channels with its type. **(W-15, 4 Marks, S-19, 6 Marks)**

Q. 2 Draw and explain GSM channels. **(S-17, 6 Marks)**

Q. 3 Explain Traffic & Control GSM channels alongwith its sub types and characteristics. **(W-17, 4 Marks, S-18, 6 Marks)**

Types of GSM traffic channels :

GSM traffic channel can be of two types :

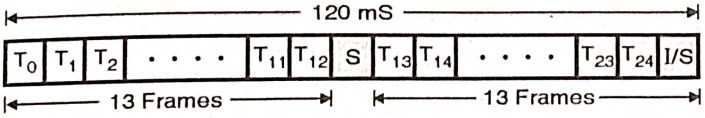
1. Full rate channel and
2. Half rate channel.

Function :

- The traffic channels (TCHs) are supposed to carry speech or data signals that are encoded into digital form.
- Their functions and formats on forward as well as reverse links are the same.
- If used as a **full rate** channel, the user data would occupy one TS (time slot) per frame.
- But if used as a **half rate** channel, the user data would occupy the same TS (time slot) but it is sent in the alternate frames.
- So two half rate channel users share the same time slot but transmitted during the alternate frames.
- Frames of TCH data are broken up after every thirteenth frame and either a slow associated control channel data or idle frames are transmitted.

Multi-frame structure :

- Fig. 1.5.1 shows how the TCH data is transmitted in consecutive frames.



S = Slow associated control channel frame
I = Idle frame

(G-1212) Fig. 1.5.1 : Multi-frame structure

- T_0, T_1 .... T_{24} are the TDMA frames. A group of 26 consecutive TDMA frames is called as a **multi-frame** and it is as shown in Fig. 1.5.1. The multiframe is also called as the **speech multi-frame**.
- Every fourteenth frame is an **"S" frame** i.e. slow associated control channel frame (SACCH) and twenty eight frame is an **idle frame (I).**
- This frame contains idle bits for the full rate TCH and it contains the SACCH data for half rate TCH.

Full Rate TCH :

- The full rate TCH are expected to support the following full rate speech and data channels :

1. Full rate speech channel (TCH / FS)
2. Full rate data channel for 9600 bps (TCH / F 9.6)
3. Full rate data channel for 4800 bps (TCH / F 4.8)
4. Full rate data channel for 2400 bps (TCH / F 2.4)

Half Rate TCH :

- The half rate TCH are expected to support the following half rate speech and data channels :

1. Half rate speech channel (TCH/HS)
2. Half rate data channel for 4800 bps (TCH / H 4.8)
3. Half rate data channel for 2400 bps (TCH / H 2.4)

1.5.2 GSM Control Channels (CCH) :

W-15, W-16

MSBTE Questions

Q. 1 State various GSM control channels in brief. **(W-15, 4 Marks)**

Q. 2 List broadcast channels of GSM and describe two of them. **(W-16, 4 Marks)**

Types of GSM control channels :

- There are three main control channels in GSM :

1. Broadcast channel (BCH)
2. Common control channel (CCCH)
3. Dedicated control channel (DCCH)

- GSM specification defines 34 standard broadcast channels.
- There are three DCCH in GSM and they are bidirectional and have same format and function on both forward and reverse links.
- DCCH can exist in any time slot and on any ARFCN except TS0 of BCH ARFCN.
- DCCH is of three types Stand-alone Dedicated Control Channel (SDCCH) used for providing signaling services required by users, Slow-Associated control Channel (FACCH) and Slow-Associated Control Channel (SACCH) used for supervisory data transmission between mobile station and the base station during a call.

Broadcast channel (BCH) :

- BCH consists of three different channels :

1. Broadcast Control Channel (BCCH) which is forward link channel used for transmission of information which controls the network, a particular cell and the neighboring cells.

2. Frequency Correction Channel (FCCH) allows mobile station to synchronize its local oscillator's frequency with the exact of the base station.

3. **Synchronization Channel (SCH)** is used for identification of the base transceiver station and frame synchronization, in whose service area the mobile station is situated.

Common Control Channel (CCCH) :

- CCCH consists of three different channels : 1. Paging Channel (PCH) which is forward link channel 2. Random Access Channel (RACH) which is reverse link channel and 3. Access Grant Channel (AGCH) which is forward link channel.
- CCCH are most commonly used control channels and are used to page specific subscribers, assign signaling channels to specific users and receive mobile requests for service.

Paging Channel (PCH) :

- The PCH provides paging signals from the base station to all mobiles in the cell, and notifies a specific mobile of an incoming call which originates from the PSTN.
- The PCH transmits the IMSI of the target subscriber along with a request for acknowledgement from the mobile unit on the RACH.
- PCH may be used to provide cell broadcast ASII text message to all subscribers as part of the SMS feature of GSM.

Random Access Channel (RACH) :

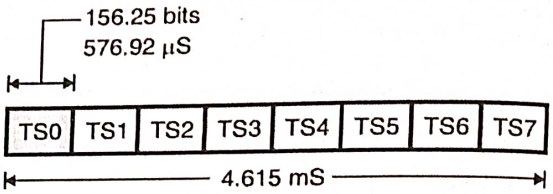
- It is a reverse link channel used by subscriber to acknowledge the page from PCH and also used by mobiles to originate a call.
- The RACH uses ALOHA access scheme. At the BTS every frame will accept RACH transmission from mobiles during TS0.
- In establishing service the GSM base station must respond to the RACH transmission by allocating a channel and assigning a stand-alone dedicated control channel for signaling during a call.
- This connection is confirmed by the base station over AGCH.

Access Grant Channel (AGCH) :

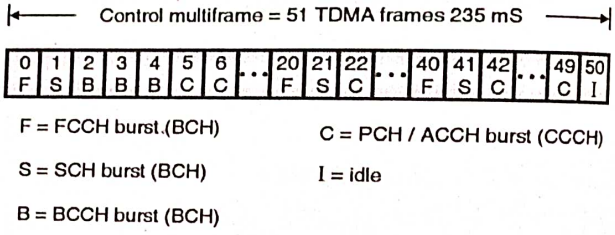
- The AGCH is used by the base station to provide forward link communication to the mobile and carries data which instructs the mobile to operate in a particular physical channel with particular dedicated control channel.
- It is the final CCCH message sent by the base station before a subscriber is moved off the control channel. It is used by the base station to respond to a RACH sent by a mobile station in a previous CCCH frame.

Function :

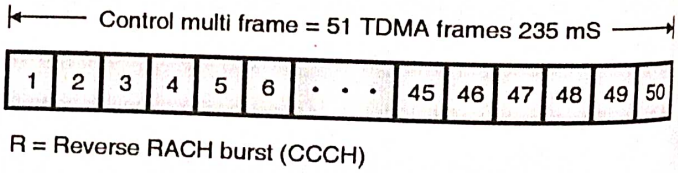
- The control channels (CCH) defined for the forward links and those defined for the reverse links are entirely different.
- Each control channel is made of many logical channels. They are separated in time in order to provide the necessary GSM control functions.
- The BCH and CCCH forward control channels can occupy only the TS0 channel as shown in Fig. 1.5.2.
- These channels are transmitted only during certain frames during a repetitive sequence of 51 frames.
- Such a sequence is called as **control channel multiframe**.
- The TS1 to TS7 channels in Fig. 1.5.2(a) can carry the regular TCH traffic.



(G-1213) Fig. 1.5.2



(G-1214(a)) Fig. 1.5.2(a) : The control channel multiframe forward link for TS0



(G-1214(b)) Fig. 1.5.2(b) : The control channel multiframe reverse link for TS0

- The control channel multiframe is as shown in Fig. 1.5.2(b). The first thirty-four ARFCNs (Absolute Radio Frequency Channel Numbers) have been defined by the GSM as the standard broadcast channels.

- The 51st frame of each broadcast channel does not contain any BCH/CCCH forward channel data. Therefore it is considered as an idle frame.
- But the reverse channel CCCH can use the TS0 of any frame to receive subscribers transmissions. Even the idle frames can be used for this purpose.
- However DCCH data can be sent during any time slot and any frame, of all the frames that are dedicated only to contain DCCH transmissions.

1.6 Frame Structure of GSM System :

S-15, W-15, S-16, W-16, S-17, W-17, S-18, S-19

MSBTE Questions

Q. 1 Draw and explain frame structure of GSM.
(S-15, W-15, S-16, S-17, W-17, S-18, 4 Marks)

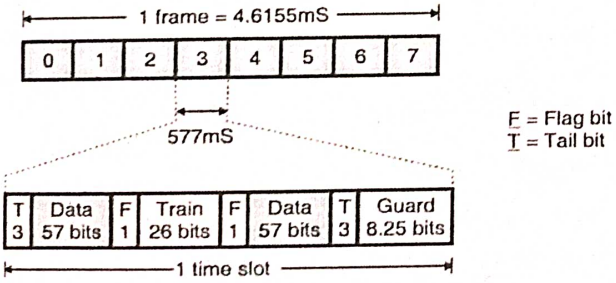
Q. 2 With neat labeled diagram describe GSM frame architecture. **(W-16, S-19, 4 Marks)**

- Fig. 1.6.1 shows the frame structure of the GSM system.
- As there are eight such time slots in one frame, the time duration of each frame is given by,

$$1 \text{ frame} = 8 \times 577\ \mu S = 4.6155\ mS$$

Where one time slot corresponds to 577 μsec.

- Fig. 1.6.1 also shows the internal organization of each time slot.
- It consists of flag bits (F), tail bits (T), training interval for equalizer (train bits), data bits and guard time interval.



(G-1215) Fig. 1.6.1 : Frame structure of GSM system

- The 1-bit flag is always at the beginning of each data burst of 57 bits.
- The three tail-bits are all logical zeros are used in the convolutional decoding of the channel encoded data bits.
- The data bit bursts are of 57 bit length and there are two such data bit bursts per time slot as shown in Fig. 1.6.1.
- The training sequence of 26 bits at the center of each time slot is used for channel equalization.
- The guard time of 8.25 bits has been included at the end of each time slot in order to avoid overlapping of the data bits sent over the adjacent time slots.
- Thus the number of bits corresponding to each time slot can be calculated as follows :

$(57 \times 2 + 8.25 + 3 \times 2 + 2) = 156.25$ bits.

- Out of these 156.25 bits, the number of data bits is only 114. Excluding the two fag bits, the remaining bits will be 40.25 which do not carry any information are called as the overhead bits.
- Hence the frame efficiency of GSM is given by,

$$\eta = \left(1 - \frac{40.25}{156.25}\right) \times 100 = 74.24\ \%$$

1.7 Signal Processing in GSM :

S-15, W-15, S-16, W-16, S-17, W-17, S-18, W-18, S-19

MSBTE Questions

Q. 1 How a signal is processed in GSM ?
(S-15, S-16, S-17, 4 Marks)

Q. 2 Explain TCH channel coding in GSM signal processing. **(W-15, 4 Marks)**

Q. 3 Describe signal processing in GSM in detail.
(W-16, W-18, 8 Marks)

Q. 4 Draw a block diagram and explain voice signal processing in GSM. **(W-17, S-18, 4 Marks)**

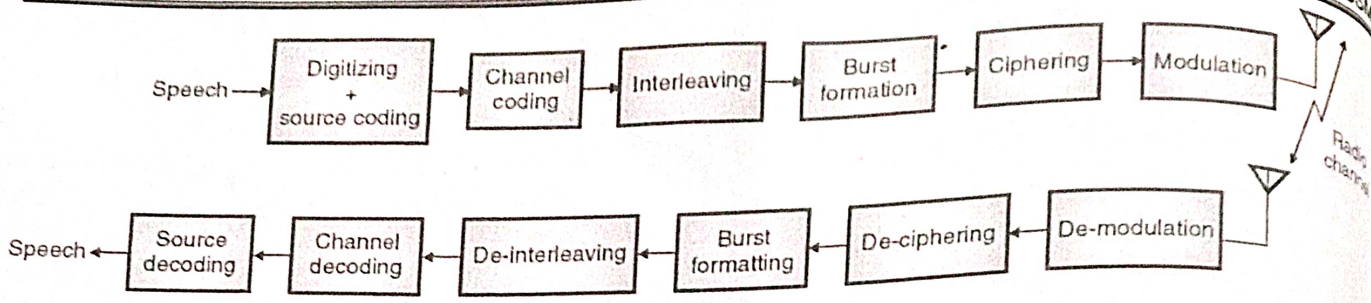
Q. 5 Explain signal processing in GSM with block diagram. **(S-19, 4 Marks)**

Block diagram :

Refer Fig. 1.7.1 which shows the block diagram, to understand all GSM operations from transmitter to receiver.

1. Speech coding :

- The working of speech coding in GSM is based on the principle of Residually Excided Linear Predictive Coder (RELP) which uses a Long Term Predictor (LTP).



(G-1216) **Fig. 1.7.1 : GSM signal processing**

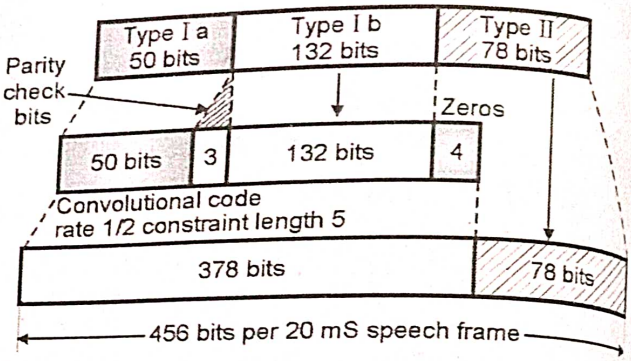
- The operation of GSM speech coder makes use of a very interesting fact that, each person speaks for about 40% of the total conversation time in a normal conversation,
- Therefore GSM works in the discontinuous transmission mode (DTX) by using a voice activity detector (VAD).
- Due to DTX mode the battery life increases and reduces the radio interference.
- However there is a disadvantage of the DSX mode of operation, called as switched muting.
- The annoying effect of switched muting due to DTX, is reduced by using a comfort noise subsystem (CNS) at the receiving end.
- The length of each speech block is 20 mS. The speech coder provides 260 bits for each speech block.
- Thus 260 bits correspond to 20 mS. Therefore number of bits per second will be equal to :

  $260/(20 \times 10 - 3) = 13{,}000$ bits or 13 kbps.

2. TCH / FS, SACCH and FACCH channel coding :

- The output bits of a speech coder, are arranged into groups, so as to facilitate the error protection.
- Such a grouping is performed on the basis of significance of these bits in contributing to speech quality.
- Out of the total 260 bits in a frame, the most significant 50 bits grouped together to form a group.
- These bits are called as Ia bits. Then three parity check bits are added to them. This makes a group of 53 bits.
- The parity check bits are used to detect those errors that cannot be corrected at the receiver.
- These first 53 bits and the next 132 bits are taken and four zeros are appended to them as shown in Fig. 1.7.2.
- This makes a data block of 189 bits which is then encoded into a sequence of 378 bit for error protection.

  No error protection is provided to the remaining less significant 78 bit from the 260 bits.



(G-1217) **Fig. 1.7.2 : Error protection for speech signals in GSM**

- These 78 bits are concatenated to the existing sequence as shown in Fig. 1.7.2.
- Thus the total number of bits per block will be (378 + 78 = 456) a 20 mS frame.

3. Channel coding for data channels :

The channel coding used for GSM full rate data channels (TCH / F 9.6) is meant to handle 60 bits of user data at 5 mS intervals.

4. Channel coding for control channels :

The length of GSM control channel messages is 184 bits. They are encoded using the **fire codes**.

5. Interleaving :

- The bits travelling from transmitter to receiver sometimes have to face a problem called fading.
- In order to avoid or minimize the effect of fading on all the 456 bits in a block simultaneously, the speech frame or control frame are divided in eight equal length sub-blocks each containing 57 bits.

- These eight sub blocks are placed one each, over eight consecutive TCH time slots.
- This arrangement ensures that, even if a fw bits are lost due to fading, it is possible to use the remaining bits to reconstruct the speech, without a significant loss of information.

6. Ciphering :

- Ciphering is a process of modifying the contents of the eight inter-leaved blocks with the help of some encryption technique.
- The security can be improved further by modifying the encryption algorithm for every call.
- GSM uses two different types of ciphering algorithms called A3 and A5. Out of which, A3 prevents the unauthorized network access and A5 ensures the privacy of radio transmission.

7. Modulation :

- The modulation scheme used by GSM is the 0.3 GMSK. Here the number 0.3 indicates the 3 dB bandwidth of the Gaussian pulse shaping filter in relation with the bit rate.

8. Equalization :

- Equalization process is carried out at the receiver and the type of equalizer for GSM is not specified.
- The selection of equalizer is manufacturer's choice.

9. Demodulation :

- The receiver carries out the demodulation of the received signal with the help of synchronizer.
- The processes such as deciphering, de-interleaving, channel decoding and speech decoding are carried out after demodulation.

1.7.1 Short Message Mobile Terminated (SMMT) :

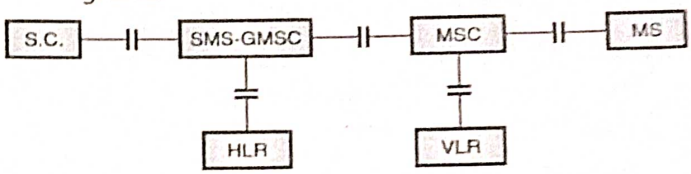
- The short message service SMS is currently supported on the following mobile networks :

1. GSM 2. GPRS 3. CDMA

- SMS are of the following two types :

1. SMMT (Short Message Mobile Terminated point to point)
2. SMMO (Short Message Mobile Originated point to point)

- **SMMT** is an incoming short message from the network side and it is terminated in the MS (Mobile Station).
- **SMMO** is an outgoing message originated in the mobile station (MS) that is forwarded to the network for its delivery.
- The path followed by an SMMT message is from SC (Service Center) to the MS via HLR (Home Location Register) and the GMSC (Gateway MSC) function of the home MSC.
- A SMMT message is sent from SC to MS as shown in Fig. 1.7.3.



(G-1570) **Fig. 1.7.3 : SMMT procedure**

1.7.2 Authentication in GSM :

Definition :

- The authentication of a user is the process of ensuring and verifying that the user is really the person who claims he is.
- Authentication is essential to ensure that the communication over the wireless radio medium is secured.
- The authentication process involves two functional entities :
  1. The SIM card in mobile phone.
  2. The Authentication Center (AUC).
- A specially designed algorithm A3 is used for carrying out authentication.
- After carrying out the authentication, a key is generated for encryption, with the help of another specially designed algorithm A8.

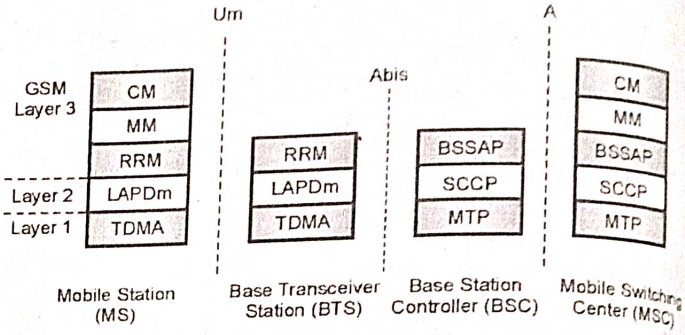
Authentication Algorithm A3 :

- During the authentication process the Mobile Switching Center (MSC) or MTSO challenges the Mobile Station (MS) with a random number (RAND).
- The SIM card makes use of this RAND received from the MSC alongwith a secret key k_i stored within the SIM as input. Both RAND and k_i are basically 128 bit digital numbers.

- The A3 algorithm works on the RAND and k_i inputs to produce a 32 bit output called as the signature response (SRES).
- The SRES is then sent back to MSC from MS as the answer to the challenge. Using the same algorithm the AUC also generates a SRES.
- Then the SRES generated by MS (SIM) and AUC are compared. If they are identical then it is an indication that MS is an authentic user. That means it is concluded that SIM card is genuine.

1.8 GSM Protocol Model / Network Signalling : I-Scheme : S-22

- Fig. 1.8.1 shows the Signaling Protocol Structure in GSM.
- In the signaling protocol structure in GSM there are three general layers depending on the interface.
- **Layer 1** is the physical layer. It makes use of the channel structures over the interface.
- **Layer 2** is data link layer. Across the U_m interface (Refer Fig. 1.8.1), the DLL is actually a modified version of the **Link Access Protocol D(LAPD)** used in ISDN.
- It is called as the LAPDm.
- Across the **A** interface, as shown in Fig. 1.8.1 the message transfer part layer 2 of signal system number 7 (SS7) has been used.
- The air interface of GSM consists of TDMA time slots and FDMA frequency bands.
- LAPDm protocol is used over the air interface between the base station trans-receiver and the mobile device.
- Some additional control information, apart from the actual data is required to be used for transmitting the information to a desired destination.
- It is called as the **signaling message.**
- The signaling channels are time division multiplexed on an aggregate of the TDM slots.
- Layer-3 of the GSM signaling protocol is divided into the three following sub-layers :
  1. Mobility Management (MM).
  2. Radio Resource Management (RRM) and
  3. Connection Management (CM) for calls routing.
- The layer-3 protocol is used for different purposes o mobility, communication of network resources, cod format and call related management message between different network entities.
- The radio recourse management (RRM) between th Mobile Station and the Base Station Subsystem (BSS) can be implemented.
- Mobility Management and Connection Management i the communication between the Mobile Station an MSC (Mobile Switching Centre).



(G-1892) Fig. 1.8.1 : Signaling protocol structure in GSM

- The A interface uses an SS7 protocol called Signal Correction Control Protocol (SCCP) that supports communication between the MSC and BSS and the network messages between the individual subscribers and the MSC.

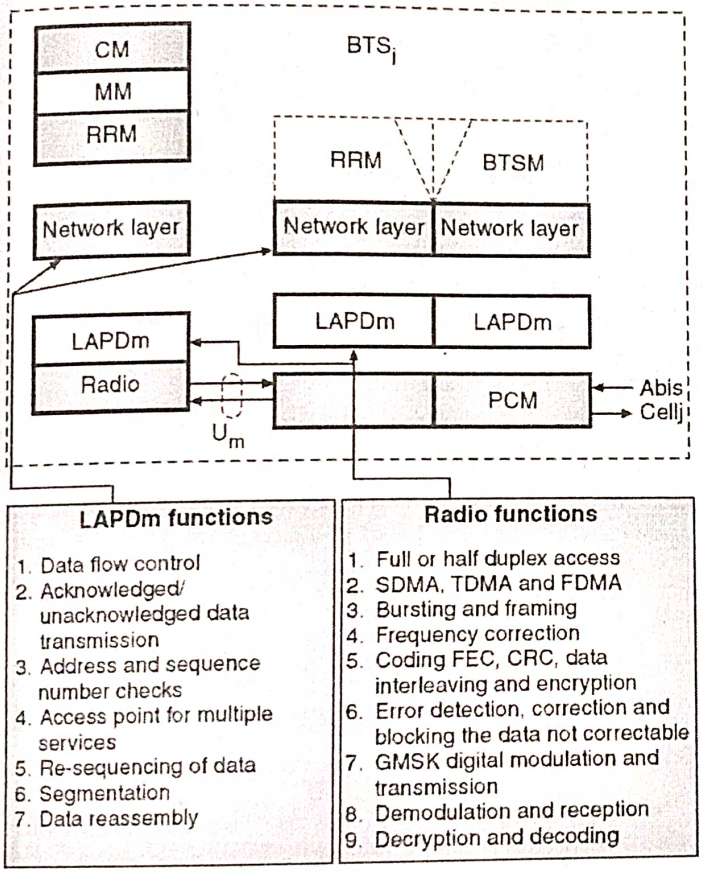
1.8.1 Link Layer LAPDm Protocol (Mobile Station-Base Transceiver Station Signalling Protocols) : I-Scheme : S-22

- Fig. 1.8.2 shows the functions and protocol layers between the MS and BTS.

Radio Interface / Physical Layer :

- Radio (U_m interface) is the physical layer between the Mobile Station (MS) and the Base Transceiver Station (BTS).
- The data link layer is supposed to control the flow of packets sent to and coming from the network layer and provide access to different services.
- LAPDm (Link Access Protocol D-channel modified) is the data link layer protocol, which is located between MS and BTS.
- Refer Fig. 1.8.2 that enlists the functions of LAPDm.

- It does not use any flag for frame delimitation. Instead, the frame delimitation is taken care of by the physical layer that defines the frame boundaries.
- The information carrying field in LAPDm is differentiated field from the fill-in bits (used to fill the transmission frame) with the help of the length indicator.
- A 3-bit Service Access Point Identifier **(SAPI)** used as an address field in LAPDm. It can take eight different values from 0 to 7.
- Out of them, SAPI 0 is used for call control, MM and RRM signaling where as SAPI 3 is used for SMS. All other fields are reserved for future purpose.



(G-1893) Fig. 1.8.2 : Functions and protocol layers between the MS and BTS

Network layer sub layers :

- The network layer has the following three sub layers :
  1. Connection Management (CM)
  2. Mobility Management (MM)
  3. Radio Resource Management (RRM).

1. Connection Management (CM) for calls routing :

- The CM sub layer protocol has been designed to support the following three aspects of a call :
  1. Call establishment.
  2. Call maintenance.
  3. Call termination.
- It also controls and supports the functioning of SMS, supplementary services and DTMF signaling.

2. Mobility Management (MM) :

- This network sub layer has been designed to handle the issues related to mobility management when a mobile station travels from one cell to the other.
- The functions of MM are as follows :
  1. Registration.
  2. Update the location.
  3. Authentication.
  4. Identification.
  5. Maintaining a reliable communication with the upper layers.
  6. To use TMSI allocated by VLR in place of IMSI at HLR.

3. Radio Resource Management (RRM) :

- This network sub layer is supposed to handle the following issues in setting up point-to-point communication between a mobile device and network: establishment, maintenance and release of RRM connection.
- RRM is used for data and user signaling.
- This sub layer carries out procedures such as, selection, reselection, and the hand off process.
- When RRM is established, it handles the reception of BCCH and CCCH as well.
- A mobile station always initiates the RRM session, either in response to a paging message or in order to make a call.
- The functions of RRM are as follows :
  1. To manage the quality of radio link.
  2. Assignment of frequency.
  3. It provides options for frequency hopping sequence.
  4. Measurements of signal strength.
  5. To manage the handover process.
  6. RRM session management.
  7. To manage synchronization.

1.8.2 Base Transceiver Station (BTS) – Base Station Controller (BSC) Signalling Protocols :

- The interface between the BTS and BSC that carries out the traffic and maintenance data is the known as the **Abis interface** which is standardized for GSM systems.
- A wired network such as PSTN, ISDN, PSPDN etc. is used to connect the BTS and BSC.
- The voice signal is encoded into the 64 kbps PCM format in a PSTN network. The same format is also used by the Abis interface.
- PCM coding techniques are different from 22.8 kbps. TCH radio interface U_m (between MS and BTS). Therefore a translation between the coding formats is essential.
- This is done by translating the TCH bits received from caller mobile station (MS) to 64 kbps PCM and then from PCM to TCH for receiver MS.
- The voice quality gets affected due to the translation and retranslation. Therefore, a procedure called **TFO (tandem free operation)** is adopted, to improve the voice quality at the BTSs, BSCs and MSCs.
- The data link layer protocol for the Abis interface between the BTS and BSC is **LAPD (link access protocol D channel)** which prescribes the standard procedure for D-channel of ISDN.
- The network layer protocol between the BTS and BSC is called as BTSM (BTS management).

1.8.3 Base Station Controller (BSC) – Mobile Switching Centre (MSC) Signalling Protocols :

- The physical layer between the BSC and MSC uses PCM multiplexing.
- The MSC is connected to the networks such as PSTN, ISDN and other data networks that use either 64 kbps PCM or 2.048 Mbps CCITT that carries 32 PCM channels.
- The interface between BSC and MSC is the A interface. The type of communication between BSCs and MSCs is wired communication.
- **MTP (message transfer protocol)** and **SCCP (signal correction control protocol)** are the two data link layer protocols between the BSC and MSC. Both of them are parts of SS7 (Signaling System No. 7) used by A interface.
- The network layer protocol that is used at BSC is BSSAP (Base Sub System Application Protocol).

1.9 Signalling System Number 7 (SS7) :

- The common-channel signaling is more flexible and powerful than in channel signaling. Hence it is suitable for integrated digital networks.
- One of the most widely used scheme is signaling system 7 or SS7.
- SS7 has been designed to be an open ended common channel signaling standard which can be used over a variety of digital switched networks.
- Furthermore the SS7 is specifically designed to be used in ISDN.
- SS7 provides an internationally standardized, general purpose common channel signaling system.

Primary Characteristics of SS7 :

Some of the important primary characteristics of SS7 are as follows :

1. It is optimized for use in digital telecommunication networks along with control exchanges that utilize 64 kbps digital channels.
2. It is designed to satisfy the present and future requirements of information transfer for call control, remote control, management and maintenance.
3. It is designed for transfer of information reliably, in a correct sequence ensuring that there is no loss or duplication of information.
4. It is suitable for operation over analog channels and at speeds below 64 kbps.
5. It is suitable for point to point terrestrial and satellite links.

Functions of SS7 :

- It covers all the aspects of control signaling for digital networks.
- To facilitate the routing of control messages in a reliable manner.
- To deliver the control messages.

Features of SS7 :

- In SS7 the control messages are routed through the network for different functions such as setup, maintenance management, termination etc.
- These messages are short blocks or packets. So although the network being controlled is a circuit switched network, the control signaling is implemented using the packet switching technology.
- The mode used is associated channel mode but the use of disassociated mode is also possible.

1.10 Identifiers used in GSM :

S-17, W-18

MSBTE Questions

Q. 1 Define the following identifiers :
1. MSISDN 2. IMSI 3. IMEI 4. TMSI
(S-17, W-18, 4 Marks)

- Following are the identifiers used in GSM.

MSISDN (Mobile Station ISDN Number) :

- It is an authentic telephone number of the Subscriber Identity Module (SIM) card displayed on mobile or cellular phones.
- A MSISDN is a subscription in the Global System for Mobile Communications (GSM) or Universal Mobile Telecommunications System (UMTS) networks.
- Based on the SIM card, a mobile station can have many MSISDNs. Each subscriber is assigned with a separate MSISDN to their SIM.

IMEI (International Mobile Equipment Identity) :

- IMEI is a 15 or 17-digit code that uniquely identifies mobile handsets.
- The International Mobile Station Equipment Identity (IMEI) is similar to a serial number which distinctively identifies a mobile station internationally.
- This is allocated by the device manufacturer and registered by the network operator.By using IMEI number one can recognize outdated, stolen, or non-functional equipment.

IMSI (International Mobile Subscriber Identity) :

- It uniquely identifies the MS. It is used as the key to search any data in the databases from VLR, HLR and GSN.
- IMSI is usually fifteen digit unique number. Every registered user has an original International Mobile Subscriber Identity IMSI with a valid IMEI

MSIN (Mobile Subscriber Identification Number) :

- It is an identification number of the subscriber in the home network.

MSRN (Mobile Station Roaming Number) :

- Mobile Station Roaming Number MSRN is an temporary location dependent ISDN number, assigned to a mobile station by a regionally responsible Visitor Location Register VLR. Using MSRN, the incoming calls are channeled to the MS.

LAI (Location Area Identity) :

- Within a PLMN, a Location Area identifies its own authentic Location Area Identity LAI. The LAI hierarchy is based on international standard.

TMSI [Temporary Mobile Subscriber Identity] :

- The Temporary Mobile Subscriber Identity (TMSI) is most common identity sent between the mobile and a network.
- The moment mobile is switched on, the VLR randomly assigns TMSI to each mobile in the area.
- Whenever the mobile moves to a new geographical area, TMSI has to be updated every time because the TMSI number is local to a location area.
- In order to avoid the subscriber from being identified, and tracked by eavesdroppers on the radio interface, the network can change the TMSI of the mobile at any time.
- TMSI is used in paging a mobile. "Paging" is the one-to-one communication between the base station and the mobile.

- The Size of TMSI is **4 octet** with all hex digits, it can't be all FF because, to indicate that no valid TMSI is available the SIM uses 4 octets with all bits equal to 1.

1.11 Call Processing in GSM / Typical Call Flow Sequences in GSM :

- In this section we will discuss the following call flow sequences related to GSM :
  1. Registration / Location updating
  2. Mobile terminated call
  3. Mobile originated call

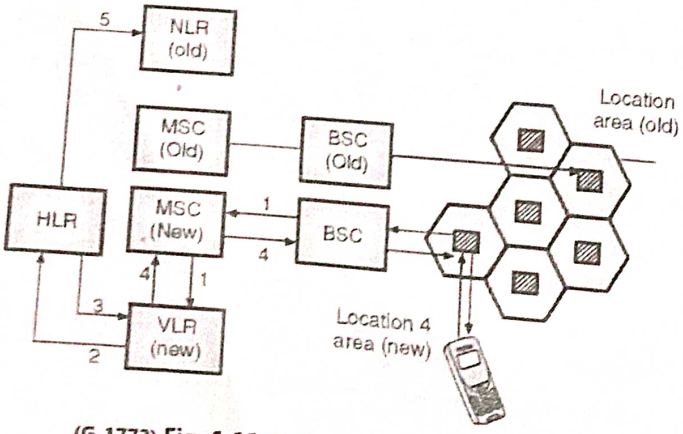
1. Location Updating :

S-16, W-18

MSBTE Questions

Q. 1 Describe location tracking and call setup in GSM. **(S-16, 6 Marks, W-18, 4 Marks)**

- In order to receive the incoming calls from a mobile station that moves within and outside the service area, the home network should somehow keep a track of the location of all the active mobile stations.
- The location updating feature is activated when a mobile station either moves to other MSC or tries to access the network and is not registered in the VLR of that location.
- Each service area consists of many adjacent cells recognized by location area identities (LAI).
- The mobile station (MS) generally has the information from the neighbouring base stations and if it sees that a subscriber has moved to a new location then it initiates the sequence as shown in Fig. 1.11.1 and following steps.



(G-1773) **Fig. 1.11.1 : Location updating in GSM**

Location Updating Procedure :

Step 1 : When a new location is identified, the mobile station (MS) sends a request for location update to the new VLR via the BSC and MSC.

Step 2 : The location update message is sent to the HLR from the VLR. This message consists of the address of the VLR (new) and the IMSI of the MS.

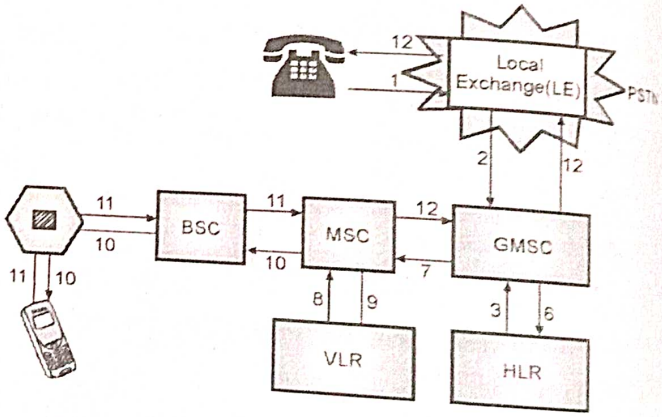
Step 3 : The security and service related information for the MS is transferred to the new VLR.

Step 4 : An acknowledgement message is sent to the mobile station as soon as the location update is done successfully.

Step 5 : The HLR instructs the old VLR to delete all the information related to the relocated MS.

2. Mobile terminated call :

- A call originating from PSTN and terminating on a mobile station is called as the mobile terminated call.
- Fig. 1.11.2 shows the steps in which a mobile terminated call is processed by GSM.



(G-1774) **Fig. 1.11.2 : Mobile terminated call in GSM**

Step 1 : The call originating landline user dials the Mobile Station ISDN of the mobile user(called party) in GSM.

Step 2 : The Local Exchange sends the call to the GMSC of the called GSM subscriber.

Step 3 : The GMSC searches the HLR for the GSM to obtain the desired routing number.

Step 4 : The HLR requests the current VLR of the called MS to obtain a Mobile station Roaming Number so as to rout the call to the correct MSC.

Step 5 : The current VLR sends the mobile station roaming number to the HLR.

Step 6 : The HLR sends the mobile station roaming number to the GMSC.

Step 7 : The GMSC transfers the call to the MSC by using the MS roaming number.

Step 8 : The MSC enquires about the Location Area Identity (LAI) of the mobile station subscriber to the VLR.

Step 9 : The VLR passes the LAI of the mobile station subscriber to the MSC.

Step 10 : The MSC sends a pager message to the Mobile Station subscriber through BSC. The Mobile Station then sets up the required signaling links.

Step 11 : After establishing the signaling links, the BSC informs the MSC about the same and the call is delivered to the mobile station subscriber.

Step 12 : The connection to the calling landline is completed after the mobile subscriber answers the call.

3. Mobile Originated Call :

S-15, S-16, S-17, W-17, S-18, W-18, S-19

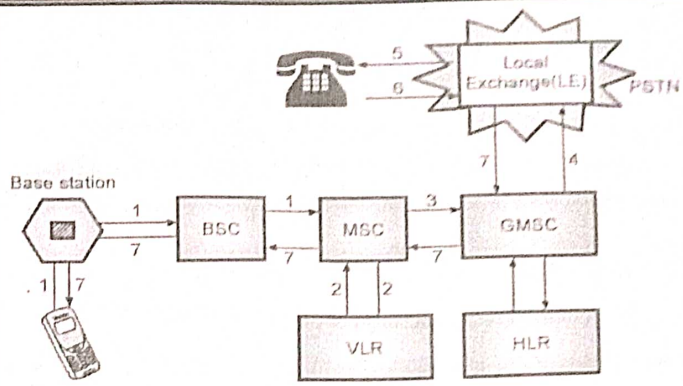
MSBTE Questions

Q. 1 Explain how GSM to PSTN call takes place in mobile environment. **(S-15, S-16, W-17, S-18, W-18, S-19, 4 Marks)**

Q. 2 State the procedure for Mobile originated call in GSM. **(S-18, 4 Marks)**

Q. 3 Describe basic call originating procedure. **(S-17, 4 Marks)**

- This type of call is originated by a mobile subscriber and it is meant for a landline user.
- First the calling mobile subscriber enters the phone number to be called on the mobile and presses the send key.
- Then the mobile station connects the correct signaling links to the BSC.
- After that the call is processed by following the steps shown in Fig. 1.11.3.



(G-1775) **Fig. 1.11.3 : Originating mobile call in GSM**

Step 1 : The mobile station passes on the dialed number to the MSC via BSC to indicate that it needs service.

Step 2 : The VLR tells the MSC if the mobile station can access the requested service or not. If the MS can access the requested service, then the MSC instructs the BSC to assign the resources required for the call.

Step 3 : The allowed call is then routed to GMSC via MSC.

Step 4 : The GMSC then routes the call to the Local Exchange (LE) of called landline subscriber.

Step 5 : The LE then gives a ring on the called landline terminal.

Step 6 : The landline terminal returns an answer back tone to the LE.

Step 7 : The answer back tone is sent back to the Mobile Station thus completing the call.

1.12 Mobility Management in GSM :

- One of the major function of a GSM network is **Mobility management** which allows mobile phones to work.
- The goal of mobility management in GSM is :
  1. To track the location of subscribers.
  2. To allow calls, SMS and other mobile phone services to be delivered.

1.13 Basic Location Update Procedure :

S-17, W-17, I-Scheme : S-22

MSBTE Questions

Q. 1 Write the GSM location updating procedure. **(S-17, W-17, 4 Marks)**

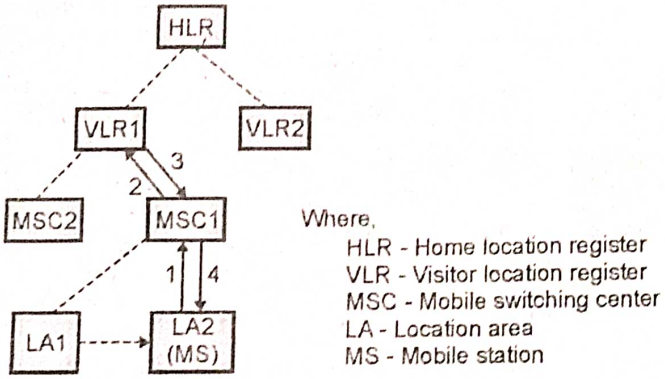
Q. 2 Write the steps of Inter-MSC movement of location update procedure. **(S-17, 4 Marks)**

Q. 3 What is location area (LA) ? Describe any three situation when GSM location area update is performed. **(W-17, 4 Marks)**

- The location update procedure in GSM occurs when the MS (Mobile station) moves from one LA into another area.
- The basic location updates procedure handles following movements without considering fault tolerance and VLR overflow :
  1. Inter-LA movement.
  2. Inter-MSC movement.
  3. Inter-VLR movement.

Case 1 : Inter-LA Movement :

- In this case the MS moves from a LA1 to LA2. Here both the LAs are connected to the same MSC (Mobile station controller) as shown in Fig. 1.13.1(a).
- Fig. 1.13.1(a) shows the steps in Inter-LA movement registration within the same MSC.



(G-2630) **Fig. 1.13.1(a) : Inter-LA movement registration within the same MSC**

Step 1 : The mobile station (MS) sends a request for location update to the MSC through the BTS. This message consists of the addresses of the previously visited VLR, MSC and LA.

Step 2 : The location update message is sent to the VLR by a TCAP (Transaction Capabilities Application Part) message i.e.

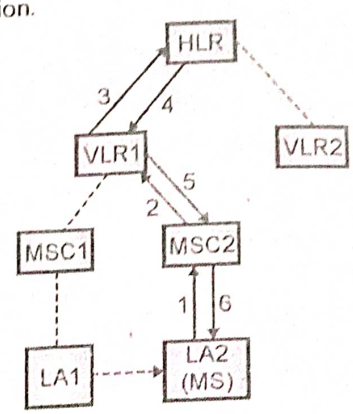
MAP_UPDATE_LOCATION_AREA. This message consists of the address of the MSC, TMSI of the MS, ID of LA1 and LA2 and other related information.

Step 3 : The VLR observes that LA1 and LA2 belongs to the same MSC.

Step 4 : VLR updates LAI (local area identification) field of VLR record and replies with an acknowledgement **MAP_UPDATE_LOCATION_AREA_ACK** to the MS via MSC.

Case 2 : Inter-MSC Movement :

- In this case LA1 and LA2 belongs to different MSCs having the same VLR as shown in Fig. 1.13.1(b).
- Fig. 1.13.1(b) shows the steps in Inter-MSC movement registration.



(G-2631) **Fig. 1.13.1(b) : Inter-MSC movement registration**

Step 1 : The mobile station (MS) sends a request for location update to the MSC through the BTS. This message consists of the addresses of the previously visited VLR, MSC and LA.

Step 2 : The location update message is sent to the VLR by a TCAP (Transaction Capabilities Application Part) message i.e.

MAP_UPDATE_LOCATION_AREA. This message consists of the address of the MSC, TMSI of the MS, ID of LA1 and LA2 and other related information.

Step 3 : The VLR observes that previous LA and target LA belongs to different MSCs i.e. MSC1 and MSC2 respectively which are connected to the same VLR. The HLR address of the MS is obtained from the MS's IMSI which is stored in VLR record. VLR sends

MAP_UPDATE_LOCATION message to the HLR which includes IMSI of MS, address of MSC2 and VLR1 and other related information.

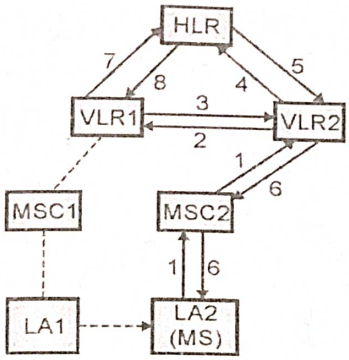
Step 4 : The HLR identifies the MS's record by using the received IMSI and updates MSC address in the record. HLR replies with an acknowledgement to the VLR.

Step 5 : The VLR observes LA1 and LA2.

Step 6 : VLR updates LAI (local area identification) field of VLR record and replies with an acknowledgement **MAP_UPDATE_LOCATION_AREA_ACK** to the MS via MSC.

Case 3 : Inter-VLR Movement :

- In this case LA1 and LA2 belongs to different MSCs having different VLRs as shown in Fig. 1.13.1(c).
- Fig. 1.13.1(c) shows the steps in Inter-VLR movement registration.



(G-2632) **Fig. 1.13.1(c) : Inter-VLR movement**

Step 1 : The mobile station (MS) sends a request for location update to the MSC through the BTS. This message consists of the addresses of the previously visited VLR, MSC and LA.

Step 2 : The location update message is sent to the VLR by a TCAP (Transaction Capabilities Application Part) message i.e. **MAP_UPDATE_LOCATION_AREA.** This message consists of the address of the MSC, TMSI of the MS, ID of LA1 and LA2 and other related information.

Step 3 : As the Mobile Station moves from VLR1 to VLR2, VLR2 do not have the VLR record and IMSI of the MS. VLR2 identifies the address of VLR1 from the message **MAP_UPDATE_LOCATION_AREA.** VLR2 sends MAP_SEND_IDENTIFICATION message to VLR1.

Step 4 : The HLR identifies the MS's record by using the received IMSI and updates MSC address in the record. HLR replies with an acknowledgement to the VLR containing the TMSI of the MS. VLR1 uses this TMSI to find the corresponding IMSI in the database. This IMSI is then sent back to VLR2.

Step 5 : The VLR2 generates a VLR record of the MS. It sends registration message for the updating the HLR. HLR updates the record of MS and sends acknowledgment back to the VLR2.

Step 6 : VLR2 creates a new TMSI and sends it to the MS.

Steps 7 & 8 : From the VLR1, outdated record of MS is deleted.

1.14 Concept of Roaming :

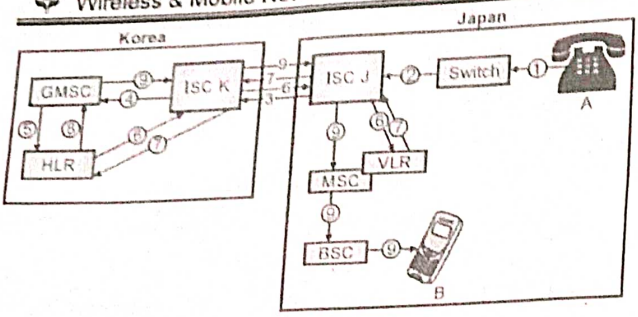
- Roaming is one of the basic mobility management process in all cellular networks.
- **Roaming** is defined as the capability of a cellular customer to make and receive voice calls automatically, send and receive data, or to access other services containing home data services, while travelling outside the geographical coverage area of the home network, by means of using a visited network.
- Roaming can be done by using a communication terminal or by using the subscriber identity in the visited network.
- Technically Roaming is supported by a mobility management, authorization, authentication and billing procedures.

Roaming process :

- B is a GSM service subscriber in Korea. If B travels from Korea to Japan. There are following three scenarios in the International roaming :

1. If a person in Korea calls the B, caller will be charged for a local GSM call and B will be charged for an international call from Korea to JAPAN.
2. If a person in another country (say Singapore) calls the B, caller will be charged for an international call from Hong Kong to Korea and B will be charged for an international call from Korea to Japan.
3. If a person in Japan calls the B, caller and B, both will be charged for an international call though both are in the same country.

- As the scenario 3 is the special case we will see why the call delivery to GSM roamer is so expensive. Here A in Japan calls to B who has roamed from Korea to Japan as shown in Fig. 1.14.1.



(G-2627) **Fig. 1.14.1 : International Call set up Process (Roaming)**

- The call delivery process to a GSM roamer is same as that of procedure in the Mobile Terminated Call explained in the section 1.11.
- Only one change in the set up of international roaming is that it uses two ISCs (International Switch Centers) in the voice path.
- Segments in the call path of international call :

1. The source country.
2. The international network.
3. The destination country.

- These segments are interconnected by two ISCs, one in the source country and another in the destination country.

Step 1 : The call originating landline user A in Japan dials the International switch centre access code (ISCA), then country code (CC) and Mobile Station ISDN of the GSM mobile user B (called party) in Korea.

Step 2 : The switch S interprets the first part of dialed digits of ISCA then it understands the call is an international call and sets the call to Japan's ISC J (International Switch Centre) with the help of IAM (Initial address message).

Step 3 : Based on the country code, ISC J routes the call to the ISC K of Korea. ISC K interprets the prefix of remaining digits.

Step 4 : ISC K sends the call to the GMSC of the called GSM subscriber B.

Step 5 : The GMSC searches the HLR for the GSM to obtain the desired mobile station routing number (MSRN).

Step 6 : The HLR requests the current VLR of the called MS to obtain a Mobile station Roaming Number so as to route the call to the correct MSC (HLR → ISC K →ISC J→VLR).

Step 7 : The VLR sends the mobile station roaming number to the HLR (VLR → ISC J → ISC K → HLR).

Step 8 : The HLR sends the mobile station roaming number to the GMSC.

Step 9 : The GMSC transfers the call to the MSC by using IAM based on the MS roaming number and A and B gets connected.

- As a result, B is charged for the international call from Japan to Korea and A is charged for the international call from Korea to Japan.

1.15 Types of Areas in GSM :

- There are three types of area in GSM :
  1. Location area.
  2. Routing area.
  3. Tracking area.

1.15.1 Location Area : W-17, I-Scheme : S-22

MSBTE Questions

Q. 1 What is location area (LA) ? Describe any three situation when GSM location area update is performed. **(W-17, 4 Marks)**

- A **location area** is a set of base stations grouped together to optimize signaling.
- A single Base Station Controller (BSC) in the GSM can be shared among many base stations, typically tens or even hundreds of base stations.
- The BSC in the GSM handles allocation of radio channels, receives measurements from the mobile phones, and controls handovers.
- A unique number called a **location area code (LAC)** is assigned to each location area. Each base station broadcasts the location area code at regular intervals. Each base station assigns a different **cell identifier (CI) number** within a location area.
- In case of very large location areas, there will be many mobiles operating simultaneously, which results in a very high paging traffic.
- In the location area, as every paging request has to be broadcast to every base station results in the waste of bandwidth and power on the mobile.

- On the other hand, in case of too many small location areas, for changes of the location the mobile should contact the network very often, which will drain the mobile's battery.

1.15.2 Routing Area : I-Scheme : S-22

- The routing area is the packet-switched domain similar to the location area. The subdivision of a location area is a routing area.
- Mobile uses routing areas that are attached to GPRS. For bursty data communication services, such as wireless internet / intranet and multimedia services GPRS is optimized. It is also known as GSM-IP (Internet Protocol) as it will connect users directly to an Internet Service Providers.
- As the bursty nature of packet traffic means that more paging messages are expected per mobile, hence it is important to know the accurate location of the mobile.
- Routing Area Update i.e change from routing area to routing area is done in an almost similar way to a change from location area to location area.

1.15.3 Tracking Area :

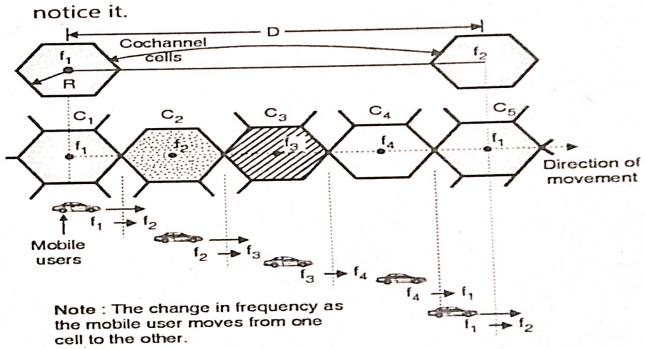
- The LTE counterpart of the location area and routing area is the tracking area. A tracking area is a set of cells.
- Tracking areas are grouped into lists of tracking areas (TA lists), which can be configured on the User Equipment (UE).
- Tracking areas are updated periodically or when the User Equipment moves to a tracking area, which is not included in its TA list. Operators can allocate different TA lists to different UEs.

1.16 Hand Off (Hand Over) in GSM : S-19

MSBTE Questions

Q. 1 With a diagram, describe Hand off procedure. List the types of Hand offs. **(S-19, 4 Marks)**

- Assume that there is a call going on between two parties over a voice channel.
- When the mobile unit moves out of coverage area of a particular cell site, the reception becomes weak.
- Then the present cell site will request a handover.
- The system will switch the call to a new cell site without interrupting the call. This procedure is called as the handover procedure or handover procedure.
- The user can continue talking without even noticing that the handover procedure has taken place.
- The advantage of handover procedure is increase in the effectiveness of the mobile system.
- Refer Fig. 1.16.1 to understand the handover procedure clearly.
- Fig. 1.16.1 shows two co-channel cells separated by a distance D and using the frequency f_1.
- Other cells such as C_1, C_2, C_3, C_4, C_5 etc. exist in-between the two co-channel using frequency f_1.
- The cells C_1, C_2, C_3 and C_4 use different frequencies f_1, f_2, f_3, f_4, etc. as shown in Fig. 1.16.1.
- Suppose a mobile unit initiates a call in cell C_1 and then moves to cell C_2. Then as it starts going away from C_1, the call is dropped and reinitiated in the frequency channel from f_1 to f_2 when the mobile unit (such as car) moves form C_1 to C_2.
- Similarly when the mobile unit moves from cell C_2 to C_3 the frequency is changed automatically from f_2 to f_3 as shown in Fig. 1.16.1.
- The process of changing the frequency is done automatically by the system and the user does not even notice it.



(G-1033) Fig. 1.16.1 : Handover procedure

1.16.1 Handover Strategies :

S-15, S-16, W-16, S-17, S-18, W-18

MSBTE Questions

Q. 1 Describe hand off strategies. **(S-15, S-16, S-17, W-18, 4 Marks)**

Q. 2 State different handoff strategies used in analog generation and second generation. **(W-16, 4 Marks)**

Q. 3 With neat diagram describe the handoff strategies. State the types of handoffs. **(S-18, 4 Marks)**

- It is important to process handovers in any cellular system. In many handover strategies, higher priority is given to the handover request than the call initiation request.
- Handovers should be performed successfully and they should not be repeated frequently.
- So as to satisfy these requirements, system designers should decide and specify an optimum signal level at which the handover should be initiated.
- Fig. 1.16.1 illustrates handover diagrammatically.
- First a minimum signal level for maintaining the call is decided. Then a slightly stronger signal level is used as the **handover threshold**. The handover will be made at this signal level.
- The margin between these two levels is denoted by Δ and given by,

$$\Delta = P_{r\ handover} - P_{r\ minimum\ usable} \quad ...(1.16.1)$$

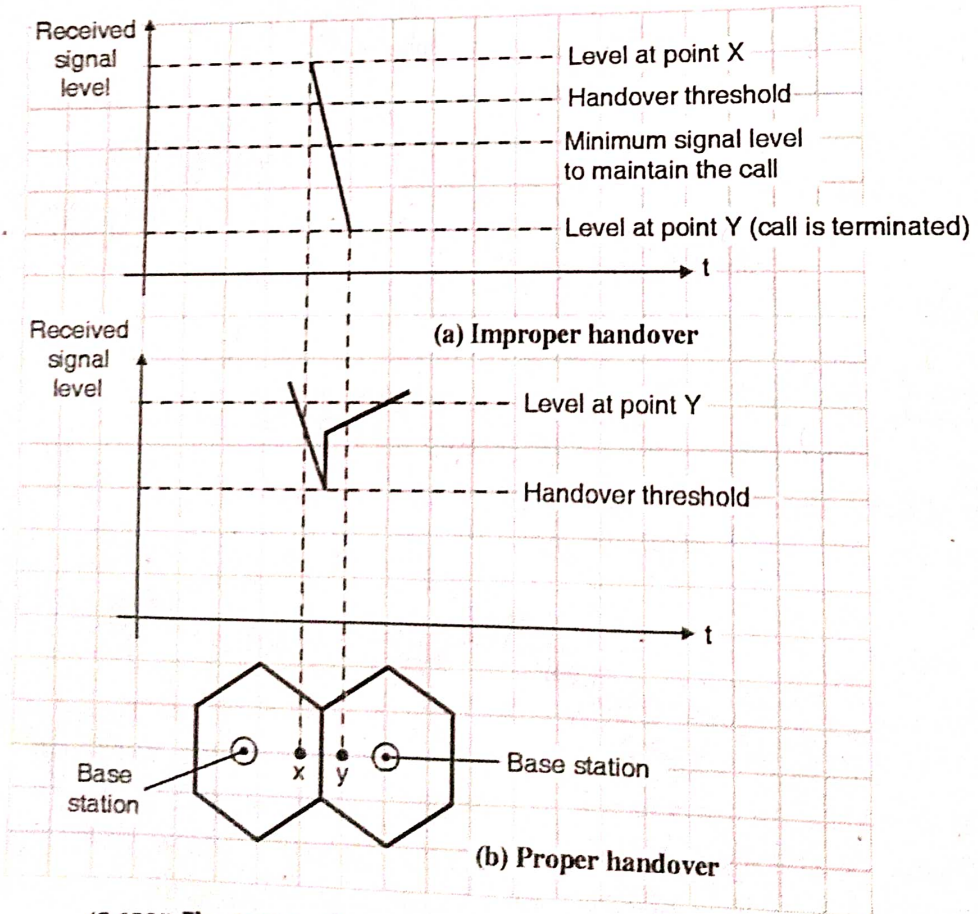
- Note the choice of the value of Δ is critical. Δ cannot be too small and it cannot be too large as well.
- If Δ is too large, then unnecessary handovers will take place and if Δ is too small, there won't be sufficient time to complete the handover and the call may lost due to weak signal.

Improper Handover :

- Refer Fig. 1.16.2(a) which illustrates the improper handover situation i.e. handover is not made and signal drops below the minimum signal level. The call is terminated.
- In Fig. 1.16.2(b), the handover has taken place as soon as the received signal level drops to the handover threshold. Note the increase in the signal level at point Y after handover.
- Before initiating the handover, it is necessary to ensure that the reduction in the measured signal level is not due to the momentary signal fading and that the drop in signal level is due to the actual movement of the mobile station.

Dwell time :

The time duration over which a call may be maintained within a cell without initiating a handover is called as **dwell time**. The dwell time depends on propagation, interference, distance between the subscriber and base station etc.



(G-1564) **Fig. 1.16.2 : Illustration of improper and proper handover**

1.16.2 Different Types of Handover :

S-18, S-19

MSBTE Questions

Q. 1 With neat diagram describe the handoff strategies. State the types of handoffs. **(S-18, 4 Marks)**

Q. 2 With a diagram, describe Hand off procedure. List the types of Hand offs. **(S-19, 4 Marks)**

- Following are various types of handovers, in relation with a mobile station (MS) :
  1. Hard handover.
  2. Soft handover.
  3. Queued handover.
  4. Delayed handover.
  5. Forced handover.

1. Hard handover :

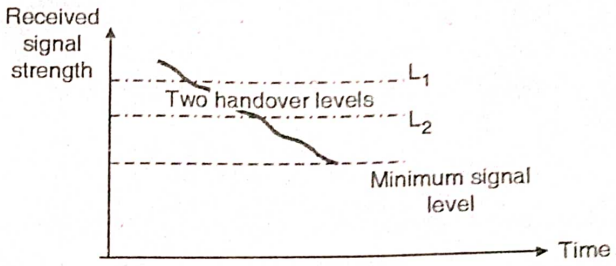
- The handover is known as **hard handover** if a mobile station transmits between two base stations operating on different frequencies.

2. Soft handover :

- The handover is known as soft handover if the MS starts communication with a new base station without stopping the communication with the older base station.
- In a soft handover the operating frequencies of the old and new base stations are identical.
- Soft handover enhances the signal by providing different-site selection diversity.
- If the handover takes place within the same cell then it is known as **softer handover**.

3. Delayed handover :

- In many situations, instead of one level, a two level handover procedure is followed, in order to ensure a higher possibility of a successful handover.
- A handover can be **delayed** if no available cell could accept the call.
- Fig. 1.16.3 shows a graph of signal strength with two handover levels.
- When the signal level drops below the first handover level, the MS initiates a handover request.
- If due to some reason the mobile unit is in a hole (Place in a cell with low signal level) or neighbouring cell is busy then the MS will repeat the handover request after every 5 seconds.



(G-1415) **Fig. 1.16.3 : A two level handover scheme**

- But if the signal strength drops down further and reaches the second handover level (L_2) then the handover will take place without any condition, immediately.
- This process is called as **delayed handover**.

Advantages :

1. It is possible to delay the handover if neighbouring cells are busy.
2. The number of handovers required to be carried out will reduce.

   This will allow the processor to handle calls more efficiently.
3. It makes the handover occur at the proper location and eliminates the possible interference in the system.

4. Forced handover :

- A **forced handover** is defined as the handover which would normally occur but is not allowed to happen by force or a handover that should not occur but is forced to take place.

5. Queued handover :

- In the queued handover process, the MTSO arranges the handover requests in a queue instead of rejecting them, if it finds that new cell sites are too busy to makes the handover possible.
- These handover requests are then acted upon in a sequential manner. Queueing of handovers is more effective than the two threshold handover. Also, a queueing scheme is effective only when the handover requests arrive at the MTSO in the form of batches or bundles.

1.16.3 Handover in GSM :

- We have already discussed the concept and need of handover in cellular systems.
- With reduction in the size of a cell, the number of handovers increases. However a handover is not supposed to cause a cut-off (also called as a **call drop**).
- The maximum duration for a handover in GSM has been decided to be equal to 60 ms.

Reasons for a handover :

- The two most important reasons for handovers are as follows :
  1. A MS (Mobile Station) moves out of range of a BTS.
  2. If the wired infrastructure decides that the traffic in one particular cell is too high than that in some other cells.

1.16.4 Types of Handover in GSM :

- There are four types of possible handovers in a GSM system. They are :
  1. Intra-cell handover.
  2. Inter cell, Intra BSC handover.
  3. Inter-BSC, Intra-MSC handover.
  4. Inter MSC handover.
- All these have been demonstrated in Fig. 1.16.4.

1. Intra-cell handover :

- This is the first scenario in Fig. 1.16.4 which is the handover within a cell.
- If a narrow band interference makes transmission at a certain frequency impossible, then the BSC can decided to change the carrier frequency.
- This will lead to the intra-cell handover.

2. Inter-cell, Inter BSC handover :

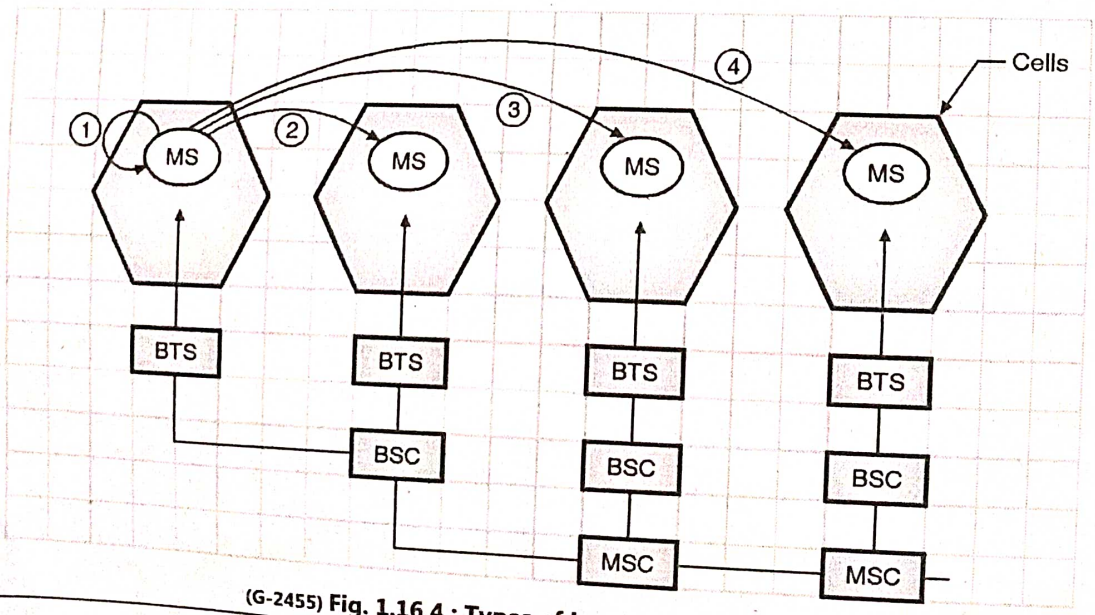
- Refer to the second scenario in Fig. 1.16.4. This type of handover takes place when a mobile station (MS), moves from one cell to the other but remains in control of the same BSC.
- The BSC will carry out the handover by assigning a new radio channel in the new cell to the MS and then release the old one.

3. Inter BSC, Intra-MSC handover :

- Refer to the third scenario in Fig. 1.16.4. This type of handover takes place when a mobile station (MS) moves between two cells controlled by different BSCs but same MSC.
- Such a handover is controlled by the MSC.

4. Inter-MSC handover :

- Refer to the fourth scenario in Fig. 1.16.4. This type of handover is required when a mobile station (MS) moves between two cells belonging to two different MSCs.
- Such a handover is performed by two MSCs together.



(G-2455) **Fig. 1.16.4 : Types of handovers in GSM**

1.17 Security :

- GSM offers different security services with the help of the personal information stored in AuC and in the SIM.

Types :

- GSM offers the following security services :
  1. Access control and authentication.
  2. Confidentiality.
  3. Anonymity.

1.17.1 Access Control and Authentication :

Definition :

- Authentication is the process of ensuring that the communication over the wireless radio medium is secured. The authentication of a user is the process of ensuring and verify that the user is really the person who claims he is.
- There are two steps in authentication process of GSM. In the first step the authentication of a valid user is carried out for the SIM. The user needs a secret PIN to access the SIM.
- And in the second step the authentication of the subscriber is done.

1.17.2 Confidentiality :

- The confidentiality of all the user related data is ensured by encrypting it.
- The BTS and MS apply **encryption** to voice, data and signaling information, once the authentication is done.
- Due to encryption, it is possible to apply confidentiality only between MS and BTS but not over the entire end to end GSM network.

1.17.3 Anonymity :

- In order to provide anonymity to the user, all data is first encrypted. The user identifiers (the information which could reveal the user's identity) is not transmitted.
- Instead a temporary identifier (TMSI) is transmitted by GSM. The VLR assigns this identifier newly after each location update.
- Additionally the TMSI can be changed anytime by the VLR.

Algorithms :

- GSM provides the security services by using three algorithms called **A_3, A_5 and A_8.** Their functions are as follows :

Sr. No.	Algorithm	Function
1.	A_3	Used for Authentication
2.	A_5	Used for Encryption
3.	A_8	Used for generation of cipher key.

1.17.4 GSM Specifications :

Sr. No.	Specification	Value
1.	Number of full duplex channel	125
2.	BW of each channel	200 kHz
3.	Number of users per channel	8
4.	Type of modulation	GMSK
5.	Data rate	270.833kb/s
6.	Frame duration	4.615 mS
7.	Company using this technology	Idea
8.	SIM card	Yes
9.	Handover type	Hard
10.	Types of multiple access method	FDMA or TDMA
11.	Cost	High
12.	Frequency spectrum	25 MHz
13.	SMS length	160 characters or 140 octets

Review Questions

Q. 1 Explain the concept of Personal Communication Services.

Q. 2 What is GSM ?

Q. 3 What are the services provided by GSM ?

Q. 4 State important features of GSM.

Q. 5 Explain the GSM system architecture.

Q. 6 Give the specifications of GSM.

Q. 7 State and explain the GSM channel types.

Q. 8 Explain the frame structure of GSM.

Q. 9 Write a note on : Signal processing in GSM.

Q. 10 Explain the SS7.

Q. 11 What is roaming ?

Q. 12 What are personal communication services ?

Q. 13 With neat block diagram explain PCS architecture.

Q. 14 Write a short note on teleservices of GSM.

Q. 15 Explain reference model of GSM services.

Q. 16 Write a short note on GSM frequency band allocation.

Q. 17 Explain how authentication of a user is performed in GSM.

Q. 18 Write short note on security services in GSM.

Q. 19 What are the specifications of GSM ?

Q. 20 What are the security algorithms used in GSM ? State their functions.

Q. 21 Explain the types of handover in GSM.

Q. 22 Which are the different types of areas in GSM ?

Q. 23 Explain international call set up process.

Q. 24 Write short note on mobility management in GSM.

Q. 25 Explain identifiers used in GSM.

Q. 26 What are the features of SS7 ?

1.18 I-Scheme Questions and Answers :

Summer 2022 [Total Marks - 18]

Q. 1 Define the term :

i. Routing area. **(Section 1.15.2)**

ii. Location area. **(Section 1.15.1)** **(2 Marks)**

Q. 2 Draw the block diagram of the architecture of PCS (Personal Communication Services) and explain. **(Section 1.1.1)** **(4 Marks)**

Q. 3 Explain location update procedure for a inter LA movement in GSM with suitable diagram.

(Section 1.13) **(6 Marks)**

Q. 4 Explain the network signaling and radio interfaces in GSM. **(Sections 1.8 and 1.8.1)** **(6 Marks)**