GSM

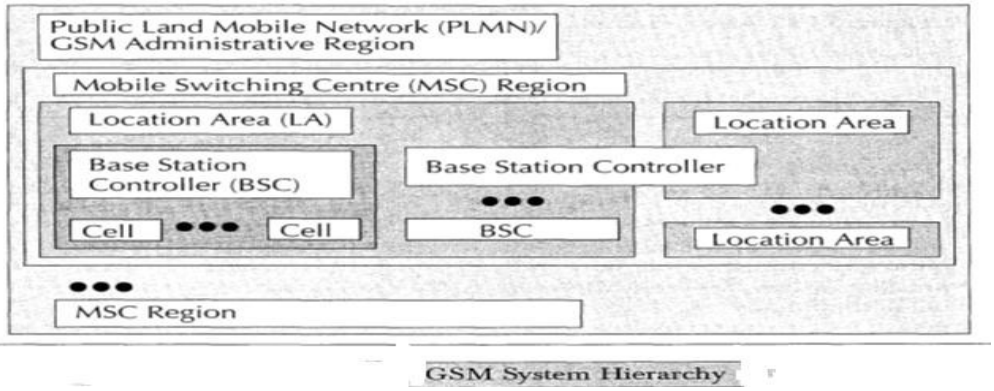
In 1982, the Conference of European Posts and Telegraphs (CEPT) -ETSI formed a study group called the Groupe Special Mobile (GSM) to study and develop a pan-European mobile system . Now it is known as Global System for Mobile Communication. Its business objectives are:

- Support for international roaming
- Good speech quality
- Ability to support handheld terminals
- Spectral efficiency
- Support for a range of new services and facilities

- The GSM system has an allocation of 50 MHz (890-915 MHz and 935-960 MHz) bandwidth in the 900 MHz frequency band. GSM uses a combination of FDMA and TDMA.
- Using FDMA, this band is divided into 124 (125 channels, 1 not used) channels each with a carrier bandwidth of 200 KHz. Using TDMA, each of these channels is then further divided into 8 time slots. (a maximum of 992 channels) The frequency must be reused to support multiple users. done through cells.

GSM ARCHITECTURE

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



GSM System Hierarchy

- For each LA there will be at least one BSC. Message center is also referred to as Service Centre (SC) or SMS Controller (SMSC). Cells are formed by the radio areas covered by a BTS (Base Transceiver Station). Several BTSs are controlled by one BSC. Traffic from the MS (Mobile Station) is routed through MSC. Calls originating / terminating in a fixed network or other mobile networks is handled by the GMSC (Gateway).

Three subsystems :

- **the radio sub system (RSS),**
- **the network and switching subsystem**
- **(NSS) and the operation subsystem (OSS**

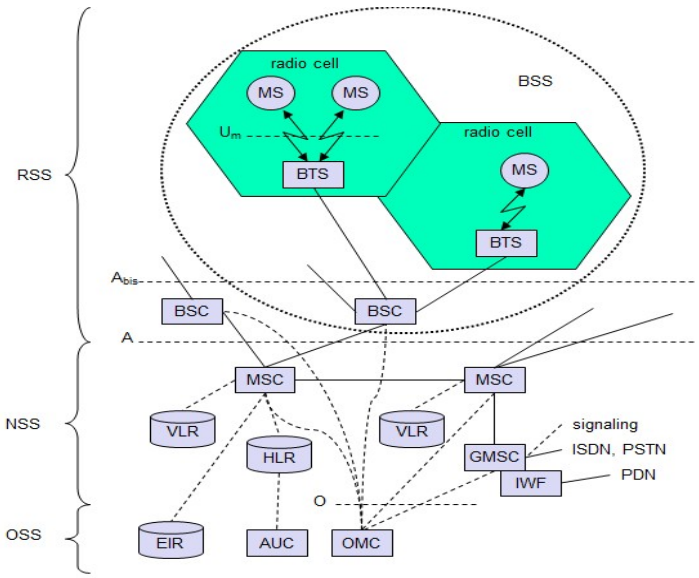
Radio subsystem It comprises all radio specific entities

- **Base transceiver station** (BTS): A BTS comprises all radio equipment, i.e., antennas, signal processing, amplifiers necessary for radio transmission. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell.
- **Base station controller (BSC**): The BSC basically manages the BTSs. 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 in GSM. It consists of user independent hard and software and of the subscriber identity module (SIM). 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 and the international mobile subscriber identity (IMSI).

- The MS stores dynamic information such as the cipher key and the location information consisting of a temporary mobile subscribers identity (TMSI) and the location area identification (LAI).
- **Base station subsystem** (BSS): A GSM network comprises many BSSs, each controlled by a base station controller (BSC).

A interface is based on circuit-switched PCM whereas the O interface uses the signaling system no.7 (SS7) based on X.25 carrying management data to/from the RSS.



MS - Mobile Station
BTS - Base transceiver station
BSC - Base Station Controller

MSC- Mobile services switches center
VLR- Visitor Location Register
HLR –Home Location Register
GMSC- Gateway MSC

EIR - Equipment identity register
AUC – Authentication Center.

Network and switching subsystem: It consists of the following switches and database

- **Mobile services switches center** (MSC): MSCs are high-performance digital ISDN switches. An MSC manages several BSCs in a geographical region. It can also connect to public data network.
- **Gateway MSC (GMSC**) is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user and vice versa.
- **Home location register** (HLR): The HLR is the most important Database in a GSM system as its stores all user-relevant information. This comprises static information, such as the mobile subscriber ISDN number (MSISDN). It contains Dynamic information like the current location area (LA) of the MS, the mobile subscriber roaming number (MSRN), the current VLR and MSC.
- **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 associated to the MSC. VLR is similar to a cache, whereas HLR is the persistent storage. The VLR contains selected administrative information borrowed from the HLR, necessary for call control and provisioning. When a MS enters the covering area of a new MSC, the VLR associated with this MSC will request information from its corresponding HLR in the home network, so subscribers use services without referring to the HLR.

Operation subsystem

contains the necessary functions for network operation and maintenance. It is also in charge of controlling the traffic load of the BSS.

- **Operation and maintenance center** (OMC) : The OMC monitors and controls all other network entities via the O interface (SS7 with X.25). OMCs use the concept of telecommunication management network (TMN) as standardized by the ITU-T.

- **Authentication centre** (AuC) : is responsible for the authentication of a subscriber. This is a protected database and stores a copy of the secret key stored in each sub scriber' s SIM card. These data help to verify the user' s identity.

- **Equipment identity register** (EIR): The EIR is a database for all IMEIs, i.e., it stores all device identification registered for this network. The EIR has a blacklist of stolen (or locked) devices. The EIR also contains a list of malfunctioning devices

INTERFACES

SIGNALLING SYSTEM

- **The Signaling system No.7(SS7)** is used for signaling between an MSC and a BSC. Any data related to user call (connection, teardown etc.) are processed with SS7 protocol for signaling
- For mobile specific signaling a protocol stack called MAP (Mobile Application Part) is used over the SS7 network. This protocol also transfers all management information between MSCs, HLR, VLR, AUC,EIR,
  AND
  OMC.
- Additionally, an MSC can control a BSS via a BSS application part**(BSSAP).**

Interfaces are

- The Mobile station MS is connected to the base transceiver station(BTS) by the **Um i**nterface.
- Base Station Controller (BSC) that manages the BTS is interfaced by the **Abis.**
- The Mobile Services Switching centre(MSC) and BSC is connected by **A** interface. Within the switching management system, 2 Mbits/sec interface is called El interface in India and

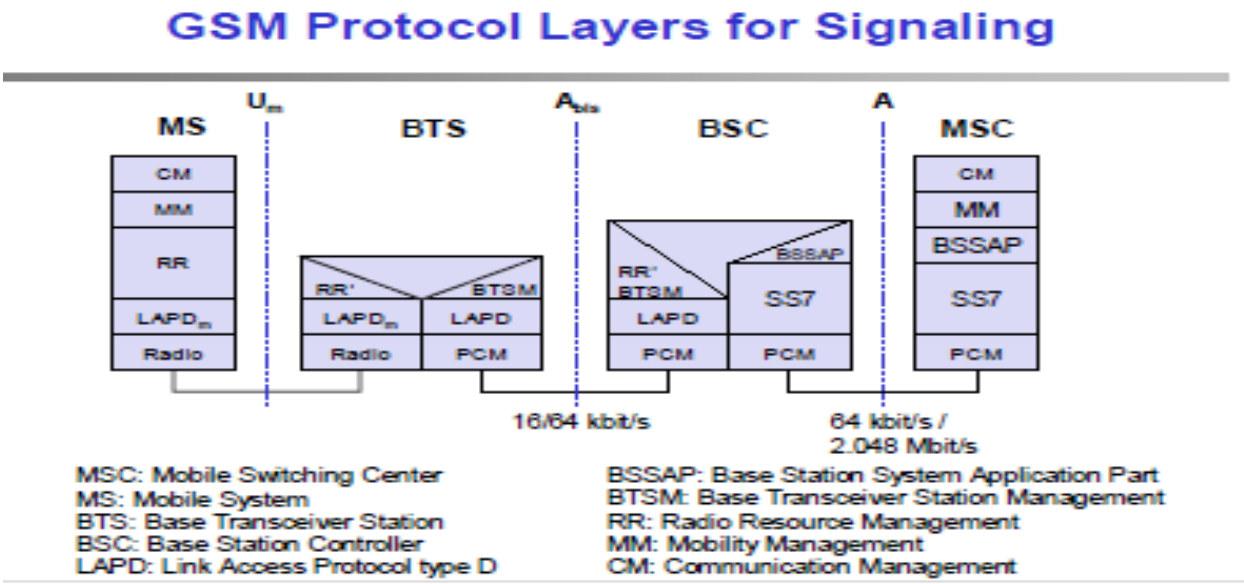
PROTOCOL ARCHITECTURE OF GSM /Network Aspects of GSM

MS and MSC have five Protocol Layers whereas the BTS and BSC have only first three Layers

LAYER 1 (PHYSICAL LAYER) :-It performs **Radio specific functions** ,Modulations, Encryption / Decryption of Data , Channel Coding and Error Deduction / Correction, Voice Activity Deduction(VAD) Radio specific functions are **Creation of burst**, **Multiplexing** of burst into a TDMA frame, sy**nchronization** with the BTS.

- S**ynchronization** includes correction of individual path delay between an MS and the BTS. Difference in Round Trip Time is an issue. An MS close to the BTS have very short RTT. It requires Large Guard spaces. To reduce the Guard space adjustment is done via the variable **Timing Advance,** where a burst can be shifted upto 63 bit Times earlier, with each bit having a duration of 3ms Physical layer at U_m uses (GMSK) Gaussian Minimum Shift Keying for Digital **Modulation.**
- **Encryption** is performed between MS and BTS over the air interface.
- **Channel Coding** make use of different Forward Error Correction Schemes(FEC) to add redundancy to the user data and to correct selected data.

Voice Activity Detection transmits voice data only when there is a voice signal. During Periods of silence, the physical layer generates the **Comfort Noise** to fake a connection, but no actual transmission takes place.



LAYER 2: LAPDM(Link Access procedure for D-channel) protocol has been defined at the Um interface for layer 2. It is the version of HDLC and it is a light weight LAPD as it does not need synchronization flags or checksum for error deduction. LAPDm has to obey the frame structure, recurrence pattern defined for Um interface. It provides Reliable data transfer over connection , Re-sequencing of data frames ,Flow control
_Segmentation and reassembly of data _Acknowledged / Unacknowledged data transfer

LAYER 3:NETWORK LAYER : It Comprises many sub layers, lowest sub layer is **Radio Resource Management**(Rr). The main task of RR include

- Setup, Maintenance and Release of Radio channels
- RR directly access the physical layer for Radio information
- Offers a reliable connection to the next higher layer

RR' : RR' is a part of this layer that is implemented in the BTS, and the rest is in the BSC. The function of RR'
are supported by the BSC via the **BTS management** (BTSM) .

LAYER 4: MOBILITY MANAGEMENT(MM): It contains functions for

- Registration ,Authentication ,Identification
- Location Updating and Provision of a **Temporary Mobile Subscriber**
- a reliable connection to the next higher layer

LAYER 5:CALL MANAGEMENT LAYER(CM) CM layer consist of 3 entities

- **Short Message Service :** SMS allows Message transfer using control channels **SDCCH** and
- **SACCH Call Control (CC) :** CC is used by higher layers for Call Establishment, Call Clearing, Change of call parameter.CC layer provides functions to send in-band tones , called **Dual Tone Multiple Frequency**(DTMF) over the GSM control. These tones are used for remote control of answering machines ,entry of PINs for Electronic Banking
- **Supplementary Services(SS):** These services offer various enhancement for the standard telephone services. Typical services are User Identification ,Call redirection, Forwarding of ongoing calls ,Closed user groups and Multiparty Communication

CALL ROUTING IN GSM

Steps in call routing of GSM :

1. **Digitizer and source coding:** The user speech is digitized at 8 KHz sampling rate. The encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech com- pressed into 1625 bytes and achieving a rate of 13 Kbits/sec.
2. **Channe l coding:** It introduces redundancy info with data for error detection and correction.

3. **Interleaving:** This step rearranges a group of bits in a particular way. This is to improve the performance of the error-correction mechanisms. The interleaving decreases the possibility of losing whole bursts during the transmission, by dispersing the errors.
4. **Ciphering:** Encrypts blocks of user data using a symmetric key shared by MS and the BTS.
5. **Burst formatting:** Adds some binary information to the ciphered block. This additional information is used synchronization and equalization of the received data.
6. **Modulation:** Gaussian Minimum Shift Keying (GMSK) is used to convert the binary data into analog signal to fit the frequency and time requirements for the multiple access rules. This signal is then radiated as radio wave over the air.

7. **Multipath and equalization:** At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So many reflected signals, which corrupt the information, with different phases are received. An equalizer is can extract the 'right' signal from the received signal. In order to extract the 'right' signal, the received signal is passed through the inverse filter.
8. **Synchronization:**. Frequency synchronization is necessary for frequency match in FDMA. Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA).When a mobile station moves further away, the burst transmitted by this mobile may overlap with the timeslot of the adjacent timeslot. To avoid such collisions, the **Timing Advance** technique is used. In this technique, the frame is advanced in time so that this offsets the delay due to greater distance. Using this technique and the triangulation of the intersection cell sites, the location of a mobile station can be determined from within the network.

MOBILE TERMINATED CALL: (MTC)

The situation in which a station calls a mobile station (the calling station could be outside the GSM network or another mobile station).

1. a user dials the phone number of a GSM subscriber
2. PSTN forward the call setup to the GMSC
3. GMSC identifies the HLR for the subscriber and signals the call setup to the HLR
4. HLR requests an MSRN mobile station roaming number from the current VLR

5.& 6.After receiving the MSRN(5) the HLR forwards the MSC responsible for the MS the GMSC (6).

7.The GMSC can now forward the call setup request to the MSC indicated .

From this point on, MSC is responsible for all further steps.

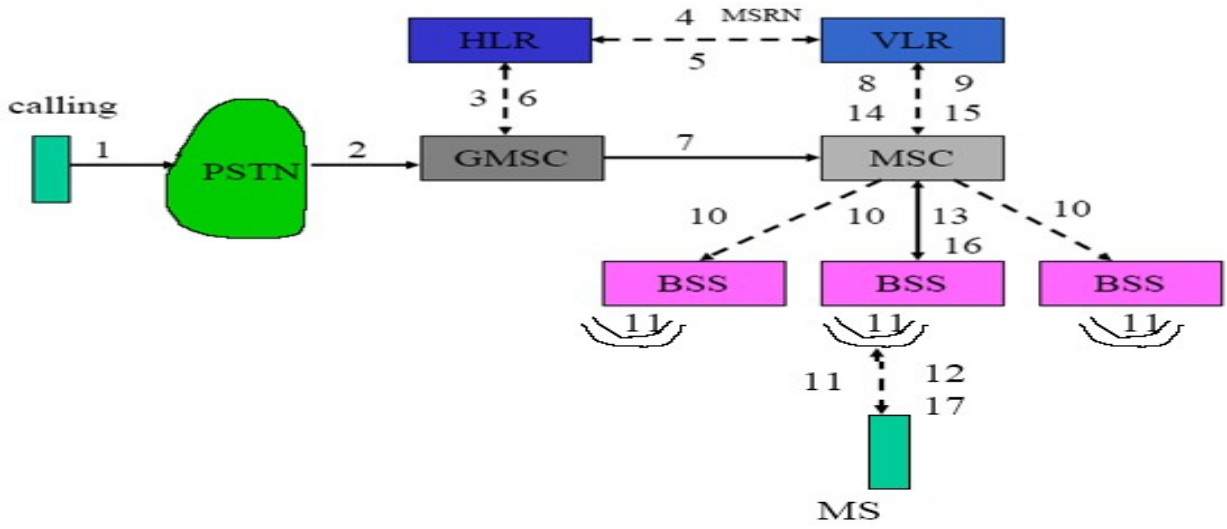
8 & 9 MSC requests the current status of the MS from the VLR (8),reply (9)

10 MSC initiates paging in all cells for location area, LA, 10

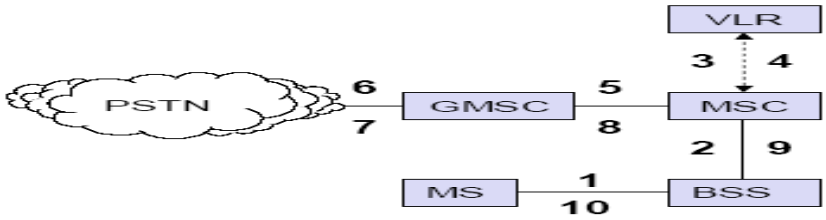
11 All BTSs of all BSSs transmit this paging signal to the MSC (11).

12 13 If the MS answers (12 & 13), the VLR has to perform the security check

15 to 17 The VLR then signals to the MSC to setup a connection (15 – 17).



MOBILE ORIGINATED CALL:



MOC simpler than MTC

- The MS transmits the requests for a new connection
- (1). The BSS forwards the request to the MSC (2).

- The MSC then checks whether the user is allowed to setup a call with the requested service (3 & 4) and checks the availability of the resources through the GSM network and in to the PSTN.

ADDRESS & IDENTIFIERS

The **MSISDN** categories follow the international ISDN (Integrated Systems Data Network) numbering plan as the following:

- Country Code (CC): 1 to 3 decimal digits of country code
- National Destination Code (NDC): Typically 2 to 3 decimal
- digits Subscriber Number (SN): maximum 10 decimal digits.

SN consists of 2 decimal digits of operator code, followed by one decimal digit level number with 5 decimal

digit subscriber number- 919845062050. In this number 91 is the CC, 98 is the NDC, and 45062050 is the SN.

- **Location Area Identity:** Each LA in a PLMN has its own identifier. The Location Area Identifier (LAI) is structured hierarchically and unique. LAI consists of 3 digits of CC, 2 digits of Mobile Network Code and maximum 5 digits of Location Area Code.
- **Mobile Station Roaming Number (MSRN):** When a subscriber is roaming in another network a temporary ISDN number is assigned to the subscriber. This ISDN number is assigned by the local VLR in charge of the mobile station. The MSRN has the same structure as the MSISDN.

- **Temporary Mobile Subscriber Identity (TMSI):** it is assigned by the serving VLR. TMSI is assigned during the presence of the mobile station in a VLR in the place of IMSI and can change (ID hopping). The

  TMSI is never stored in the HLR. It is stored in the SIM card. Together with the current location area, a TMSI allows a subscriber to be identified uniquely. IMSI is replaced by the (LAI, TMSI)
- **Local Mobile Subscriber Identity (LMSI):** This is assigned by the VLR and also stored in the HLR. This is used as a searching key for faster database access within the VLR.
- **Cell Identifier:** Within a LA, every cell has a unique Cell Identifier (CI). A cell can be identified uniquely through Global Cell Identity (LAI+CI).
- **Identification of MSCs and Location Registers:** MSCs, Location Registers (HLR, VLR), SCs are addressed with ISDN numbers. In addition, they may have a Signaling Point Code

GSM SECURITY & AUTHENTICATION

- GSM offers several security services using confidential information stored in the AUC(Authentication Centre) and individual SIM(Subscriber Identity Module)

Important security services are

- **Authentication & Access Control**: It does Authentication of valid user for the SIM. The user need a secrete PIN to access the SIM. Subscriber authentication is based on challenge response scheme

- **Confidentiality :** User related data is encrypted. BTS and MS apply encryption to voice, data, and signaling. This confidentiality exists only between MS and BTS and not end-to-end
- **Anonymity :**To provide user anonymity, all data is encrypted before transmission, and user identifiers
  which would reveal an identity are not used over the air. GSM transmits a temporary identifier(TMSI),which is newly assigned by the VLR after each location update.

ALGORITHMS USED

- **A3** : For Authentication **A5** : For Encryption **A8** : For Generation of a Cipher key

AUTHENTICATION: Any subscriber must be authenticated before using service from GSM network. It is done at AUC

- ✓ Authentication is based on
  - SIM-which stores the individual authentication key Ki ,User identification IMSI and

    A3 – an algorithm used for authentication
- ✓ Authentication uses a **CHALLENGE – RESPONSE METHOD**
  - The access control AC generates a random number RAND as challenge
  - SIM with MS answer with SRES (signature response)as response
  - The AUC performs the basic generation of random values RAND, signed responses SRES, and cipher keys Kc for each IMSI, and then forwards this information to the HLR,
  - The current VLR requests the appropriate values for RAND, SRES, and Kc, from the HLR for Authentication the VLR sends the random values RAND to SIM
- ✓ Both sides, network and subscriber module ,perform the same operation with RAND and the key Ki called A3
- ✓ The MS sends back the SRES generated by the SIM, the VLR can now compare both values. If they are the same, the VLR accept the subscriber, otherwise the subscriber is rejected.

DATA ENCRYPTION

- ✓ Encryption is done to ensure privacy and is done by applying the cipher key Kc. Kc is generated using the individual key Ki and a random value by applying the algorithm A8.
- ✓ The SIM in the MS and the network both calculate the same Kc, based on the random value RAND. The key Kc itself is not transmitted over the air interface.MS and BTS can now encrypt and decrypt data using the algorithm A5 and the cipher key Kc.
- ✓ **Kc** should be a 64 bits key which is not very strong but at least a good protection against simple eavesdropping.

The original A5 algorithm was not allowed to be used outside Europe. Therefore, the first 'original' A5 algorithm was renamed A5/1. Other algorithms including A5/0, which means no encryption at all, and A5/2, a weaker over- the-air privacy algorithm were developed. The A5 algorithms after A5/1 have been named A5/x. Most of the A5/x algorithms are considerably weaker than the original A5/1.

MOBILITY MANAGEMENT / ROAMING

- The Mobility Management (MM) function handles the functions that arise from the mobility of the subscriber: especially the roaming, the location management, and the authentication of the subscriber.
- **Location management** is concerned with the procedures that enable the system to know the **current location of a powered-on mobile station** so that the incoming call routing can be completed.
- When a mobile station is switched on in a new location area the subscriber must register with the new network to indicate its current location.
    - ❖ The first location update procedure is called the **IMSI attach procedure** where the MS indicates its IMSI to the network.
    - ❖ When a mobile station is powered off, it performs an **IMSI detach procedure i**n order to tell the network that it is no longer connected. Normally, a location update message is sent to the new MSC/VLR, and then sends it to HLR.
    - ❖ If the mobile station is **authenticated and authorized** in the new MSC/VLR, the subscriber's HLR cancels the registration of the mobile station with the old MSC/VLR. The information sent to the HLR is normally the SS7 address of the new VLR. HLR sends a subset of the subscriber information needed for call control to the new MSC/VLR, and cancels the old registration.
    - ❖ The **routing procedure** begins with the GMSC querying the called subscriber's HLR for an MSRN. The HLR typically stores only the SS7 address of the subscriber's current VLR. The VLR temporarily allocates an MSRN from its pool for the call.
    - ❖ This MSRN is returned to the HLR and back to the GMSC, which can then route the call to the new MSC. At the new MSC, the IMSI corresponding to the MSRN is looked up, and the mobile is paged in its current location area. HLR is referred for incoming call; whereas VLR is referred for outgoing call.

Roaming is of two types : These are,

- **Horizontal Roaming:** Horizontal Roaming is between two networks from same family. For example, GSM to GSM roaming or GSM to UMTS roaming.
- **Vertical Roaming:** Vertical Roaming is between two networks from different families. For example, GSM to CDMA roaming or GPRS to WiFi roaming. Seamless roaming is Vertical Roaming without disruption of session.

HANDOVER

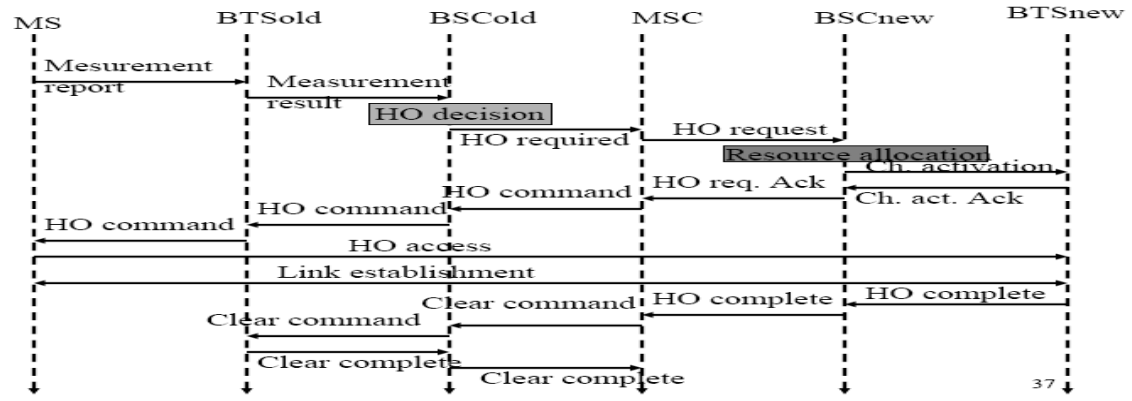
- When the user moves away from a tower, the radio signal strength or the power of the signal keeps reducing. This can result in change of the channel or cell. This procedure of changing the resources is called **handover.** This procedure is called `**handoff' in North America**.

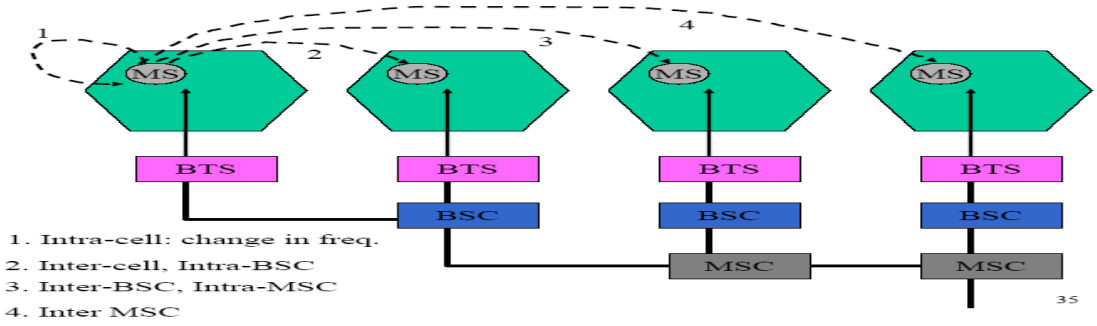
Two reasons for Handover

- The mobile station moves out of range of a BTS or a certain antenna of a BTS respectively. The received signal level decreases continuously The error rate may grow due to interference,
- (MSC, BSC) may decide do Handover may due to load balancing.

The following figure shows four possible handover scenarios in GSM:

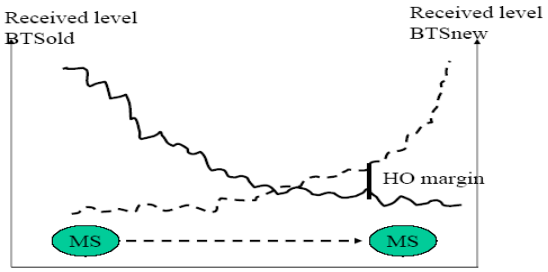
1. **Intra – cell Handover:** When transmission at a certain frequency is impossible the BSC could then decide to change the carrier frequency.
2. **Inter-cell, intra – BSC handover:** The mobile station moves from one cell, to another but stays within the control of the same BSC. The BSC then performs a handover, assigns a new radio channel in the new cell and releases the old one.
3. **Inter – BSC, intra –MSC handover:** As a BSC only controls a limited number of cells; GSM also has to perform handovers between cells controlled by different BSCs. This handover then has to be controlled by the MSC.
4. **Inter MSC Handover:**A handover could be required between two cells belonging to different MSCs. Now both MSCs perform the handover together.





HANDOVER DECISION BASED ON RECEIVED SIGNAL:

- MS and BTS both perform periodic measurements of the downlink and uplink quality respectively.



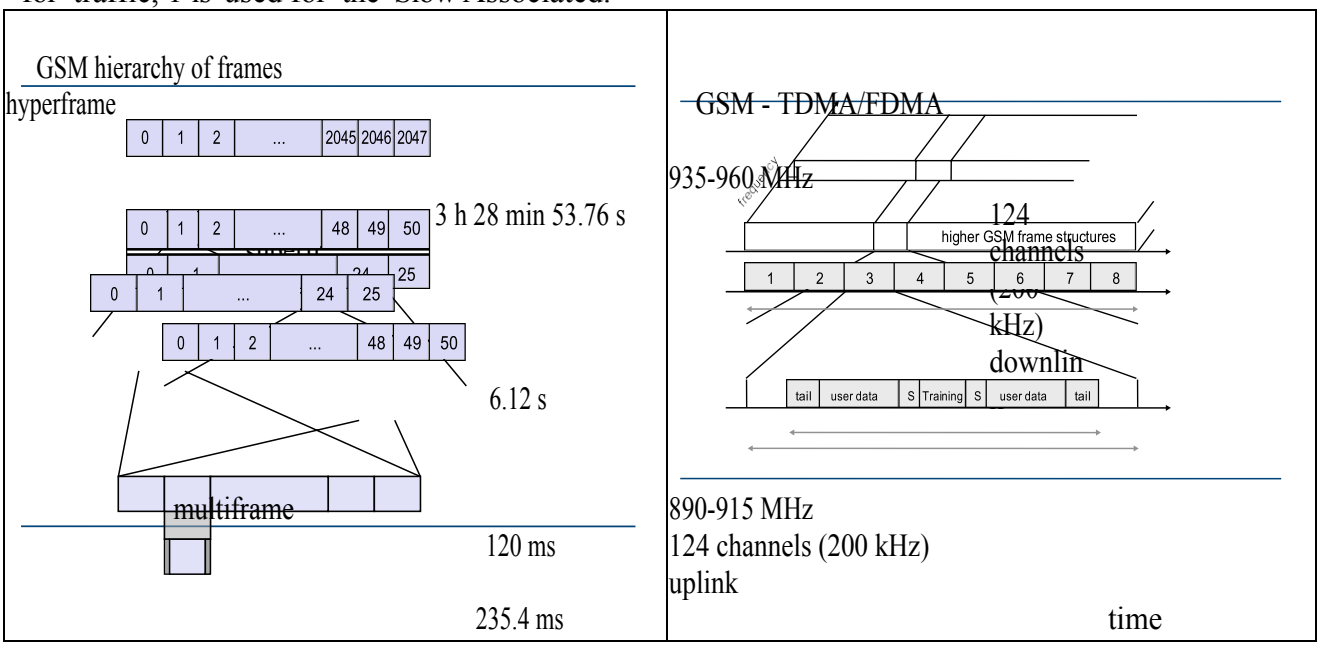
- The MS sends its periodic measurement reports, the BTS (old) forwards these reports to the BSC(old) with its own measurements BSC collects all the values .These values are then compared to thresholds, /the handover margin, to avoid a ping-pong effect.
- Based on these values the BSC may decide to perform a handover and sends the message HO_ required to the MSC. This BSC checks if enough resources are available and activates the physical channel at the BTS (new).The BTS (new) acknowledges the successful channel activation, BSC (new) acknowledges the handover request.
- The MSC then issues the handover command that id is forwarded to the MS.
- H*ard handover* is one in which the channel in the first cell is released and only then the channel in the second cell is engaged. Thus the connection to the source is broken before or 'as' the connection to the target is made—for this reason such handovers are also known as *break-before-make*. When the mobile is between base stations, then the mobile can switch with any of the base stations, so the base stations bounce the link with the mobile back and forth. This is called 'ping-ponging'.
- A *soft handover* is one in which the channel in the source cell is retained and used for a while in parallel with the channel in the target cell. In this case the connection to the target is established before the connection to the source is broken, hence this handover is called *make-before-break*

GSM FREQUENCY ALLOCATION

GSM in general uses, 890-915 MHz are allocated for the uplink (mobile station to base station) and 935-960 MHz for the downlink (base station to mobile station).
Each way the bandwidth for the GSM system is 25 MHz which provides 125 carriers uplink/downlink each having a bandwidth of 200 kHz.In other bands are 1800 MHz and 1900 MHz.

To share the bandwidth for multiple users, GSM uses a combination of TDMA & FDMA. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme.
The fundamental unit of time is called a burst period and it lasts approximately 0.577 ms defines one physical channel. Eight burst periods are grouped into a TDMA frame approximately 4.615 ms, which forms the basic unit for the definition of logical channels.

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames . Out of the 26 frames, 24 are used for traffic, 1 is used for the Slow Associated.



GPRS

- GPRS is introduced as an intermediate step to efficiently transport high-speed data over the current GSM and TDMA-based wireless network infrastructures. GPRS is therefore called the 2.5G
- **GPRS Capacity and End-user Aspects**
- GPRS has the ability to offer data speeds of 14.4 KBps to 171.2 KBps. It allows for short `bursty' traffic, such as e-mailand web browsing, as wellas large volumes of data. GPRS is less costly mobile data service compared to SMS . It offers fast connection set-up mechanism to offer a perception of being 'always on'. This is why GPRS users are sometimes referred to as being 'always connected'.

GPRS Quality of Service (QoS)

- **Service precedence** is the priority of a service in relation to other. Three levels: high, normal, and
- low. **Reliability** Three classes are defined, which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing and corruption of packets.
- **Delay parameters** define maximum values for the mean delay and the 95-percentile delay. It is end-to-end
  transfer time.
- **Throughput** specifies the maximum/peak bit rate and the mean bit rate.

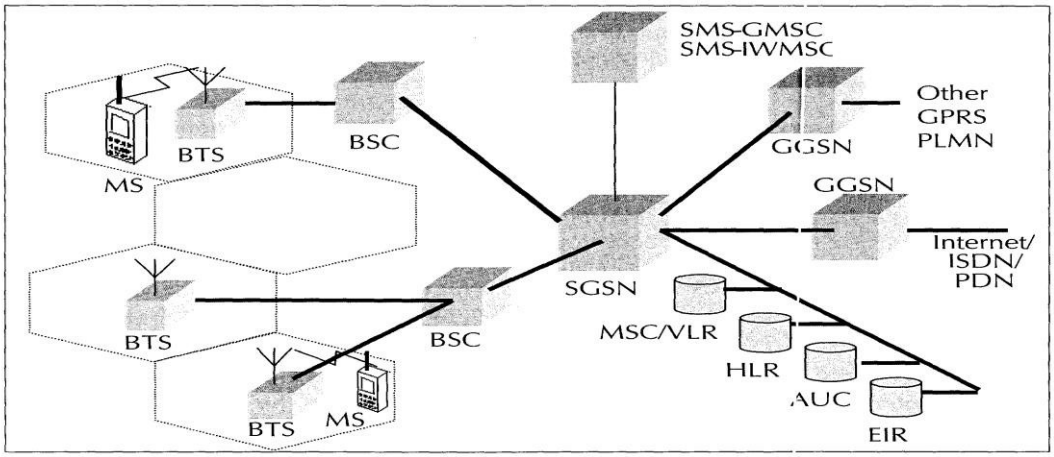
QoS profiles can be negotiated between the mobile user and the network for each session.

GPRS ARCHITECTURE

GPRS uses the GSM architecture for voice. Its network nodes are called GPRS support nodes (GSN). GSNs are responsible for the delivery and routing of data packets between the mobile stations and PDN.

Serving GPRS Support Node (SGSN): (lll[r] to MSC) SGSN's tasks include packet switching, routing, mobility management, logical link management, authentication and charging. The location register of the SGSN stores location information (e.g., current cell, current VLR). SGSN sends queries to HLR to obtain profile data of GPRS
subscribers. It is connected to the base station system with Frame Relay.

Gateway GPRS Support Node (GGSN): GGSN acts as an interface between the GPRS backbone network and the external packet data networks. (lll[r] to that of a router in a LAN). GGSN maintains routing information to tunnel the PDUs to the SGSNs. It converts the GPRS packets coming from SGSN into appropriate packet data protocol (PDP) format. So, GGSN stores the current SGSN address of the user and his or her profile in its location register. It also does authentication and charging functions related to data transfer.



GSM network elements to be enhanced to support packet data:

Base Station System (BSS): BSS system needs enhancement to recognize and send packet data.

This includes BTS upgrade to allow transportation of user data to the SGSN. and support packet data transportation between the BTS and the MS (Mobile Station) over the radio.

Home Location Register (HLR): It needs enhancement to register GPRS user profiles and respond to queries from GSNs regarding profiles.

Mobile Station (MS): It is different from that of GSM.

SMS nodes: SMS-GMSCs and SMS-IWMSCs are upgraded 1.o support SMS transmission via the SGSN. Optionally, the MSC/VLR can be enhanced for more efficient co-ordination of GPRS and non-GPRS services and functionality.

Channel Coding: It is used to protect the transmitted data packets against errors. Reliable coding scheme is used. In this scheme a data rate of 9.05 KBps is achieved per time slot. Under good channel conditions, no encoding scheme , higher data rate of 21.4 KBps per time slot.

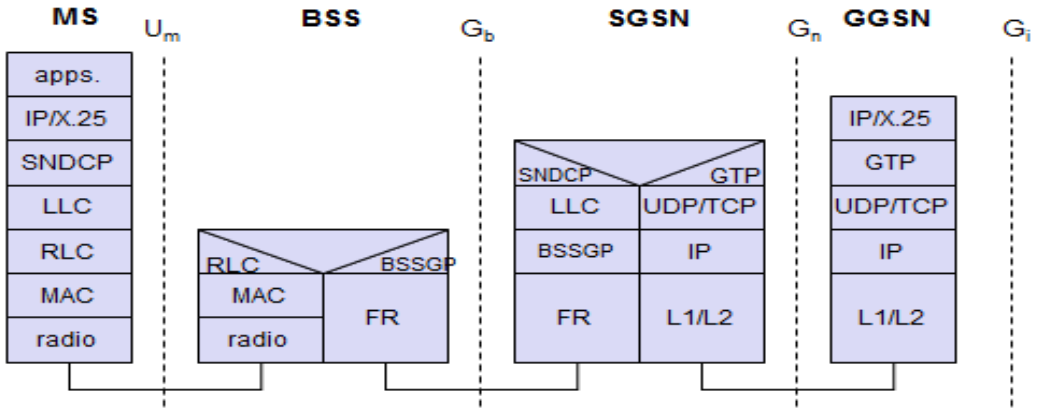
GPRS PROTOCOL ARCHITECTURE

Signaling Plane

It uses the same protocols as GSM but with extension.

An enhanced MAP (Mobile Application Part) is a mobile network-specific extension of the Signaling System SS#7 used in GSM. It transports the signaling information related to location updates, routing information and handovers.

The base station system application part (BSSAP+) is an enhancement of GSM's BSSAP. It is used to transfer signaling information between the SGSN and the VLR.



GPRS Backbone (Between GCSN and SGSN)

GTP protocol tunnels the user data packets through the GPRS backbone with specific routing information. GTP packets carry the user's data packets from both IP and X.25. Below GTP, the standard TCP or UM' are used. TCP is used for X.25 UDP for IP data. Ethernet, ISDN, or ATM-based protocols are lower layer protocols.

BSS-SGSN Interface

- **Sub-Network Dependent Convergence Protocol (SNDCP):** It is used to transfer data packets between SGSN and MS. Its functionality includes:
  Multiplexing, Segmentation, compression, and decompression of user data.
- **Logical Link Control (LLC):** a dll protocol for GPRS which functions lll r
- LAPD.
  Base Station System GPRS Protocol (BSSGP): The BSSGP delivers routing and QoS-related information between BSS and SGSN.
- **Network Service** : This layer manages the convergence sublayer that operates between BSSGP and the Frame Relay Q922 Core by mapping.

Between MS and BSS

Data Link Layer: The data link layer between the MS and the BSS is divided into three sublayers:

- **Logical Link Control** (LLC): It provides a reliable logical link between an MS and its assigned SGSN. Its functionality includes sequence control, in-order delivery, flow control, detection of errors, and retransmission ARQ, Encryption acknowledged and unacknowledged data transmission modes. It is an improved version of the LAPDm.

- **Radio Link Control (RLC):** It establishes a reliable link between the MS and BSS. This includes the segmentation and reassembly of LLC frames into RLC data.
- **Medium Access Control (MAC):** It controls the access attempts of an MS on the radio channel shared by several VISs. It employs algorithms for contention resolution, multiuser multiplexing on a packet data traffic channel (PDTCH), and scheduling and prioritizing based on the negotiated QoS.

Physical Layer : sublayers:

- **Physical Link Layer (PLL**): This layer provides services for information transfer over a physical channel between the MS and the network. These functions include data unit framing, data coding, and the detection and correction of physical medium transmission errors
- **Physical RF Layer (RFL)**: This layer performs the modulation of the physical waveforms based on the sequence of bits received from the Physical Link layer above. The Physical RF layer also demodulates.

GPRS Multiple Access Radio Resource Management

GPRS uses a combination of FDMA and TDMA. GPRS uses two frequency bands : 890-915 MHz for uplink (MS to BTS) and 935-960 MHz for downlink (BTS to MS).
Each of these bands of 25 MHz width is divided into 124 single carrier channels of 200 kHz. Each of these 200 kHz frequency channels is divided into eight time slots. Each time slot of a TDMA frame lasts for duration of 156.25 bit times and contains a data burst.

- On top of the physical channels, a series of logical channels are defined to perform functions like signaling, broadcast of general system information, synchronization, channel assignment, paging or payload transport. In GPRS traffic, channels are only allocated when data packets are sent or received. They are released after the transmission of data. GPRS allows a single mobile station to use multiple time slots of the same TDMA frame for data transmission. This is known as multi slot operation and uses a very flexible channel allocation. One to eight time slots per TDMA frame can be allocated for one mobile station. Moreover, separate uplink and downlink allocation supports asymmetric data traffic like Internet.
- In GPRS, physical channels to transport user data packet is called data traffic channel (PDTCH). The PDTCHs are taken from a common pool of all channels -radio resources of a cell. The mapping of physical channels to either packet switched data (in GPRS mode) or circuit switched data (in GSM mode) services are performed dynamically depending on demand.

GPRS Security

GPRS security functionality is similar to the existing GSM security. The SGSN performs authentication and cipher-setting procedures based on the same algorithms, keys and Criteria as in GSM. GPRS uses a ciphering algorithm optimized for packet data transmission. Like its predecessor, a GPRS device also uses SIM card.

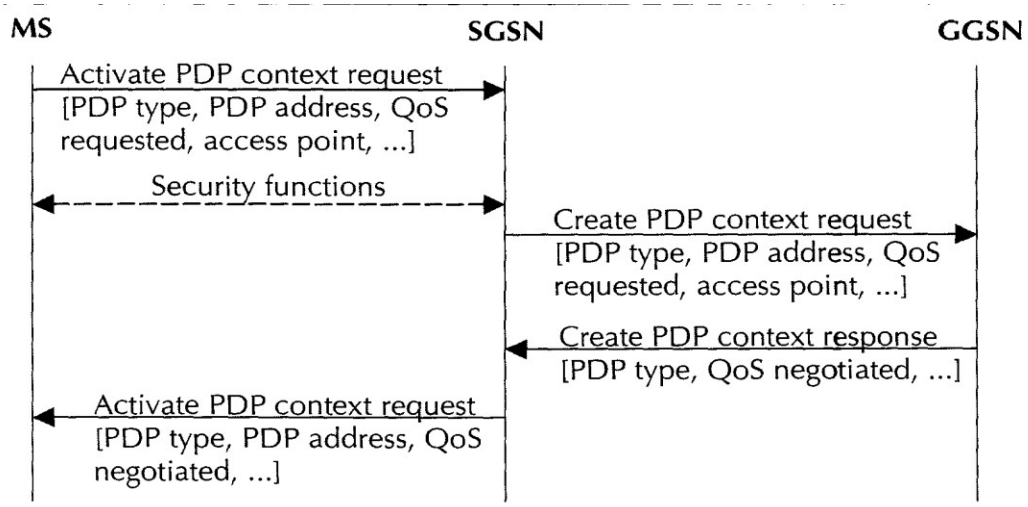
GPRS NETWORK OPERATIONS

Once a GPRS mobile station is powered on, it 'introduces' itself to the network by sending a –GPRS
attach‖ request

Attachment and Detachment Procedure

- MS must **register** itself with an SGSN of the network (i.e) a logical link between the MS and the SGSN. The network checks if the MS is authorized to use the services; if so, it copies the user profile from the HLR to the SGSN, and **assigns a Packet-TMSI** to the MS.
- Then, MS must **apply for an address** . This address is called PDP (Packet Data Protocol) address. For each session, a PDP context is created. It contains the PDP type, the address assigned, the requested QoS, and the address of the GGSN. This context is stored in the MS, the SGSN and the GGSN. Now the MS is 'visible' to the external PDN.

- User data is transferred through GTP encapsulation and tunneling. User data can be compressed and encrypted for efficiency and reliability. The allocation of the PDP address can be static or dynamic. GGSN is responsible for the dynamic PDP address assignment allocation



PDP context activation procedure

- 'activate PDP context request,' -MS informs the SGSN about the requested PDP
- context 'create PDP context request' – from SGSN to the GGSN if authentication is successful.

GGSN creates a new entry in its PDP context table to route between SGSN and external PDN.

- 'create PDP context response' - GGSN returns confirmation to SGSN with the PDP address
- _activate PDP context accept'-SGSN updates its PDP table and confirms the activation to MS.

- The disconnection from the GPRS network is called **GPRS detach**. All the resources are released following a GPRS detach. Detach process can be initiated by the mobile station or by the network.

GPRS Mobility Management

- As a mobile station moves from one area to another, SGSNs communicate with each other to update the MS's location in the relevant registers. The mobile station's profiles are preserved in the VLRs that are accessible to SGSNs via the local MSC. A logical link is established and

maintained between the mobile station and the SGSN at each PLMN.

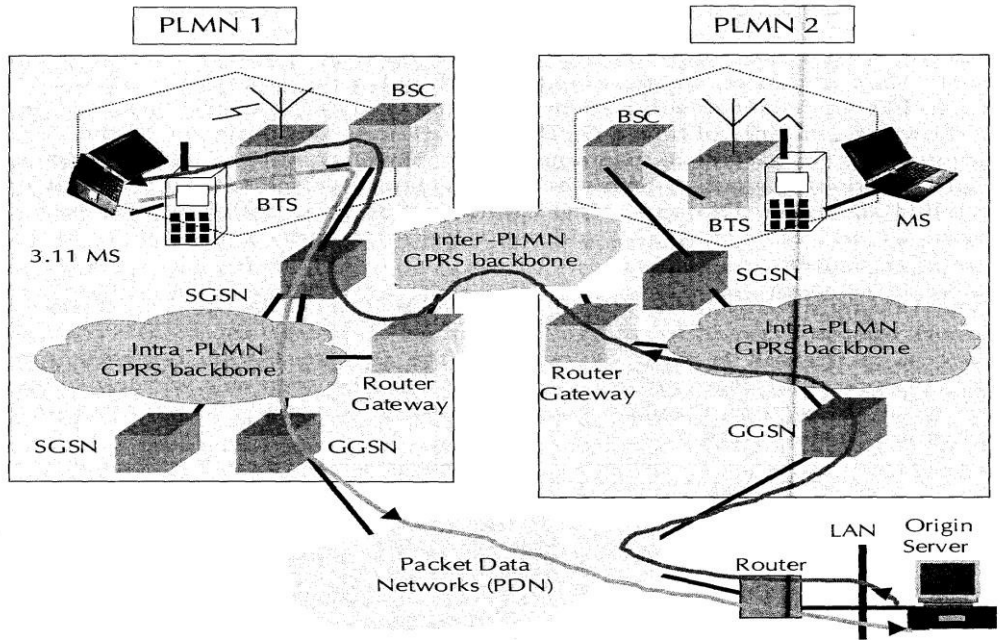
- ***Routing*** Consider two intra-PLMN backbone networks of different PLMNs. Intra-PLMN backbone networks connect GSNs of the same PLMN or the same network operator.

- These intra-PLMN networks are connected with an inter-PLMN backbone. An inter-PLMN backbone network connects GSNs of different PLMNs and operators.

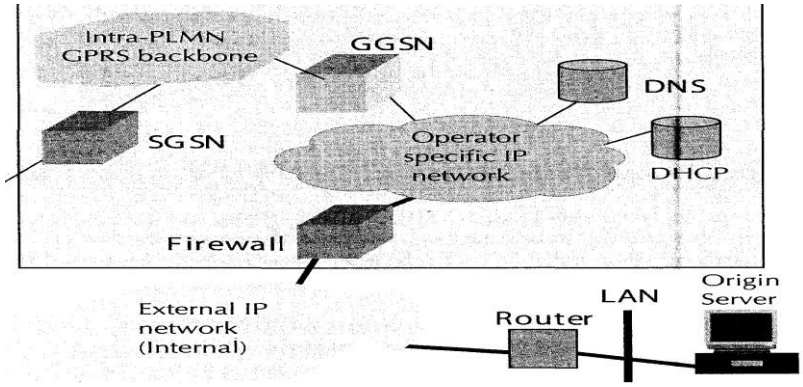
- The gateways between the PLMNs and the external inter-PLMN backbone are called border gateways. They perform security functions to protect against unauthorized users and attacks.

- **From MS:** A GPRS mobile station located in PLMN1 sends IP packets to a host connected to the IP network, The SGSN that the mobile station is registered with encapsulates the IP packets coming from the mobile station, examines the PDP context and routes them through the intra-PLMN GPRS backbone to the appropriate GGSN. The GGSN decapsulates the packets and sends them out on the IP network,

- **TO MS:** Let us assume the home-PLMN of the MS is PLMN2. MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2. The packets are sent out onto the IP network and are routed to the GGSN of PLMN2 (the home-GGSN of the MS). The latter queries the HLR and obtains the information that the MS is currently located in PLMN1. It encapsulates
  the incoming IP packets and tunnels them through the inter-PLMN GPRS backbone to the appropriate SGSN in PLMN1. The SGSN decapsulates the packets and delivers them to the MS.



Communicating with the IP Networks



- GPRS supports both IPv4 and IPv6. Each registered user gets an IP address from the address space of the GPRS operator maintained by a DHCP. The address resolution between IP address and GSM address is performed by the GGSN, using the appropriate PDP context. DNS managed by the GPRS operator or the external IP network operator is used to resolve host names.

- To protect the PLMN from unauthorized access, a firewall is installed between the private GPRS network and the external IP network. The mobile user has direct connection to the Internet.

BEAR ER SER VICE S in GPRS

It offers end-to-end packet switched data transfer. It supports: the point-to-point (PTP) service and the point-to- multipoint (PTM) service.

DATA **Services in GPRS**

SMS: It was originally designed for GSM network. GPRS will continue to support SMS as a bearer.

WAP: It is a data bearer service over HTTP protocol.

MMS: MMS is Multimedia Messaging Service. This is the next generation messaging service.

Two mode of services are **Application mode** or **Tunneling mode.**

- **Application mode: Users** use GPRS mobile phone to access the applications running on the phone itself. The phone is the end user device. This mode supports mobile execution environment. These devices support development of client application that can run on the device --- Symbian and J2ME.
- **Tunneling mode:** This mode is for mobile computing where the user will use the GPRS interface as an access to the network. For, end user device like laptop computer or small footprint device like PDAs, access can be gained via a PC Card (PCMCI) or via a serial cable to a GPRS-capable phone.

GPRS Handsets three classes: A, **B** or C. A Class A terminal

Class A terminal can make or receive calls on two services simultaneously. GPRS VC will be held or placed on busy. It supports GPRS data and other GSM services such as SMS and voice simultaneously.

Class B terminal can monitor GSM and GPRS channels simultaneously, but can support only one of these services at any time. It can support simultaneous attach, activation, and monitor but not simultaneous traffic.

Class C terminal supports only non-simultaneous attach. It can make or receive calls from only the manually selected network service. Support of SMS is optional for Class C terminals.

APPLICATIONS OF GPRS

Generic Applications

Information services, Internet access, email, Web Browsing, mass market applications offering contents like sports scores, weather, flight information, news headlines, prayer reminders, lottery results, jokes, horoscopes, traffic information ,Access to corporate net, Intranet Mobile commerce Banking over wireless

GPRS-Specific Applications

- **Chat** GPRS will offer ubiquitous chat by integrating Internet chat and wireless chat using SMS and WAP.
- **Multimedia Service:** Multimedia objects like photographs, pictures and presentations, static web pages can be sent and received over the mobile network.
- **Virtual Private Network:** GPRS network can be used to offer VPN services. Many banks 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 are kept in the phone some in the organizer and some in the Intranet.
- **Job Sheet Dispatch:** GPRS can be used to assign and communicate job sheets from office-based staff to mobile field staff. It can be combined with vehicle positioning applications so that the nearest 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.
- **Vehicle Positioning:** This application integrates GPS that tell people 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 and services 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.

LIMITATIONS OF GPRS

- **Limited Cell Capacity for All Users:** limited radio resources. Voice and GPRS calls use the same resources.
- **Speed Lower in Reality:** Achieving the theoretical maximum GPRS speed (172.2 kbps) would require a single user taking over all 8 time slots without any error protection. But GPRS can support only 1/2/3 slots
- **GPRS Mobile Terminate Connection for a Mobile Server not Supported: S**erver needs to be mobile for mobile healthcare center for rural population. Using GPRS network, such communication is not possible.

UMTS - Universal Mobile Telecommunications System.

UMTS is one of the emerging mobile phone technologies known as third-generation, or *3G*. Third-generation systems are designed to include such traditional phone tasks as calls, voice mail, and paging, but also new technology tasks such as Internet access, video, and SMS, or text messaging.

One of the main benefits of UMTS is its speed. Current rates of transfer for broadband information are 2 Mbits a second. This speed makes possible the kind of streaming video that can support movie downloads and video conferencing. In a sense, UMTS makes it possible for you to enjoy all of the functionality of your home computer while you are roaming. By combining wireless and satellite cellular technologies, UMTS takes advantage of all existing options to result in the Holy Grail of 3G presentation: seamless transitions between WiFi and satellite.

Universal Mobile Telecommunication System

The Universal Mobile Telecommunication System (UMTS) is a third generation (3G) mobile communications system that provides a range of broadband services to the world of wireless and mobile communications. The UMTS delivers low-cost, mobile communications at data rates of up to 2 Mbps. It preserves the global roaming capability of second generation GSM/GPRS networks and provides new enhanced capabilities. The UMTS is designed to deliver pictures, graphics, video communications, and other multimedia information, as well as voice and data, to mobile wireless subscribers.

The UMTS takes a phased approach toward an all-IP network by extending second generation (2G) GSM/GPRS networks and using Wide-band Code Division Multiple Access (CDMA) technology. Handover capability between the UMTS and GSM is supported. The GPRS is the convergence point between the 2G technologies and the packet-switched domain of the 3G UMTS.

UMTS Services

The UMTS provides support for both voice and data services. The following data rates are targets for UMTS:

- 144 kbps—Satellite and rural outdoor
- 384 kbps—Urban outdoor
- 2048 kbp—Indoor and low range outdoor

Data services provide different quality-of-service (QoS) parameters for data transfer. UMTS network services accommodate QoS classes for four types of traffic:

- Conversational class—Voice, video telephony, video gaming
- Streaming class—Multimedia, video on demand, webcast
- Interactive class—Web browsing, network gaming, database access
- Background class—E-mail, short message service (SMS), file downloading

The UMTS supports the following service categories and applications:

- Internet access—Messaging, video/music download, voice/video over IP, mobile commerce (e.g., banking, trading), travel and information services
- Intranet/extranet access—Enterprise application such as e-mail/messaging, travel assistance, mobile sales, technical services, corporate database access, fleet/warehouse management, conferencing and video telephony
- Customized information/entertainment—Information (photo/video/music download), travel assistance, distance education, mobile messaging, gaming, voice portal services
- Multimedia messaging—SMS extensions for images, video, and music; unified messaging; document transfer
- Location-based services—Yellow pages, mobile commerce, navigational service, trading

UMTS Architecture

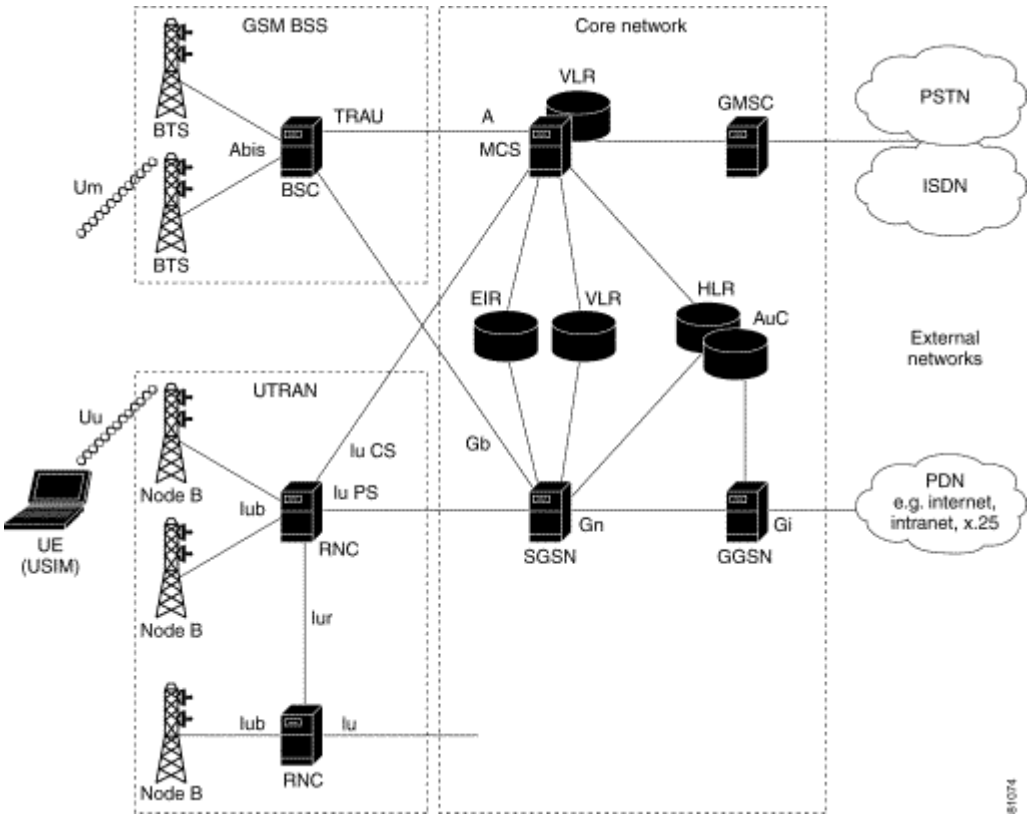
The public land mobile network (PLMN) described in UMTS Rel. '99 incorporates three major categories of network elements:

- GSM phase 1/2 core network elements—Mobile services switching center (MSC), visitor location register (VLR), home location register (HLR), authentication center (AuC), and equipment identity register (EIR)
- GPRS network elements—Serving GPRS support node (SGSN) and gateway GPRS support node (GGSN)
- UMTS-specific network elements—User equipment (UE) and UMTS terrestrial radio access network (UTRAN) elements

The UMTS core network is based on the GSM/GPRS network topology. It provides the switching, routing, transport, and database functions for user traffic. The core network contains circuit-switched elements such as the MSC, VLR, and gateway MSC (GMSC). It also contains the packet-switched elements SGSN and GGSN. The EIR, HLR, and AuC support both circuit- and packet-switched data.

The Asynchronous Transfer Mode (ATM) is the data transmission method used within the UMTS core network. ATM Adaptation Layer type 2 (AAL2) handles circuit-switched connections. Packet connection protocol AAL5 is used for data delivery.

UMTS Architecture



General Packet Radio System

The General Packet Radio System (GPRS) facilitates the transition from phase1/2 GSM networks to 3G UMTS networks. The GPRS supplements GSM networks by enabling packet switching and allowing direct access to external packet data networks (PDNs). Data transmission rates above the 64 kbps limit of integrated services digital network (ISDN) are a requirement for the enhanced services supported by UMTS networks. The GPRS optimizes the core network for the transition to higher data rates. Therefore, the GPRS is a prerequisite for the introduction of the UMTS.

UMTS Interfaces

The UMTS defines four new open interfaces

- *Uu* interface—User equipment to Node B (the UMTS WCDMA air interface)

- *Iu* interface—RNC to GSM/GPRS (MSC/VLR or SGSN)
  - *Iu-CS*—Interface for circuit-switched data
  - *Iu-PS*—Interface for packet-switched data
- *Iub* interface—RNC to Node B interface
- *Iur* interface—RNC to RNC interface (no equivalent in GSM)

The *Iu*, *Iub*, and *Iur* interfaces are based on the transmission principles of aynchronous transfer mode (ATM).

UMTS Terrestrial Radio Access Network

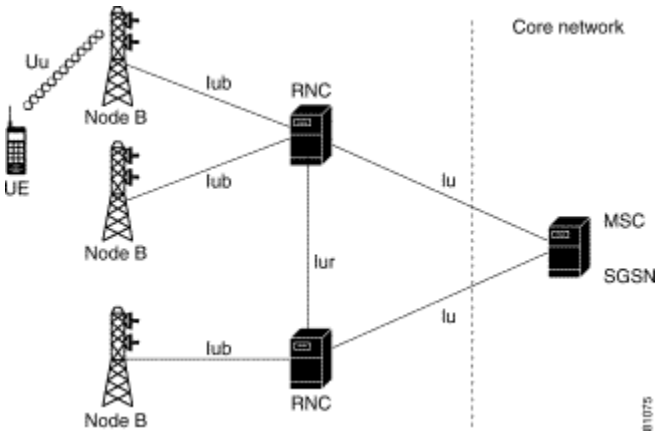
The major difference between GSM/GPRS networks and UMTS networks is in the air interface transmission. Time division multiple access (TDMA) and freqency division multiple access (FDMA) are used in GSM/GPRS networks. The air interface access method for UMTS networks is wide-band code division multiple access (WCDMA), which has two basic modes of operation: frequency division duplex (FDD) and time division duplex (TDD). This new air interface access method requires a new radio access network (RAN) called the UTMS terrestrial RAN (UTRAN). The core network requires minor modifications to accommodate the UTRAN.

Two new network elements are introduced in the UTRAN: the radio network controller (RNC) and Node B. The UTRAN contains multiple radio network systems (RNSs), and each RNS is controlled by an RNC. The RNC connects to one or more Node B elements. Each Node B can provide service to multiple cells.

The RNC in UMTS networks provides functions equivalent to the base station controller (BSC) functions in GSM/GPRS networks. Node B in UMTS networks is equivalent to the base transceiver station (BTS) in GSM/GPRS networks. In this way, the UMTS extends existing GSM and GPRS networks, protecting the investment of mobile wireless operators. It enables new services over existing interfaces such as *A*, *Gb*, and *Abis*, and new interfaces that include the UTRAN interface between Node B and the RNC (*Iub*) and the UTRAN interface between two RNCs (*Iur*).

The network elements of the UTRAN are shown below:

Figure 2-18 UTRAN Architecture



Radio Network Controller

The radio network controller (RNC) performs functions that are equivalent to the base station controller (BSC) functions in GSM/GPRS networks. The RNC provides centralized control of the Node B elements in its covering area. It handles protocol exchanges between UTRAN interfaces (*Iu*, *Iur*, and *Iub*). Because the interfaces are ATM-based, the RNC performs switching of ATM cells between the interfaces. Circuit-switched and packet-switched data from the *Iu-CS* and *Iu-PS* interfaces are multiplexed together for transmission over the Iur, Iub, and Uu interfaces to and from the user equipment (UE). The RNC provides centralized operation and maintenance of the radio network system (RNS) including access to an operations support system (OSS).

The RNC uses the *Iur* interface. There is no equivalent to manage radio resources in GSM/GPRS networks. In GSM/GPRS networks, radio resource management is performed in the core network. In UMTS networks, this function is distributed to the RNC, freeing the core network for other functions. A single

serving RNC manages serving control functions such as connection to the UE, congestion control, and handover procedures. The functions of the RNC include:

- Radio resource control
- Admission control
- Channel allocation
- Power control settings
- Handover control
- Macro diversity
- Ciphering
- Segmentation and reassembly
- Broadcast signalling
- Open loop power control

Node B

Node B is the radio transmission/reception unit for communication between radio cells. Each Node B unit can provide service for one or more cells. A Node B unit can be physically located with an existing GSM base transceiver station (BTS) to reduce costs of UMTS implementation. Node B connects to the user equipment (UE) over the *Uu* radio interface using wide-band code division multiple access (WCDMA). A single Node B unit can support both frequency division duplex (FDD) and time division duplex (TDD) modes. The *Iub* interface provides the connection between Node B and the RNC using asynchronous transfer mode (ATM). Node B is the ATM termination point.

The main function of Node B is conversion of data on the *Uu* radio interface. This function includes error correction and rate adaptation on the air interface. Node B monitors the quality and strength of the connection and calculates the frame error rate, transmitting this information to the RNC for processing. The functions of Node B include:

- Air interface transmission and reception
- Modulation and demodulation
- CDMA physical channel coding
- Micro diversity
- Error handling
- Closed loop power control

Node B also enables the UE to adjust its power using a technique called downlink transmission power control. Predefined values for power control are derived from RNC power control parameters.

UMTS User Equipment

The UMTS user equipment (UE) is the combination of the subscriber's mobile equipment and the UMTS subscriber identity module (USIM). Similar to the SIM in GSM/GPRS networks, the USIM is a card that inserts into the mobile equipment and identifies the subscriber to the core network.

The USIM card has the same physical characteristics as the GSM/GPRS SIM card and provides the following functions:

- Supports multiple user profiles on the USIM
- Updates USIM information over the air
- Provides security functions
- Provides user authentication
- Supports inclusion of payment methods
- Supports secure downloading of new applications

The UMTS standard places no restrictions on the functions that the UE can provide. Many of the identity types for UE devices are taken directly from GSM specifications. These identity types include:

- International Mobile Subscriber Identity (IMSI)
- Temporary Mobile Subscriber Identity (TMSI)
- Packet Temporary Mobile Subscriber Identity (P-TMSI)
- Temporary Logical Link Identity (TLLI)
- Mobile station ISDN (MSISDN)
- International Mobile Station Equipment Identity (IMEI)
- International Mobile Station Equipment Identity and Software Number (IMEISV)

The UMTS UE can operate in one of three modes of operation:

- PS/CS mode—The UE is attached to both the packet-switched (PS) and circuit-switched (CS) domain, and the UE can simultaneously use PS and CS services.
- PS mode—The MS is attached to the PS domain and uses only PS services (but allows CS-like services such as voice over IP [VoIP]).
- CS mode—The MS is attached to the CS domain and uses only CS services.