CHAPTER 5

Global System for Mobile Communications (GSM)

5.1 GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

GSM is much more than just an acronym for Global System for Mobile Communication. It signifies an extremely successful technology and bearer for mobile communication system. GSM today covers 71% of all the digital wireless market. The mobile telephone has graduated from being a status symbol to a useful appliance. People use it not only in business but also in personal life. Its principal use is for wireless telephony, and messaging through SMS. It also supports facsimile and data communication.

GSM is based on a set of standards, formulated in the early 1980s (see Table 5.1 for the GSM timeline). In 1982, the Conference of European Posts and Telegraphs (CEPT) formed a study group called the Groupe Spécial Mobile (GSM) to study and develop a pan-European mobile system, which was later rechristened as Global System for Mobile Communication. See Chapter 1 for cellular network evolution and standards. The proposed GSM system had to meet certain business objectives. These are:

- Support for international roaming.
- Good speech quality.
- Ability to support handheld terminals.
- Low terminal and service cost.
- Spectral efficiency.
- Support for a range of new services and facilities.
- ISDN compatibility.

Due to its innovative technologies and strengths, GSM rapidly became truly global. Many of the new standardization initiatives came from outside Europe. Depending on locally available frequency bands, different air interfaces were defined. Of these prominent ones are 900 MHz, 1800 MHz and 1900 MHz. However, architecture, protocols, signaling and roaming are identical in all networks independent of the operating frequency bands.

Table 5.1 GSM history timeline

Year	*Event*
1982	Groupe Spécial Mobile (GSM) established
1987	Essential elements of wireless transmission specified
1989	GSM becomes an ETSI technical committee
1990	Phase 1 GSM 900 specification (designed 1987 through 1990) frozen
1991	First GSM network launched
1993	First roaming agreement came into effect
1994	Data transmission capability launched
1995	Phase 2 launched. Fax and SMS roaming services offered
2002	SMS volume crosses 24 billion/year, 750 million subscribers

GSM uses a combination of FDMA (Frequency Division Multiple Access) and TDMA (Time Division Multiple Access). See Section 3.2 for definition of these multiple access procedures. The GSM system has an allocation of 50 MHz (890–915 MHz and 935–960 MHz) bandwidth in the 900 MHz frequency band. 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 eight time slots. Therefore, with the combination of FDMA and TDMA we can realize a maximum of 992 channels for transmitting and receiving. In order to be able to serve hundreds of thousands of users, the frequency must be reused. This is done through cells.

The frequency reuse concept led to the development of cellular technology as originally conceived by AT&T and Bell Labs way back in 1947. The essential characteristics of this reuse are as follows:

- The area to be covered is subdivided into radio zones or cells (Fig. 5.1). Though in reality these cells could be of any shape, for convenient modeling purposes these are modeled as hexagons. Base stations are positioned at the center of these cells.
- Each cell i receives a subset of frequencies fbi from the total set assigned to the respective mobile network. To avoid any type of co-channel interference, two neighboring cells never use the same frequencies.
- Only at a distance of D (known as frequency reuse distance), the same frequency from the set fbi can be reused. Cells with distance D from cell i, can be assigned one or all the frequencies from the set fbi belonging to cell i.
- When moving from one cell to another during an ongoing conversation, an automatic channel change occurs. This phenomenon is called handover. Handover maintains an active speech and data connection over cell boundaries.

The regular repetition of frequencies in cells result in a clustering of cells. The clusters generated in this way can consume the whole frequency band. The size of a cluster is defined by k, the number of cells in the cluster. This also defines the frequency reuse distance D. Figure 5.1 shows an example of a cluster size of 4.

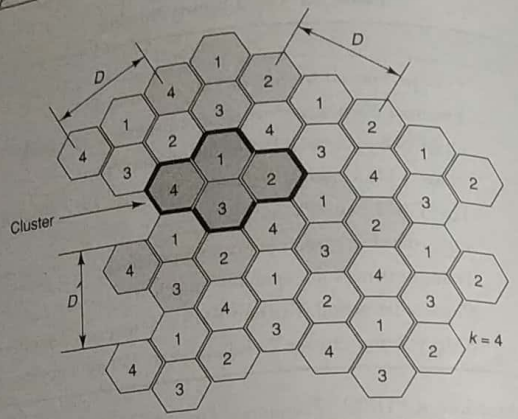


Figure 5.1 Cell Clusters in GSM

5.2 GSM Architecture

GSM networks are structured in hierarchic fashion (Fig. 5.2). It consists at the minimum administrative region assigned to one MSC (Mobile Switching Centre). The administrative re is commonly known as PLMN (Public Land Mobile Network). Each administrative regio subdivided into one or many Location Area (LA). One LA consists of many cell groups. Each group is assigned to one BSC (Base Station Controller). For each LA there will be at least one B Cells in one BSC can belong to different LAs.

Cells are formed by the radio areas covered by a BTS (Base Transceiver Station) (Fig. Several BTSs are controlled by one BSC. Traffic from the MS (Mobile Station) is routed thro MSC. Calls originating from or terminating in a fixed network or other mobile networks is hand by the GMSC (Gateway MSC). Figure 5.3 depicts the architecture of a GSM PLMN fr technology point of view, whereas Figure 5.4 depicts the same architecture from the operato point of view.

For all subscribers registered with a cellular network operator, permanent data such as service profile is stored in the Home Location Register (HLR). The data relate to the follow information:

- Authentication information like International Mobile Subscriber Identity (IMSI).
- Identification information like name, address, etc., of the subscriber.
- Identification information like Mobile Subscriber ISDN (MSISDN), etc.
- Billing information like prepaid or postpaid customer.
- Operator selected denial of service to a subscriber.

- Handling of supplementary services like for CFU (Call Forwarding Unconditional), CFB (Call Forwarding Busy), CFNR (Call Forwarding Not Reachable) or CFNA (Call Forwarding Not Answered).

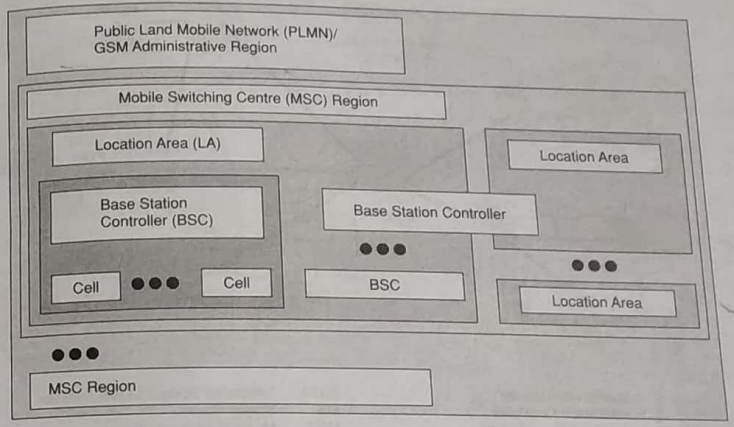


Figure 5.2 GSM System Hierarchy

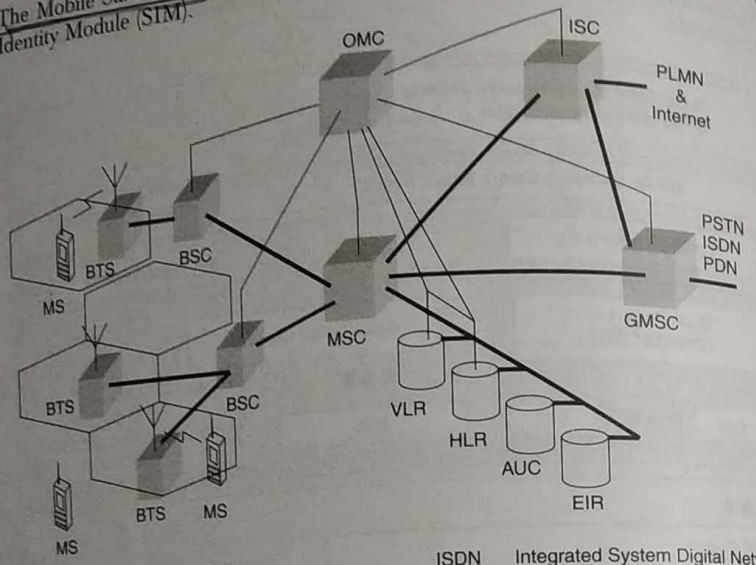
- Storage of SMS Service Center (SC) number in case the mobile is not connectable so that whenever the mobile is connectable, a paging signal is sent to the SC.
- Provisioning information like whether long distance and international calls are allowed or not.
- Provisioning information like whether roaming is enabled or not.
- Information related to auxiliary services like Voice mail, data, fax services, etc.
- Information related to auxiliary services like CLI (Caller Line Identification), etc.
- Information related to supplementary services for call routing. In GSM network, one can customize the personal profile to the extent that while the subscriber is roaming in a foreign PLMN, incoming calls can be barred. Also, outgoing international calls can be barred, etc.

There is some variable information, which could also be part of the HLR. This includes the pointer to the VLR, location area of the subscriber, Power OFF status of the handset, etc.

5.3 GSM Entities

The GSM technical specifications define different entities that form the GSM network by defining their functions and interface requirements. The GSM network can be divided into five main groups (Fig. 5.4):

- The Mobile Station (MS). This includes the Mobile Equipment (ME) and the Subscriber Identity Module (SIM).



AUC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
EIR	Equipment Identity Register
GMSC	Gateway MSC
HLR	Home Location Register
ISC	International Switching Center
ISDN	Integrated System Digital Network
MS	Mobile Station
MSC	Mobile Switching Center
OMC	Operation and Maintenance Center
PDN	Packet Data Network
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
VLR	Visitor Location Register

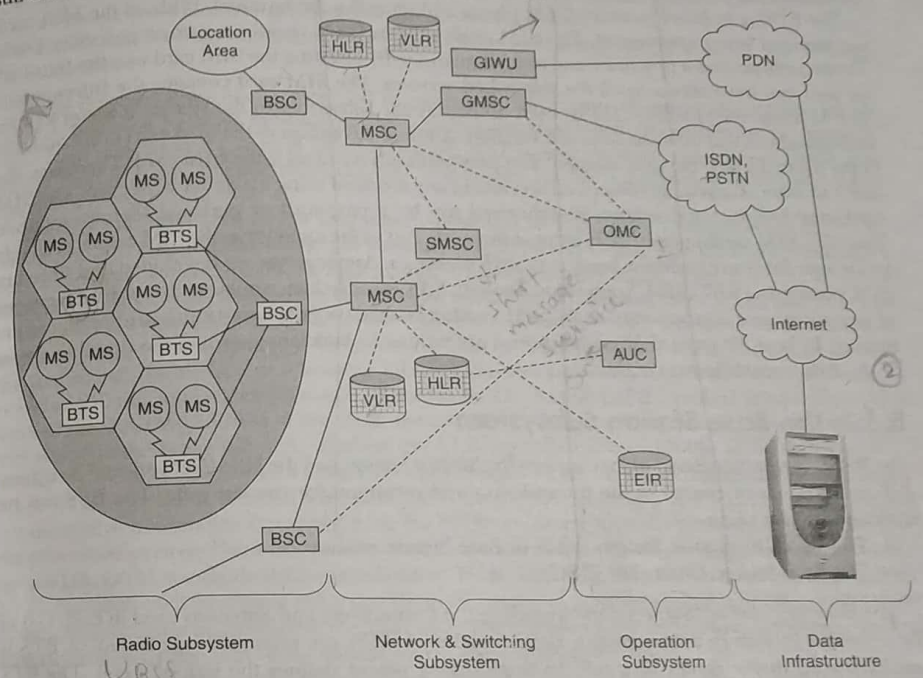
Figure 5.3 Architecture of GSM

- The Base Station Subsystem (BSS). This includes the Base Transceiver Station (BTS) and the Base Station Controller (BSC).
- The Network and Switching Subsystem (NSS). This includes Mobile Switching Center (MSC), Home Location Register (HLR), Visitor Location Register (VLR), Equipment Identity Register (EIR), and the Authentication Center (AUC).
- The Operation and Support Subsystem (OSS). This includes the Operation and Maintenance Center (OMC).
- The data infrastructure that includes Public Switched Telephone Network (PSTN), Integrated System Digital Network (ISDN), and the Public Data Network (PDN).

5.3.1 Mobile Station

Mobile Station is the technical name of the mobile or the cellular phone. In early days mobile phones were a little bulky and were sometimes installed in cars like other equipment. Even the

handheld terminals were quite big. Though the phones have become smaller and lighter, they are still called Mobile Stations. MS consists of two main elements:



AUC	Authentication Center	MS	Mobile Station
BSC	Base Station Controller	MSC	Mobile Switching Center
BTS	Base Transceiver Station	OMC	Operation and Maintenance Center
EIR	Equipment Identity Register	PDN	Public Data Network
GIWU	Gateway Interworking Unit	PSTN	Public Switched Telephone Network
GMSC	Gateway MSC	SC	Service Center/SMS Controller
HLR	Home Location Register	SMSC	Short Message Service Center
ISDN	Integrated System Digital Network	VLR	Visitor Location Register

Figure 5.4 System Architecture of GSM

- The mobile equipment or the mobile device. In other words, this is a phone without the SIM card.
- The Subscriber Identity Module (SIM).

There are different types of terminals distinguished principally by their power and application. The handheld GSM terminals have experienced the highest evolution. The weight and volume of

these terminals are continuously decreasing. The life of a battery between charging is also increasing. The evolution of technologies allowed decrease of power requirement to less than 1 W.

The SIM is installed in every GSM phone and identifies the terminal. Without the SIM card, the terminal is not operational. The SIM cards used in GSM phones are smart processor cards. These cards possess a processor and a small memory. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. The SIM card contains the International Mobile Subscriber Identity (IMSI) used to identify the subscriber to the system, a secret key for authentication, and other security information. Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using his or her SIM card. The SIM card may be protected against unauthorized use by a password or personal identity number. Typically, SIM cards contain 32 K bytes of memory. Part of the memory in the SIM card is available to the user for storing address book and SMS messages. Applications are developed and stored in SIM cards using SAT (SIM Application Toolkit). SAT is something similar to Assembly languages of computers and is proprietary to the SIM vendor. Nowadays Java Smart cards are coming to the market. In Java Smart card, the applications are written in Java language and are portable across SIM cards from different vendors.

5.3.2 The Base Station Subsystem

The BSS (Base Station Subsystem) connects the Mobile Station and the NSS (Network and Switching Subsystem). It is in charge of the transmission and reception for the last mile. The BSS can be divided into two parts:

- The Base Transceiver Station (BTS) or Base Station in short.
- The Base Station Controller (BSC).

The Base Transceiver Station corresponds to the transceivers and antennas used in each cell of the network. In a large urban area, a large number of BTSs are potentially deployed. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. The BTS houses the radio transmitter and the receivers that define a cell and handles the radio-link protocols with the Mobile Station. Each BTS has between one and 16 transceivers depending on the density of users in the cell.

Base Station Controller is the connection between the BTS and the Mobile service Switching Center (MSC). The BSC manages the radio resources for one or more BTSs. It handles handovers, radio-channel setup, control of radio frequency power levels of the BTSs, exchange function, and frequency hopping.

5.3.3 The Network and Switching Subsystem

The central component of the Network Subsystem is the Mobile Switching Center (MSC). It does multiple functions. They are:

- It acts like a normal switching node for mobile subscribers of the same network (connection between mobile phone to mobile phone within the same network).
- It acts like a normal switching node for the PSTN fixed telephone (connection between mobile phone to fixed phone).

- It acts like a normal switching node for ISDN.
- It provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers and call routing.
- It includes databases needed in order to store information to manage the mobility of a roaming subscriber.

These different services are provided in conjunction with several functional entities, which together form the Network Subsystem. The signaling between functional entities in the Network Subsystem uses Signaling System Number 7 (SS7). SS7 is used for trunk signaling in ISDN and widely used in today's public networks. SS7 is also used for SMS, prepaid, roaming and other intelligent network functions.

The MSC together with Home Location Register (HLR) and Visitor Location Register (VLR) databases, provide the call-routing and roaming capabilities of GSM. The HLR is considered a very important database that stores information of subscribers belonging to the covering area of a MSC. Although a HLR may be implemented as a distributed database, there is logically only one HLR per GSM network. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network. This includes information like current location of the mobile, all the service provisioning information and authentication data. When a phone is powered off, this information is stored in the HLR. The location of the mobile is typically in the form of the signaling address of the VLR associated with the mobile station. HLR is always fixed and stored in the home network, whereas the VLR logically moves with the subscriber.

The VLR can be considered a temporary copy of some of the important information stored in the HLR. 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 of the subscribed services. This is true for each mobile currently located in the geographical area controlled by a VLR. GSM standards define interfaces to HLR; however, there is no interface standard for VLR. Although each functional entity can be implemented as an independent unit, all manufacturers of switching equipment implement the VLR as an integral part of the MSC, so that the geographical area controlled by the MSC corresponds to that controlled by the VLR.

Note: MSC contains no information about a particular mobile station—this information is stored in location registers.

When a subscriber enters the covering area of a new MSC, the VLR associated with this MSC will request information about the new subscriber from its corresponding HLR in the home network. For example, if a subscriber of a GSM network in Bangalore is roaming in Delhi, the HLR data of the subscriber will remain in Bangalore with the home network, however, the VLR data will be copied to the roaming network in Delhi. The VLR will then have enough information in order to assure the subscribed services without needing to refer to the HLR each time a communication is established. Though the visiting network in Delhi will provide the services, the billing for the services will be done by the home network in Bangalore.

Within the NSS there is a component called Gateway MSC (GMSC) that is associated with the MSC. A gateway is a node interconnecting two networks. The 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. The GMSC is often implemented in the same node as the MSC. Like the GMSC, there is another node called GIWU (GSM Interworking Unit). The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

5.3.4 The Operation and Support Subsystem (OSS)

As the name suggests, Operations and Support Subsystem (OSS) controls and monitors the GSM system. The OSS is connected to different components of the NSS and to the BSC. It is also in charge of controlling the traffic load of the BSS. However, the increasing number of base stations, due to the development of cellular radio networks, has resulted in some of the maintenance tasks being transferred to the BTS. This transfer decreases considerably the costs of maintenance of the system. Provisioning information for different services is managed in this subsystem.

Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment within the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). EIR contains a list of IMEIs of all valid terminals. An IMEI is marked as invalid if it has been reported stolen or is not type approved. The EIR allows the MSC to forbid calls from this stolen or unauthorized terminals.

Authentication Center (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 subscriber's SIM card. These data help to verify the user's identity.

5.3.5 Message Centre

Short Message Service or SMS is one of the most popular services within GSM. SMS is a data service and allows a user to enter text message up to 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit characters (some European alphabets or binary data) are used, and 70 characters in length when non-Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16-bit Unicode). SMS is a proactive bearer and is an always ON network. Message center is also referred to as Service Centre (SC) or SMS Controller (SMSC). SMSC is a system within the core GSM network, which works as a store and forward system for SMS messages. Refer to Figure 5.5 for SMS architecture.

There are two types of SMS, SMMT (Short Message Mobile Terminated Point-to-Point), and SMMO (Short Message Mobile Originated Point-to-Point). SMMT is an incoming short message from the network and is terminated in the MS (phone or Mobile Station). SMMO is an outgoing message, originated in the MS, and forwarded to the network for delivery. For an outgoing message, the SMS is sent from the phone to SC via the VLR and the Interworking MSC (IWMSC). For incoming SMS message the path is from SC to the MS via the HLR and the Gateway MSC (GMSC). Please see Chapter 6 for SMS and related technologies.

5.4 Call Routing in GSM

Human interface is analog. However, the advancement in digital technology makes it very convenient to handle information in digital fashion. In GSM there are many complex technologies used between the human analog interface in the mobile and the digital network (Fig. 5.6).

Digitizer and source coding: The user speech is digitized at 8 KHz sampling rate using Regular Pulse Excited–Linear Predictive Coder (RPE–LPC) with a Long Term Predictor loop. In this technique, information from previous samples is used to predict the current sample. Each sample

is then represented in signed 13-bit linear PCM value. This digitized data is passed to the coder with frames of 160 samples. The encoder compresses these 160 samples into 260-bits GSM frames resulting in one second of speech compressed into 1625 bytes and achieving a rate of 13 Kbits/sec.

Channel coding: This step introduces redundancy information into the data for error detection and possible error correction. The gross bit rate after channel coding is 22.8 kbps (or 456 bits every 20 ms). These 456 bits are divided into eight 57-bit blocks, and the result is interleaved amongst eight successive time slot bursts for protection against burst transmission errors.

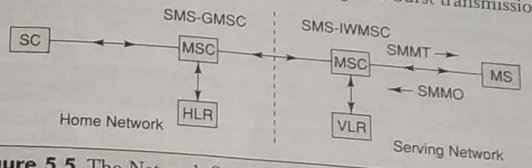


Figure 5.5 The Network Structure for the Short Message Transfer

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.

Ciphering: Encrypts blocks of user data using a symmetric key shared by the mobile station and the BTS.

Burst formatting: Adds some binary information to the ciphered block. This additional information is used for synchronization and equalization of the received data.

Modulation: The modulation technique chosen for the GSM system is the Gaussian Minimum Shift Keying (GMSK). Using this technique the binary data is converted back 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. Each time slot burst is 156.25 bits and contains two 57-bit blocks, and a 26-bit training sequence used for equalization (Fig. 5.6). A burst is transmitted in 0.577 ms for a total bit rate of 270.8 Kbps.

Multipath and equalization: At the GSM frequency bands, radio waves reflect from buildings, cars, hills, etc. So not only is the "right" signal (the output signal of the emitter) received by an antenna, but many reflected signals, which corrupt the information, with different phases are also received. An equaliser is in charge of extracting the "right" signal from the received signal. It estimates the channel impulse response of the GSM system and then constructs an inverse filter. In order to extract the "right" signal, the received signal is passed through the inverse filter.

Synchronization: For successful operation of a mobile radio system, time and frequency synchronization are needed. Frequency synchronization is necessary so that the transmitter and receiver frequency match (in FDMA). Time synchronization is necessary to identify the frame boundary and the bits within the frame (in TDMA).

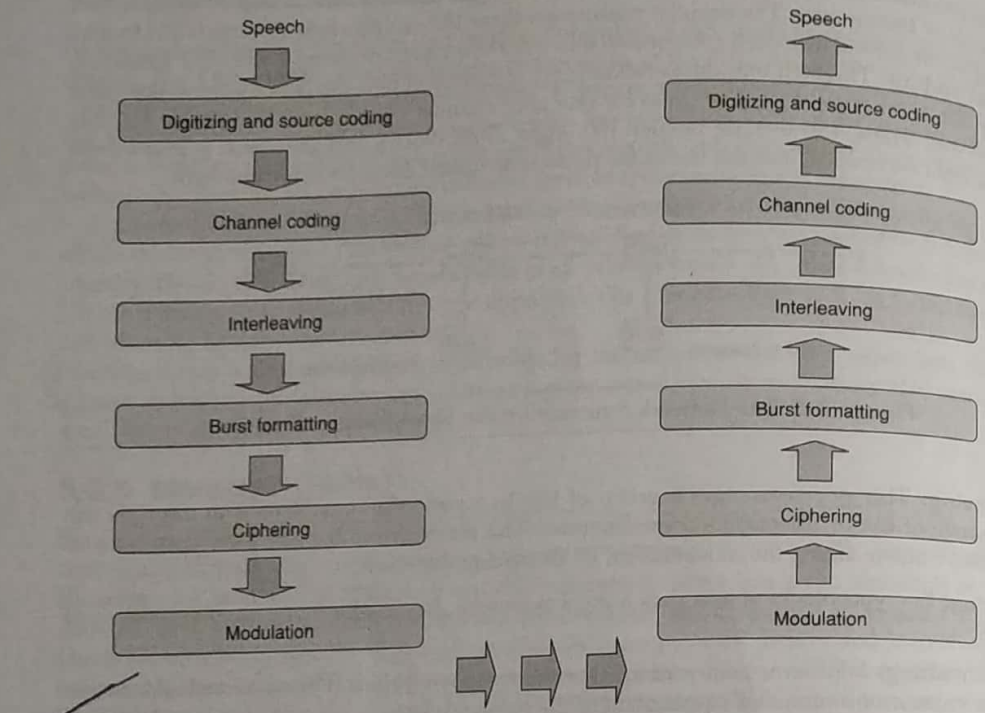


Figure 5.6 Sequence of Operation from Speech to Radio Wave

The mobile station can be anywhere within a cell. Also, the distance between the base station and the mobile station vary. Due to mobility of the subscriber, the propagation time between the base station and the mobile keeps varying. When a mobile station moves further away, the burst transmitted by this mobile may overlap with the time slot of the adjacent time slot. 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.

5.4.1 An Example

In this section let us take an example of how and what happens within the GSM network when someone from a fixed network calls someone in a GSM network. Let us assume that the called party dialed a GSM directory number +919845052534. Figure 5.7 depicts the steps for this call processing.

The directory number dialed to reach a mobile subscriber is called the Mobile Subscriber ISDN (MSISDN), which is defined by the E.164 numbering plan. This number includes a country code and a National Destination Code, which identifies the subscriber's operator. The first few digits of the remaining subscriber number may identify the subscriber's HLR within the home PLMN. For example, the MSISDN number of a subscriber in Bangalore associated with Airtel network is +919845XYYYYY. This is a unique number and understood from anywhere in the world. In this example + means the prefix for international dialing like 00 in UK/India or 011 in USA. 91 is the country code for India (404 as defined in GSM). 45 is the network operator's code (Airtel in this case). X is the level number managed by the network operator ranging from 0 to 9. YYYYY is the subscriber code managed by the operator as well.

The call first goes to the local PSTN exchange. The PSTN exchange looks at the routing table and determines that it is a call to a mobile network. It forwards the call to the Gateway MSC (GMSC) of the mobile network. The MSC enquires the HLR to determine the status of the subscriber. It will decide whether the call is to be routed or not. If the user has not paid the bills, the call may not be routed. If the phone is powered off, a message may be played or forwarded to the voice mail. However, if MSC finds that the call can be processed, it will find out the address of the VLR where the mobile is expected to be present. If the VLR is that of a different PLMN, it will forward the call to the foreign PLMN through the Gateway MSC. If the VLR is in the home network, it will determine the Location Area (LA). Within the LA it will page and locate the phone and connect the call.

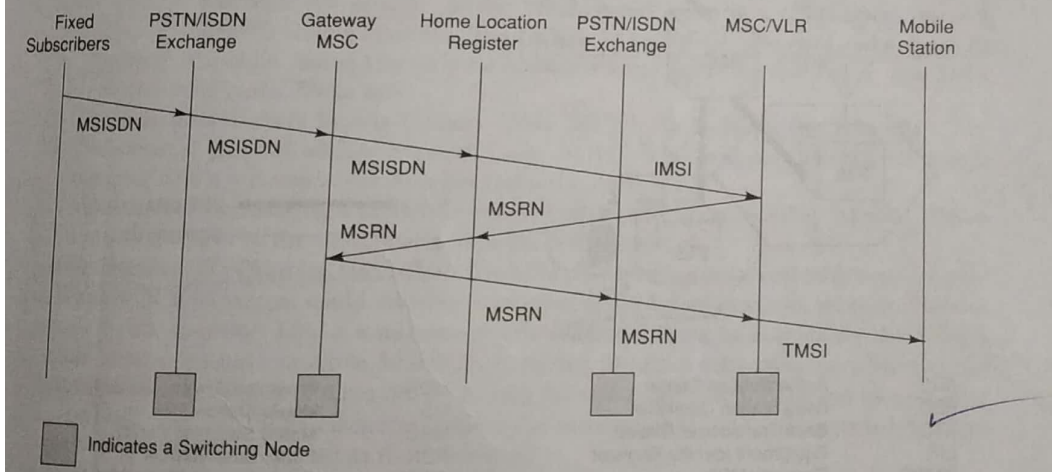
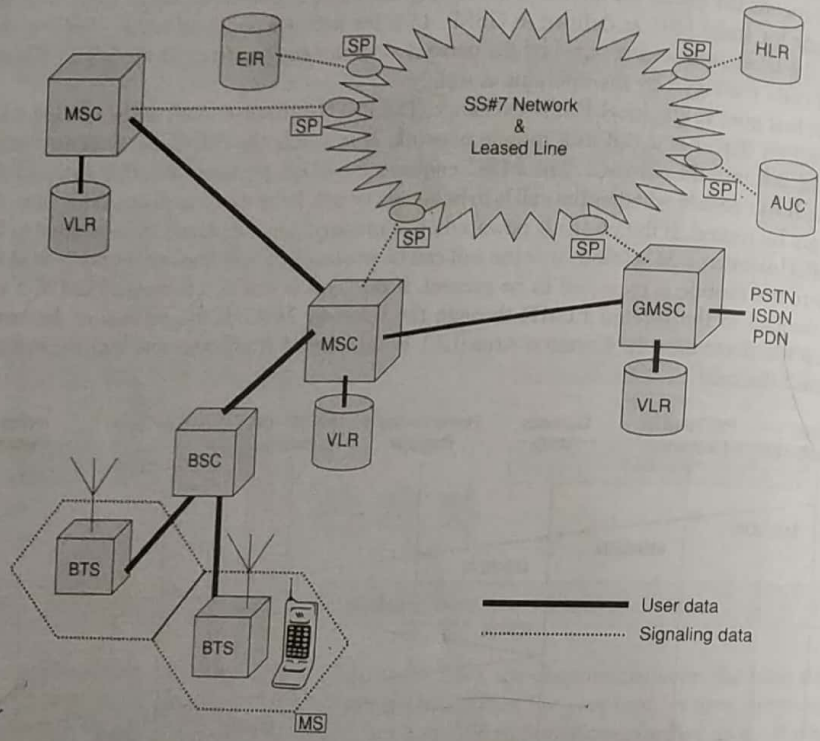


Figure 5.7 Call Routing for a Mobile Terminating Call

5.5 PLMN INTERFACES

The basic configuration of a GSM network contains a central HLR and a central VLR. HLR contains all security, provisioning and subscriber-related information. VLR stores the location information and other transient data. MSC needs subscriber parameter for successful call set-up. Figure 5.8 shows a basic configuration of a GSM mobile communication network.



AUC	Authentication Center	ISDN	Integrated System Digital Network
BSC	Base Station Controller	MS	Mobile Station
BTS	Base Transceiver Station	MSC	Mobile Switching Center
EIR	Equipment Identity Register	PDN	Public Data Network
GMSC	Gateway MSC	PSTN	Public Switched Telephone Network
HLR	Home Location Register	SP	Signaling Point
		VLR	Visitor Location Register

Figure 5.8 Configuration of a GSM PLMN

Within the switching and management system, the transmission rate is 2 Mbits/s. This 2 Mbits/ interface is called E1 interface in India and in Europe. These are realized typically through

microwave or leased lines. Any data related to user call (connection, teardown, etc.) are processed with SS7 protocol for signaling using ISUP (ISDN User Part) stack between network nodes. For mobile specific signaling a protocol stack called MAP (Mobile Application Part) is used over the SS7 network. All database transactions (enquiries, updates, etc.) and handover/roaming transactions between the MSC are performed with the help of MAP. For this purpose, each MSC uses registers known as SP (Signaling Point). These SPs are addressable through a unique code called Signaling Point Code (SPC). Signaling between MSC and BSS uses Base Station System Application Part (BSSAP) over SS7. Within BSS and at the air interface, signaling is GSM proprietary and does not use SS7.

5.6 GSM ADDRESSES AND IDENTIFIERS

GSM distinguishes explicitly between the user and the equipment. It also distinguishes between the subscriber identity and the telephone number. To manage all the complex functions, GSM deals with many addresses and identifiers. They are:

- *International Mobile Station Equipment Identity (IMEI):* Every mobile equipment in this world has a unique identifier. This identifier is called IMEI. The IMEI is allocated by the equipment manufacturer and registered by the network operator in the Equipment Identity Register (EIR). In your mobile handset you can type *#06# and see the IMEI.
- *International Mobile Subscriber Identity (IMSI):* When registered with a GSM operator, each subscriber is assigned a unique identifier. The IMSI is stored in the SIM card and secured by the operator. A mobile station can only be operated when it has a valid IMSI. The IMSI consists of several parts. These are:
  - Three decimal digits of Mobile Country Code (MCC). For India the MCC is 404.
  - Two decimal digits of Mobile Network Code (MNC). This uniquely identifies a mobile operator within a country. For Airtel in Delhi this code is 10.
  - Maximum 10 decimal digits of Mobile Subscriber Identification Number (MSIN). This is a unique number of the subscriber within the home network.
- *Mobile Subscriber ISDN Numbers (MSISDN):* The MSISDN number is the real telephone number as is known to the external world. MSISDN number is public information, whereas IMSI is private to the operator. This is a number published and known to everybody. In GSM a mobile station can have multiple MSISDN numbers. When a subscriber opts for fax and data, he is assigned a total of three numbers: one for voice call, one for fax call and another for data call. The MSISDN categories follow the international ISDN (Integrated Systems Data Network) numbering plan as the following:
  - Country Code (CC): One to three decimal digits of country code.
  - National Destination Code (NDC): Typically 2 to 3 decimal digits.
  - Subscriber Number (SN): Maximum 10 decimal digits.

The CC is standardized by the ITU-T through the E.164 standard. There are CCs with one, two, or three digits. For example, the CC for USA is 1, for India it is 91, and for Finland it is 358.The national regulatory authority assigns the NDC. In India it is 94 for BSNL and 98 for all other operators. In India the subscriber number SN is eight decimal digits. SN consists of two decimal

digits of operator code, followed by one decimal digit level number with a five de... subscriber number. In India, a MSISDN number looks like 919845062050. In this nu... the CC, 98 is the NDC, and 45062050 is the SN. In India, the SN is subdivided into op... and subscriber code (45 is the operator code and 062050 is the subscriber code). ... subscriber code is also subdivided into one digit level number (0 in this case) followed by ... subscriber ID (62050).

- *Location Area Identity:* Each LA in a PLMN has its own identifier. The Location Area ... (LAI) is structured hierarchically and unique. LAI consists of three digits of CC, two ... Mobile Network Code and maximum five digits of Location Area Code.
- *Mobile Station Roaming Number (MSRN):* When a subscriber is roaming in another ... temporary ISDN number is assigned to the subscriber. This ISDN number is assigned ... local VLR in charge of the mobile station. The MSRN has the same structure as the M...
- *Temporary Mobile Subscriber Identity (TMSI):* This a temporary identifier assigned by the ... VLR. It is used in place of the IMSI for identification and addressing of the mobile ... TMSI is assigned during the presence of the mobile station in a VLR and can cha... hopping). Thus, it is difficult to determine the identity of the subscriber by listening to th... channel. The TMSI is never stored in the HLR. However, it is stored in the SIM card ... with the current location area, a TMSI allows a subscriber to be identified uniquely ... ongoing communication the IMSI is replaced by the 2-tuple LAI, TMSI code.
- *Local Mobile Subscriber Identity (LMSI):* This is assigned by the VLR and also stored ... 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). Together with ... a cell can be identified uniquely through Global Cell Identity (LAI+CI).
- *Identification of MSCs and Location Registers:* MSCs, Location Registers (HLR, VLR, ... addressed with ISDN numbers. In addition, they may have a Signaling Point Code ... within a PLMN. These point codes can be used to address these nodes uniquely with ... Signaling System number 7 (SS#7) network.

5.7 NETWORK ASPECTS IN GSM

Transmission of voice and data over the radio link is only a part of the function of a cellular ... network. A GSM mobile can seamlessly roam nationally ... registration, authentication, call routing and ... GSM networks. The geographical ... When a call is in progress ... ne cell to ...

CHAPTER 6

Short Message Service (SMS)

6.1 MOBILE COMPUTING OVER SMS

GSM supports data access over CSD (Circuit Switched Data). GSM is digitized but not packetized. In case of CSD, a circuit is established and the user is charged based on the time the circuit is active and not on the number of packets transacted. GPRS (General Packet Radio Service), also known as 2.5G, which is the next phase within the evolution of GSM, supports data over packets. WAP is a data service supported by GPRS and GSM to access Internet and remote data services. WAP has been covered in Chapter 8. Other data services in GSM include Group 3 facsimile, which is supported by use of an appropriate fax adaptor. A unique data service of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS enables sending and receiving text messages to, and from, GSM mobile phones. In this chapter we discuss SMS and developing applications using SMS bearer.

6.2 SHORT MESSAGE SERVICE (SMS)

Like many other eccentric technologies, SMS was also allegedly the right idea at the wrong time. On December 3, 1992, a scientist named Neil Papworth at Sema, a British technology company, sent the first text message "Merry Christmas" to the GSM operator Vodafone. It was sent to Vodafone director Richard Jarvis in a room at Vodafone's HQ in Newbury in southern England. The message was an overly premature seasonal greeting, some three weeks ahead of the festivities. Vodafone offered this service as a text messaging service with a brand name TeleNotes service targeted for the business community. The service was not at all popular in its early days. SMS was almost forgotten and became an unwanted child until seven years later in 1999 when other mobile phone operators started to allow customers to swap SMS. Today SMS is the most popular data bearer/service within GSM with an average of one billion SMS messages (at the end of 2002) transacted every day around the world, with a growth of on an average half a billion every month. The SS7

signaling channels are always physically present but mostly unused, be it during an active user connection or in the idle state. It is, therefore, quite an attractive proposition to use these channels for transmission of used data. SMS uses the free capacity of the signaling channel. Each short message is up to 160 characters in length when 7-bit English characters are used. It is 140 octets when 8-bit characters (some European alphabets) are used, and 70 characters in length when non-Latin alphabets such as Arabic, Chinese or Hindi are used (70 characters of 16 bit Unicode).

6.2.1 Strengths of SMS

Following is the list of unique characteristics of SMS, which make this an attractive bearer for mobile computing.

Omnibus nature of SMS: SMS uses SS7 signaling channel, which is available throughout the world. SMS is the only bearer that allows a subscriber to send a long distance SMS without having long distance subscription. For example, you cannot make a voice call to a mobile phone in UK unless you have an international calling facility. However, you can send a SMS to a subscriber in UK, without having an international call facility.

Stateless: SMS is sessionless and stateless. Every SMS message is unidirectional and independent of any context. This makes SMS the best bearer for notifications, alerts and paging. SMS can be used for proactive information dissemination for "unsolicited response" and business triggers generated by applications (referred as "Push" in Fig. 8.4).

Asynchronous: In HTTP, for every command (e.g., GET or POST) there is a request and a response pair making it synchronous at the transaction level. Unlike HTTP, SMS is completely asynchronous. In case of SMS, even if the recipient is out of service, the transmission will not be abandoned. Therefore, SMS can be used as message queues. In essence, SMS can be used as a transport bearer for both synchronous (transaction oriented) and asynchronous (message queue and notification) information exchange.

Self-configurable and last mile problem resistant: SMS is self-configurable. In case of Web or WAP, it is no trivial task to connect to a service from a foreign network without any change in the configuration or preference setting. The device needs to be configured interactively by the user or system administrator to access the network. This makes the access dependent on the last mile. SMS has no such constraints. While in a foreign network, one can access the SMS bearer without any change in the phone settings. The subscriber is always connected to the SMS bearer irrespective of the home and visiting network configurations. While roaming in a foreign network, even if the serving network does not have an SMSC (SMS Center) or SC (Service Center), SMS can be sent and received.

Non-repudiable: SMS message carries the SC and the source MSISDN as a part of the message header. Unlike an IP address it is not easy to handcraft an MSISDN address in the SMS. It is possible for an application connected to an SMS to handcraft an MSISDN address like "999" or even alphabetic addresses like "MYBANK". However, an application can not handcraft the SC address. Therefore, an SMS can prove beyond doubt the origin of itself.

Always connected: As SMS uses the SS7 signaling channel for its data traffic, the bearer media is always on. User cannot SWITCH OFF, BAR or DIVERT any SMS message. When a phone is busy and a voice, data or FAX call is in progress, SMS message is delivered to the MS (Mobile Station) without any interruption to the call.

6.2.2 SMS Architecture

SMS are basically of two types, SM MT (Short Message Mobile Terminated Point-to-Point), and SM MO (Short Message Mobile Originated Point-to-Point). SM MT is an incoming short message from the network side and is terminated in the MS. SM MO is an outgoing message, originated in the user device (MS), and forwarded to the network for delivery. For outgoing message, the path is from MS to SC via the VLR and the IWMSC function of the serving MSC, whereas for incoming message the path is from SC to the MS via HLR and the GMSC function of the home MSC (Fig. 6.1).

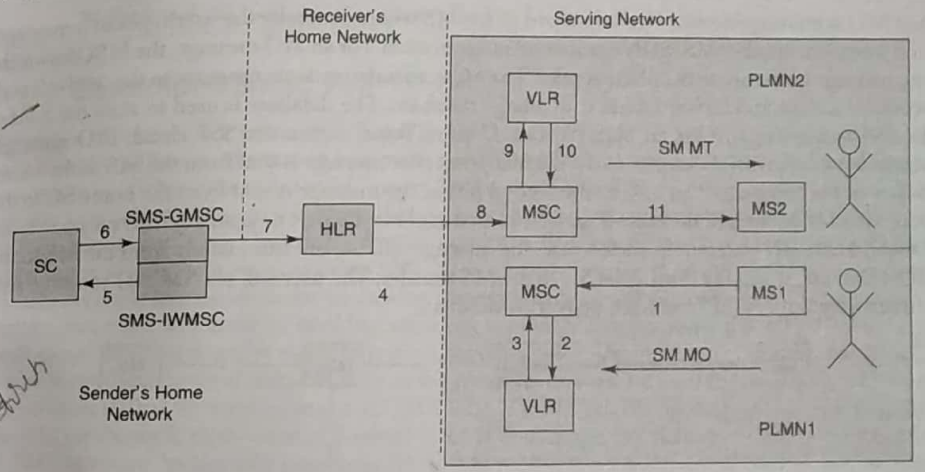


Figure 6.1 Flow of SMS between Two MS

To use SMS as a bearer for information exchange, the Origin server or the Enterprise server needs to be connected to the SC through a short message entity (SME) as in Figure 6.2. The SME in this case works as an SMS gateway, which interacts to the SC in one side, and the enterprise server on the other side.

6.2.3 Short Message Mobile Terminated (SM MT)

For an SM MT message, the message is sent from SC to the MS. This whole process is done in one transaction (Fig. 6.2). For the delivery of MT or incoming SMS messages, the SC of the serving

network is never used. This implies that an SMS message can be sent from any SC in any network to a GSM phone anywhere in the world. This makes any SM MT message mobile operator independent

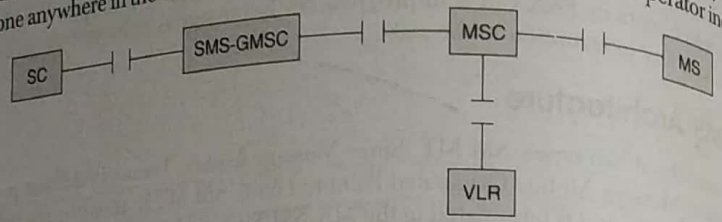


Figure 6.2 Interface Involved in the SM MT Procedure

6.2.4 Short Message Mobile Originated (SM MO)

SM MO is an outgoing message originated in the MS where generally the user types in a message and sends it to another MSISDN number or an application. For an MO message, the MSC forwards the message to the home SC of the sender. The SC is an independent computer in the network and works as a store and forward node with a large database. The database is used to store the SMS. In SS7 terminology SC is an SCP (Service Control Point) within the SS7 cloud. MO message works in two asynchronous phases. In the first phase, the message is sent from the MS to the home SC as an MO message (Fig. 6.3). In the second phase, the message is sent from the home SC to the receiving MS as an MT message (Fig. 6.2). It is possible to attempt to send an SMS message to an invalid MSISDN number. In such a case, the message will be sent successfully from the MS to the SC. However, it will fail during the SC to the MS transfer. The user will see SM MO message as successfully but SM MT message delivery would fail.

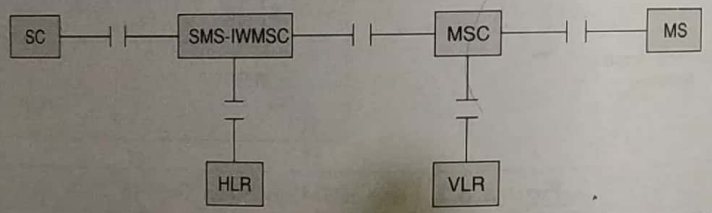


Figure 6.3 Interface Involved in the Short Message Mobile Originated (SM MO) Procedure

6.2.5 SMS as an Information Bearer

SMS is a very popular bearer in the person-to-person, mobile-to-mobile or point to point messaging domain. However, it is gaining popularity in other verticals like enterprise applications, services provided by independent service providers as ASP (Application Service Provider), and notification services, where one endpoint is a mobile phone but the other endpoint is a mobile application. Here SMS functions as an input-output media for information exchange for a mobile application (Fig. 6.4).

To use SMS as a bearer for any information service, we need to connect the services running on the Enterprise Origin server to the SC through an SME (Short Message Entity) or ESME (External Short Message Entity). SME in any network is generally a SMS gateway. With respect to SMS, a GSM subscriber is always in control of the SC in the home network irrespective of the serving network. Thus, if there is any SMS-based data service in the home network, it will be available to the subscriber from any foreign network.

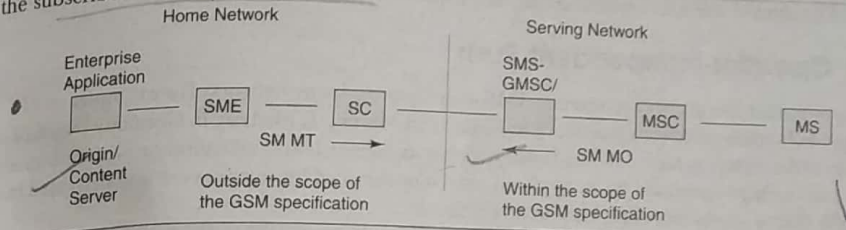


Figure 6.4 SMS as an Information Bearer/Medium for Mobile Applications

6.2.6 Operator-centric Pull

For an SMMO to work it is mandatory that an SC is used. As a part of SMS value added services, operators offer different information on demand and entertainment services. These are done through connecting an Origin server to the SC via an SMS gateway. In different parts of the world a new industry vertical has emerged to address this market. These service providers are known as MVNO (Mobile Virtual Network Operators). Virtual operators develop different systems, services, and applications to offer data services using SMS. Many enterprises use these MVNOs to make their services available to mobile phone users. There are quite a few banks in India which offer balance enquiry and other low security banking services over SMS. For example, if a HDFC customer wants to use these services, he needs to register for the service. During the registration, the HDFC customer needs to mention the MSISDN of the phone which will be used for this service. Once a user is registered for the service, he enters "HDFCBAL" and sends the message to a service number (like 333 for example in the case of Escotel) as an MO message. SC delivers this MO message to the SMS gateway (technically known as SME–Short Message Entity) connected to this service number. The SMS gateway then forwards this message to the enterprise application. The response from the enterprise application is delivered to the MS as an MT message from the SME. Even if the subscriber is in some remote region of a foreign network within GSM coverage, he can send the same SMS to the same service number in his home network. This makes the home services available in the foreign network. This also implies that an operator-centric SMS pull service is completely ubiquitous.

The connectivity between SC to SME and SME to Enterprise Origin server is not defined by GSM. However, there are a few de facto standard protocols for this communication. The most popular protocol is Short Message Peer to Peer (SMPP). There are certain other protocols like CIMD from Nokia as well. The connectivity between SME and Origin server could be anything like SOAP (Simple Object Access Protocol), or direct connection through TCP socket. However, common practice is through HTTP. HTTP helps user to get information from the Internet via SMS. There is an open source for SMS gateway called Kannel, which supports a multitude of

protocols and forwards the SMS enquiry as an HTTP request and gets information from the Internet. This is how an SMS can be converted into a simple Internet access. Conventionally SMS queries are keywords driven like "CRI" for live cricket score, or "RSK 2627 3 03" to get the availability of seat/berth in Indian Railways train number 2627 (Karnataka Express) for March 3. There are applications where SMS is used in session-oriented transactions. Applications like "SMS chat" and "SMS contests" need to remember the user context over multiple transactions.

6.2.7 Operator-independent Push

We have seen that it is possible to send an SMS to any phone in any network. For example, an MT message can be delivered from a network in India to an MS of UK roaming in Germany (Fig. 6.5). Which in other words means that any push, which may be an alert, notification or even response from a pull message generated by an application, can be serviced by any network and delivered to any GSM phone in any network without any difficulty.

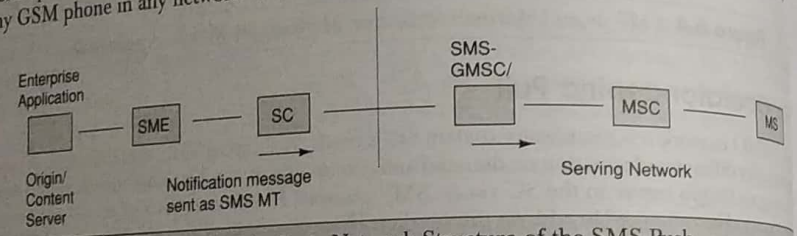


Figure 6.5 The Basic Network Structure of the SMS Push

Assuming that appropriate roaming tie-ups are in place, an enterprise can use SMS to send business alerts or proactive notifications to its customer anywhere, anytime on any GSM phone. With roaming tie-ups, operators reach an agreement on revenue share and call forwarding mechanism. Roaming tie-ups are a commercial issue rather than technical. Some credit card companies in India send SMS notifications to its cardholders in different networks using operator independent push.

6.2.8 Challenge for SMS as a Mobile Computing Bearer

When it comes to offering enterprise services using SMS, the scene becomes difficult to manage. Let us take the example of Indian Bank. In Delhi, a customer of this bank who is a subscriber of operator "A" (Airtel) sends "HDFCBAL" to 300 to know the balance in his account. In the same city of Delhi another customer of the same bank who happens to be a subscriber of a different operator "B" (Essar) sends "HDFCBAL" to 1234 to get the balance information. HDFC bank has a sizable population of customers in the Middle East. The same banking services, which are available in India, are not available in the Middle East. The reason being both cellular operators "A" and "B" connect to the bank's application through their private SC and SME, whereas the operators in Middle East do not have an SME to connect to the bank's application. This is like in the early days of telephony when an enterprise used to announce different customer care numbers for different cities. If the enterprise did not have an office in a city, the customers had to make long distance

calls to customer care in some other city. All these changed with the introduction of the 1–800 service. Enterprises need something similar to 1–800 in SMS. Also, this gives some identity to the enterprise. My Inc for example may like to publish a number like +9198375MYINC for any of its customer anywhere in the world.

The major challenge for implementing ubiquitous service through SMS requires operator independent SM MO messages or operator independent pull services. The SMS routing needs to work exactly in the same fashion as 1–800 services.

6.2.9 Operator-independent Pull

As the SME is always connected to the home network's SC, with the conventional framework, it is not possible to route mobile originated SMS messages to any application or any SME of choice. There are ways by which an SMS message can be routed to some enterprise SME connected to external SC. This is achieved through SAT, where the SAT application running on the SIM card changes the SC number during the transmission of the SMS and forces the SMS to recognize a different SC of a different network as its home SC. In this case also, technically the SMS is sent to the SME connected to the home SC. SMS has always been considered a revenue generating tool for cellular operators. Therefore, the current framework suits a cellular operator very well. If a SMS service is operator dependent, the cellular operator can use this to its advantage. In today's global scenario an enterprise or a MVNO has its customers around the world subscribing to different GSM networks. To make this possible, enterprises need operator-independent pull as well. Operator-independent pull services can be achieved using GSM modem technology described in the following sections. Also, the same can be done using Intelligent Network Technologies.

6.3 Value Added Services through SMS

Value Added Services (VAS) can be defined as services, which share one or more of the following characteristics:

- Supplementary service (not a part of basic service) but adds value to total service offering.
- Stimulates incremental demand for core services offering.
- Stands alone in terms of profitability and revenue generation potential.
- Can sometimes stand-alone operationally.
- Does not cannibalize basic service unless clearly favorable.
- Can be an add-on to basic service, and as such, may be sold at a premium price.
- May provide operational and/or administrative synergy between or among other services and not merely for diversification.

A GSM operator's primary business goal is to offer the network infrastructure. Voice, SMS are basic services provided by a GSM operator. However, offering different other services using SMS as a bearer will be a VAS. There are various flavors and variations of VAS over SMS. We will give some examples and discuss how to develop them. The most popular VAS over SMS are entertainment and information on demand. Information on demand has three categories as described below.

1. **Static information.** This type of information does not change frequently. A good example is a restaurant guide. It is sufficient to update this type of information once in a fortnight or even less frequently. These contents generally fall in mass market category.
2. **Dynamic information.** This type of information changes in days. For example, the daily horoscope needs to be updated on daily basis. Mass market contents fall in this category as well.
3. **Real-time information.** This type of information changes continually. Third-party contents fall in this category. For example, scores in a live cricket match or stock quote undergo continual change. All the enterprise contents will fall in this category. For enterprise contents the content will be obtained directly from the enterprise.

6.3.1 User Interface in SMS Value Added Services

We have already seen that SMS is sessionless. In Chapter 1 also we have discussed session-oriented transaction and short transaction (Section 1.4). Majority of services over SMS will use the short transaction model. For a SMS-based service, the user interface is always keyword-based. This is something similar to the character-based command interfaces, where the first word is the keyword (command) and rest are the parameters for the command. For example, I want to know the latest news. For this I enter News and send it to the VAS service. If I want business news, I enter News Biz. News is the keyword. Another example could be **RSA 2627 Bangalore New Delhi 20** (. This example is for finding out the seat availability on the Indian Railways train number 2627 from Bangalore to New Delhi for 20 January. For Indian Railways, the tickets are available only 60 days in advance. Therefore, we do not need the year. The response for this enquiry will be **Date: 20-1 Train: 2627 KARNATAKA EXP Class:2A Status: WL 31/WL 14 Class: 3A Status: WL 63/WL 51 Class: SL Status: WL 59/WL 29**. Please note that the response from a service may sometimes be more than 160 characters. If it is more than 160 characters, we need to split the response into multiple message responses. It is advised that while the message is broken into multiple messages, it is broken at the word boundary. It is also advised that a sequence number like ... 1/3, ... 2/3, and ... 3/3 is added in the first, second and third messages, respectively.

6.3.2 VAS Examples

In this section we describe some of the popular value-added services.

News/Stock Quotes Service

In a service like News or Stock Quote, we get the latest news or stock information. This will be Short transaction. The keyword for news will be News, whereas the keyword for stock quote will be BSE. BSE Infosys will give the stock price of Infosys at the Bombay Stock Exchange. These are examples for real-time information on demand. For services like News and Stock Quote we need to have a relationship with some content provider who will supply us the up-to-date information. For example, we could tie up with *CNN* for international news, *The Indian Express* for general news, *weather.com* for weather news, etc. For stock quote, we may need to tie up with a stock exchange like Bombay Stock Exchange or National Stock Exchange. We will receive live feed from these content providers and update the content database on a real-time basis. As and when a subscriber wants these information, we supply the latest information from the live database.

Session-based Chat Application

A chat service is essentially a session-oriented transaction. In a chat service the user needs to log in. The user needs to explicitly log out or will be logged out implicitly following a period of inactivity. Every time the user sends a chat keyword, we need to know the previous transactions. Every SMS message carries the unique MSISDN number. This unique MSISDN number of the phone can be used as the session key. In the chat software we remember the state of the transaction using this MSISDN.

Email through SMS

This is a very useful service and is a transaction-oriented dialogue. To send an email through SMS, the user message will be **mail roopa@iitb.ac.in we will meet tomorrow 6:00 pm**. This VAS will send a mail to Roopa with mail id roopa@iitb.ac.in. The body of the mail will be "we will meet tomorrow 6:00 pm." The mail will be sent to Roopa by a SMTP server.

Health Care Services

Health care applications need both pull and push. A typical health care application could be ICU (Intensive Care Unit) system. The system will include alerts to doctor. In status monitoring service, a doctor or a nurse can enquire the status of a patient in the ICU. A limited enquiry facility will be provided to one MSISDN outside the hospital staff. This could be for someone in the family. This enquiry will be a short transaction. We will have alert services as well. In the alert service, nurses and doctors are notified periodically about the status of the patients in the ICU. The alerts can also be integrated with medical equipment.

Micro-payment Services

Let us take an example of micro-payment for a vending machine. This will be a session-oriented dialogue. In this application there will be some number of identifier (ID) pasted on the vending machine. The customer enters this identification number and sends a request to purchase a merchandise to the service provider. The service provider will authenticate the user and check whether the user has sufficient money in credit. Based upon the credit the transaction will either be approved or rejected. If approved, an authorization message will be sent back to the vending machine. The vending machine will ask the user to select merchandise. The user selects the merchandise, a soft drink, for example. Once the merchandise is dispensed, the vending machine will send back a message to the VAS indicating that the merchandise has been dispensed. The price for the merchandise is debited from the user account.

6.3.3 Alert Services

These are proactive alert services. For a stock quote the alert services can be of the following kind.

Time-based: In this service, proactive alerts are sent to the mobile phone at a pre-assigned time of the day. The alert contains the stock quote of different scripts of the portfolio.

Watermark-based: In this service whenever the stock price goes up or falls down to a certain level, alerts are sent. This information will help the subscriber to decide whether to buy or sell some particular stock.

For other services, like cricket score, it can be a periodic alert (every 10 minutes) during the match. There can be other alerts like inform the live score whenever a player is out etc.

6.3.4 Location-based Software

Location-based services could be road direction, restaurant guide, etc. Some location-aware VAS services provide shopping alerts as well. In location-based services only the information relevant to the current location of the mobile phone (or the subscriber) is provided. In a shopping service, the user will receive alerts on discount or sale information when they pass through close the proximity of the shopping malls. In the case of a restaurant guide, let us assume that the subscriber is in a office on M.G. Road in Bangalore and sends Res to the VAS. Only the restaurants in, and around, M.G. Road will be provided as response to this request. When the same user asks for the same information in Mumbai, restaurants in Mumbai will be given as response. For location-aware software, the precise location of the user needs to be determined. The location of a mobile phone can be determined either from the network or from the device. Using Time Advancing techniques within the BTS, the location of the mobile phone can be determined. This technique however requires the support of the network. The other option is to find out the location from the device. Device-specific location awareness requires either of the following technologies:

1. Cell ID (CID)-based system.
2. Global Positioning System (GPS)-based system.

In a CID-based system, the CID of the current BTS is determined. The CID-based system needs a mapping of the cell identifier to the geographical location. To handle the growing subscribers, new cell sites are added and the CIDs reconfigured. In such cases the mapping between locations versus CIDs need to be synchronized. For CID-based system, the signal strength from all the different CIDs are extracted from the device and sent to the server through a SMS. The location of the user is determined using the signal strength and triangulation algorithms. In a GPS-based system, the location is detertmined through a GPS receiver installed within the phone. GPS provides facility to compute position, velocity and time of a GPS receiver. To offer a travel direction through GPS, the GPS system will inform the application about the exact location of the phone. From the velocity it will also know the direction the user is moving. Based on the location and direction, the direction will be provided. Please note that sometimes it may not be a trivial task to take a U turn on a freeway or motorway. GPS-based system is not dependent on the network operator.

In Figure 6.6 we describe the basic value added service provisioning architecture for SMS. The reader should try to map an application scenario and get a feeling of how information travels across in the case of pull/push . ●

6.4 Accessing the SMS Bearer

There are two ways the SMS bearer can be accessed:

1. Use a mobile phone as a GSM modem and connect it to the computer.
2. Use the SMSC of an operator through SMPP or similar interface.

CHAPTER 7

General Packet Radio Service (GPRS)

7.1 INTRODUCTION

People love freedom. In Hollywood movies of yesteryears, we see actors moving around the room and talking on the telephone holding the phone in the left hand and the handset in the right. Today all this has changed. We have cordless phones and wireless mobile phones. People can move around (inside and outside their homes or even inside vehicles) and still talk. As the world is changing, people's expectations are also changing. People are looking for freedom from wire with respect to data. Tech Pundits believe that the trend taking place in fixed networks whereby the growth of data traffic is overtaking that of voice traffic, will also influence the wireless networks. GSM started with voice in mind and offered whatever a wireless voice user wanted. The popularity of GSM, Internet, and digital communication forced GSM to look for wireless data with higher band-width. General Packet Radio Service (GPRS) is a step to efficiently transport high-speed data over the current GSM and TDMA-based wireless network infrastructures.

7.2 GPRS AND PACKET DATA NETWORK

GPRS will thrive in both vertical and horizontal markets where high-speed data transmission over wireless networks is necessary. The deployment of GPRS networks allows a variety of new applications ranging from mobile e-commerce to mobile corporate VPN access. Deployments of GPRS networks has already taken place in several countries in Europe and the Far East. In Mumbai and Delhi GPRS was launched quite sometime ago.

7.2.1 Capacity and Other End-user Aspects

GPRS has the ability to offer data speeds of 14.4 Kbps to 171.2 Kbps, which allow for comfortable Internet access. It allows for short "bursty" traffic, such as e-mail and web browsing, as well as large

volumes of data. To support GPRS operations, new protocols and new network devices are required. By allowing information to be transmitted more quickly, immediately and efficiently across the mobile network, GPRS may well be a relatively less costly mobile data service compared to SMS and Circuit Switched Data. For GPRS, no dial-up modem connection is necessary. 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". This is like SMS, which is an always-on service. Immediacy is one of the advantages of GPRS compared to Circuit Switched Data.

7.2.2 Quality of Service (QoS)

The Quality of Service (QoS) requirements of typical mobile packet data applications are very diverse. For example the QoS for real-time multimedia content is different from web browsing or email transfer. GPRS allows definition of QoS profiles using the parameters of service precedence, reliability, delay and throughput.

- **Service precedence** is the priority of a service in relation to another service. There exist three levels of priority: high, normal, and low.
- **Reliability** indicates the transmission characteristics required by an application. Three reliability classes are defined, which guarantee certain maximum values for the probability of loss, duplication, mis-sequencing and corruption (an undetected error) of packets.
- **Delay** parameters define maximum values for the mean delay and the 95-percentile delay. The delay is defined as the end-to-end transfer time between two communicating mobile stations or between a mobile station and the signaling interface to an external packet data network.
- **Throughput** specifies the maximum/peak bit rate and the mean bit rate.

Using these QoS classes, QoS profiles can be negotiated between the mobile user and the network for each session.

7.2.3 Integral Part of the Future 3G Systems

The different approaches to third generation (3G) wireless systems (IMT-2000, UMTS, CDMA, WCDMA, 3GPP, 3GPP2 etc.) were intended to address the challenge of voice-to-data crossover and integration. The complexities of new and exciting wireless technologies have slowed down progress in their development and widespread deployment. To lessen the impact of the delay in implementing 3G wireless systems, GPRS was 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 (two and half G or two and half generation) in the evolution process of wireless cellular networks.

7.3 GPRS NETWORK ARCHITECTURE

GPRS uses the GSM architecture for voice. In order to offer packet data services through GPRS, a new class of network nodes need to be introduced as an upgrade to the existing GSM network.

These network nodes are called GPRS support nodes (GSN). GPRS support nodes are responsible for the delivery and routing of data packets between the mobile stations and the external packet data networks (PDN). There are two types of support nodes, viz., SGSN (Serving GSN) and GGSN (Gateway GSN). Figure 7.1 depicts GPRS system components for data services.

Serving GPRS Support Node (SGSN): A serving GPRS support node (SGSN) is at the same hierarchical level as the MSC. Whatever functions MSC does for voice, SGSN does the same for packet data. SGSN's tasks include packet switching, routing and transfer, mobility management (attach/detach and location management), logical link management, and authentication and charging functions. SGSN processes registration of new mobile subscribers and keeps a record of their location inside a given service area. The location register of the SGSN stores location information (e.g., current cell, current VLR) and user profiles of all GPRS users registered with this SGSN. SGSN sends queries to Home Location Register (HLR) to obtain profile data of GPRS subscribers. The SGSN is connected to the base station system with Frame Relay.

Gateway GPRS Support Node (GGSN): A gateway GPRS support node (GGSN) acts as an interface between the GPRS backbone network and the external packet data networks. GGSN's function is similar to that of a router in a LAN. GGSN maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations. It converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like Internet or X.25. PDP sends these packets out on the corresponding packet data network. In the other direction, PDP receives incoming data packets from data networks and converts them to the GSM address of the destination user. The readdressed packets are sent to the responsible SGSN. For this purpose, the GGSN stores the current SGSN address of the user and his or her profile in its location register. The GGSN also performs authentication and charging functions related to data transfer.

7.3.1 GPRS Network Enhancements

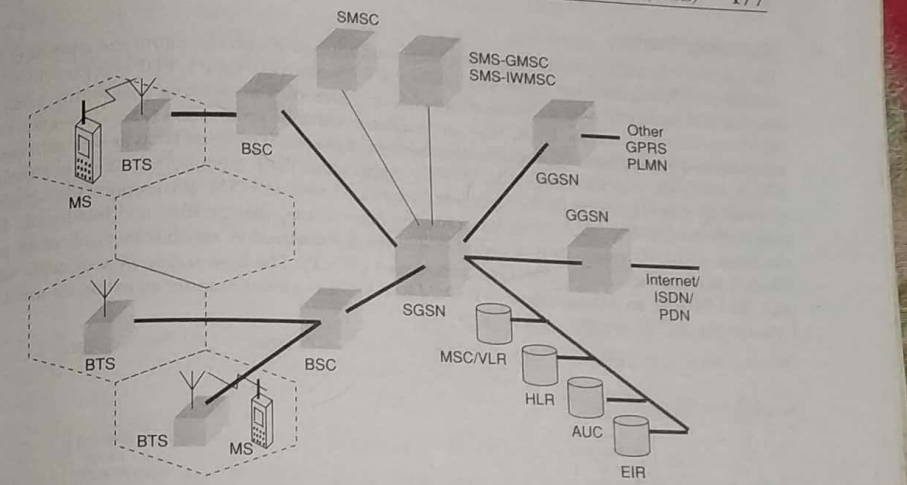
In addition to the new GPRS components (SGSN and GGSN), some existing GSM network elements must also be enhanced in order to support packet data. These are:

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

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

Mobile Station (MS): The mobile station or the mobile phone for GPRS is different from that of GSM.

SMS Nodes: SMS-GMSCs and SMS-IWMSCs are upgraded to support SMS transmission via the SGSN. Optionally, the MSC/VLR can be enhanced for more efficient coordination of GPRS and non-GPRS services and functionality.



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

Figure 7.1 GPRS System Architecture

7.3.2 Channel Coding

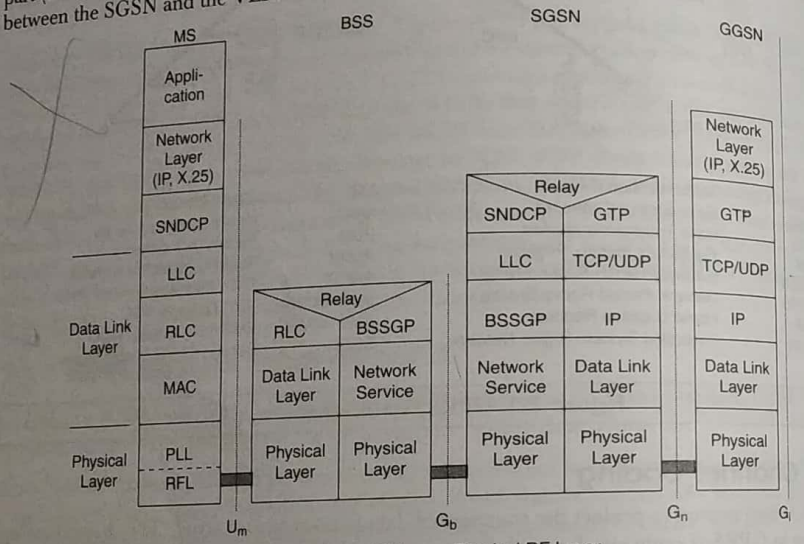
Channel coding is used to protect the transmitted data packets against errors. The channel coding technique in GPRS is quite similar to the one employed in conventional GSM. Under very bad channel conditions, the reliable coding scheme is used. In reliable coding scheme many redundant bits are added to recover from burst errors. In this scheme a data rate of 9.05 Kbps is achieved per time slot. Under good channel conditions, no encoding scheme is used resulting in a higher data rate of 21.4 Kbps per time slot. With eight time slots, a maximum data rate of 171.2 Kbps can be achieved.

7.3.3 Transmission Plane Protocol Architecture

Figure 7.2 illustrates the protocol architecture of the GPRS transmission plane, providing transmission of user data and its associated signaling.

Signaling Plane

The protocol architecture of the signaling plane comprises protocols for control and support of the functions of the transmission plane. This includes GPRS attach and detach, PDP context activation, control of routing paths, and allocation of network resources. The signaling architecture between SGSN and the registers like HLR, VLR, and EIR uses the same protocols as GSM. However, they are extended to support GPRS-specific functionality. Between SGSN and HLR as well as between SGSN and EIR, an enhanced MAP (Mobile Application Part) is employed. MAP is a mobile network-specific extension of the Signaling System SS7 used in GSM. It transports the signaling information related to location updates, routing information, user profiles, and handovers. The exchange of MAP messages is accomplished over the transaction capabilities application part (TCAP) and the signaling connection control part (SCCP). 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.



BSSGP	BSS GPRS Application Protocol	RFL	Physical RF Layer
GTP	GPRS Tunneling Protocol	RLC	Radio Link Control
IP	Internet Protocol	SNDCP	Subnetwork Dependent Convergence Protocol
LLC	Logical Link Control	TCP	Transmission Control Protocol
MAC	Medium Access Control	UDP	User Datagram Protocol
PLL	Physical Link Layer		

Figure 7.2 Transmission Plane and GPRS Protocol Stack

GPRS Backbone

GPRS backbone includes the transmission plane between SGSN and GGSN. User data packets and related signaling information within the GPRS network are encapsulated using the GPRS

Tunneling Protocol (GTP). The GTP protocol is used in both intra- PLMN (between SGSN and GGSN within one PLMN) and inter-PLMN (between SGSN and GGSN of different PLMNs). In the transmission plane, GTP protocol tunnels the user data packets through the GPRS backbone by adding GPRS specific routing information. GTP packets carry the user's data packets from both IP and X.25 data networks. Below GTP, the standard protocols TCP or UDP are used to transport the GTP packets within the backbone network. X.25 expects a reliable data link; therefore TCP is used for tunneling X.25 data. For IP based user data, UDP is used as it does not expect reliability in the network layer or below. Ethernet, ISDN, or ATM-based protocols may be used in the physical layer in the IP backbone. In essence, in the GPRS backbone we have an IP/X.25-over-GTP-over-UDP/TCP-over-IP transport architecture.

BSS–SGSN Interface

The BSS and SGSN interface is divided into the following layers:

Sub-Network Dependent Convergence Protocol (SNDCP): The SNDCP is used to transfer data packets between SGSN and MS. Its functionality includes:

- Multiplexing of several connections of the network layer on to one virtual logical connection of the underlying LLC layer.
- Segmentation, compression, and decompression of user data.

Logical Link Control (LLC): A data link layer protocol for GPRS which functions similar to Link Access Procedure–D (LAPD). This layer assures the reliable transfer of user data across a wireless network.

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 Q.922 Core by mapping BSSGP's service requests to the appropriate Frame Relay services.

Air Interface

The air interface of GPRS comprises the physical and data link layer.

Data Link Layer

The data link layer between the MS and the BSS is divided into three sublayers: the logical link control (LLC) layer, the radio link control (RLC) layer and the medium access control (MAC) layer.

Logical Link Control (LLC): This layer provides a reliable logical link between an MS and its assigned SGSN. Its functionality is based on HDLC (High-level Data Link Control) protocol and includes sequence control, in-order delivery, flow control, detection of transmission errors, and retransmission (automatic repeat request, ARQ). Encryption is used in this interface to ensure data confidentiality. Variable frame lengths are possible. Both acknowledged and unacknowledged data transmission modes are supported. This protocol is an improved version of the LAPDm protocol used in GSM.

Radio Link Control (RLC): The main purpose of the radio link control (RLC) layer is to establish a reliable link between the MS and the BSS. This includes the segmentation and reassembly of LLC frames into RLC data blocks and ARQ of uncorrectable data.

Medium Access Control (MAC): The medium access control (MAC) layer controls the acce
attempts of an MS on the radio channel shared by several MSs. It employs algorithms for contentio
resolution, multiuser multiplexing on a packet data traffic channel (PDTCH), and scheduling acc
prioritizing based on the negotiated QoS.

Physical Layer

The physical layer between MS and BSS is divided into two sublayers: the physical link laye
(PLL) and the physical RF Layer (RFL).

Physical Link Layer (PLL): This layer provides services for information transfer over a phys
channel between the MS and the network. These functions include data unit framing, data cod
and the detection and correction of physical medium transmission errors. The Physical Link la
uses the services of the Physical RF layer.

Physical RF Layer (RFL): This layer performs the modulation of the physical waveforms bas
on the sequence of bits received from the Physical Link layer above. The Physical RF layer al
demodulates received wave forms into a sequence of bits that are transferred to the Physical Li
layer for interpretation.

Multiple Access Radio Resource Management

On the radio interface, GPRS uses a combination of FDMA and TDMA. As in GSM (Fig. 3.1
GPRS uses two frequency bands at 45 MHz apart; viz., 890–915 MHz for uplink (MS to BTS) an
935–960 MHz for downlink (BTS to MS). Each of these bands of 25 MHz width is divided int
124 single carrier channels of 200 kHz width. Each of these 200 kHz frequency channels is divided
into eight time slots. Each time slot of a TDMA frame lasts for a duration of 156.25 bit times an
contains a data burst.

On top of the physical channels, a series of logical channels are defined to perform functio
like signaling, broadcast of general system information, synchronization, channel assignment, pag
or payload transport. As with GSM, these channels can be divided into two categories: traf
channels and signaling channels. Traffic channel allocation in GPRS is different from that of GS
In GSM, a traffic channel is permanently allocated for a particular user during the entire ca
period (whether any data is transmitted or not). In contrast, in GPRS traffic, channels are onl
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 dat
transmission. This is known as multislot operation and uses a very flexible channel allocation. On
to eight time slots per TDMA frame can be allocated for one mobile station. Moreover, uplink an
downlink are allocated separately, which efficiently supports asymmetric data traffic like Interne
where the bandwidth requirements in uplink and downlink are different.

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 available in a cell. Thus, the radio
resources of a cell are shared by all GPRS and non-GPRS mobile stations located within the cel
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. This is done
depending on the current traffic load, the priority of the service and the multislot class. A load
supervision procedure monitors the load of the PDTCHs in the cell. According to the demand, th

number of channels allocated for GPRS can be changed. Physical channels not currently in use by GSM can be allocated as PDTCHs to increase the bandwidth of GPRS.

7.3.4 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.

7.4 GPRS Network Operations

Data transmission in a GPRS network requires several steps as described below in the context of the protocol layers described in the previous section. Once a GPRS mobile station is powered on, it "introduces" itself to the network by sending a "GPRS attach" request. Network access can be achieved from either the network side or the MS side of the GPRS network.

7.4.1 Attachment and Detachment Procedure

In order to access the GPRS services, an MS needs to make its presence known to the network. It must register itself with an SGSN of the network. This is done through a GPRS attach. This operation establishes 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 temporary mobile subscriber identity (P-TMSI) to the MS. In order to exchange data packets with external PDNs after a successful GPRS attach, a mobile station must apply for an addressee. If the PDN is an IP network, it will request for an IP address; for a X.25 network it will ask for a X.25 DTE (Data Terminal Equipment) address. This address is called PDP (Packet Data Protocol) address. For each session, a PDP context is created. It contains the PDP type (e.g., IPv4), the PDP address assigned to the mobile station (e.g., 129.187.222.10), the requested QoS, and the address of the GGSN that will function as the access point to the PDN. This context is stored in the MS, the SGSN and the GGSN. With an active PDP context, the MS is "visible" to the external PDN. A user may have several simultaneous PDP contexts active at a given time. User data is transferred transparently between the MS and the external data networks trough 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. In case of static address, the network operator permanently assigns a PDP address to the user. In the other case, a PDP address is assigned to the user upon activation of a PDP context. The PDP address can be assigned by the home network (dynamic home–PLMN PDP address) or by the visited network (dynamic visited–PLMN PDP address). In case of dynamic PDP address assignment, the GGSN is responsible for the allocation and the activation/deactivation of the PDP addresses. This function is similar to the DHCP (Dynamic Host Configuration Protocol) function.

Figure 7.3 shows the PDP context activation procedure. Using the message "activate PDP context request," the MS informs the SGSN about the requested PDP context. If the request is for dynamic

PDP address assignment, the parameter PDP address will be left empty. In following steps security functions (e.g., authentication of the user) are performed. If authentication is successful, the SGSN will send a "create PDP context request" message to the GGSN. The GGSN creates a new entry in its PDP context table, which enables the GGSN to route data packets between the SGSN and the external PDN. The GGSN returns a confirmation message "create PDP context response" to the SGSN, which contains the PDP address. The SGSN updates its PDP context table and confirms the activation of the new PDP context to the MS ("activate PDP context accept").

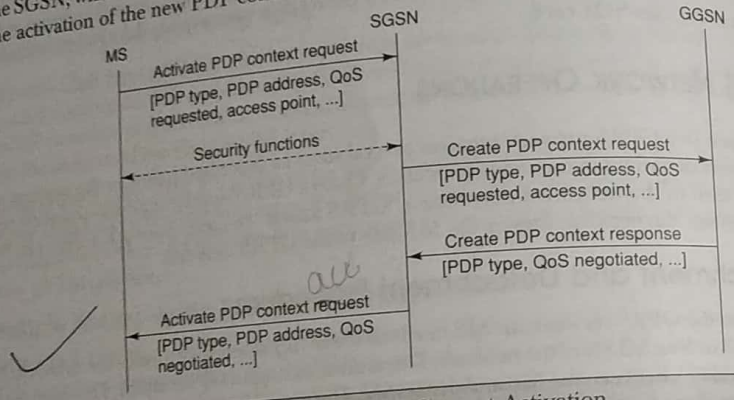


Figure 7.3 PDP Context Activation

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.

7.4.2 APN—Access Point Name

GPRS/EDGE cellular data networks use a mechanism called an Access Point Name (APN) to determine how a Mobile Station (MS), communicates via the GPRS network to a host site; in other words, how does the carrier network passes IP traffic to the host network through the SGSN and GGSN. A mobile device connects to a GPRS network by setting up a PDP (Packet Data Protocol) context. Following this, an Access Point Name (APN) is chosen according to the setting in the mobile device and the SIM card. Next, the chosen APN is used to query the network operator's Domain Name Server (DNS) server. This process gives the IP address of a GGSN allowing the PDP connection to be activated. An APN provides routing information for SGSN and GGSN and defines how users can access the data network at that entry point, what IP address are assigned to the mobile station, what security methods are used. APNs are general-purpose are available to multiple customers or can be customized for particular customers to address unique requirements. For example, some APN by default will not allow mobile terminated connections while others use RADIUS servers and require user name/password authentication in addition to SIM authentication.

7.4.3 Mobility Management

As a mobile station moves from one area to another, mobility management functions are used to track its location within each PLMN. 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. At the end of transmission or when a mobile station moves out of the area of a specific SGSN, the logical link is released and the resources associated with it can be reallocated.

7.4.4 Routing

Figure 7.4 depicts an example of how packets are routed in GPRS. The example assumes two intra-PLMN backbone networks of different PLMNs. Intra-PLMN backbone networks connect

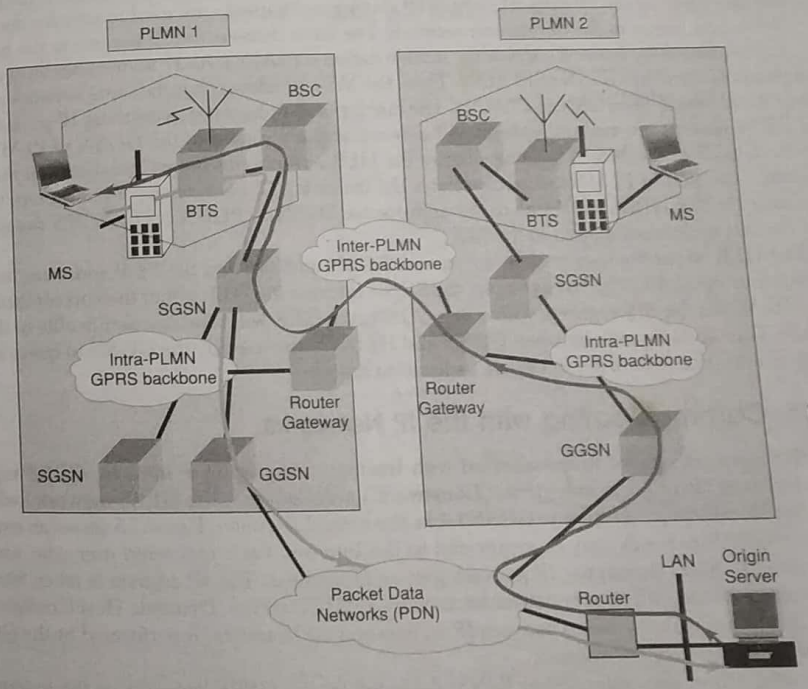


Figure 7.4 GPRS System Architecture and Routing Example

GSNs of the same PLMN or the same network operator. These are private packet-based networks of the GPRS network provider; for example, Airtel GSNs in Bangalore connecting to Airtel GSNs in Delhi through a private data network. In the diagram, these intra-PLMN networks are connected with an inter-PLMN backbone. An inter-PLMN backbone network connects GSNs of different PLMNs and operators. To install such a backbone, a roaming agreement is necessary between two GPRS network providers. For example, Airtel GSNs in Bangalore connect to Vodafone GSNs in Delhi. The gateways between the PLMNs and the external inter-PLMN backbone are called border gateways. Among other things, they perform security functions to protect the private intra-PLMN backbones against unauthorized users and attacks.

We assume that the packet data network is an IP network. A GPRS mobile station located in PLMN1 sends IP packets to a host connected to the IP network, e.g., to a Web server connected to the Internet. 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, where IP routing mechanisms are used to transfer the packets to the access router of the destination network. The latter delivers the IP packets to the host.

Let us assume the home-PLMN of the mobile station is PLMN2. An IP address has been assigned to the mobile by the GGSN of PLMN2. Thus, the MS's IP address has the same network prefix as the IP address of the GGSN in PLMN2. The correspondent host is now sending IP packets to the MS. 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.

The HLR stores the user profile, the current SGSN address, and the PDP addresses for every GPRS user in the PLMN. For example, the SGSN informs the HLR about the current location of the MS. When the MS registers with a new SGSN, the HLR will send the user profile to the new SGSN. The signaling path between GGSN and HLR may be used by the GGSN to query a user's location and profile in order to update its location register.

7.4.5 Communicating with the IP Networks

A GPRS network can be interconnected with Internet or a corporate intranet. GPRS supports both IPv4 and IPv6. From an external IP network's point of view, the GPRS network looks like any other IP sub-network, and the GGSN looks like a usual IP router. Figure 7.5 shows an example of how a GPRS network may be connected to the Internet. Each registered user who wants to exchange data packets with the IP network gets an IP address. The IP address is taken from the address space of the GPRS operator maintained by a DHCP server (Dynamic Host Configuration Protocol). The address resolution between IP address and GSM address is performed by the GGSN, using the appropriate PDP context.

Moreover, a domain name server (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. With this