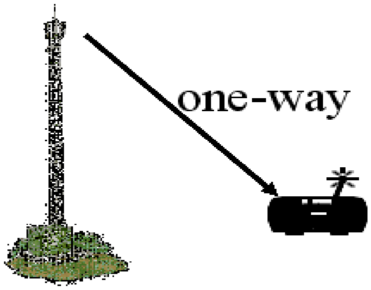
2 GSM Architecture

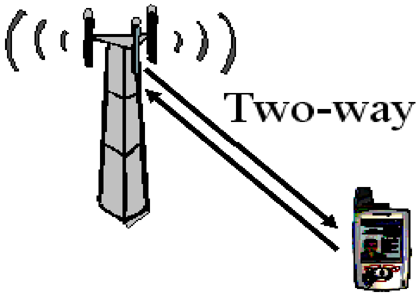
Wireless communications: Basic concepts

From ancient to modern times, mankind has been looking for means of long distance communications. For centuries, letter proved to be the most reliable way to transmit information. Fire, flags, horns, etc. were used to transmit information faster. Technical improvements in the 19th century simplified long distance communications resulting in Telegraphy, and later on telephony. Both techniques were wire line. In 1873, J.C.Maxwell laid the foundation of the electro-magnetic theory, which is still valid today. It would however several decades after (in 1895) that Marconi made economic use of this theory by developing devices for wireless transmission of Morse signals (in 1895). Voice was transmitted on wireless for the first time in 1906 (R. Fesseden), and one of the first radio broadcast transmission 1909 in New York.

Simplex



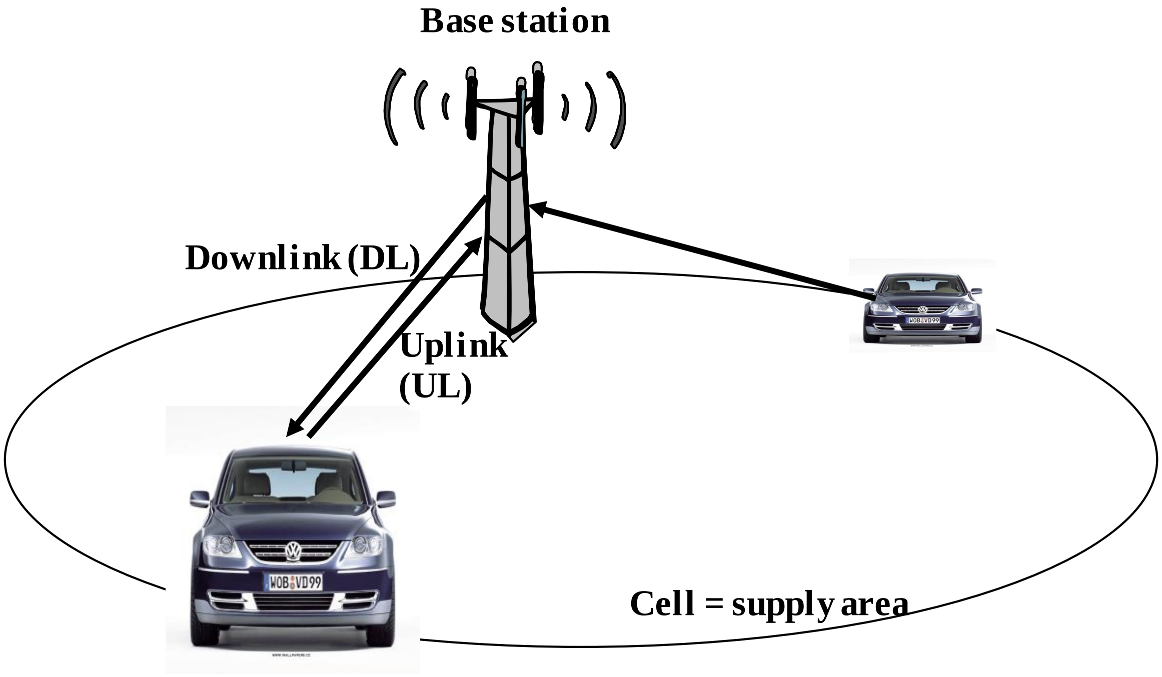
Duplex



The economically most successful wireless application in the first half of the 20th century was radio broadcast. There is one transmitter, the so-called radio station. Information, such as news, music, etc. is transmitted from the radio station to the receiver equipment, the radio device. This type of one-way transmission is called simplex transmission. The transmission takes place only in one direction, from the transmitter to the receiver. This was the first type of fixed wireless transmission.

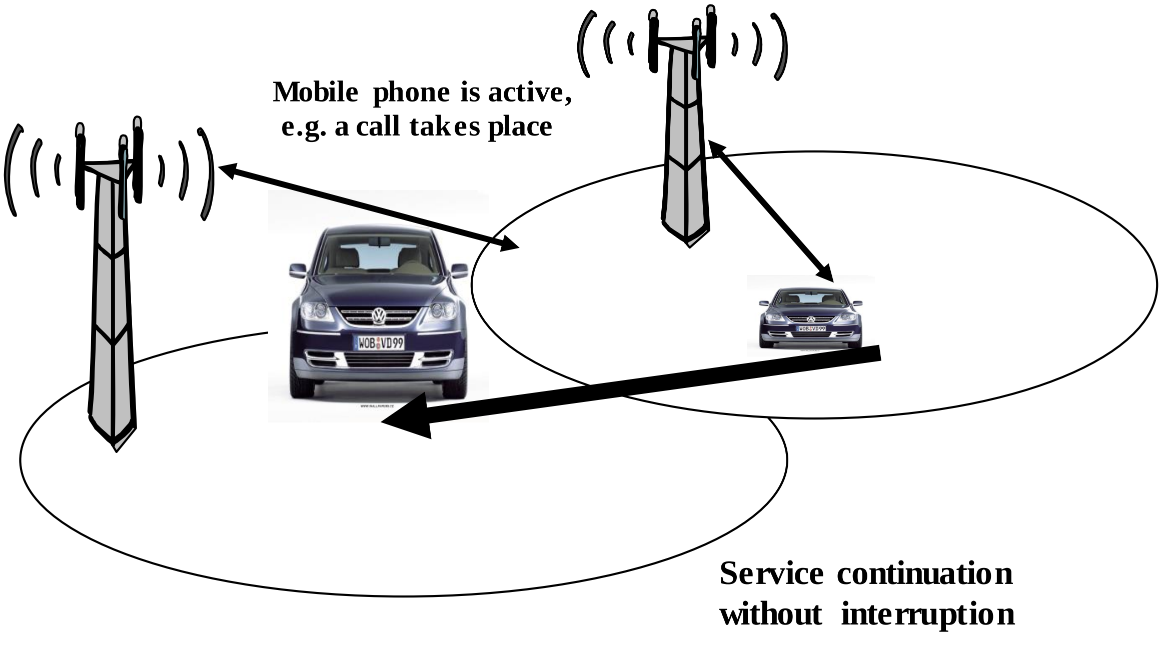
For conversation, a technical solution is required, where the information flow can take place in two directions. This type of transmission is called duplex transmission. Walky-talky was already available the early 1930i's. This system already allowed a transmission of user data in two directions, but there was a limitation: The users were not allowed to transmit at the same time. In words, you could only receive or transmit user information at any given instant of time. This type of transmission was therefore often called semi-duplex transmission. For telephony services, a technical solutions is required, where subscribers have the impression, that they can speak (transmit) and hear (receive) simultaneously. This type of transmission solution is regarded as full duplex transmission.

A limited amount of mobility along with duplex transmission resulted in the Mobile Telephony. The first commercial wireless car phone telephone service started in the late 1940 in St. Louise, Missouri (USA). It was a car phone service, because at this time, the mobile phone equipment was bulky and heavy. Actually, in the start-up, it occupied the whole back of the car. But it was a real full duplex transmission solution. In the 1950s, several vehicle radio systems were installed in Europe also. These systems are called single cell systems. The user data transmission takes place between the mobile phone and the base station (BS). A base station transmits and receives user data. While a mobile phone is only responsible for its user's data transmission and reception, a base station is capable to handle the calls of several subscribers simultaneously. The transmission of user data from the base station to the mobile phone is called downlink (DL), the transmission from the mobile phone to the base station uplink (UL) direction. The area, where the wireless transmission between mobile phones and the base station can take place, is the base stations supply area, called cell.



Single cell systems are quite limited. The more and more distant the subscriber is from the base station, the lower the quality of the radio link. If the subscriber is leaving the supply area of the cell, the communication is not possible any more. In other words, the mobile communication service was only available within the cell. In order to overcome this limitation, Multi-cellular systems were introduced. A cellular mobile communication system consists of several cells, which can overlap. By doing so, a whole geographical area can be supported with the mobile communication service.

But what happens, when a subscriber moves during a call from one cell to another cell? It would be very annoying, if the call is dropped. If the subscriber is leaving a cell, and in parallel is entering a new cell, then the system makes new radio resource available in the neighboring cell, and then the call is handed over from on cell to the next one. By doing so, service continuation is guaranteed, even when the subscriber is moving. This process is called handover (HO).



A handover takes place during a call, i.e. when the mobile phone is in active (dedicated) mode. A mobile phone can also be in idle mode. In this case, the mobile phone is switched on, but no resources are allocated to it to allow transmission of user data. In this mode, the mobile phone is still listening to information, broadcasted by the base station. Why? Imagine, there is an incoming call to this mobile. The mobile phone is then paged in the cell. This means the phone receives information that there is a mobile terminated call. A cellular system may consist of hundreds of cells. If the mobile network does not know, in which cell the mobile phone is located, it must be paged in all of them. To reduce load on networks, paging is done in small parts rather to a group of cells of a mobile network. The group cells in administrative units in a operation is called location area (LA). A mobile phone is paged in only one location area at a time. The LA is used by the GSM system to search for a subscriber in a active state.

But how does the cellular system know, in which location area the mobile phone is located? And how does the mobile phone know? In every cell, system information is continuously transmitted. The system information includes the location area information. In the idle mode, the mobile phone is listening to this system information. If the user moves from one cell to the next cell, and the new cell belongs to the same location area, the mobile stays idle. If the new cell belongs to a new location area, then the mobile phone has to become active. It starts a communication with the network; information is send to the mobile network. This is stored in databases within the mobile network, and if there is a mobile terminated call, the network knows where to page the subscriber.

The process, where the mobile phone informs the network about its new location is called Location Update Procedure (LUP). The registration of the Mobile is done at the VLR (Visitor Location Register) associated with the Mobile Switching Network.

GSM Frequency Bands

From MS to BTS or from BTS to MS the user information (Voice & Data) and the control information (signaling between MS & GSM Network) for authentication, Location Update Procedure, call setup, disconnection etc, is transmitted through the air interface over the Radio Carrier frequencies. On the basis of Radio carrier frequency band used a number of GSM systems have been developed as tabulated below:

GSM System	Up-Link	Down-Link
GSM - 850	824 – 849 MHz	869-894 MHz
GSM - 900	890-915 MHz	890-915 MHz
GSM - 1800	1710-1785 MHz	1710-1785 MHz
GSM - 1900	1710-1785 MHz	1930-1990 MHz

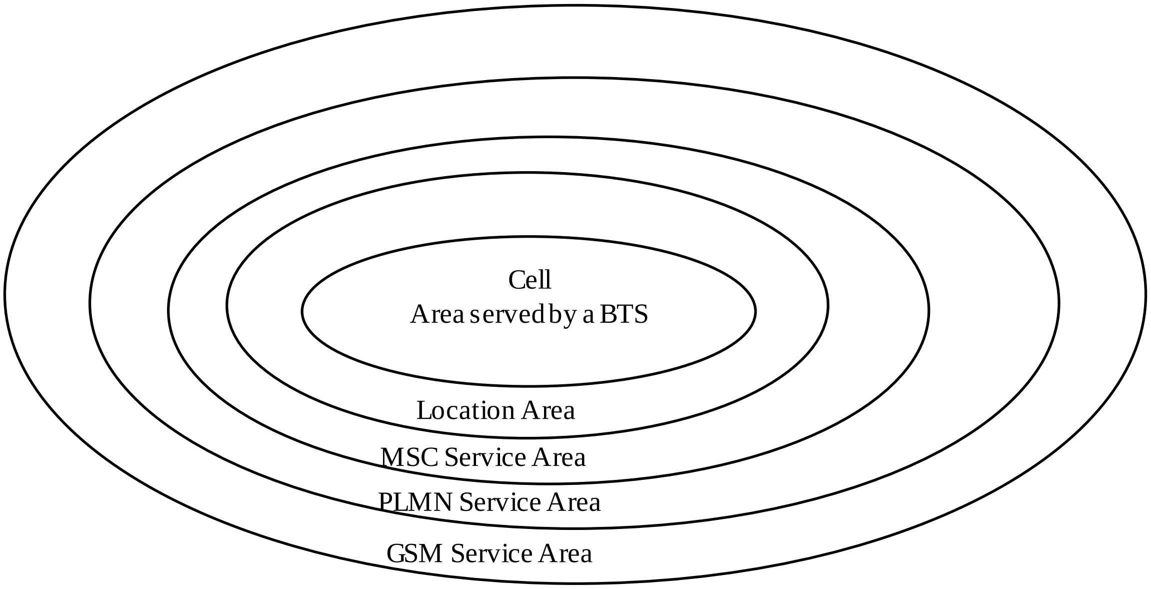
GSM Handsets

Today, most of the mobile handsets support multiple bands as used in different countries. These are typically referred to as multi-band phones. Dual-band phones can cover GSM networks in pairs such as 900 and 1800 MHz frequencies or 850 and 1900. European tri-band phones typically cover the 900, 1800 and 1900 bands giving good coverage in Europe and allowing limited use in North America, while North American tri-band phones utilize 850, 1800 and 1900 for wide-spread North American service but limited world-wide use. A new addition has been the quad-band phone, supporting all four major GSM bands, allowing for global use.

GSM NETWORK STRUCTURE

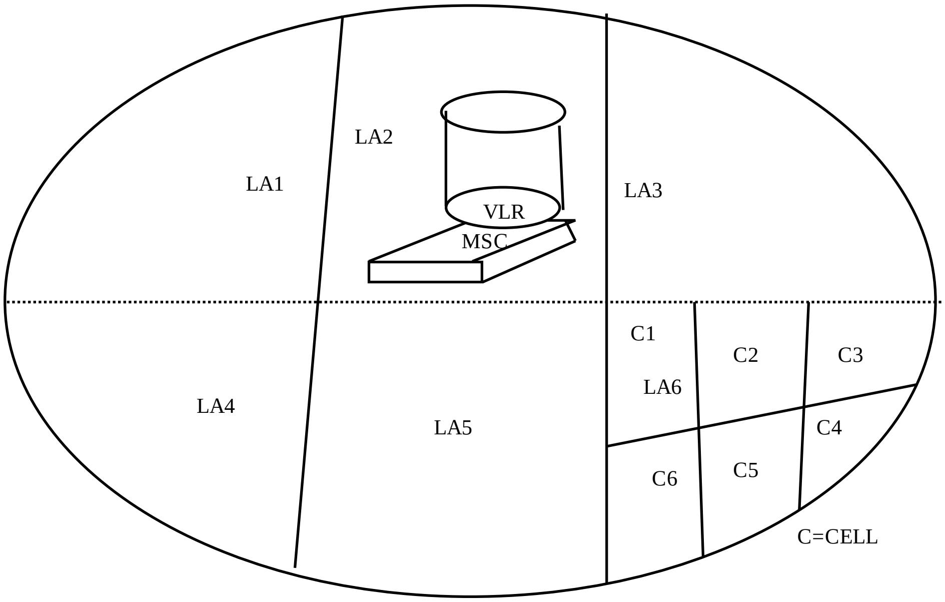
Every telephone network needs a well-designed structure in order to route incoming called to the correct exchange and finally to the called subscriber. In a mobile network, this structure is of great importance because of the mobility of all its subscribers [1-4]. In the GSM system, the network is divided into the following partitioned areas.

- GSM service area;
- PLMN (Public Land Mobile Network) service area;
- MSC (Mobile Switching Center) service area;
- Location area;
- Cells.



The GSM service is the total area served by the combination of all member countries where a mobile can be serviced. The next level is the PLMN service area. There can be several within a country, based on its size. The links between a GSM/PLMN network and other PSTN, ISDN, or PLMN network will be on the level of international or national transit exchange. Call connections between PLMNs, or to fixed networks, must be routed through certain designated MSCs called a gateway MSC. All incoming calls for a GSM/PLMN network will be routed to a gateway MSC. A gateway MSC works as an incoming transit exchange for the GSM/PLMN. In a GSM/PLMN network, all mobile-terminated calls will be routed to a gateway MSC. The gateway MSC contains the inter-working functions to make these connections. They also route incoming calls to the proper MSC within the network. The next level of division is the MSC service area. In one PLMN there can be several MSC service area. MSC has the role as a controller of calls within its jurisdiction. In order to route a call to a mobile subscriber, the path is through to the MSC in the MSC area where the subscriber is currently located. The mobile location can be uniquely identified since the MS is registered in a VLR, which is generally associated with an MSC.

The next division level is that of the LA's within a MSC combination. There are several LA's within one MSC combination. A LA is a part of the MSC/VLR service area in which a MS may move freely without updating location information to the associated MSC that control the LA. Within a LA a paging message is broadcast in order to find the called mobile subscriber. The LA can be identified by the system using the Location Area Identity (LAI).



Lastly, a LA is divided into many cells. A cell is an identity served by one BTS. The MS distinguishes the cells by the Base Station Identification Code (BSIC) of the each cell broadcast over the air.

MOBILE STATION

The wireless mobile telephone used by the subscriber is called the MS (Mobile Station). MS includes radio equipment and the man machine interface (MMI) that a user needs, in order to access the services provided by the GSM PLMN. MS can be installed in Vehicles or can be portable or hand-held. The MS may include provisions for data communication as well as voice.

Functions of MS

The primary functions of MS are to transmit and receive voice and data over the air interface of the GSM system. MS performs the signal processing function of digitizing, encoding, error protecting, encrypting, and modulating the transmitted signals. It also performs the inverse functions on the received signals from the BS.

In order to transmit voice and data signals, the mobile must be in synchronization with the network system so that the messages can be transmitted and received by the mobile at the correct instant. To achieve this, the MS automatically tunes and synchronizes to the frequency and time with the network.

The MS continuously monitors the power level and signal quality received on the downlink, by reading the error rate and strength of the signals received from its current BTS and the six surrounding BTSs. The MS sends this information to the BTS & BSC to facilitate the network to take decision on handover.

MS keeps the GSM network informed of its location during both national and international roaming, even when it is inactive. This enables the System to page it in its present LA.

Finally, the MS can store and display short alphanumeric messages on the liquid crystal display (LCD) that is used to show call dialing and status information. These messages are limited to 160 characters in length. (Some mobiles handsets are capable of taking more characters and then splicing into smaller parts while sending)

Power Levels

There are five different categories of mobile telephone units specified by the European GSM system: The 20-W and 8-W units (peak power) are either for vehicle-mounted or portable station use. The handsets normally used are of 2W.

The MS power is adjustable in steps from its normal value down up to 20mW. This is done automatically under remote control from the BTS, which monitors the received power and adjusts the MS transmitter to the minimum power setting necessary for reliable transmission.

Subscriber Identity Module (SIM) Card

The SIM is a removable smart card bearing a unique identification number. At the very beginning of the service, GSM subscribers are provided with a SIM card. The subscriber is identified in the system when the user inserts the SIM card in the mobile equipment. This provides an enormous amount of flexibility to the subscribers since they can now use the SIM in the mobile equipments, as the SIM card is portable between Mobile Equipment (ME) units. The user only needs to take his smart card on a trip. He can then rent a ME unit at the destination, even in another country, and insert his own SIM. Any calls he makes will be charged to his home GSM account. Also, the GSM system will be able to reach him at the ME unit he is currently using.

The SIM contains an integrated circuit chip with a microprocessor, random access memory (RAM), and read only memory (ROM).

When a mobile subscriber wants to use the system, user mounts the SIM card and provides the Personal Identification Number (PIN), which is compared with a PIN stored within the SIM. If the user enters three incorrect PIN codes, the SIM is disabled. The PIN can also be permanently bypassed by the service provider, if requested by the subscriber. Disabling the PIN code simplifies the call setup but reduces the protection of the user’s account in the event of a stolen SIM card.

Each MS is identified by a unique identification number named as International Identification Number (IMEI), which is permanently stored in the mobile unit. Upon request, the MS sends this number over the signaling channel to the MSC. The IMEI can also be used to identify mobile units those are reported stolen or operating incorrectly.

Just as the IMEI identifies the mobile equipment, mobile subscribers are identified by their internationally unique numbers named as International Mobile Subscriber Identity (IMSI). Different subscriber identities are used in different phases of call setup. The IMSI is the primary function to identify the subscriber within the mobile network and is permanently assigned to him. The Mobile Station International Subscriber Directory Network Number (MSISDN) is the number that the calling party dials in order to reach the subscriber. It is used by the landline or other network to route calls toward an appropriate MSC.

International Mobile Equipment Identity (IMEI)

The IMEI is the unique identity of the equipment used by a subscriber and is used to determine authorized (white), unauthorized (black), and malfunctioning (gray) GSM hardware. In conjunction with the IMSI, it is used to ensure that only authorized user are granted access to the system. An IMEI is never sent in cipher mode by MS.

International Mobile Subscriber Identity (IMSI).

An IMSI is assigned to each authorized GSM user. It consists of a mobile country code (MSC), mobile network code (MNC), and a PLMN unique mobile subscriber identification number (MSIN). The IMSI is not hardware-specific. Instead, it is maintained on a SC by an authorized subscriber and is the only absolute identity that a subscriber has within the GSM system. The IMSI consists of the MCC followed by the NMSI and shall not exceed 15 digits.

Mobile Station International Subscriber Directory Number (MSISDN)

The MSISDN number is composed of the country code (CC) followed by the National Significant Number (N (S) N), which shall not exceed 15 digits. In order to obtain a mobile subscriber in another country, the MS should dial an international prefix before the MSISDN. (Example: 919412024567)

Network Details:

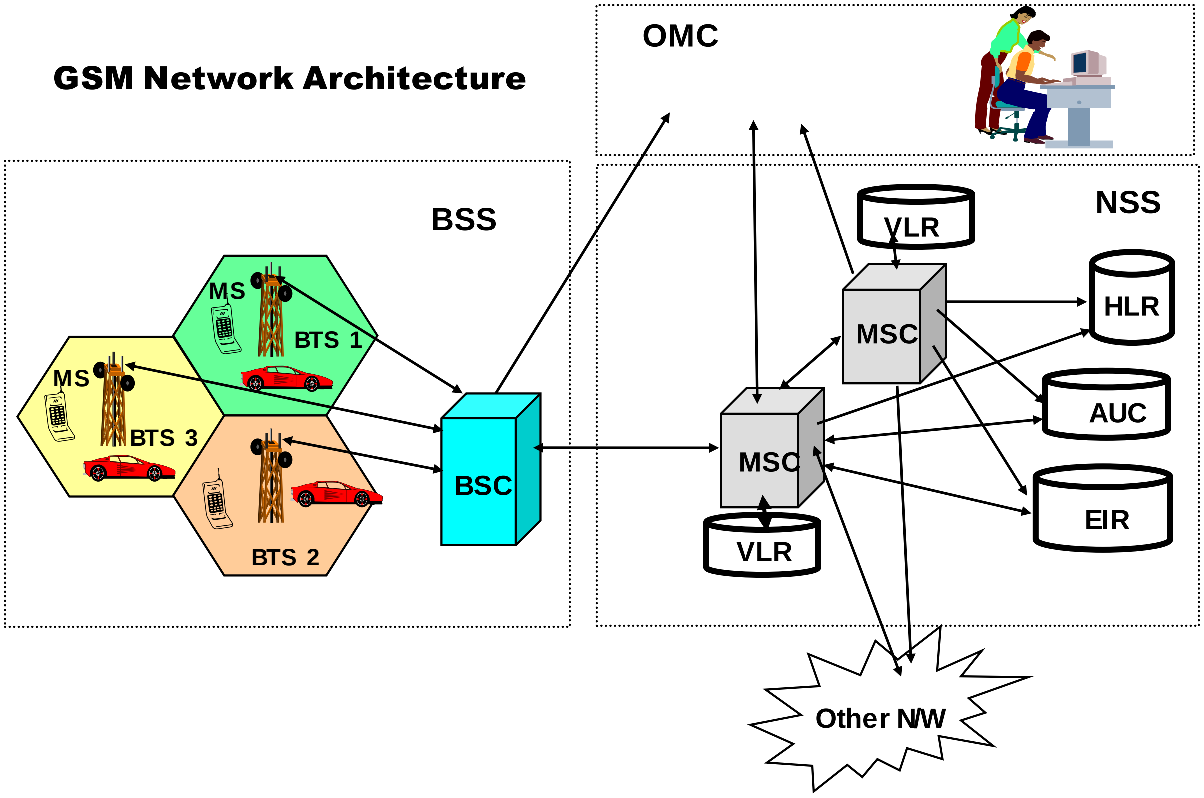
(1) Base Station Subsystem (BSS) :

BTS	-	Base Transrecieve Station
BSC	-	Base Station Controller
MS	-	Mobile Station

(2) Network Switching Subsystem (NSS):

MSC	-	Mobile Switching Centre
VLR	-	Visitor Location Register
HLR	-	Home Location Registered
AuC	-	Authentication Centre
EIR	-	Equipment Identity Register

(3) OMC	-	Operation & Maintenance Centre


GSM Network Architecture

(4) Important Intefaces:

Interface		Interfacing Nodes
Um	-	MS and BTS
Abis	-	BTS and BSC
A	-	BSC and MSC

BASE STATION SUBSYSTEM (BSS)

The BSS is a set of Base Station equipments, such as BTS & BSC, responsible for communicating with MSs in a certain area. The BSS includes two types of machines: the BTS in contact with the MSs through the radio interface and the BSC, the latter being in contact with the MSC. BSS is the system interfaced with MSC. BSC is the nodal unit in the BSS. A BSC is a network component in the PLMN that functions for the control of one or more BTS. It is a functional entity that handles common control functions within a BTS. Typically one BSC can control more than one BS or BTS. The radio equipment of a BSS may be composed of one or more cells. A BSS may consist of one or more BTS. The mobile function is divided basically between transmission equipment, the BTS, and managing equipment at the BSC. A BTS comprises of radio transmission and reception devices, including the antennas, and also all the signal processing specific to the radio interface. A single transceiver within BTS supports eight basic radio channels.

An important component of the BSS that is considered in the GSM architecture is the Transcoder/Rate Adapter Unit (TRAU). The TRAU is the equipment in which coding and decoding is carried out as well as rate adaptation in case of data. Although the specifications consider the TRAU as a sub-part of the BTS, it can be sited away from the BTS (at BSC), and even between the BSC and the MSC.

The interface between the MSC and the BSS is a standardized SS7 interface (A-interface) that is fully defined in the GSM recommendations. This allows the system operator to purchase switching equipment from one supplier and radio equipment and the controller from another. The interface between the BSC and a remote BTS is a standard interface known as the A-bis. In splitting the BSS functions between BTS and BSC, the main principle was that only such functions that had to reside close to the radio transmitters/receivers should be placed in BTS. This will also help reduce the complexity of the BTS.

Functions of BTS

A BTS is a network component that serves one cell and is controlled by a BSC. BTS is typically able to handle three to five radio carries, carrying between 24 to 40 simultaneous communications. Reducing the BTS volume is important to keeping down the cost of the cell sites. The primary responsibility of the BTS is to transmit and receive radio signals from a mobile unit over the air interface. To perform this function effectively, the signals are encoded, encrypted, multiplexed, modulated, and then fed to the antenna system at the cell site. In order to keep the mobile station synchronized, BTS broadcasts frequency and time synchronization signals. Similarly, the received signal from the mobile is decoded, decrypted, and equalized for channel impairments.

Uplink radio channel measurement is made by the BTS and corresponding downlink measurements made by MS.

For the communication between MS and BTS, there are various types of channels to carry the voice & data facilitate call handling & control functions etc. Some channels like Paging, Power control, traffic etc. are dedicated for control functions and traffic channels are dedicated for transportation of user's data (Voice/data).

BTS-BSC Configurations

There are several BTS-BSC configurations: single site; single cell; single site -multicell; and multisite-multicell. These configurations are chosen based on the rural or urban application. These configurations make the GSM system economical since the operation has options to adapt the best layout based on the traffic requirement. Thus, in some sense, system optimization is possible by the proper choice of the configuration.

For example, in rural areas, most BTSs are installed to provide maximum coverage rather then maximum capacity, whereas in urban setup, capacity per BTS is the deciding factor; means in order to cover the same area as in rural more number of BTSs will be required in Urban.

Functions of BSC

The BSC, as discussed, is connected to the MSC on one side and to the BTS on the other. The BSC performs the Radio Resource (RR) management for the cells under its control. It assigns and release frequencies and time slots for all MSs in its own area through the BTSs. The BSC performs the inter cell handover for MSs moving among the BTSs in its control. The BSC controls the power transmission of both BTSs and MSs in its area. The BSC provides the time and frequency synchronization reference signals which is further broadcast by its

BTSs. The BSC also measures the time delay of received MS signals relative to the BTS clock. If the received MS signal is not centered in its assigned timeslot at the BTS, The BSC can direct the BTS to notify the MS to advance the timing such that proper synchronization takes place.

The BSC may also perform traffic concentration to reduce the number of transmission lines from the BSC to its BTSs, or to MSC.

NETWORK SWITCHING SUBSYSTEMS (NSS):

The Network Switching Subsystem includes the main switching functions of GSM as well as the databases needed for subscriber data and mobility management. The MSC also manages the communications between the GSM users and other telecommunication network users. The basic switching function like setting up calls to and from GSM users is performed by the MSC. The MSC has interface with the BSS on one side (through which MSC/VLR is in contact with GSM users) and the external networks on the other (ISDN/PSTN/PSPDN) & other PLMN or MSCs.

Functions of MSC

The main function of the MSC is to coordinate the set up of calls between GSM mobile and other telecom users. Specifically, it performs functions such as paging, resource allocation, location registration, and encryption.

The MSC is a telephony switch that performs all the switching functions for MSs located in a geographical area i.e. in the MSC area. The MSC must also handle different types of numbers and identities related to the same MS and contained in different registers: In general, identities are used in the interface between the MSC and the MS, while numbers are used in the fixed part of the network, such as, for routing. The main difference between a MSC and an exchange in a fixed network is that the MSC has to take into account the impact of the allocation of Radio Resources and the mobile nature of the subscribers and hence has to perform, in addition, the activities required for the location registration and handover.

Specifically, the call-handling function of paging is controlled by MSC. The dynamic allocation of access resources is done in coordination with the BSS. More specifically, the MSC decides when and which types of channels should be assigned to which MS. The channel identity and related radio parameters are the responsibility of the BSS; The MSC also provides the control of interworking with different networks. It is transparent for the subscriber authentication procedure.

The MSC supervises the connection transfer between different BSSs for MSs. This is ensured if the two BSSs are connected to the same MSC but also when they are not. The connection transfer procedure is more complex, when more then one MSCs are involved. The MSC performs billing on calls for all subscribers based in its areas. When the subscriber is roaming elsewhere, the MSC obtains data for the call billing from the visited MSC. The exchange of signaling information on the various interfaces towards the other network elements and the management of the interfaces themselves are all controlled by the MSC. Finally, the MSC serves as a SMS gateway to forward SMS messages from Short Message Service Centers (SMSC) to the subscribers and from the subscribers to the SMSCs. It thus acts as a message mailbox and delivery system.

Visitor Location Register (VLR)

The VLR is co-located with an MSC. A VLR may be in charge of one or several MSC LA’s. The VLR constitutes the databases that support the MSC in the storage and retrieval of the data of all subscribers present at given time, in its area. When an MS enters the MSC area borders, it signals its arrival to the MSC, which subsequently stores its identity in the VLR. An MS roaming in an MSC area is controlled by the VLR, responsible for that area. When a MS appears in a LA, it starts a registration procedure. The MSC for that area notices this registration and transfers the identity of the LA where the MS is situated to the current VLR. The information necessary to manage the MS is available in the HLR and is transferred to the VLR so that they can be easily retrieved whenever required.

HOME LOCATION REGISTER

The HLR is a database that permanently stores data related to a given set of subscribers registered to the GSM operator in the area served by that HLR. The HLR is the reference database for subscriber parameters. Various identification numbers and addresses as well as authentication parameters, services subscribed, and special routing information etc. are stored. Current subscriber status including a subscriber’s temporary roaming number and associated VLR, if the mobile is roaming, is also maintained in the HLR.

The HLR provides data needed to route calls to all home based MS-SIMs in its MSC area, even when they are roaming out of area or in other GSM networks. The HLR provides the current location data needed to support searching for and paging the MS-SIM for incoming calls, wherever the MS-SIM may be. The HLR is responsible for storage and provision of SIM authentication and encryption parameters needed by the MSC where the MS-SIM is operating. It obtains these parameters from the AUC.

The HLR maintains records such as which supplementary service each user has subscribed to and provides permission for granting services to the user depending on that. The HLR stores the identification of SMS gateways those have messages for the subscriber until they can be transmitted to the subscriber and receipt is acknowledged.

In HLR some data are mandatory, some others are optional. Both the HLR and the VLR can be implemented in the same equipment in an MSC (co-located). A PLMN may contain one or several HLRs. More than one MSC can be connected to one HLR.

AUTHENTICATION CENTER (AUC)

The AUC stores information that is necessary to protect communication through the air interface against intrusions, to which the mobile is vulnerable. The legitimacy of the subscriber is established through authentication and ciphering, which help to protect the user information against unwanted disclosure. Authentication information and ciphering keys are stored in a database within the AUC, which protects the user information against unwanted disclosure and access. This is achieved by sending some randomly generated secret key words (Random Number). Even while the MS on roaming, cipher key is sent through the visited MSC.

The random number and cipher key is supposed to change with each phone call, so finding them on one call will not benefit using them on the next call.

The HLR is also responsible for the “authentication” of the subscriber each time he makes or receives a call. The AUC, which actually performs this function, is a separate GSM entity that will often be physically installed with the HLR. Being separate, it will use separate processing equipment for the AUC database functions.

EQUIPMENT IDENTIFY REGISTER (EIR)

EIR is a database that stores the IMEI numbers for all registered ME units. The EIR uniquely identifies all the registered MEs. There is generally one EIR per PLMN. It interfaces to the various HLRs in the PLMN. The EIR keeps track of all ME units in the PLMN. It maintains various lists of message. The database stores the ME identification and has nothing do with subscriber who is receiving or originating call. There are three classes of ME that are stored in the database and each group has different characteristics.

- White List: contains those IMEIs that are known to have been assigned to valid MS's. This is the category of genuine equipment.
- Black List: contains IMEIs of mobiles that have been reported stolen.
- Gray List: contains IMEIs of mobiles that have problems (for example, faulty software and wrong make of the equipment). This list contains all MEs with faults not important enough for barring.

ECHO CANCELER

Echo Canceller is used on the PSTN side of the MSC for all voice call between Mobile subscriber and the landline. The EC is required at the MSC-PSTN interface to reduce the effect of GSM delay when the mobile is connected to the PSTN circuit. GSM link through a hybrid transformer in the circuit. The delay causes the echo, which does not affect the land line subscriber but is an annoying factor to the mobile. The standard EC cancels the delay.

OPERATION AND MAINTENANCE CENTER

Maintenance cover both technical and administrative actions to maintain and correct the system operation, or to restore normal operations after a breakdown, in the shortest possible time. The status of network devices can be checked, and tests and diagnostics on various devices can be invoked through OMC. The OMC also provides alarm-handling functions to report and log alarms generated by the network entities. The maintenance personnel at the OMC can define the criticality of the alarm.

The fault management functions of the OMC allow network devices to be manually or automatically removed from or restored to service. For example, diagnostics may be initiated remotely by the OMC. A mobile call trace facility can also be invoked. The performance management functions include collecting traffic statistics from the GSM network entities and archiving them in disk files or displaying them for analysis. Because of the potential to collect large amounts of data, maintenance personnel can select which of the detailed statistics to be collected based on requirements and past experience. As a result of performance analysis, if necessary, an alarm can be set remotely.

The OMC provides control system for changes for the software revisions and configuration of data bases in the network entities. The OMC also keeps track of the different software versions running on different subsystem of the GSM.

MOBILE INTELLIGENT NETWORK (MOBILE IN)

Mobile IN is used in combination with the public Land Mobile Network (PLMN). It consists of service nodes that provide advanced services to subscribers. Mobile IN functions include the Service Switching Point (SSP) and the Service Control Point (SCP) or a combined Service Switching and control point (SSCP). Mechanisms to support operator-specific services that are not covered by standardized GSM services even while roaming outside the Home PLMN are provided by the Customized Applications for Mobile network Enhanced Logic (CAMEL).