**UNIT-II**

**GSM**

GSM (**Global System for Mobile communication**) is **a digital mobile telephony system** that is **widely used in Europe and other parts of the world**. GSM **uses a variation of time division multiple access (TDMA**) and is the **most widely used** of the three digital wireless telephony technologies (TDMA, GSM, and CDMA).

**1. Mobile Services:**

Global System for Mobile Communications (GSM) services are a **standard collection of applications and features** available **to mobile phone subscribers all over the world**. The GSM standards are defined by the 3GPP collaboration and implemented in hardware and software by equipment manufacturers and mobile phone operators.

GSM offers three basic types of services:

* Telephony services or teleservices
* Data services or bearer services
* Supplementary services

**i.Teleservices:**

The abilities of a Bearer Service are used by a Teleservice to transport data. These services are further transited in the following ways:

**Voice Calls**

The most basic Teleservice supported by GSM is telephony. This includes full-rate speech at 13 kbps and emergency calls, where the nearest emergency-service provider is notified by dialing three digits.

**Videotext and Facsmile**

Another group of teleservices includes Videotext access, Teletex transmission, Facsmile alternate speech and Facsmile Group 3, Automatic Facsmile Group, 3 etc.

**Short Text Messages**

Short Messaging Service (SMS) service is a text messaging service that allows sending and receiving text messages on your GSM mobile phone. In addition to simple text messages, other text data including news, sports, financial, language, and location-based data can also be transmitted.

**ii. Bearer Services:**

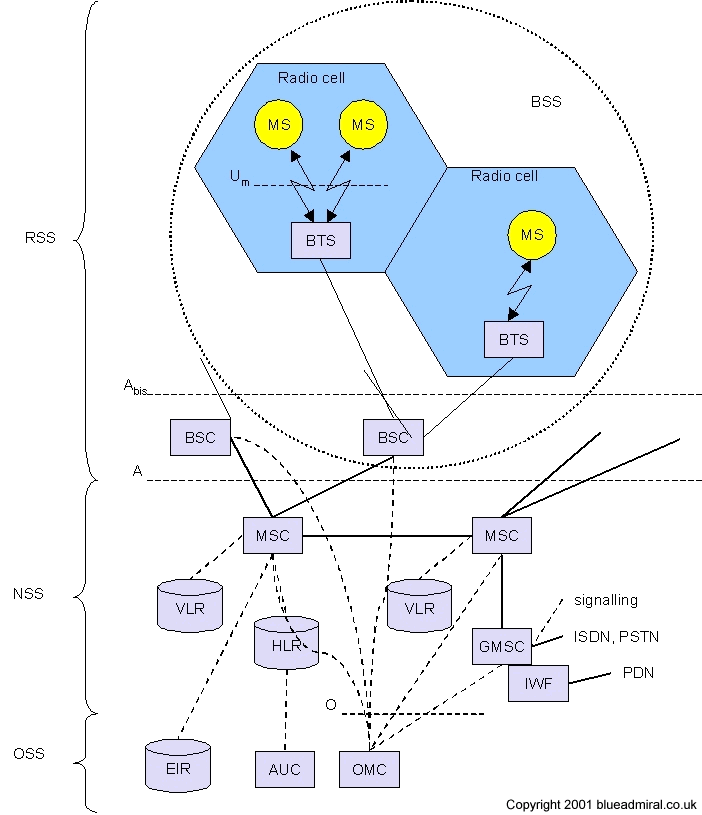
Data services or Bearer Services are **used through a GSM phone**. **to receive and send data** is the **essential building block** leading **to widespread mobile Internet access and mobile data transfer.** **GSM currently has** a **data transfer rate of 9.6k.** New developments that will push up data transfer rates for GSM users are HSCSD (high speed circuit switched data) and GPRS (general packet radio service) are now available.

**iii. Supplementary Services:**

Supplementary services are additional services that are provided in addition to teleservices and bearer services. These services include caller identification, call forwarding, call waiting, multi-party conversations, and barring of outgoing (international) calls, among others. A brief description of supplementary services is given here:

* **Conferencing**: It allows a mobile subscriber to establish a multiparty conversation, i.e., a simultaneous conversation between three or more subscribers to setup a conference call. This service is only applicable to normal telephony.
* **Call Waiting**: This service notifies a mobile subscriber of an incoming call during a conversation. The subscriber can answer, reject, or ignore the incoming call.
* **Call Hold**: This service allows a subscriber to put an incoming call on hold and resume after a while. The call hold service is applicable to normal telephony.
* **Call Forwarding**: Call Forwarding is used to divert calls from the original recipient to another number. It is normally set up by the subscriber himself. It can be used by the subscriber to divert calls from the Mobile Station when the subscriber is not available, and so to ensure that calls are not lost.
* **Call Barring**: Call barring is useful to restrict certain types of outgoing calls such as ISD or stop incoming calls from undesired numbers. Call barring is a flexible service that enables the subscriber to conditionally bar calls.
* **Number Identification** : There are following supplementary services related to number identification:
  + **Calling Line Identification Presentation**: This service displays the telephone number of the calling party on your screen.
  + **Calling Line Identification Restriction**: A person not wishing their number to be presented to others subscribes to this service.

**2. GSM Architecture:**

`

The GSM technical specifications define the different elements within the GSM network architecture. It defines the different elements and the ways in which they interact to enable the overall system operation to be maintained.

The GSM network architecture is now well established and with the other later cellular systems now established and other new ones being deployed, the basic GSM network architecture has been updated to interface to the network elements required by these systems.

Despite the developments of the newer systems, the basic GSM system architecture has been maintained, and the network elements described below perform the same functions as they did when the original GSM system was launched in the early 1990s.GSM network architecture elements

The GSM network architecture as defined in the GSM specifications can be grouped into four main areas:

* Radio Subsystem (RSS)
* Network Subsystem (NSS)
* Operation Subsystem (OSS)

The different elements of the GSM network operate together and the user is not aware of the different entities within the system.

**i. Radio Subsystem:**

## Mobile station

**Mobile stations (MS), mobile equipment (ME)** or as they are **most widely known**, **cell or mobile phones** are the **section of a GSM cellular network** that **the user sees and operates**. In **recent years their size has fallen dramatically while the level of functionality has greatly increased**. A further advantage is that the time between charges has significantly increased.

There are a number of elements to the cell phone, although the **two main elements are the main hardware and the SIM**.

The **hardware itself contains the main elements of the mobile phone** including the display, case, battery, and the electronics used to generate the signal, and process the data receiver and to be transmitted. It also **contains a number known as the International Mobile Equipment Identity (IMEI). This** is installed in the phone at manufacture and "cannot" be changed. It is **accessed by the network during registration to check whether the equipment has been reported as stolen**.

The **SIM or Subscriber Identity Module contains the information that provides the identity of the user to the network**. It contains are variety of information including **a number known** as the **International Mobile Subscriber Identity (IMSI).**

## Base Station Subsystem (BSS)

The Base Station Subsystem (BSS) section of the GSM network architecture that **is fundamentally associated with communicating with the mobiles on the network**. It consists of two elements:

* ***Base Transceiver Station (BTS):***   The BTS used in a GSM network comprises the radio **transmitter receivers, and their associated antennas** that **transmit and receive to directly communicate with the mobiles**. The BTS is the defining element for each cell. The BTS communicates with the mobiles **and the interface** between the two is known as **the Um** **interface** with its associated protocols.
* ***Base Station Controller (BSC):***   The BSC forms the next stage back into the GSM network. It **controls a group of BTSs,** and is **often co**-**located with one of the BTSs** in **its group**. It **manages** the radio resources and controls items such as h**andover** within the **group of BTSs**, allocates channels and the like. It communicates with the BTSs over what is termed the Abis interface.

**ii. Network Subsystem (NSS)**

The GSM system architecture contains a variety of different elements, and is often termed the core network. It provides the main control and interfacing for the whole mobile network. The major elements within the core network include:

***Mobile Services Switching Centre (MSC):***   The main element within the core network area of the overall GSM network architecture is the Mobile switching Services Centre (MSC). The MSC acts like a normal switching node within a PSTN or ISDN, but also provides additional functionality. These include **registration, authentication, call location, inter-MSC handovers and call routing to a mobile subscriber**. It also provides an interface to the PSTN so that calls can be routed from the mobile network to a phone connected to a landline. Interfaces to other MSCs are provided to enable calls to be made to mobiles on different networks.

***Home Location Register (HLR):***   This database contains all the administrative information about each subscriber along with their last known location. In this way, the GSM network is able to route calls to the relevant base station for the MS. When a user switches on their phone, the phone registers with the network and from this it is possible to determine which BTS it communicates with so that incoming calls can be routed appropriately. Even when the phone is not active (but switched on) it re-registers periodically to ensure that the network (HLR) is aware of its latest position. There is one HLR per network.

***Visitor Location Register (VLR):***   This contains selected information from the HLR that enables the selected services for the individual subscriber to be provided. The VLR can be implemented as a separate entity**, but it is commonly realised as an integral part of the MSC**, rather than a separate entity. In this way access is made faster and more convenient.

***Gateway Mobile Switching Centre (GMSC):***   The GMSC is the point to which a ME terminating call is initially routed, without any knowledge of the MS's location. The GMSC is thus in charge of obtaining the MSRN (Mobile Station Roaming Number) from the HLR based on the MSISDN (Mobile Station ISDN number, the "directory number" of a MS) and routing the call to the correct visited MSC. The "MSC" part of the term GMSC is misleading, since the gateway operation does not require any linking to an MSC.

**iii. Operation Subsystem (OSS)**

The OSS or operation support subsystem is an element within the overall GSM network architecture that is connected to components of the NSS and the BSC.

It is used to **control** and **monitor** the overall GSM network and it is also used to control the traffic load of the BSS.

Elements of **OSS** include:

***Equipment Identity Register (EIR):***   The EIR is the entity that **decides whether a given mobile equipment may be allowed onto the network**. Each mobile equipment has a number known as **the International Mobile Equipment Identity**. This number, as mentioned above, is installed in the equipment and is checked by the network during registration. Dependent upon the information **held in the EIR**, the mobile may be allocated **one of three states** - **allowed onto the network**, **barred access**, or **monitored in case its problems**.

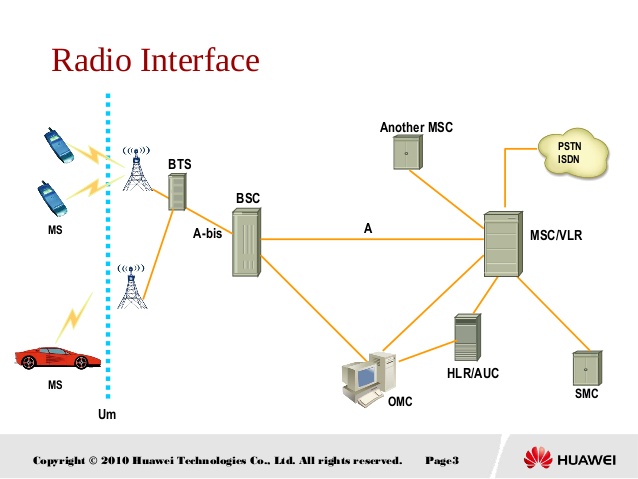
***Authentication Centre (AuC):***   **The AuC is a protected database** that contains the **secret key** **also contained in the user's SIM card**. It is **used for authentication and for ciphering** on the **radio channel.**

***Operation Maintenance Center (OMC):***  OMC is used **to monitor and maintain** the **performance of each Mobile Station (MS), Base Station (BS), Base Station Controller (BSC) and Mobile Switching Center (MSC) within a GSM system**. The OMC has **three main functions** which are:

* To maintain all telecommunications hardware and network operations with a particular market.
* Manage all charging and billing procedures.
* Manage all mobile equipment in the system.

The OMC is dedicated to each of these tasks and has provisions for adjusting all base station parameters and billing procedures, as well as for providing system operators with the ability to determine the performance and integrity of each piece of subscriber equipment in the system.

**3. Radio Interface:**



[www.slideshare.net](https://www.google.co.in/imgres?imgurl=https://image.slidesharecdn.com/gsm-radio-interface-140720014203-phpapp02/95/gsm-radiointerface-3-638.jpg%3Fcb%3D1405820596&imgrefurl=https://www.slideshare.net/engwaraabe1/gsm-radiointerface&h=479&w=638&tbnid=nNbzoauBDBTJ4M:&tbnh=158&tbnw=211&usg=__jEn85l3w2GpuCQWppLwnCU4EQ18=&vet=1&docid=Ny7cwgO5mTlwbM&sa=X&ved=0ahUKEwiU4v2NxeDVAhXGpI8KHRwjCU0Q9QEIKzAA)

**Um interface. The Um interface is the air interface for the GSM mobile telephone standard**. It is the **interface** **between the mobile station (MS) and the Base transceiver station (BTS).** It is called Um because it is the mobile analog to the U **interface** of ISDN.

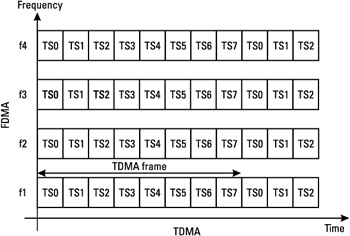
## Currently, there are several types of networks in the world using the GSM standard, but at different frequencies.

* The GSM-900 is the most common in Europe and the rest of the world. Its extension is E-GSM.
* The DCS-1800 operates in the 1,800-MHz band and is used mainly in Europe, usually to cover urban areas. It was also introduced to avoid saturation problems with the GSM-900.
* The PCS-1900 is used primarily in North America.
* The GSM-850 is under development in America.
* The GSM-400 is intended for deployment in Scandinavian countries in the band previously used for the analog *Nordic Mobile Telephony* (NMT) system.

The system **is based on *frequency-division duplex* (FDD**), which means that **the uplink** (radio link from the mobile to the network-that is, mobile transmit, base receive), and **downlink (from the network to the mobile-that is, base transmit, mobile receive**) are **transmitted on different** **frequency bands.** For instance, in the 900-MHz E-GSM band, the block 880-915 MHz is used for transmission from mobiles to network, and the block 925-960 MHz is used for the transmission from network to mobiles

Operators may implement networks that operate on a combination of the frequency bands listed above to support multiband mobile terminals.

There are **different ways of sharing the physical resource among all the users in a radio system**, and this is called **the multiple-access method.** The **multiple-access scheme defines how simultaneous communications share the GSM radio spectrum.** The **various multiple-access techniques** in use in radio systems are ***frequency-division multiple access* (FDMA**), **TDMA,** and *code-division multiple access* (**CDMA)**. **GSM is based on both FDMA and TDMA techniques (see Figure 1.3).**

 Figure 1.3: TDMA and FDMA.

**FDMA** consists in **dividing the frequency band of the system into several channels**. In GSM, **each RF channel has a bandwidth of 200 kHz**, which is u**sed to convey radio modulated signals, or carrier**s**. Each pair of uplink/ downlink channels is called an *absolute radio frequency channel* (ARFC) and is assigned an *ARFC number* (ARFCN**). The mapping of each ARFCN on the corresponding carrier frequency is given in [3].

TDMA is the **division of the time into intervals**: **within a frequency channel**, t**he time is divided into time slots**. **This division allows several users (eight) to be multiplexed on the same carrier frequency, each user being assigned a single time slot**. A packet of data information, called a burst, is transmitted during a time slot. The succession of eight time slots is called **a TDMA frame**, and each time slot belonging to a TDMA frame is identified by a *time slot number* (TN), from 0 to 7.

### Logical Channels

The **association of a radio frequency channel and a time slot**-**the pair ARFCN and TN**-uniquely defines a physical channel on both the uplink and the downlink.

On top of the physical channels, **logical channels ar mapped to convey the information of voice, data, and signaling**. This signaling information is used for setting up a call, or to adapt the link to rapidly changing radio conditions, or to manage handovers, to give a few examples. **Logical channels can be seen as pipes**, each one used for a different purpose by the higher layers of the system.

**Two types of logical channels exist, traffic channels and control channels**. Among the **control channels, according to their functions**, **four classes are defined**: **broadcast, dedicated, common, and associated**. A broadcast channel **is used by the network (in downlink only) to send general information to the MSs**. **A channel is said to be dedicated** if **only one MS can transmit or receive in the ARFCN-TN defining this channel**, and c**ommon** if it **carries information for several mobiles**. An associated control channel is allocated to one mobile, in addition to a dedicated channel, and carries signaling for the operation of this channel.

The broadcast channels are transmitted on the **beacon carrier frequency**. The purposes of the beacon are:

* **To allow a synchronization** in **time and frequency of the MSs to the BTS**. This synchronization **is needed by the MS to access the services of a cell.**
* **To help the mobile in estimating the quality of the link** during a communication, by measurements on the received signal from the BTS it is transmitting to, and from the other BTSs of the geographical area. These **measurements are used by the network** to **determine when a handover is necessary**, and **to which BTS** this handover should apply.
* To **help the mobile in the selection of a cell when it is in idle mode** (that is, not in communication, but still synchronized to the system and able to receive an incoming call or to initiate a call). This **selection is performed on the basis of the received power** measurements **made on the adjacent cells' beacon channels**.
* To **access the general parameters of the cell needed for the procedures applied by the MS**, or **general information concerning the cell**, such as its identification, the beacon frequencies of the surrounding cells, or the option supported by the cell (services).

To allow these various operations, the **logical channels transmitted on the beacon** are:

* **The *broadcast control channel* (BCCH)**, which continually broadcasts, on the downlink, general information on the cell, including base station identity, frequency allocations, and frequency-hopping sequences. The **information is transmitted within *system information* (SI) blocks**, which **can be of different types according** to the information that is carried out. **The frequency with which an SI is retransmitted on the BCCH varies with the type of information.**
* **The *frequency control channel* (FCCH)**, **used by the MS** to **adjust its *local oscillator* (LO) to the BTS oscillator**, in order **to have a frequency synchronization** between the **MS and the BTS.**
* **The *synchronization channel* (SCH)**, **used by the MS** to synchronize in time with the BTS, and to identify the cell.

As listed below, four **channels comprise the common control channels (CCCH**). Among these, the **first three are used for the MS-initiated call or for call paging (notification of an incoming call toward the MS):**

* The ***random access channel* (RACH)** is used for the **MS access requests to the network**, **for the establishment of a call**, **based on a slotted aloha** method.
* The ***paging channel* (PCH)** is defined **to inform the MS of an incoming call.**
* The ***access grant channel***(AGCH) is used **to allocate some physical resource to a mobile for signaling,** following a request on the RACH.
* The ***cell broadcast channel***(CBCH) may be used **to broadcast specific news** to the mobiles of a cell.

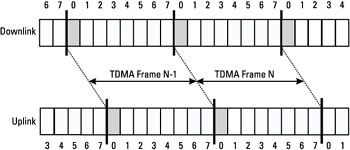
The **dedicated control channels** are:

* The ***stand-alone dedicated control channel* (SDCCH),** utilized for **registration, authentication, call setup, and location updating**.
* The ***slow associated control channel* (SACCH)**, which **carries signaling for the TCH or SDCCH with which it corresponds**. **The information that is transmitted on this channel concerns the *radio link control* (RLC**), such as the power control on the corresponding TCH or SDCCH, or the time synchronization between the MS and the BTS.
* The ***fast associated control channel* (FACCH),** carries the **signaling that must be sent by the network to the MS to notify that a handover is occurring.**

### Mapping of Logical Channels onto Physical Channels(Since logical channels are built on top of Physical Channels)

#### **TDMA Time Structure**

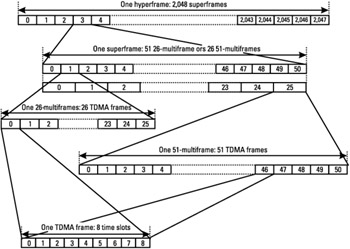
The **basic time unit is the time slot**. Its duration **is 576.9 μs = 15/26 ms, or 156.25 symbol periods (a symbol period is 48/13 μs**). The piece of information transmitted during a time slot is called **a burst.** As we saw in Section 1.5.1, the GSM multiple access scheme is TDMA, with **eight time slots per carrier.** A **sequence of eight time slots** is called a **TDMA frame,** and has a **duration of 4.615 m**s. The time slots of a TDMA frame **are numbered from 0 to 7**, as shown in Figure 1.4. Note that the **beginning and end of TDMA frames in uplink and downlink are shifted in time**: **Time slot number 0** on the **uplink corresponds to time slot 3 in the downlink**. This allows some time for the mobile to switch from one frequency to the other.

   
Figure: Slot numbering within the TDMA frame.

As seen earlier, **a physical channel is defined as a sequence of TDMA frames**, **a time slot number (from 0 to 7) and a frequency**. It **is bidirectional, with the same TN in uplink and in downlink**. In order to **support cryptographic mechanisms**, a **long time-structure** **has been defined. It is called a hyper frame and has a duration of 3 hours, 28 minutes, 53 seconds, and 760 ms (or 12,533.76 seconds).** The **TDMA frames are numbered within the hyper frame**. The **numbering is done** with the TDMA *frame number* (FN) **from 0 to 2,715,647**.

**One hyper frame** is **subdivided into 2,048 super frames**, which have a **duration of 6.12 seconds**. The **super frame** is itself **subdivided into multi-frames**. **In GSM**, there **are two types of multiframes defined**, c**ontaining 26 or 51 TDMA frames**.

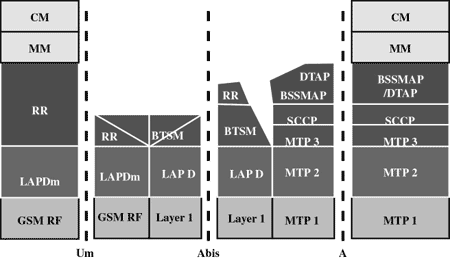
The **26 multiframe has a duration of 120 ms**, and **comprises 26 TDMA frames** this multiframe is used **to carry TCH, SACCH, and FACCH**. The 51 multiframe is made up of 51 TDMA frames. Its duration is 235.4 ms (3,060/13 ms). This multiframe is used **to carry BCH, CCCH, and SDCCH (with its associated SACCH**). Note that a **superframe is composed of twenty-six 51-multiframes, or of fifty-one 26-multiframes**. This hierarchical time structure is summarized in Figure 1.5.

   
Figure: Hierarchical structure of a hyperframe.

**4. GSM Protocol Stack:**

GSM architecture is **a layered model** that **is designed to allow communications between two different systems**. The **lower layers assure the services of the upper-layer protocols**. **Each layer passes suitable notifications** to ensure the transmitted data has been formatted, transmitted, and received accurately.

The GMS protocol stacks diagram is shown below

****

**MS Protocols**

Based on the interface, the GSM signaling protocol is assembled into three general layers:

* **Layer 1** : The physical layer. It uses the channel structures over the air interface.
* **Layer 2** : The data-link layer. Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (LAP-D) protocol used in ISDN, called Link access protocol on the Dm channel (LAP-Dm). Across the A interface, the Message Transfer Part (MTP), Layer 2 of SS7 is used.
* **Layer 3** : GSM signaling protocol’s third layer is divided into three sub layers:
  + Radio Resource Management (RR),
  + Mobility Management (MM), and
  + Connection Management (CM).

**MS to BTS Protocols**

The RR layer is the lower layer that manages a link, both radio and fixed, between the MS and the MSC. For this formation, the main components involved are the MS, BSS, and MSC. The responsibility of the RR layer is to manage the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.

The MM layer is stacked above the RR layer. It handles the functions that arise from the mobility of the subscriber, as well as the authentication and security aspects. Location management is concerned with the procedures that enable the system to know the current location of a powered-on MS so that incoming call routing can be completed.

The CM layer is the topmost layer of the GSM protocol stack. This layer is responsible for Call Control, Supplementary Service Management, and Short Message Service Management. Each of these services are treated as individual layer within the CM layer. Other functions of the CC sub layer include call establishment, selection of the type of service (including alternating between services during a call), and call release.

**BSC Protocols**

The BSC uses a different set of protocols after receiving the data from the BTS. The Abis interface is used between the BTS and BSC. At this level, the radio resources at the lower portion of Layer 3 are changed from the RR to the Base Transceiver Station Management (BTSM). The BTS management layer is a relay function at the BTS to the BSC.

The RR protocols are responsible for the allocation and reallocation of traffic channels between the MS and the BTS. These services include controlling the initial access to the system, paging for MT calls, and the handover of calls between cell sites, power control, and call termination. The BSC still has some radio resource management in place for the frequency coordination, frequency allocation, and the management of the overall network layer for the Layer 2 interfaces.

To transit from the BSC to the MSC, the BSS mobile application part or the direct application part is used, and SS7 protocols is applied by the relay, so that the MTP 1-3 can be used as the prime architecture.

**MSC Protocols**

At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3. Here, Base Station System Management Application Part (BSS MAP) is said to be the equivalent set of radio resources. The relay process is finished by the layers that are stacked on top of Layer 3 protocols, they are BSS MAP/DTAP, MM, and CM. This completes the relay process. To find and connect to the users across the network, MSCs interact using the control-signaling network. Location registers are included in the MSC databases to assist in the role of determining how and whether connections are to be made to roaming users.

Each GSM MS user is given a HLR that in turn comprises of the user’s location and subscribed services. VLR is a separate register that is used to track the location of a user. When the users move out of the HLR covered area, the VLR is notified by the MS to find the location of the user. The VLR in turn, with the help of the control network, signals the HLR of the MS’s new location. With the help of location information contained in the user’s HLR, the MT calls can be routed to the user.

**5. Localization and Calling:**

GSM (Global System for mobile communication) provides **many** **useful services** in which, one of the most important is the automatic, worldwide localization of users. The **service provider system always knows where a user currently is**, and **the same phone number is valid worldwide.**  
For **localization** of users, GSM performs **periodic location updates** even if a user does not use the mobile phones or some other devices but user should not be out of GSM network and **is not completely switched off their devices**.   
  
**GSM uses two types of databases:**  
  
Home Location Register (HLR)   
Visitor Location Register (VLR)   
  
The **Home Location Register** is a database from a mobile network in which **information from all mobile subscribers is stored.**   
  
The **VLR** contains the **exact location of all mobile subscribers currently** present in the service area.   
  
**VLR** is **responsible for the MS (Mobile Station)** **to inform the HLR** about **location changes.**   
  
As soon as **user moves from one location to another location**, the **HLR sends all user data needed to the new VLR (New Location).** [HLR->NEW VLR]

Changing of one VLR to another VLR and **their uninterrupted services** is called as **Roaming**.   
  
**Roaming can be taken place as follows**:   
  
- Within the network of one provider  
- Between two providers in one country (National Roaming)   
- Different providers in different countries (International Roaming)   
  
**To locate an MS and to address the MS, several numbers are needed:**  
  
- Mobile station international ISDN number (MSISDN)   
- International mobile subscriber identity (IMSI)   
- Temporary mobile subscriber identity (TMSI)   
- Mobile station roaming number (MSRN)

**Calling:**

Various types of calls handled by a GSM network

• Calls originating from a mobile TE to a PSTN destination TE **(Mobile→ PSTN Calls)**

• Calls originating from a mobile TE to a mobile destination TE **(Mobile → Mobile Calls)**

Calls originating from a PSTN TE to a mobile destination TE **(PSTN → Mobile Calls)**

• **Message exchanges** between the **mobile station and the base transceiver** (Mobile station ↔ Base transceiver message exchanges)

**6. Handover in GSM:**

**GSM handover** occurs when the **mobile moves out** **of the coverage area of one BTS into another BTS controlled by the same BSC**.

**Process of transferring a call** (or data transfer) **in progress** from one channel to another

**Main reasons for handover in cellular networks**

• If the mobile device **moves out of the range of one cell** (base station) and a **different base station can provide it with a stronger signal**

• **If all channels of one base station are busy** then **a nearby base station can provide service to the device**

Two main types of handover

• Hard handover

• Soft handover

**Hard Handove**r

• **Existing radio link** must be **dropped for a small period of time**

• 1) **Break in call transmission**,

2) **Handover takes place in a few ms** (at best in 60 ms)

**Soft Handover**

•Mobile station **at the boundary of two adjacent cells**─ **does not suffer call drops** due to handover in the boundary region

• **Gives seamless connectivity** to a Mobile station

**Different types of Handover in GSM(7 types)**

**Inter cell Handover**

• When the **signal strength goes weak** **due to several reason**s (for example, the **mobile moving away from the cell in which it is presently localized to the boundary region of another cell**), there is handover from a cell to another**.**

**Inter-MSC Handover[BSC—high]**

• Handover also takes place **for load balancing when the traffic from the cells and BSCs high**

• For **Eg:** An ongoing call, which is being handled by a cell, may be handed over to another MSC

• Since the **two MSCs are interfaced through PCM** the **handover performed over a wired line**

**Inter-BSC Handover [BTS—high]**

• Handover f**or load balancing when the traffic from the cells and BTSs high**

• The BSC’s connect to an MSC

• A call, which is ongoing in a cell through a BTS, **may be handed over to another BSC connected to the same MSC**

• Since the BSCs connect to the MSC interfaces by PCM, the **handover is over a wired line**

**Inter-BSC, Inter-MSC Handover**

• For load balancing when the traffic from the cells and BTSs as well as BSCs high

**Intra-cell Handover**

• Due to **interference at certain frequencies**, the **signal quality poor**

• The **BSC can handover** the **call to another frequency** of the cell in such cases

**Inter-cell, Intra-BSC Handover**

• When an MS moves to a neighbouring cell and suffers poor signal quality, the BSC can handover the call to a different BTS channel of the same BSC

**Inter-cell, intra-MSC handover**

1. The RRM sub layer transmits a signal report from MSi to BTSi and from BTSi to BSCi. In case a handover is necessary, BSCi signals the handover requirement to MSCi.

2. MSCi signals the handover requirement to another BSCj and BSCj allocates radio resources and transmits the activated channel to another BTSk.

3. BTSk sends acknowledgement of the channel to BSCj and BSCj acknowledges the handover request grant via message to MSCi

4. MSCi transmits handover command to BSCi, BSCi to BTSi, and BTSi to the MSi’s RRM layer

5. The RRM directs the MS radio interface to operate at another channel linked to BTSk

**7. Security in GSM:**

* Visitor Location Register **(VLR)** is a database of the subscribers who have roamed into the jurisdiction of the Mobile Switching Center **(MSC)** which it serves.
* Authentication Center (**AuC)** authenticates each **SIM** card that attempts to connect to the **GSM** **core network** (typically when the **phone is powered on**).

GSM is the most secured cellular telecommunications system available today. GSM has its security methods standardized. GSM maintains end-to-end security by retaining the confidentiality of calls and anonymity of the GSM subscriber.

Temporary identification numbers are assigned to the subscriber’s number to maintain the privacy of the user. The privacy of the communication is maintained by applying encryption algorithms and frequency hopping that can be enabled using digital systems and signaling.

This chapter gives an outline of the security measures implemented for GSM subscribers.

## Mobile Station Authentication

1. The GSM network authenticates the identity of the subscriber through the use of a **challenge-response mechanism**.
2. A **128-bit** Random Number **(RAND)** is **sent to the MS**.
3. The **MS computes the 32-bit** Signed Response (**SRES)** **based** on the **encryption of the RAND with** the **authentication algorithm (A3**) using the **individual subscriber authentication key (Ki)**. **Upon receiving the SRES** from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber.
4. The individual **subscriber authentication key (K**i) is **never transmitted** **over the radio channel**, as it is present in the **subscriber's SIM**, as well as the **AUC, HLR, and VLR databases**.
5. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an **authentication failure** **is indicated** **to the MS**.

The calculation of the **signed response(SRES) is processed within the SIM**. It provides **enhanced security**, as **confidential subscriber information** such as the **IMSI** or the individual subscriber **authentication key** (Ki) **is never released** **from the SIM** during the authentication process.

## Signaling and Data Confidentiality

1. The SIM contains the **ciphering key generating algorithm** (**A8**) that is used **to produce the 64-bit ciphering key (Kc)**.
2. This key is **computed** **by** **applying** the **same random number (RAND)** used in the authentication process to ciphering key generating algorithm (A8) with **the individual subscriber authentication key (Ki)**.
3. GSM provides **an additional level of security** by having a **way to change the ciphering ke**y, **making the system more resistant** to eavesdropping.
4. The **ciphering key** may be **changed at regular intervals as required**.
5. As in case of the authentication process(**AUc)**, the **computation** **of the ciphering key (Kc)** **takes place internally within the SIM**. Therefore, **sensitive information** such as the individual **subscriber authentication key** (Ki**) is never revealed** by the SIM.
6. **Encrypted voice** and **data communications** between the MS and the network is accomplished by using the ciphering algorithm (**A5)**.
7. **Encrypted communication** is **initiated** by a **ciphering mode request command** **from** the **GSM network**. **Upon receipt of this command, the mobile station begins** **encryption and decryption of data** using the ciphering algorithm (A5) and the ciphering key (Kc).

## Subscriber Identity Confidentiality

1. **To ensure subscriber identity confidentiality**, the **Temporary Mobile Subscriber Identity (TMSI)** is used.
2. Once the authentication and encryption procedures are done, the TMSI is sent to the mobile station. After the receipt, the mobile station responds.
3. The **TMSI is valid in the location area in which it was issued**. For **communications outside the location area,** the **Location Area Identification (LAI)** **is necessary** in addition to the TMSI.

**8. New Data Services:**

To enhance the data transmission capabilities of GSM, two basic approaches are possible. As

the basic GSM is based on connection-oriented traffic channels, e.g., with 9.6 kbit/s each, several channels could be combined to increase bandwidth. This system is called **HSCSD {high speed circuit switched data}.** A more progressive step is the introduction of packet-oriented traffic in GSM, i.e., shifting the paradigm from connections/telephone thinking to packets/internet thinking. The system is called **GPRS {general packet radio service}.**

**HSCSD:**

**HSCSD** (High-Speed Circuit-Switched Data) is essentially a new high speed implementation of GSM (Global System for Mobile Communication) data transfer. Four times faster than GSM, with a transfer rate of up to 57.6Kbps, it achieves this speed by allocating up to eight time slots to an individual user.

14.4Kb time slots are only available on GSM networks that operate at 1,800MHz. 900Mhz GSM networks are limited to 9.6Kb time slots. Therefore, HSCSD is limited to 38.4Kbps on 900Mhz GSM networks. HSCSD can nly achieve 57.6Kbps on 1,800Mhz GSM networks.

**The History of HSCSD**

HSCSD was an enhancement to to earlier CSD (Circuit Switched Data) standard. EDGE (Enhanced Data-Rates for GSM Evolution) enabled GSM networks are able to implement ECSD (Enhanced Circuit Switched Data), an enhanced version of HSCSD. ECSD increases the bandwidth of each timeslot to 48Kb and allows the use of eight timeslots, which gives a total transmission speed of 384Kbps.

Both HSCSD/ECSD and GPRS are likely to eventually be phased out in favor of UMTS, which is a packet switched technology with speeds up to 2Mbps.

**GPRS:**

**General Packet Radio Service** (**GPRS**) is a packet oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (**GSM**).

It provides moderate-speed data transfer, by using unused time division multiple access (TDMA) channels in, for example, the **GSM** system.

GPRS usage is typically charged based on volume of data transferred, contrasting with [circuit switched](https://en.wikipedia.org/wiki/Circuit_switching) data, which is usually billed per minute of connection time. Sometimes billing time is broken down to every third of a minute. Usage above the [bundle cap](https://en.wikipedia.org/wiki/Product_bundling) is charged per megabyte, speed limited, or disallowed.

GPRS is a [best-effort](https://en.wikipedia.org/wiki/Best-effort) service, implying variable [throughput](https://en.wikipedia.org/wiki/Throughput) and [latency](https://en.wikipedia.org/wiki/Latency_(engineering)) that depend on the number of other users sharing the service concurrently, as opposed to [circuit switching](https://en.wikipedia.org/wiki/Circuit_switching), where a certain [quality of service](https://en.wikipedia.org/wiki/Quality_of_service)(QoS) is guaranteed during the connection. In 2G systems, GPRS provides data rates of 56–114 kbit/second. [2G](https://en.wikipedia.org/wiki/2G) cellular technology combined with GPRS is sometimes described as [*2.5G*](https://en.wikipedia.org/wiki/2.5G), that is, a technology between the second ([2G](https://en.wikipedia.org/wiki/2G)) and third ([3G](https://en.wikipedia.org/wiki/3G)) generations of mobile telephony. It provides moderate-speed data transfer, by using unused [time division multiple access](https://en.wikipedia.org/wiki/Time_division_multiple_access) (TDMA) channels in, for example, the GSM system. GPRS is integrated into GSM Release 97 and newer releases.

### Services offered

GPRS extends the GSM Packet circuit switched data capabilities and makes the following services possible:

* [SMS](https://en.wikipedia.org/wiki/SMS) messaging and broadcasting
* "Always on" internet access
* [Multimedia messaging service](https://en.wikipedia.org/wiki/Multimedia_Messaging_Service) (MMS)
* [Push-to-talk](https://en.wikipedia.org/wiki/Push-to-talk) over cellular (PoC)
* [Instant messaging](https://en.wikipedia.org/wiki/Instant_messaging) and presence—[wireless village](https://en.wikipedia.org/wiki/Wireless_Village)
* Internet applications for smart devices through [wireless application protocol](https://en.wikipedia.org/wiki/Wireless_Application_Protocol) (WAP)
* [Point-to-point](https://en.wikipedia.org/wiki/Point-to-point_(telecommunications)) (P2P) service: inter-networking with the Internet (IP)
* [Point-to-multipoint](https://en.wikipedia.org/wiki/Point-to-multipoint_communication) (P2M) service[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]: point-to-multipoint multicast and point-to-multipoint group calls

If SMS over GPRS is used, an SMS transmission speed of about 30 SMS messages per minute may be achieved. This is much faster than using the ordinary SMS over GSM, whose SMS transmission speed is about 6 to 10 SMS messages per minute.

### Protocols supported

GPRS supports the following protocols:

* [Internet Protocol](https://en.wikipedia.org/wiki/Internet_Protocol) (IP). In practice, built-in [mobile browsers](https://en.wikipedia.org/wiki/Mobile_browser) use [IPv4](https://en.wikipedia.org/wiki/IPv4) since [IPv6](https://en.wikipedia.org/wiki/IPv6) was not yet popular.
* [Point-to-Point Protocol](https://en.wikipedia.org/wiki/Point-to-Point_Protocol) (PPP). In this mode, PPP is often not supported by the [mobile phone operator](https://en.wikipedia.org/wiki/Mobile_phone_operator) but if the mobile is used as a modem to the connected computer, PPP is used to tunnel IP to the phone. This allows an IP address to be assigned dynamically ([IPCP](https://en.wikipedia.org/wiki/Internet_Protocol_Control_Protocol) not [DHCP](https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol)) to the mobile equipment.
* [X.25](https://en.wikipedia.org/wiki/X.25) connections. This is typically used for applications like wireless payment terminals, although it has been removed from the standard. X.25 can still be supported over PPP, or even over IP, but doing this requires either a network-based [router](https://en.wikipedia.org/wiki/Router_(computing)) to perform encapsulation or intelligence built into the end-device/terminal; e.g., user equipment (UE).

**GPRS Benefits**

GPRS technology offered some significant benefits when it was launched:

***Speed:***   One of the headline benefits of GPRS technology is that it offers a much higher data rate than was possible with GSM. Rates up to 172 kbps are possible, although the maximum data rates realistically achievable under most conditions will be in the range 15 - 40 kbps.

***Packet switched operation:***   Unlike GSM which was used circuit switched techniques, GPRS technology uses packet switching in line with the Internet. This makes far more efficient use of the available capacity, and it allows greater commonality with Internet techniques.

***Always on connectivity:***   A further advantage of GPRS is that it offers an "Always On" capability. When using circuit switched techniques, charges are based on the time a circuit is used, i.e. how long the call is. For packet switched technology charges are for the amount of data carried as this is what uses the services provider's capacity. Accordingly, always on connectivity is possible.

***More applications:***   The packet switched technology including the always on connectivity combined with the higher data rates opens up many more possibilities for new applications. One of the chief growth areas that arose from GPRS was the Blackberry form of mobile or PDA. This provided for remote email applications along with web browsing, etc.