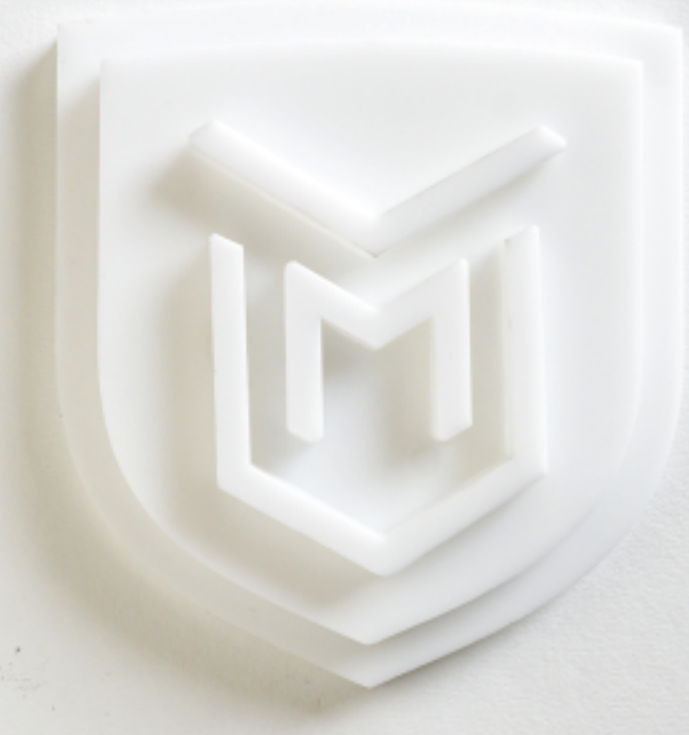


Marwadi University

Marwadi University

01CE0701 – Mobile Computing

Unit - 3 Telecommunication System (Part 1 – GSM)

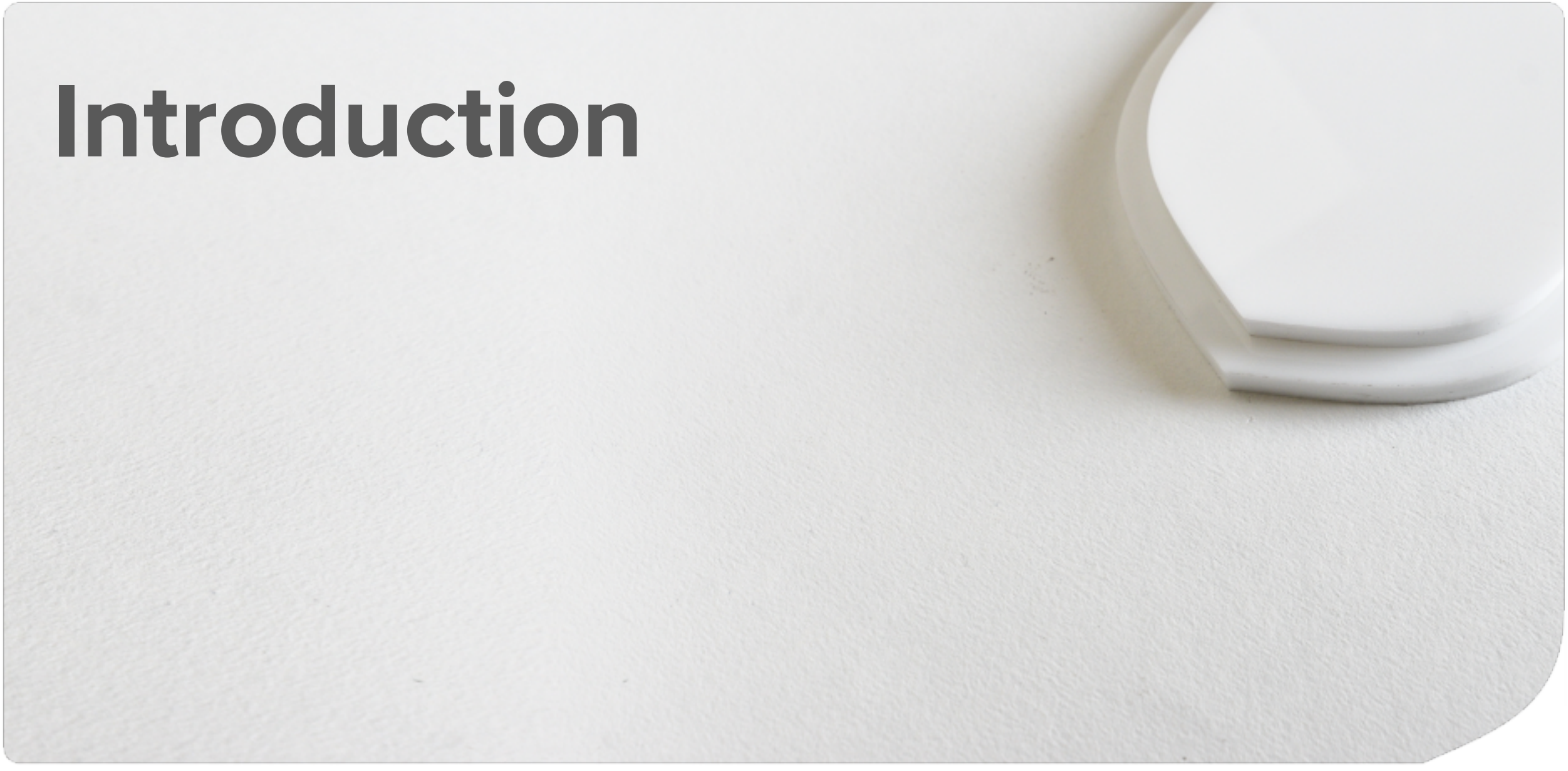
Outline

Marwadi University

- **GSM**
  - Introduction
  - GSM Architecture
  - Call routing in GSM
  - PLMN interface
  - addresses and identifiers
  - network aspects
  - frequency allocation
  - authentication and security
  - Handoffs Technique

Marwadi University

Introduction

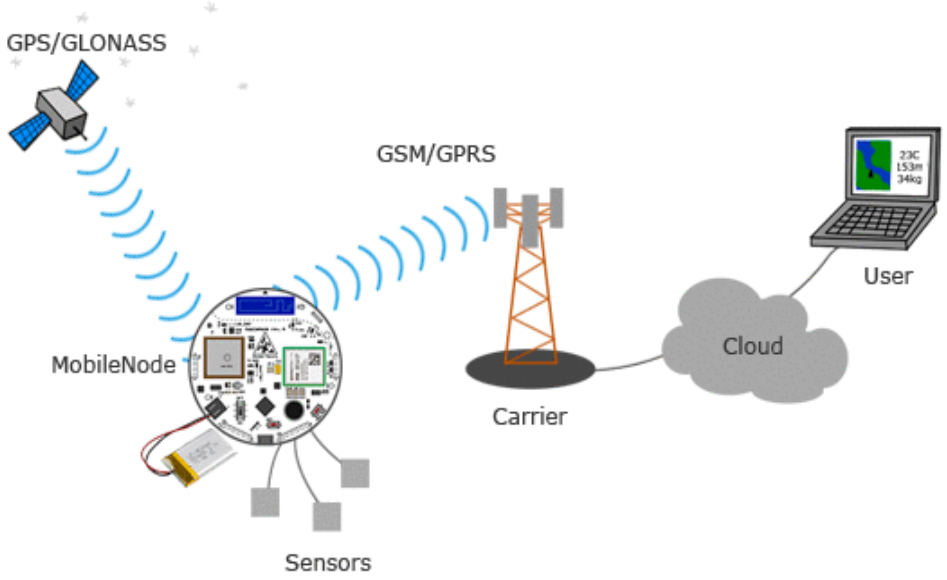


GSM vs CDMA

GSM	CDMA
Global System for Mobile communication	Code Division Multiple Access
Technology: FDMA & TDMA	CDMA
Data rate: 42Mbps in HSPA (3G)	Data rate: 3.6Mbps in CDMA
GSM supports transmitting data and voice together	CDMA doesn't support it
Customer information is stored in SIM card.	Customer information is stored in Handset.
Global market share is 75%	Global market share is 25%
SIM specific. User can use/upgrade to multiple handset	Handset specific
Support International roaming	CDMA doesn't support this facility

What is GSM?

- GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services.
- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- The use of harmonised spectrum (uniform allocation of radio frequency bands) across most of the globe, combined with GSM's international roaming capability, allows travellers to access the same mobile services at home and abroad.
- GSM enables individuals to be reached via the same mobile number in up to all countries in the world.



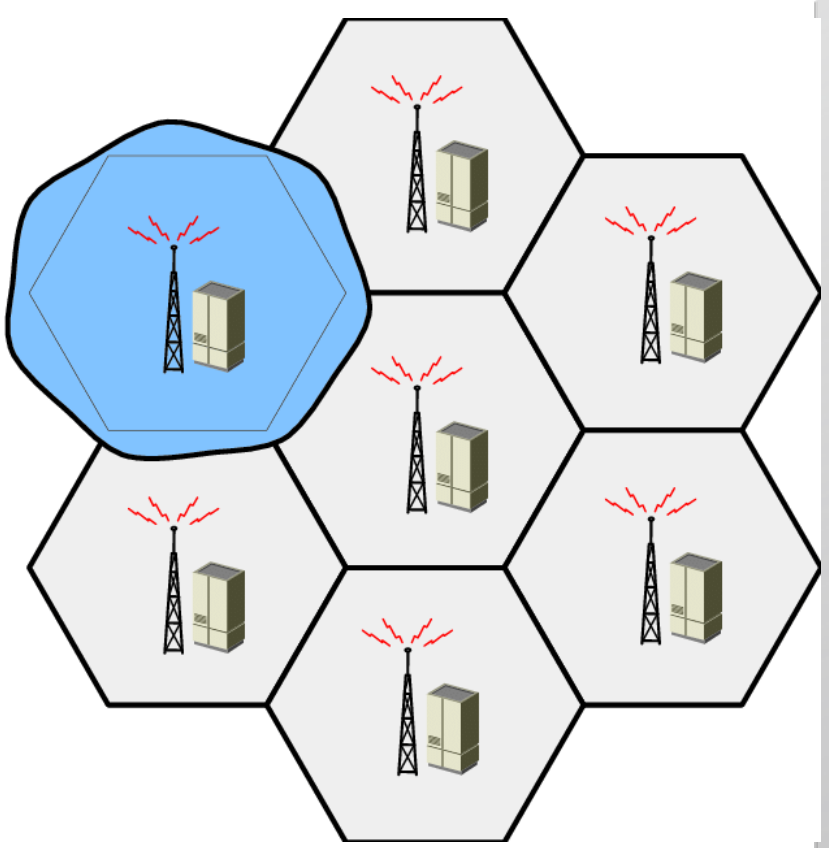
Introduction to GSM

- GSM is combination of TDMA (Time Division Multiple Access), FDMA (Frequency Division Multiple Access) and Frequency hopping.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology.
- It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 190 countries throughout the world.
- Roaming is the ability to use your GSM phone number in another GSM network.
- GSM owns a market share of more than 75% of the world's digital cellular subscribers.

Introduction to GSM

- In GSM, geographical area is divided into hexagonal cells whose size depends upon power of transmitter and load on transmitter (number of end user).

- At the centre of cell, there is a base station consisting of a transceiver (combination of transmitter and receiver) and an antenna.



Characteristics of GSM

- Fully digital system
- Security against fraud Enhance Privacy
- International roaming
- Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services
- Support for new services.
- Support of Short Message Service (SMS)
- Good subjective voice quality.

GSM Services

- There are 3 different services in GSM
  - Tele-services
  - Bearer or Data Services
  - Supplementary services

Tele Services

- Telecommunication services that enable voice communication via mobile phones.
- Offered services
  - Mobile telephony
  - Emergency calling

Bearer or Data Services

- Include various data services for information transfer between GSM and other networks like PSTN, ISDN etc at rates from 300 to 9600 bps
- Short Message Service (SMS)
  - up to 160 character alphanumeric data transmission to/from the mobile terminal
- Multimedia Messaging Services (MMS)
- Fax can send in group
- Voice mailbox
- Electronic mail

Supplementary Services

Marwadi University

- **Call related services**
  - Call Waiting
    - Notification of an incoming call while call is going on
  - Call Hold
    - Put a caller on hold to take another call
  - Call Barring
    - Stop - All calls, outgoing calls, or incoming calls
  - Call Forwarding
    - Calls can be sent to various numbers defined by the user
  - Multi Party Call Conferencing
    - Link multiple calls together

Both GSM and CDMA are 2G standards. The standard for 4G is LTE or (Long Term Evolution of 3g). However, a 4G sim works on a GSM phone.

We can receive calls and messages as usual, but the internet speed will depend on the handset's capability.

The evolution of 1G to 5G

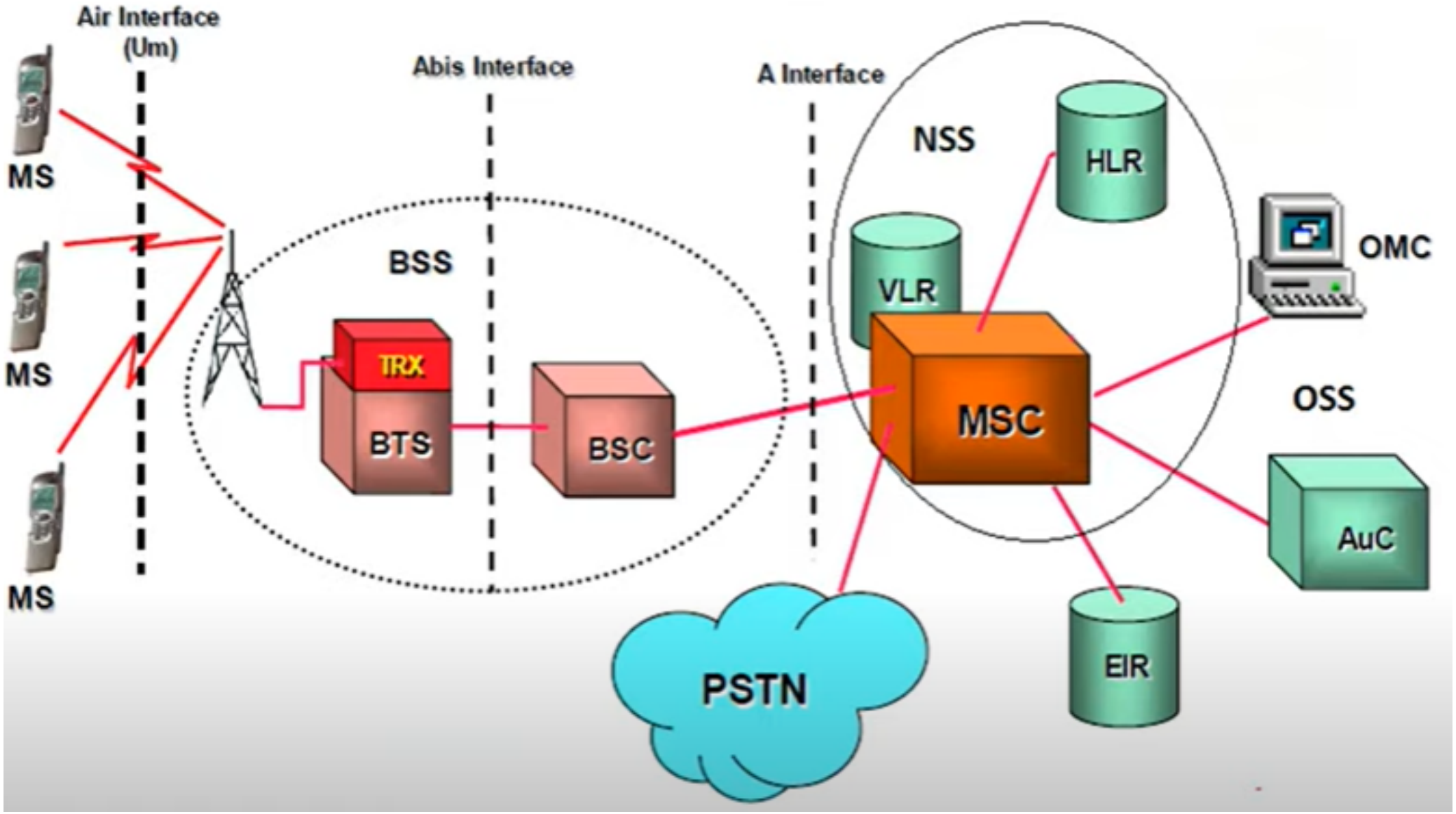
TYPE	DEPLOYMENT	TECHNOLOGIES AND STANDARDS	FEATURES
1G	Analog telecommunication deployed in the 1980s	■ Advanced Mobile Phone Service (AMPS) ■ Nordic Mobile Telephone (NMT)	Voice calls, NMT for simple integrated data and messaging
2G	Digital cellular deployed in the 1990s	■ Code-division multiple access (CDMA) ■ Global System for Mobile Communications (GSM)/ Enhanced Data rates for GSM Evolution (EDGE) ■ Time-division multiple access (TDMA)	Voice, SMS text messages, low-rate data
3G	First broadband, deployed in 2000	■ CDMA2000 1X/Evolution-Data Optimized (EVDO) ■ Universal Mobile Telecommunications Service (UMTS)/high-speed packet access (HSPA) ■ Worldwide Interoperability for Microwave Access (WiMAX)	Offers speeds from 144 Kbps to 2 Mbps indoors, enabling rich content
4G	Deployed in 2010	■ LTE	100s of Mbps to 1 Gbps with video and streaming capabilities
5G	First deployed in 2018	■ International Telecommunication Union (ITU)/ International Mobile Communications (IMT)-2020 defined technical objectives ■ 3rd Generation Partnership Project (3GPP) is developing 5G specifications	3x higher spectral efficiency than 4G and peak downlink throughputs to peak 20 Gbps

SOURCE: 5G AMERICAS

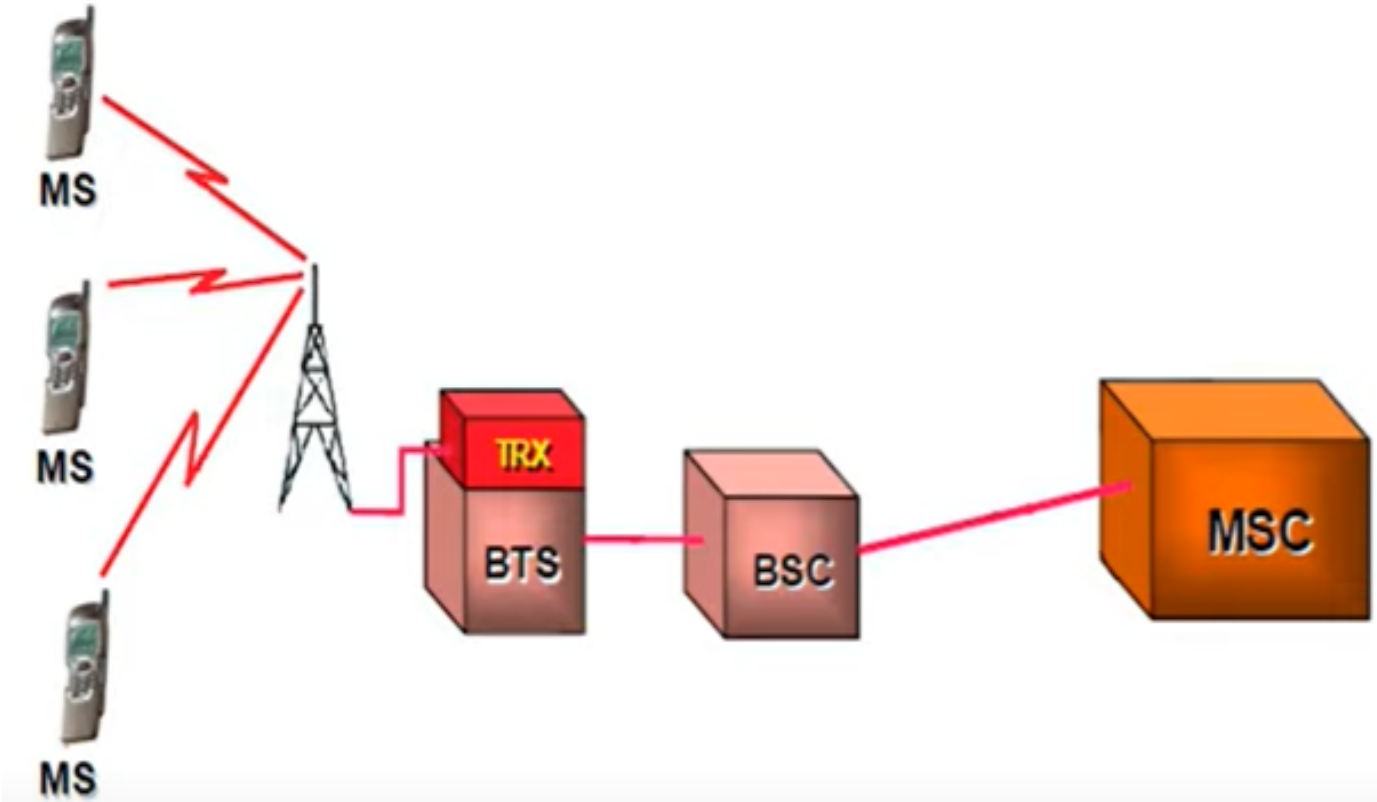
Marwadi University

GSM Architecture

GSM Architecture

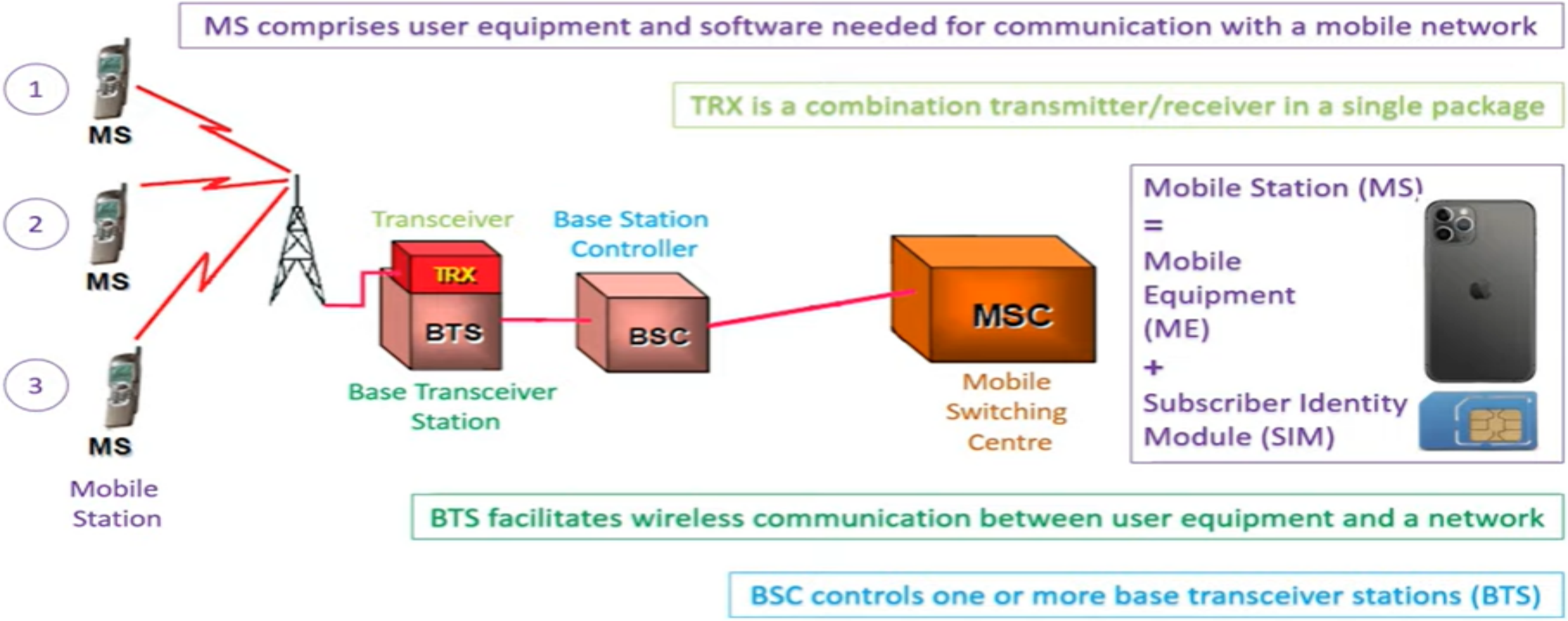


GSM Architecture



•Three mobile stations connected to a tower, which is connected to a BTS using TRX then further connected to BSC and then MSC.

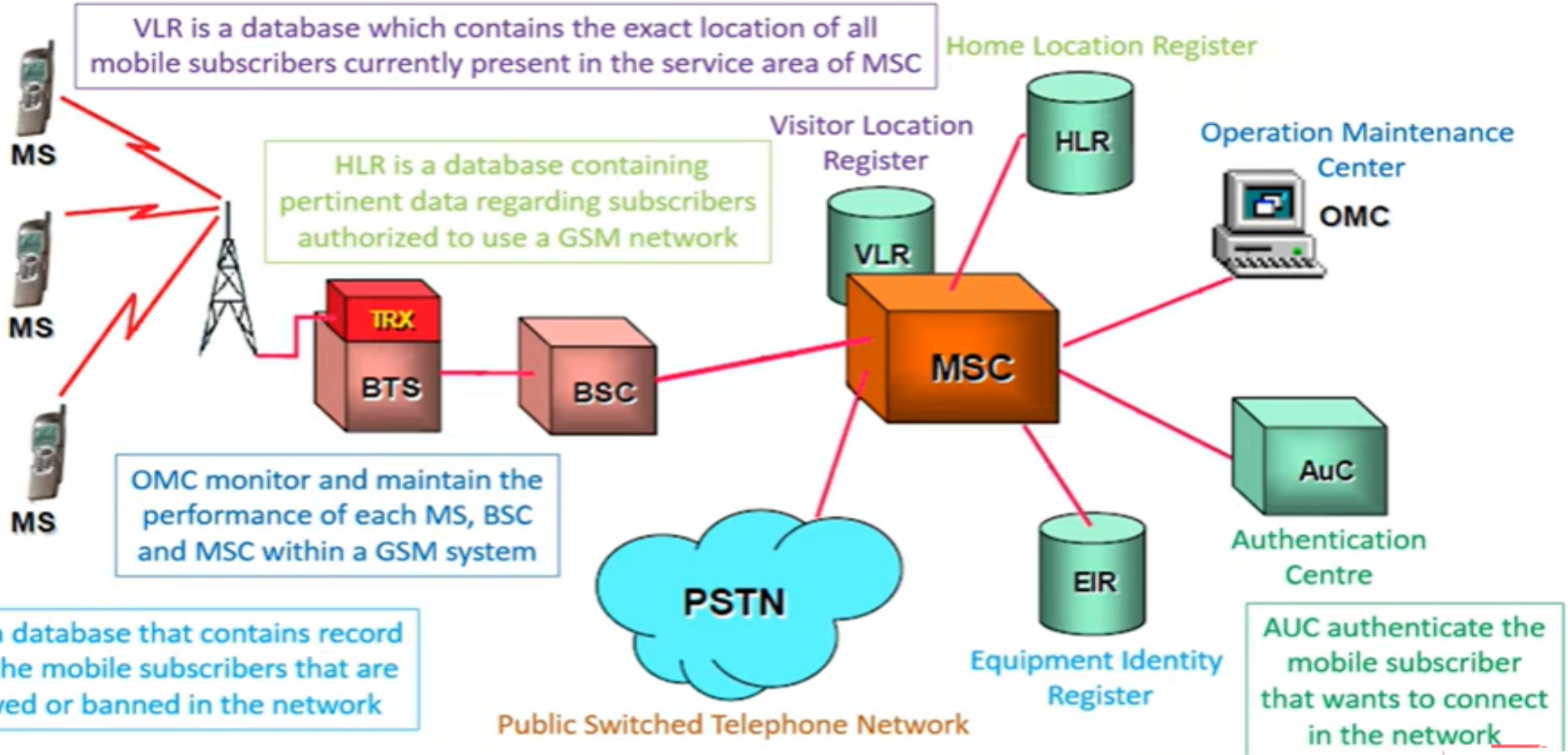
GSM Architecture



GSM Architecture

- Multiple mobile stations are connected to a single tower.
- Tower connected to BTS, which provide a wireless connection with MS.
- Every tower is having BTS.
- BSC can have multiple BTS
- A BSC can be assumed as a local exchange of your area, which can have multiple towers, and every tower having multiple BTS.
- Heart of mobile communication is MSC. Functions are call flow, call tracing, call routing, call recording etc.

GSM Architecture



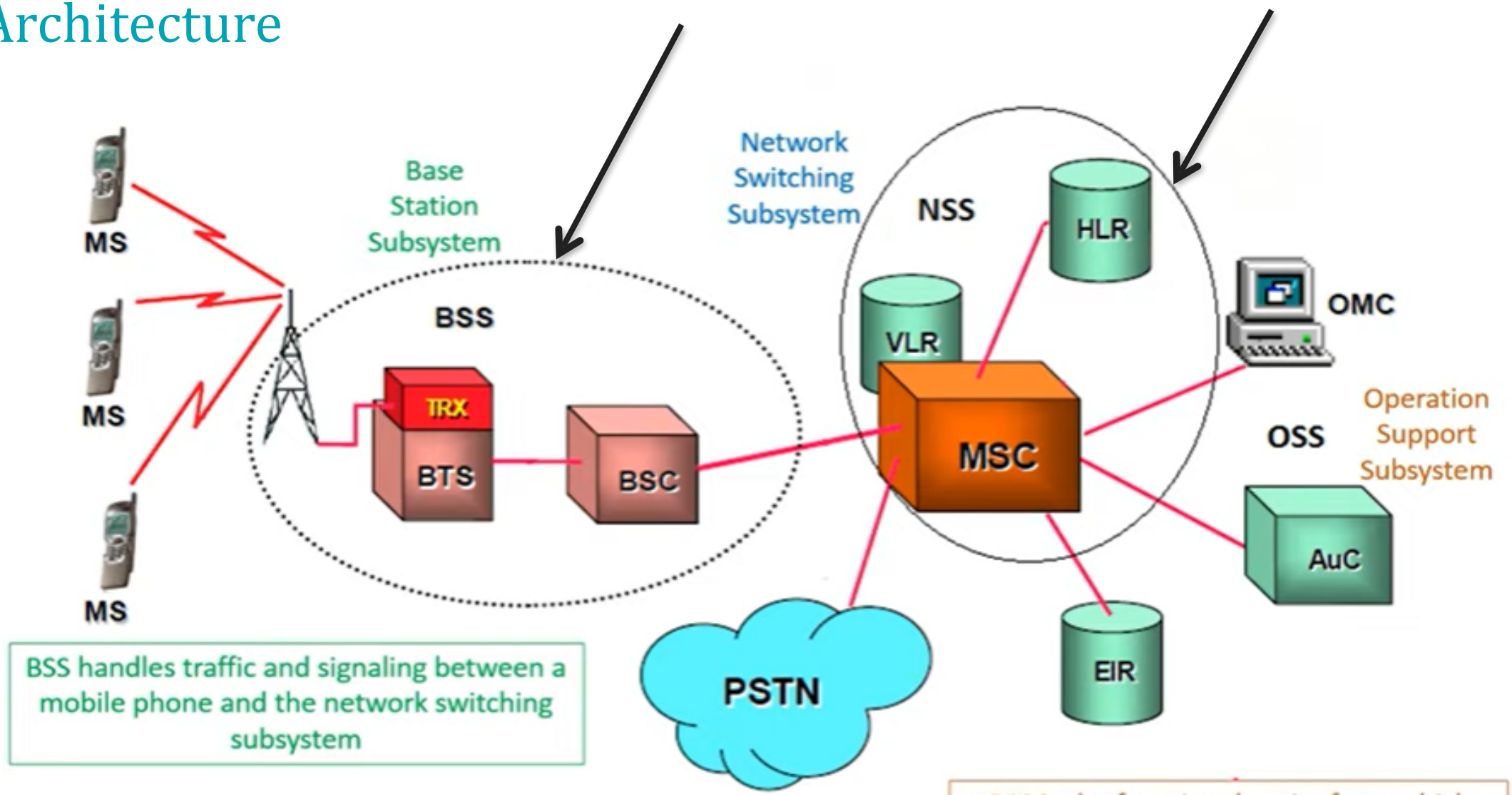
GSM Architecture

- **Components of MSC:**

- VLR –If you are moving from one state to another then your entry will marked in the database of VLR.
- HLR- If you have purchased a SIM from a specific location then your entry will be marked on that HLR, contains id proofs, plan you are taking etc.

- PSTN-Land line system.

GSM Architecture



BSS handles traffic and signaling between a mobile phone and the network switching subsystem

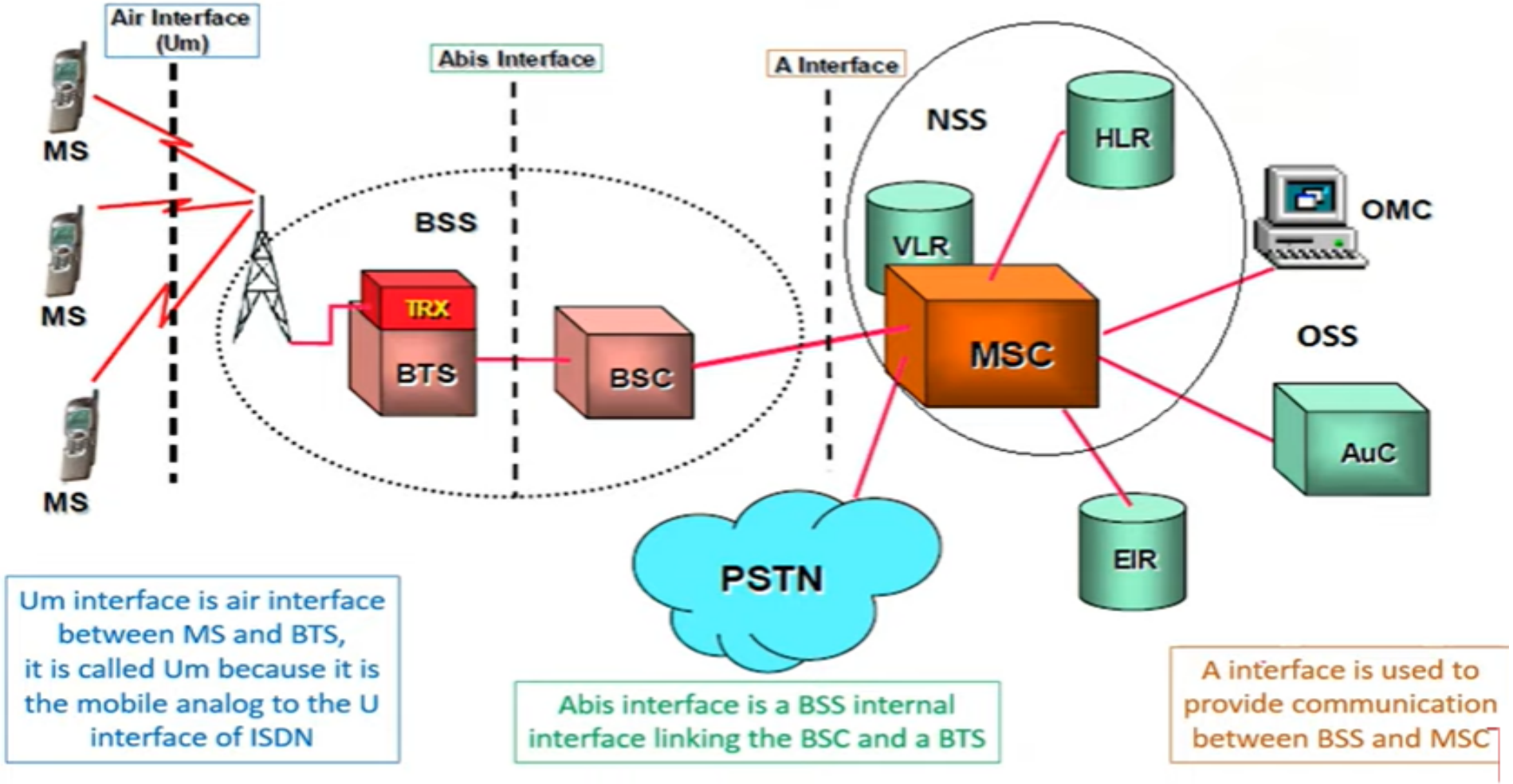
NSS is core network of GSM that carries out call and mobility management functions for mobile phones present in the network

OSS is the functional entity from which the network operator monitors and controls the system

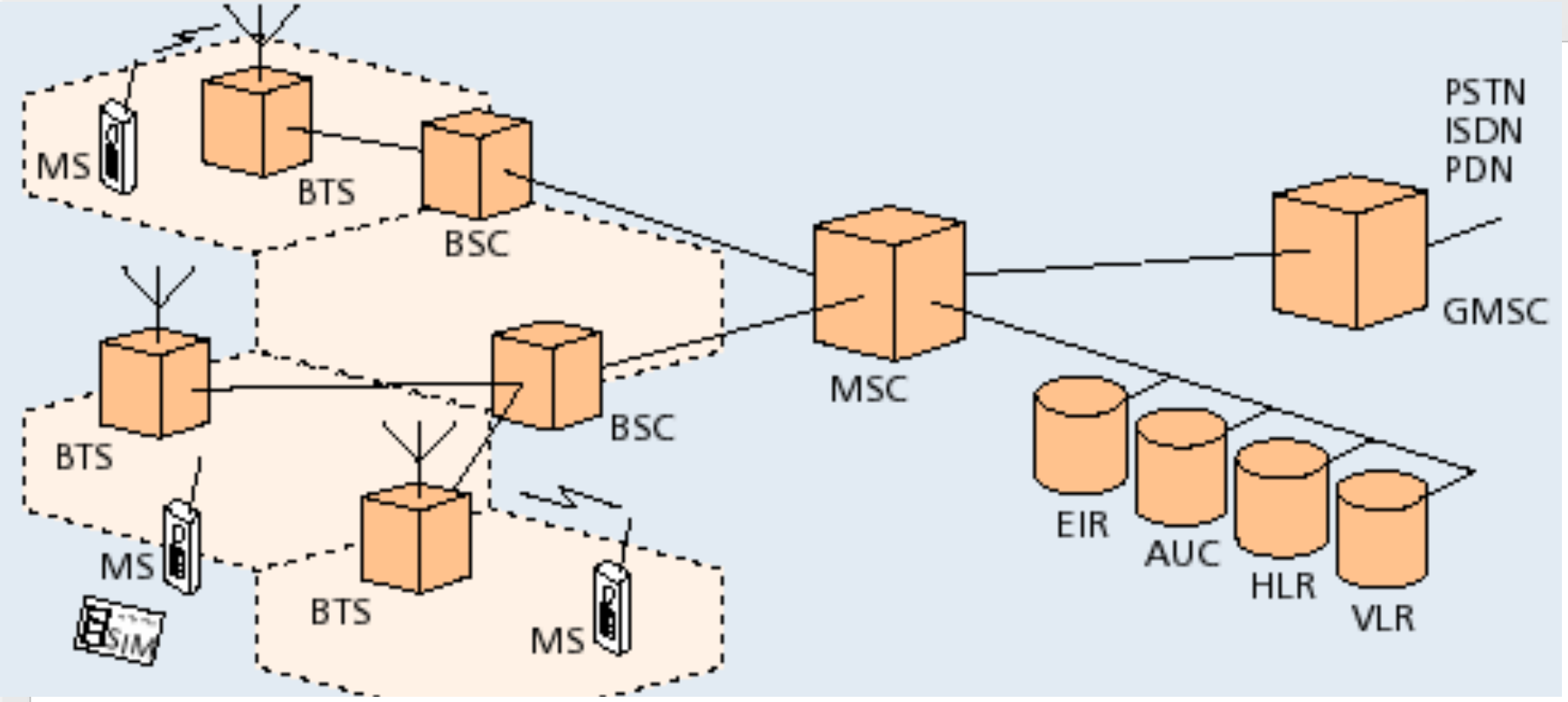
OMC is a part of OSS.

GSM Architecture

Interfaces

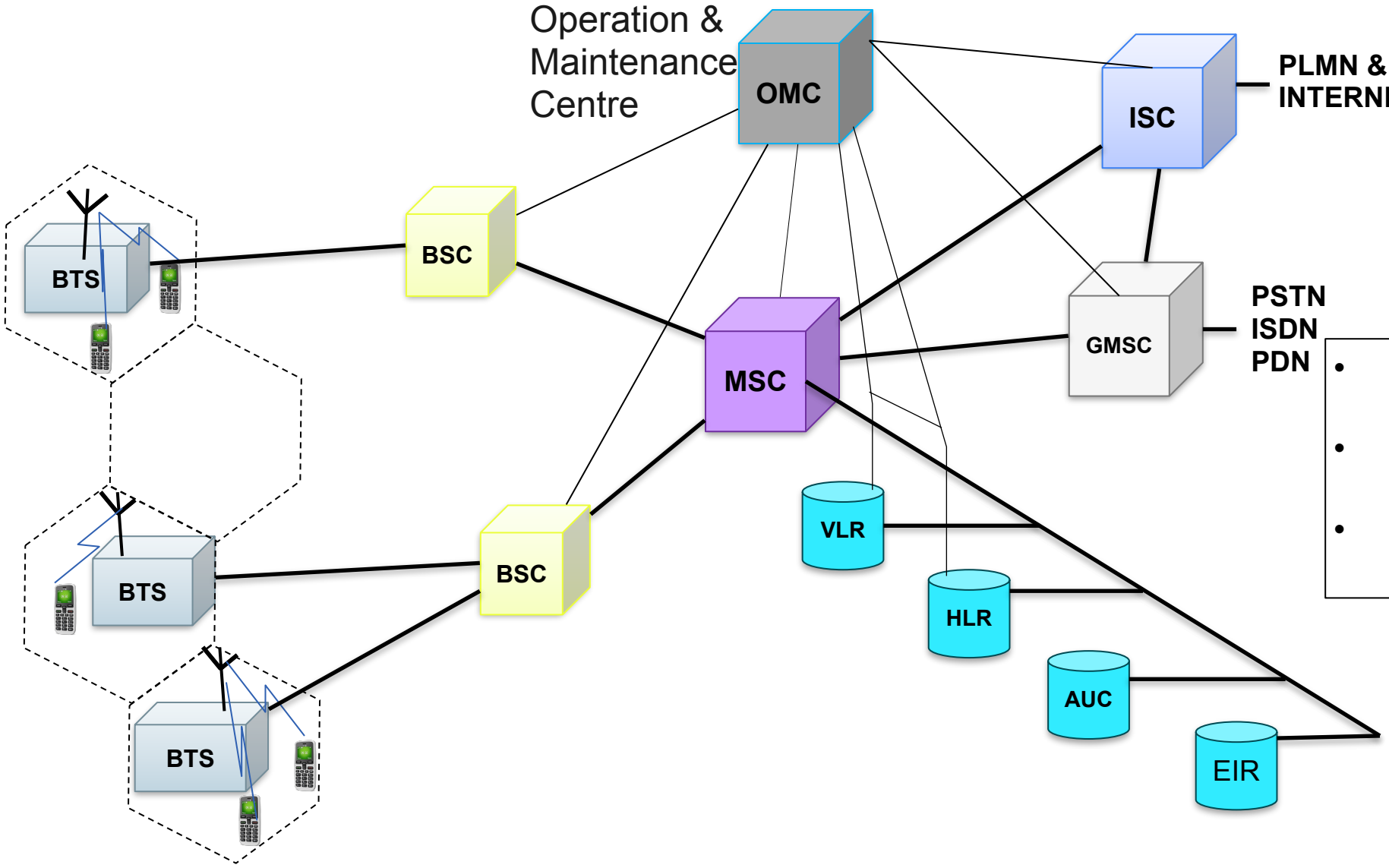


GSM Architecture-Summary



AUC	Authentication center	HLR	Home Location Register	PSTN	Public Switching Telephone Network
BSC	Base station controller	ISDN	Integrated System Digital Network	VLR	Visitor Location Register
BTS	Base trans-receiver system	MS	Mobile station		
EIR	Equipment Identity Register	MSC	Mobile Switching Centre		
GMSC	Gateway MSC	PDN	Packet Data Network		

GSM Architecture



- GMSC – Gateway Mobile Switching Centre
- ISC – International Switching Centre
- PLMN – Public Land Mobile Network

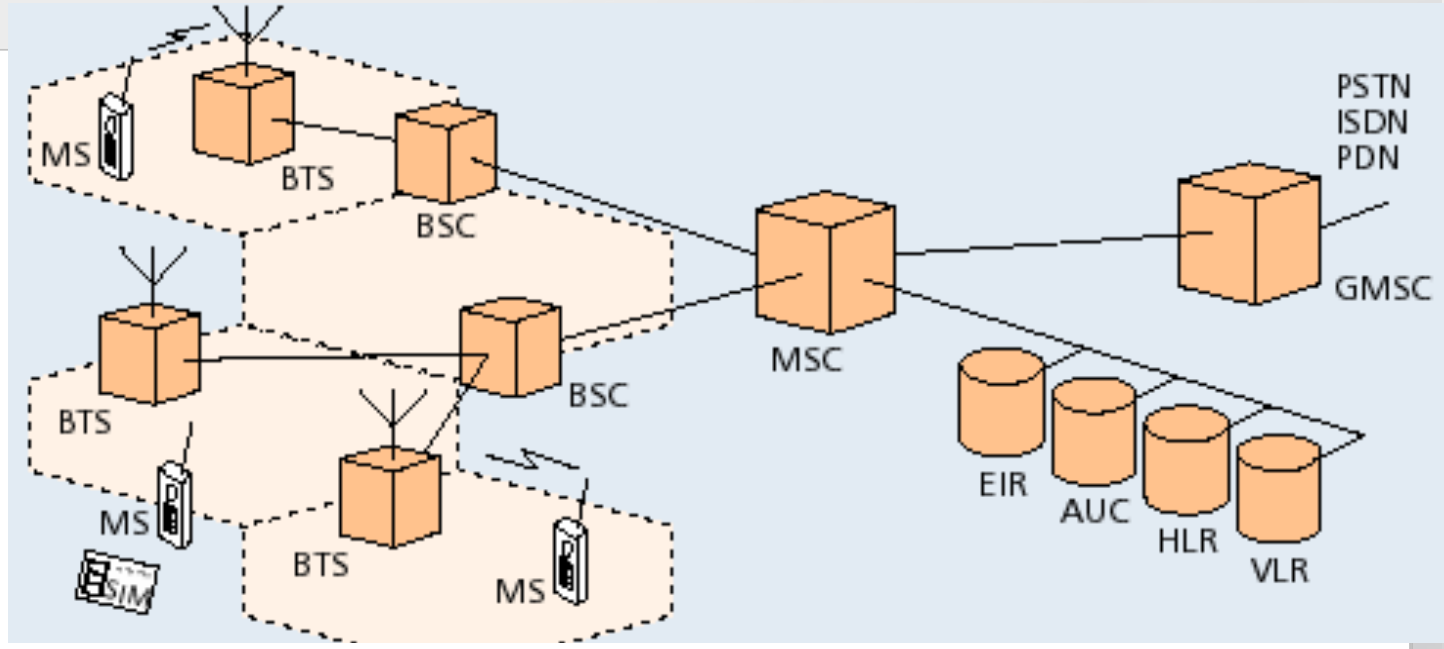
GSM Architecture: Mobile Station (MS)

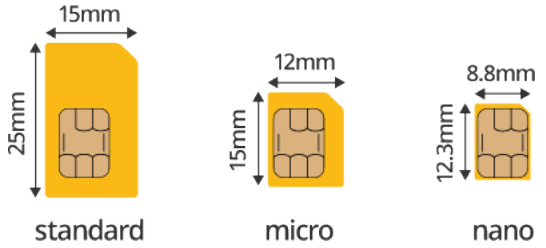
GSM Architecture: Mobile Station

- MS consists of following two components

1. Mobile Equipment (ME)
2. Mobile Subscriber Identity Module (SIM)
   - Removable plastic card
   - Stores Network Specific Data such as list of carrier frequencies and current LAI.
   - Stores International Mobile Subscriber Identity (IMSI) + ISDN
   - Stores Personal Identification Number (PIN) & Authentication Keys.
   - Also stores short messages, charging information, telephone book etc.

- Allows separation of user mobility from equipment mobility

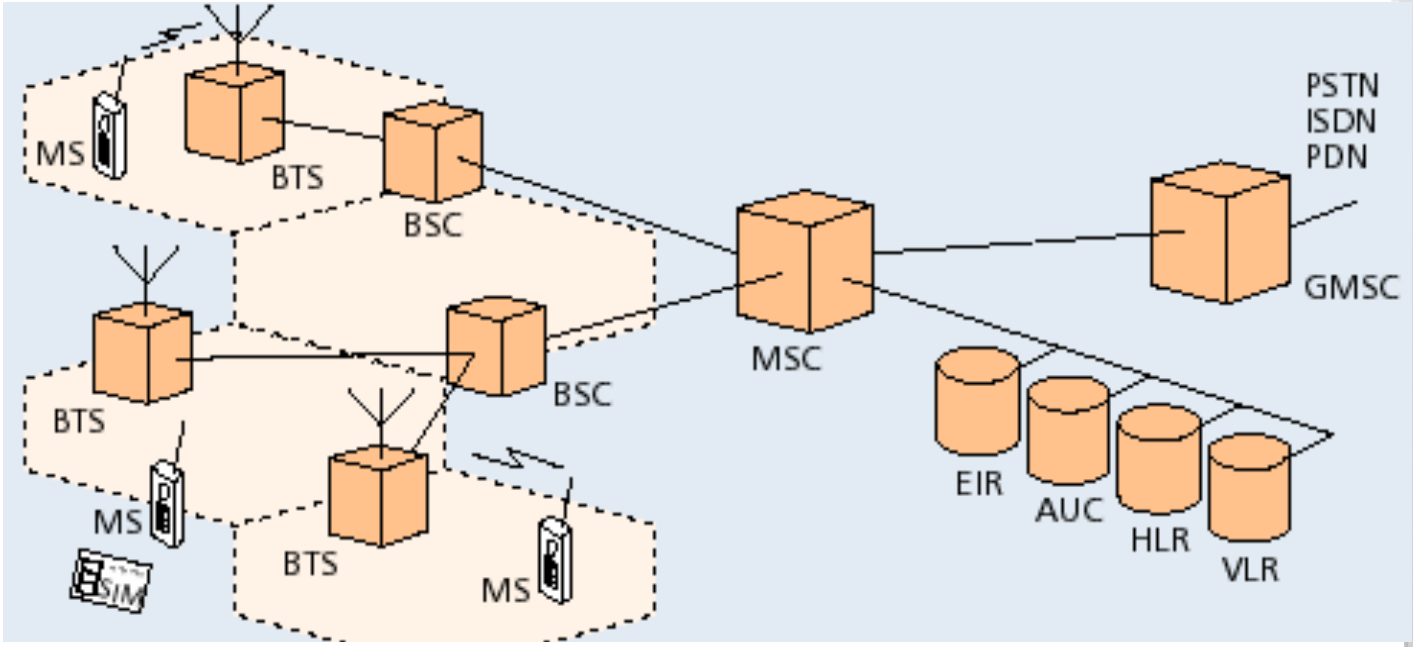


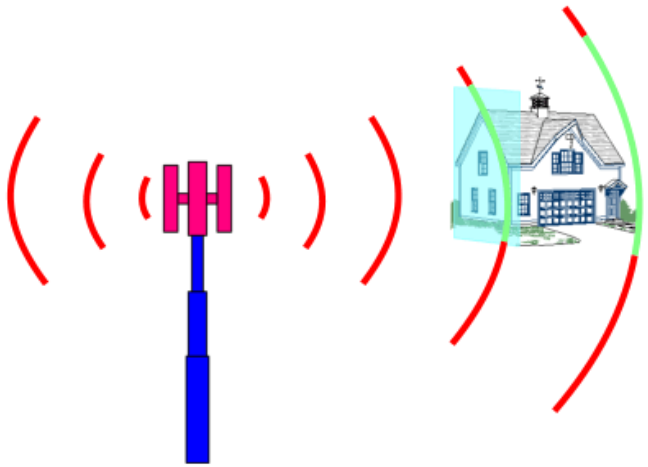


GSM Architecture: In Detail

GSM Architecture: Base Transceiver Station (BTS)

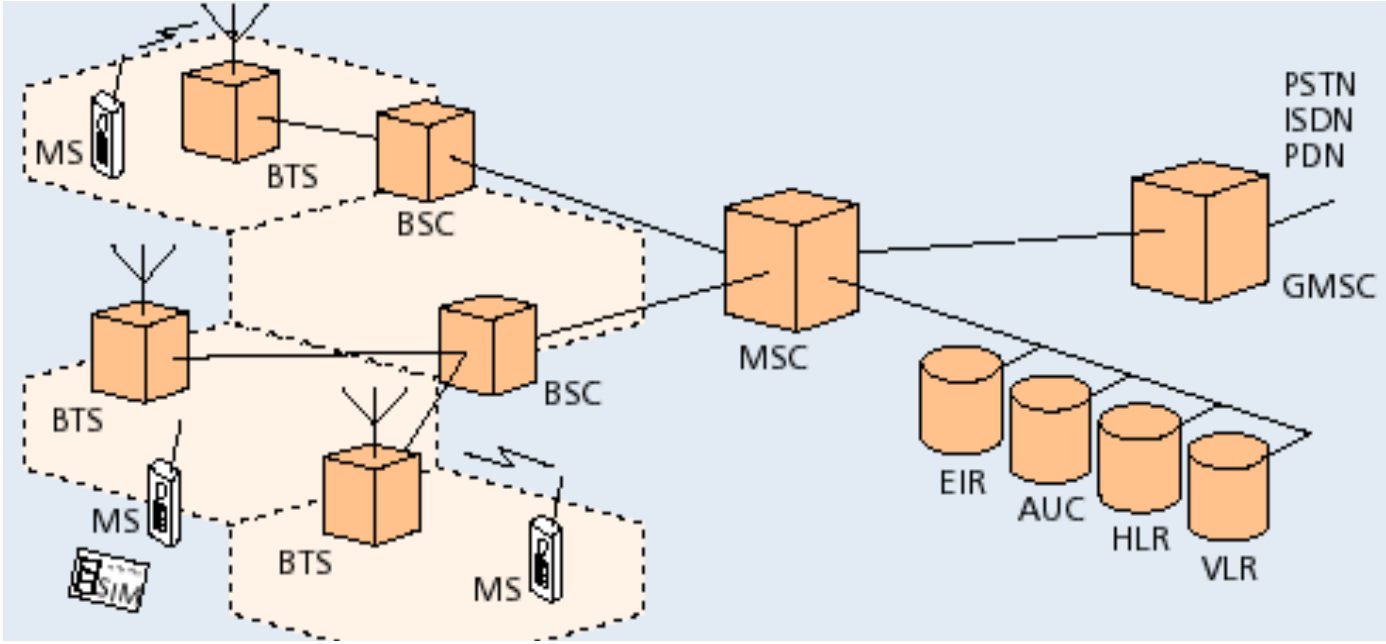
- One per cell
- Consists of high speed transmitter and receiver
- Its transmit power decides size of cell
- Function of BTS
  - Provides two channels
    - Signalling and Data Channel
  - Performs error protection coding for the radio channel





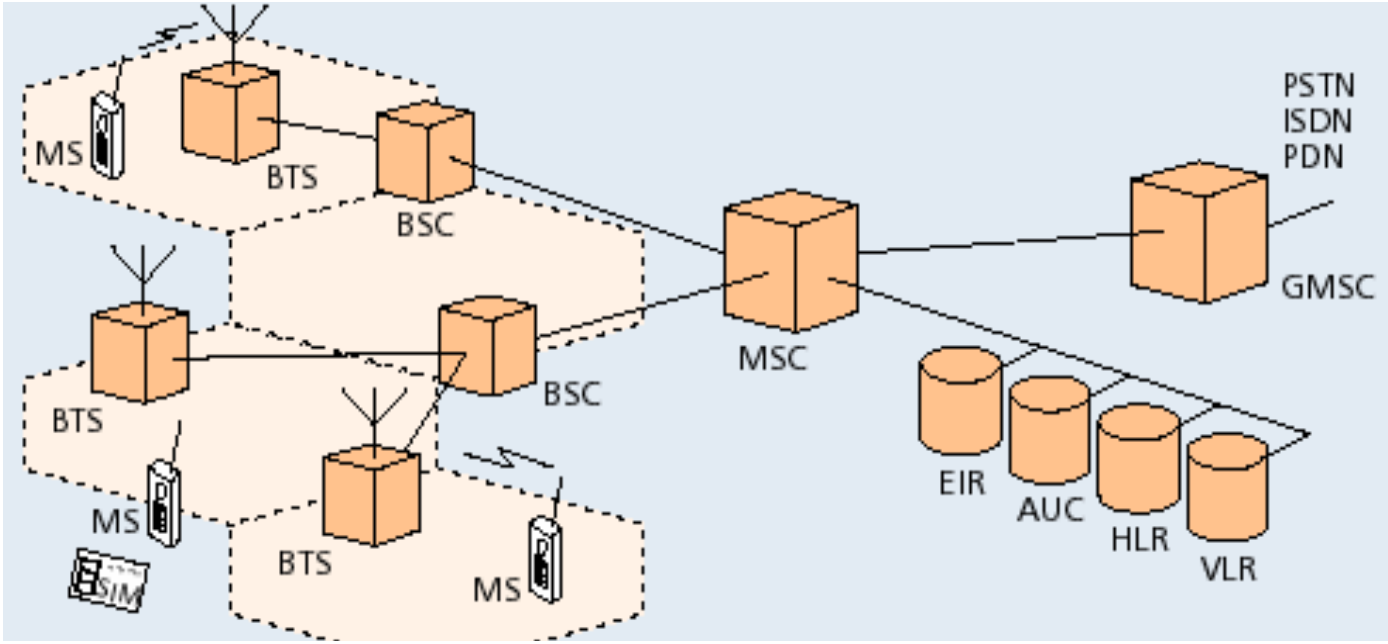
GSM Architecture: Base Station Controller (BSC)

- Controls multiple BTS
- Functions of BSC
  - Performs radio resource management
    - Assigns and releases frequencies and time slots for all the MSs in its area
    - Reallocation of frequencies among cells
    - Hand over protocol is executed here
  - Time and frequency synchronization signals to BTSs
  - Time Delay Measurement and notification of an MS to BTS
  - Power Management of BTS and MS



GSM Architecture: Mobile Switching Centre (MSC)

- Switching node of a PLMN(Public Land Mobile Network)
- Task of MSC
  1. Registration
  2. Authentication
  3. Location updating
  4. Handovers
  5. Call routing
- Mobility of subscribers
  - ➥ Location registration of subscriber
- There can be several MSCs in a PLMN



GSM Architecture: Mobile Switching Centre (MSC)

- **What is a PLMN?**

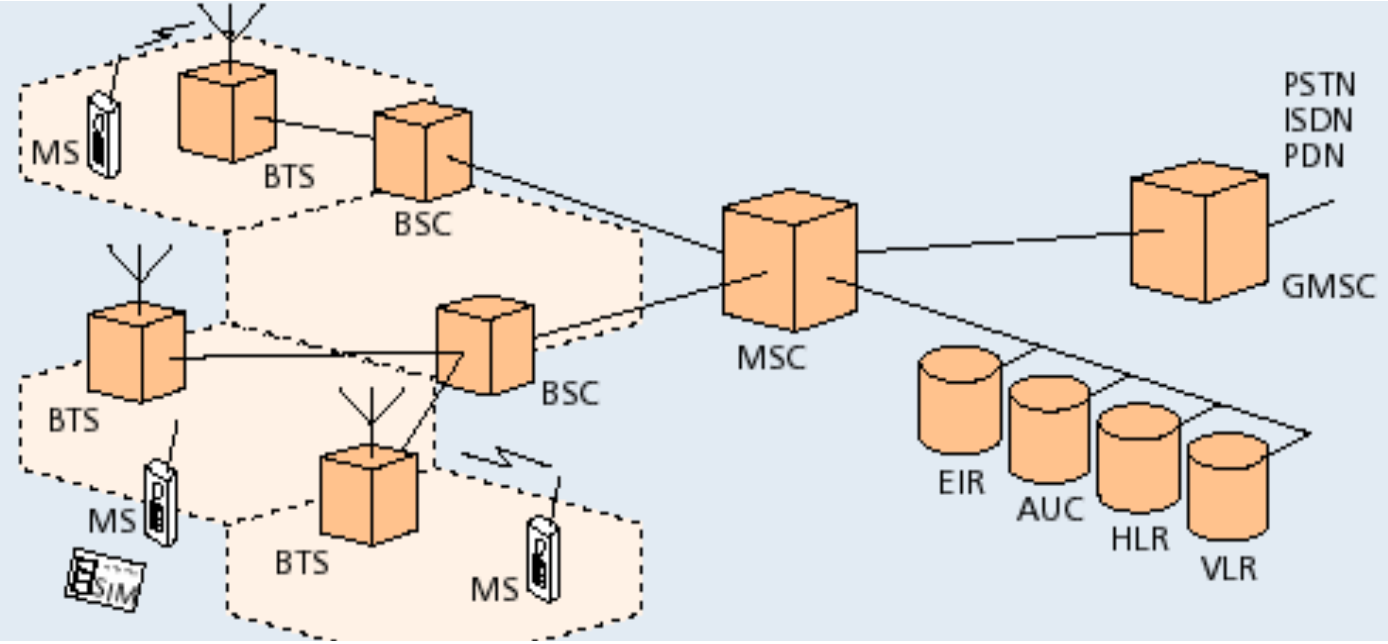
- PLMN stands for **Public Land Mobile Network** and is a mobile operator's cellular network in a specific country.

- A public land mobile network is a combination of wireless communication services offered by a specific operator in a specific country.

- Each PLMN has a unique PLMN code that combines an MCC (Mobile Country Code) and the operators' MNC (Mobile Network Code).
- When you receive a SIM from an operator, it will often have PLMN lists on it. These lists are a way to prioritize networks you would like to use on the SIM.
- Typically, PLMN lists are based on commercial agreements. So, for example, an operator will have contracts in various countries so your SIM can connect to specific networks when you roam outside their network.

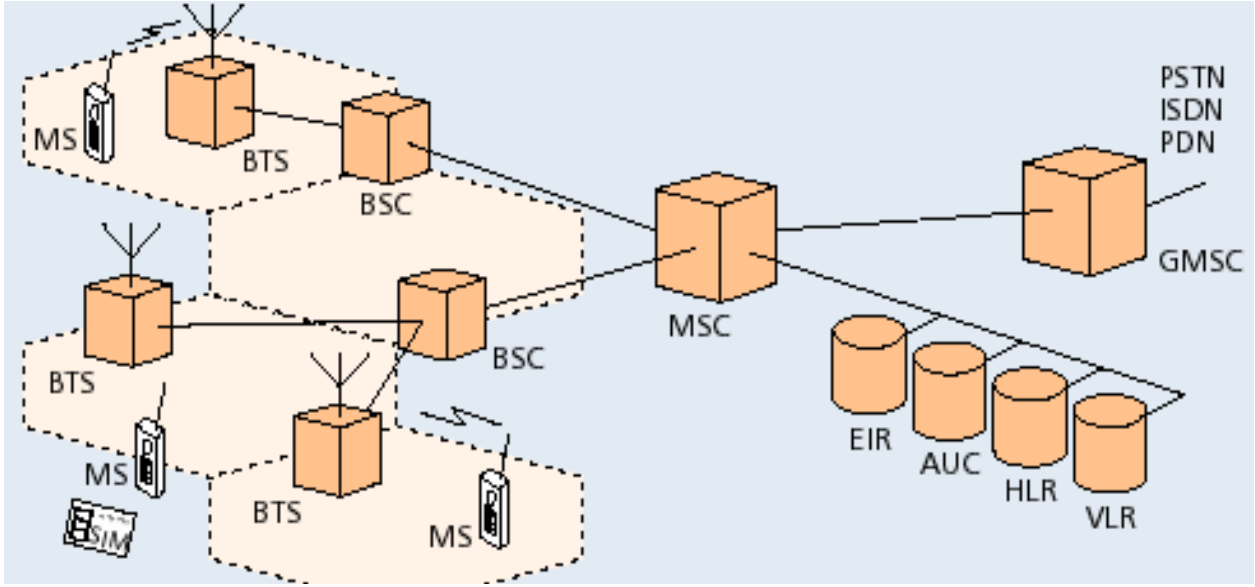
GSM Architecture: Gateway MSC (GMSC)

- Connects mobile network to a fixed network
  - ➥ Entry point to a PLMN
- Usually one per PLMN
- Request routing information from the HLR and routes the connection to the local MSC



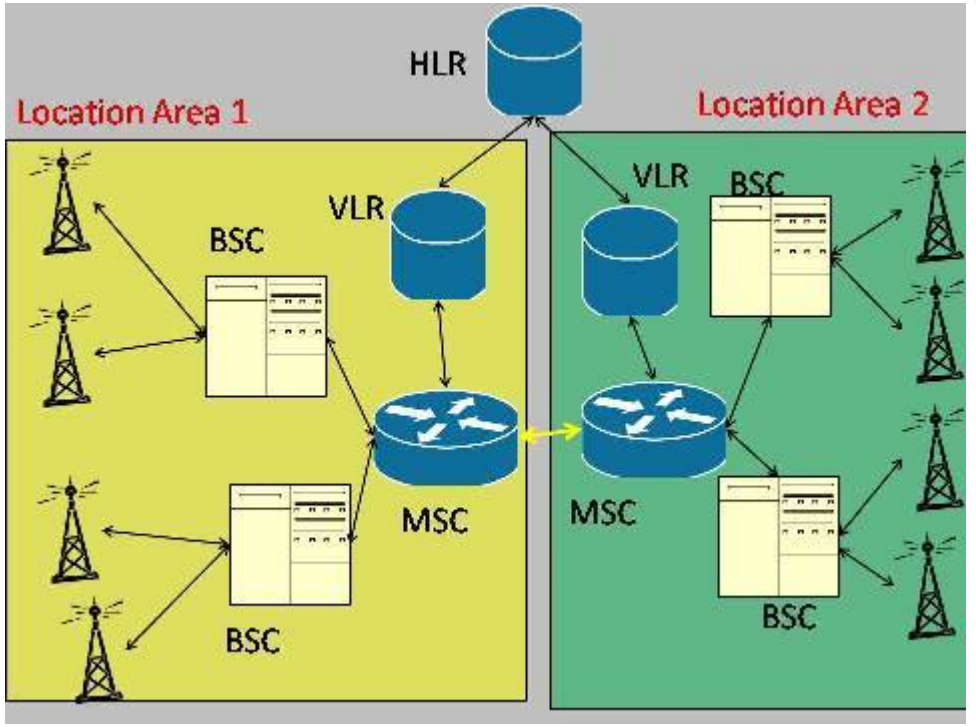
GSM Architecture: Home Location Register (HLR)

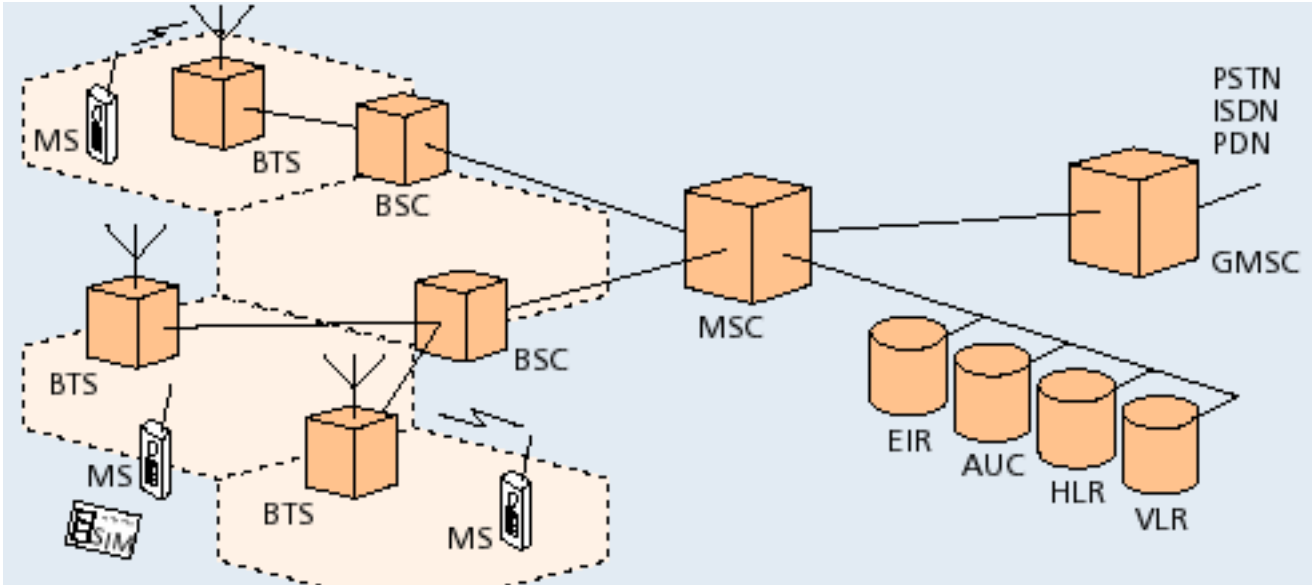
- For all users registered with the network, HLR keeps user profile.
- Logically only one HLR per PLMN
- Persistent storage of user data
- MSCs exchange information with HLR
- When MS registers with a new GMSC, the HLR sends the user profile to the new MSC
- Includes information like
  - Current location of user
  - Authentication data
  - Service provisioning information



GSM Architecture: Visitor Location Register (VLR)

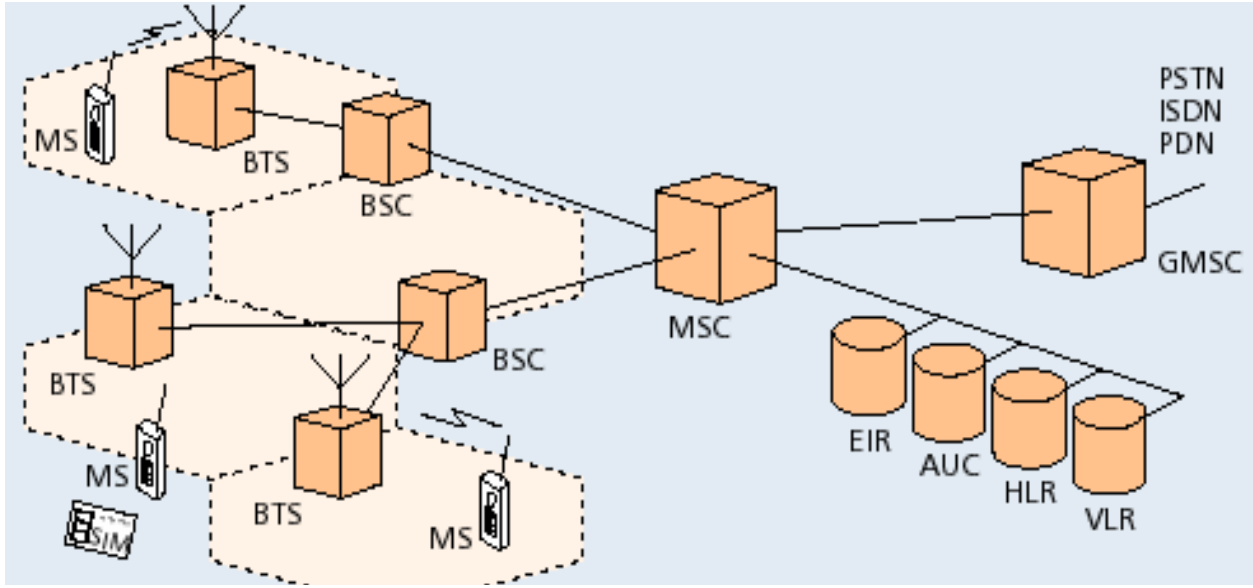
- VLR is responsible for a group of location areas, typically associated with an MSC
- Contains temporary information needed for call control typically copied from HLR.
- When subscriber enters a new MSC, VLR associated with that MSC requests user info from corresponding HLR



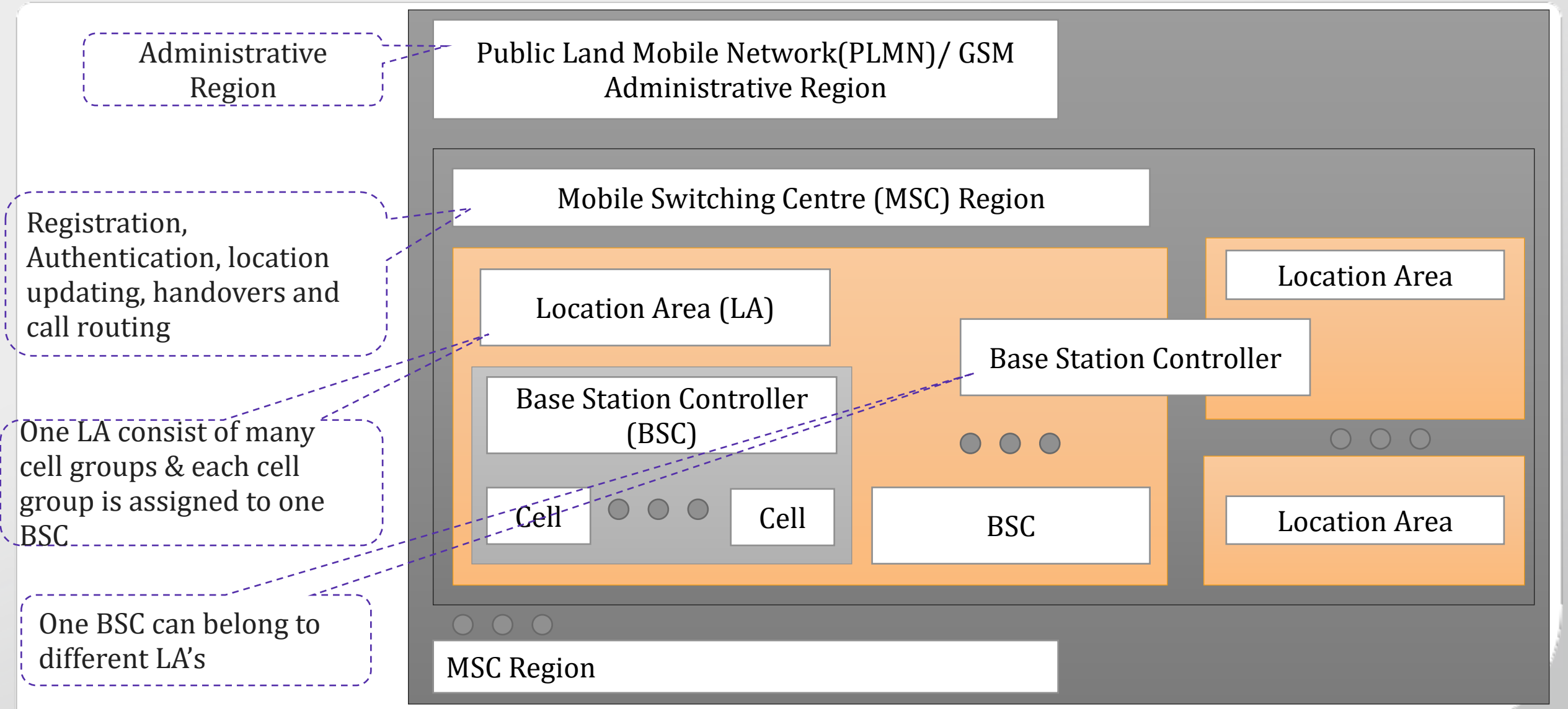


GSM Architecture: AUC and EIR

- **AUC: Authentication Center**
  - Accessed by HLR to authenticate a user for service
  - Contains authentication and encryption keys for subscribers
- **EIR: Equipment Identity Register**
  - Allows stolen or fraudulent mobile stations to be identified



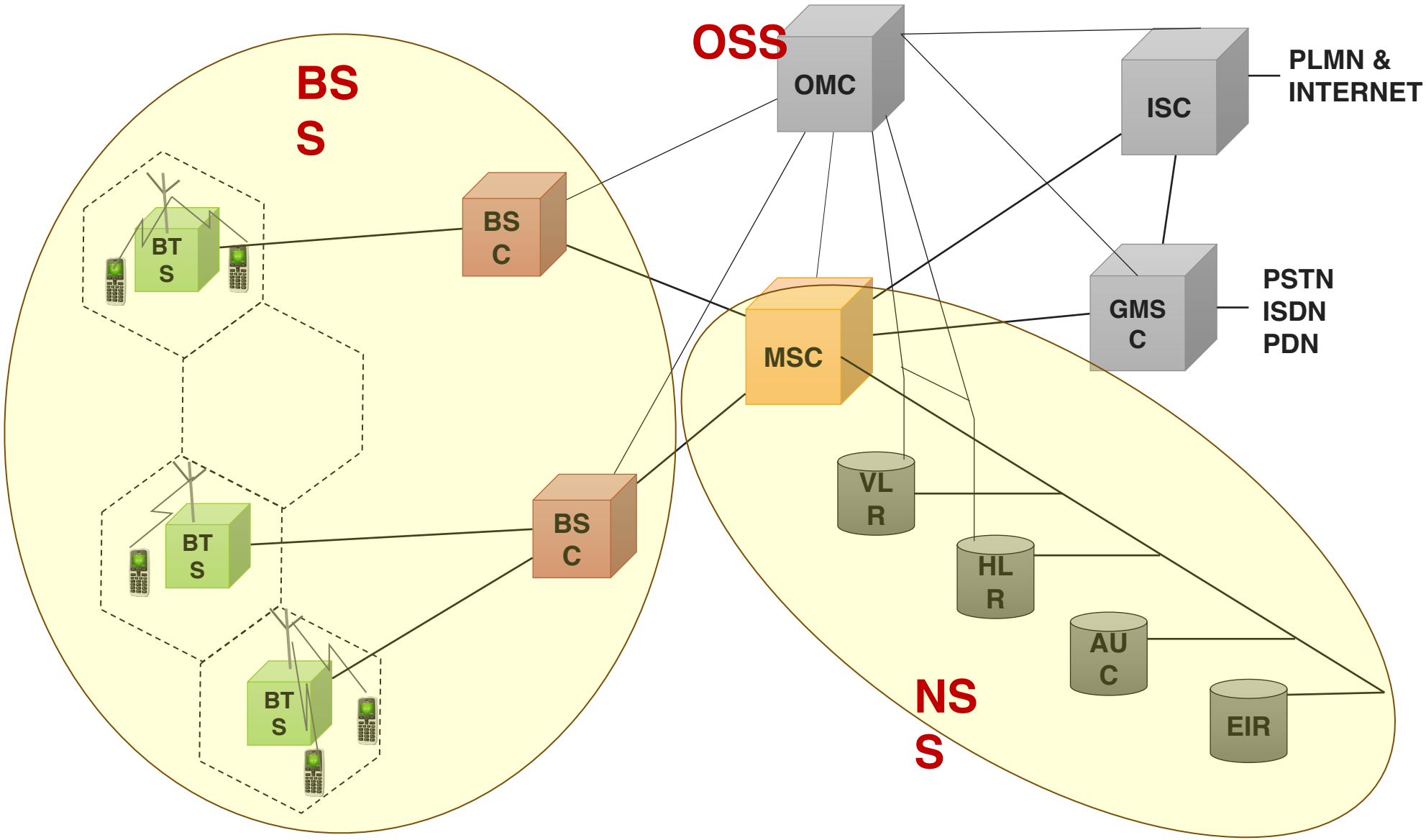
GSM System Hierarchy



GSM Entities

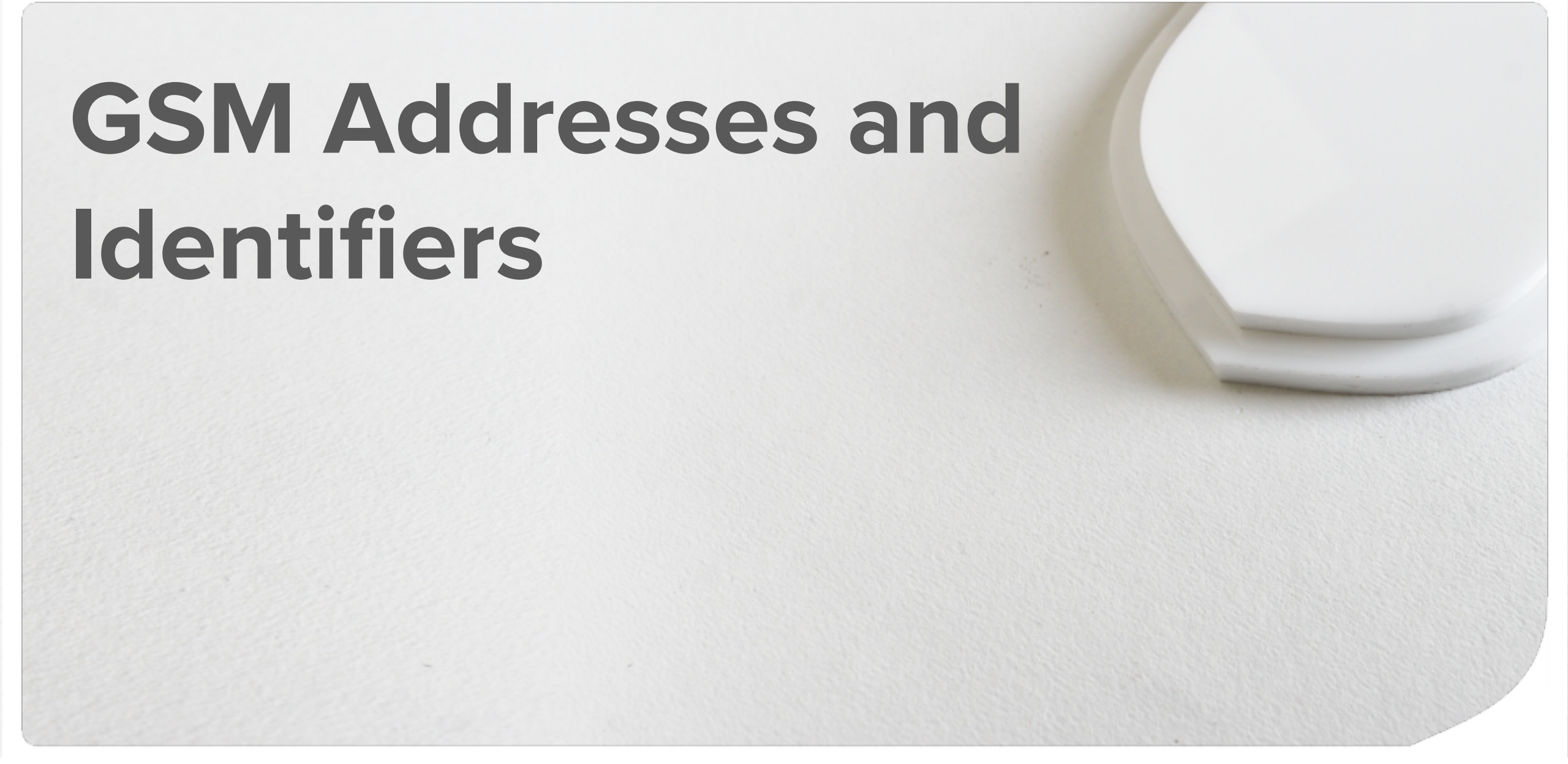
Mobile Station (MS)	1.Mobile Equipment (ME) 2.Subscriber Identity Module (SIM)
Base Station Subsystem (BSS)	1.Base Transceiver Station (BTS) 2.Base Station Controller (BSC)
Network and Switching Subsystem (NSS)	1.Mobile Switching Center (MSC) 2.Home Location Register (HLR) 3.Visitor Location Register (VLR) 4.Equipment Identity Register (EIR) 5.Authentication Center (AUC)
Operation and Support Subsystem (OSS)	1.Operation and Maintenance Center (OMC)

GSM Entities-Diagramatic Representation

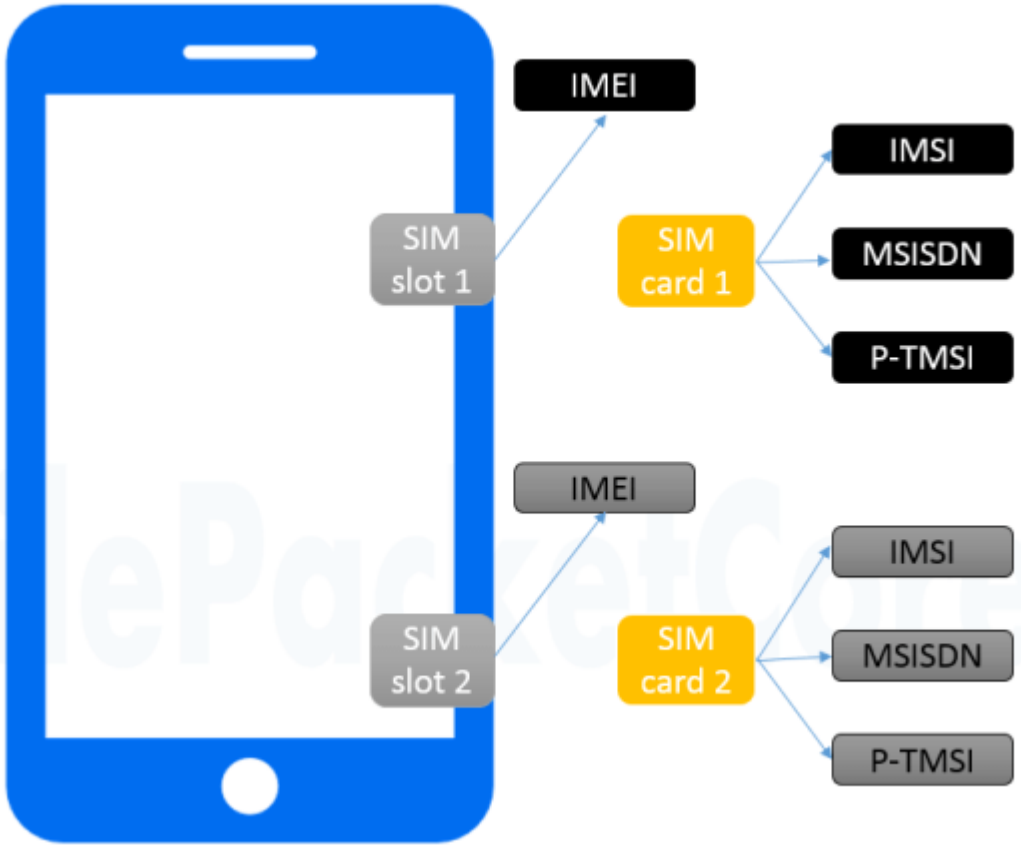


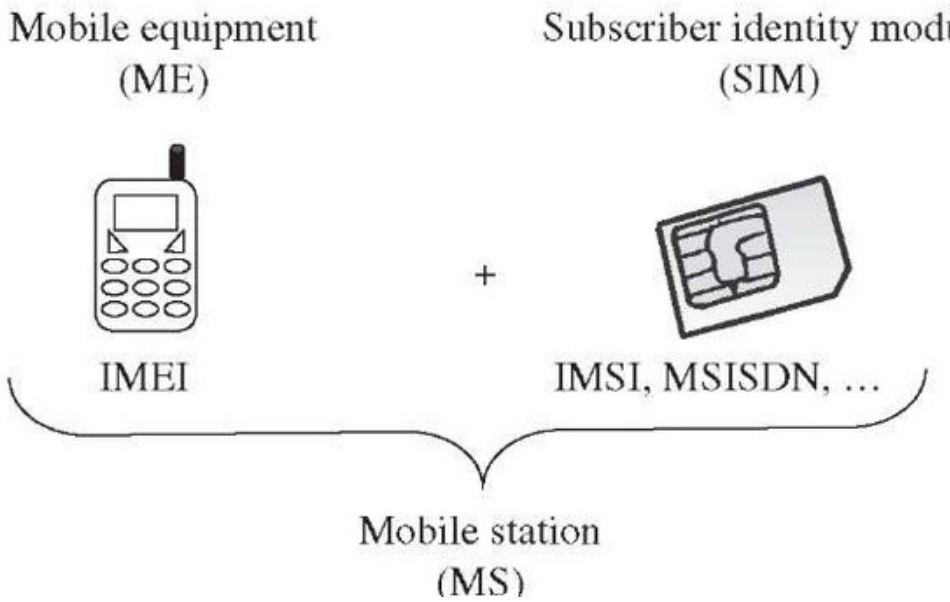
Marwadi University

GSM Addresses and Identifiers



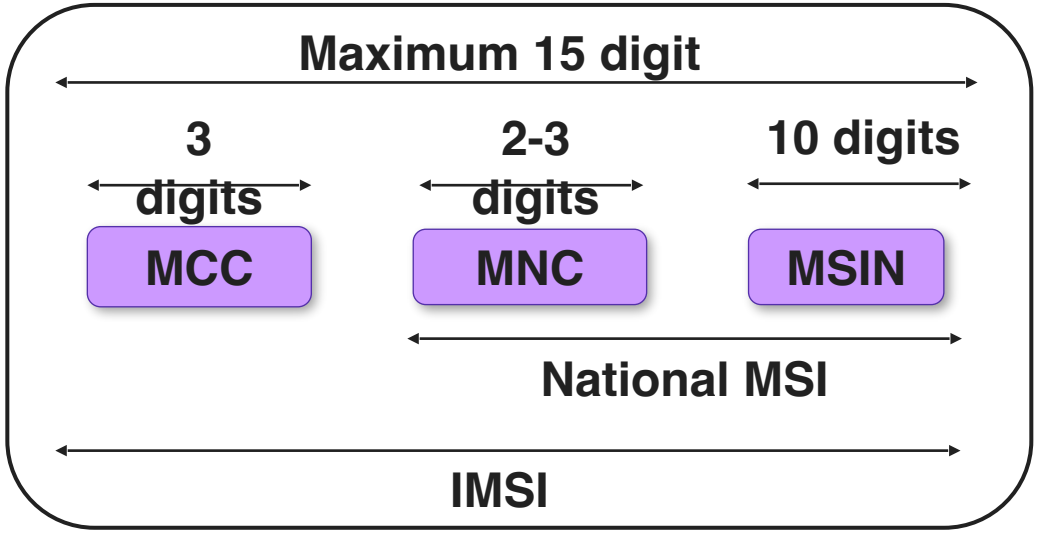
GSM Addresses and Identifiers





GSM Addresses and Identifiers: IMSI

- **IMSI**: **I**nternational **M**obile **S**ubscriber **I**dentity
- IMSI identifies registered smartphone users
- A working SIM card has a valid IMSI
- Each IMSI consists of three parts:



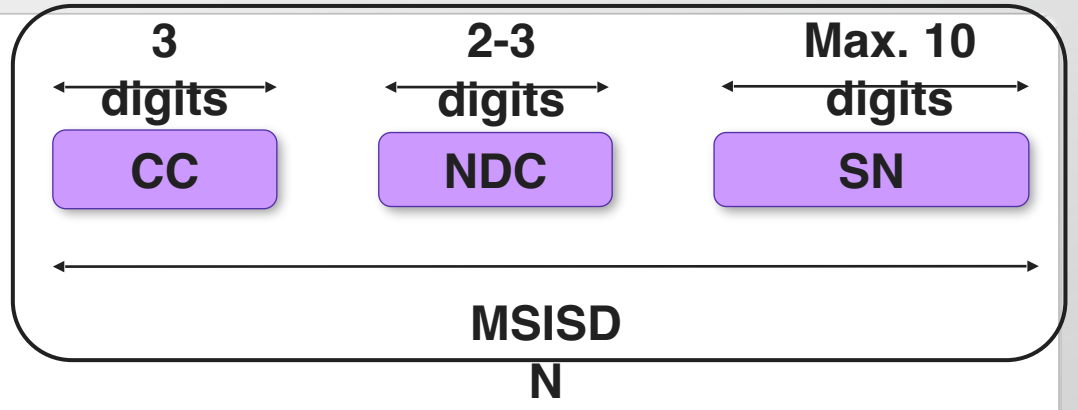
1. Mobile Subscriber Identification Number (MSIN)
   - identifies the subscriber in his or her mobile network.
2. Mobile Country Code (MCC)
   - It gets 3 decimal places and identifies the country of mobile device owner.
3. Mobile Network Code (MNC)
   - It identifies your carrier network

GSM Addresses and Identifiers: IMEI

- IMEI: International Mobile Equipment Identity
- 15-digit number to uniquely identify a mobile phone device.
- Every mobile equipment in this world has a unique identifier which is called IMEI.
  - IMEI allocated by the equipment manufacturer and registered by the network operator in the Equipment Identity Register (EIR).

GSM Addresses and Identifiers: MSISDN

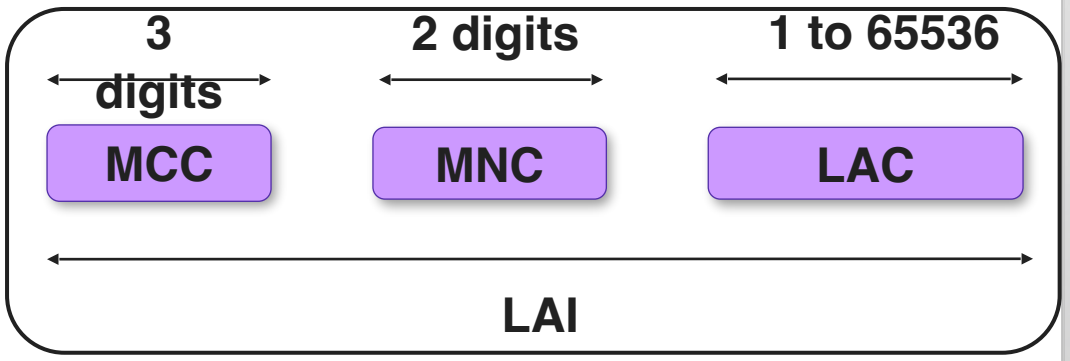
- Mobile Subscriber ISDN Number
- MSISDN is primary key to the HLR record.
- The MSISDN number is the real telephone number as is known to the external world.
  - MSISDN number is public information whereas IMSI is private to the operator.
  - IMSI is assigned a total of three numbers: one for the voice call, one for a fax call and another for the data call.
  - MSISDN follows the international ISDN (Integrated Systems Data Network) numbering plan.



Country Code - CC
National Destination Code - NDC
Subscriber Number - SN

GSM Addresses and Identifiers: LAI

- LAI: Location Area Identifier.
- Each LA in a PLMN has own identifier called Location Area Identifier (LAI) which is structured hierarchically and unique.
- Example: 502-20-60001



- Mobile Country Code - MCC
- Mobile Network Code - MNC
- Location Area Code - LAC

GSM Addresses and Identifiers: MSRN

- MSRN: Mobile Station Roaming Number.
- When a subscriber is roaming in another network, a temporary ISDN number assigned to the subscriber called MSRN.
  - MSRN assigned by the local VLR in charge of the mobile station and follows the structure of MSISDN.

GSM Addresses and Identifiers

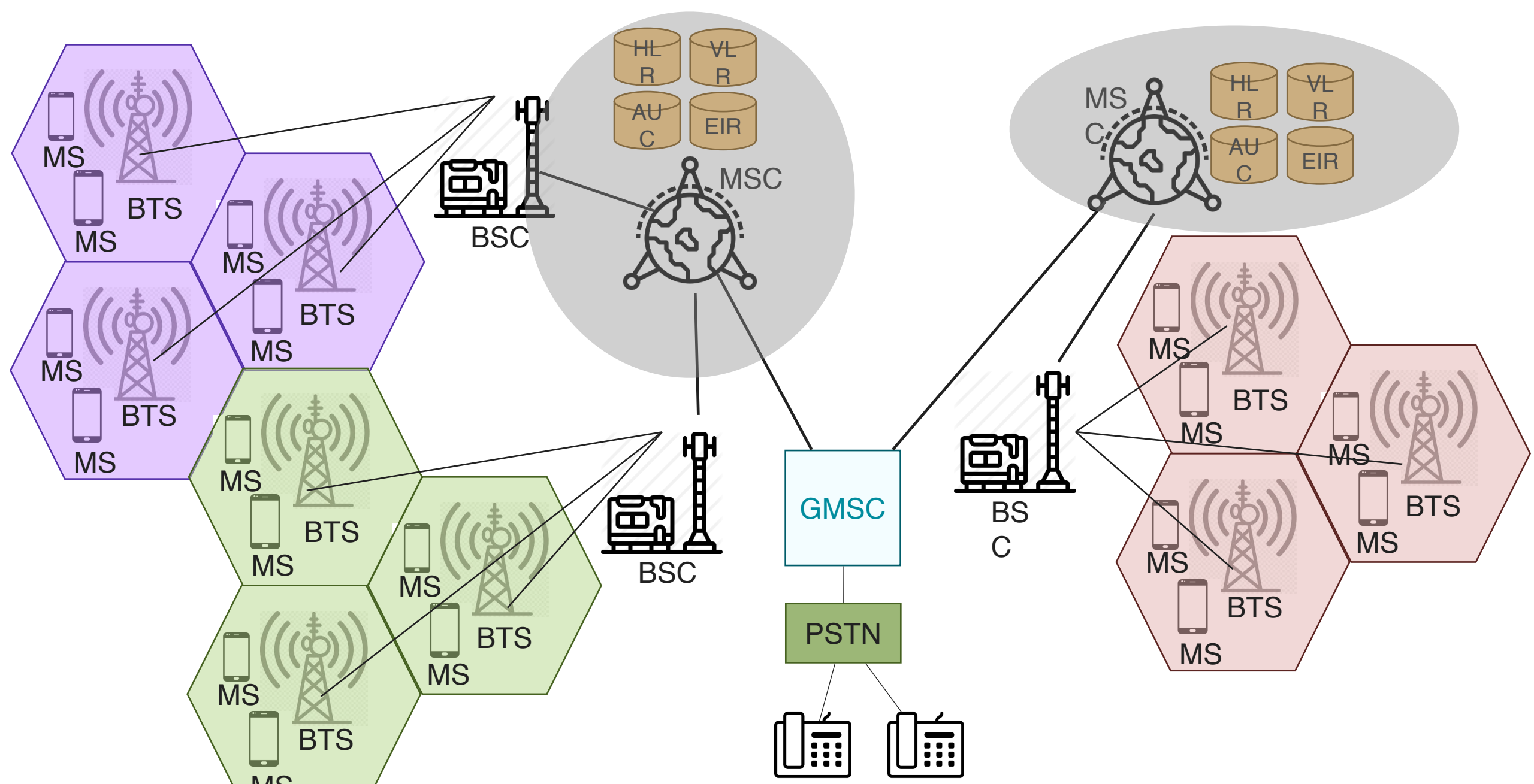
- Temporary Mobile Subscriber Identity (TMSI): TMSI is a temporary identifier assigned by the serving VLR used in place of the IMSI for identification and addressing of the mobile station.
  - Together with the current location area, a TMSI allows a subscriber to identified uniquely.
- Local Mobile Subscriber Identity (LMSI): LMSI assigned by the VLR and stored in the HLR and used as a searching key for faster database access within the VLR.
- Cell Identifier: Within an LA, every cell has a unique Cell Identifier (CI) together with an LAI, a cell can be identified uniquely through Global Cell Identity (LAI & CI).

GSM Addresses and Identifiers (Summery)

IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
MSISDN	Mobile Subscriber ISDN
LAI	Location Area Identifier
MSRN	Mobile Station Roaming Number
TMSI	Temporary Mobile Subscriber Identity
LMSI	Local Mobile Subscriber Identity

Marwadi University

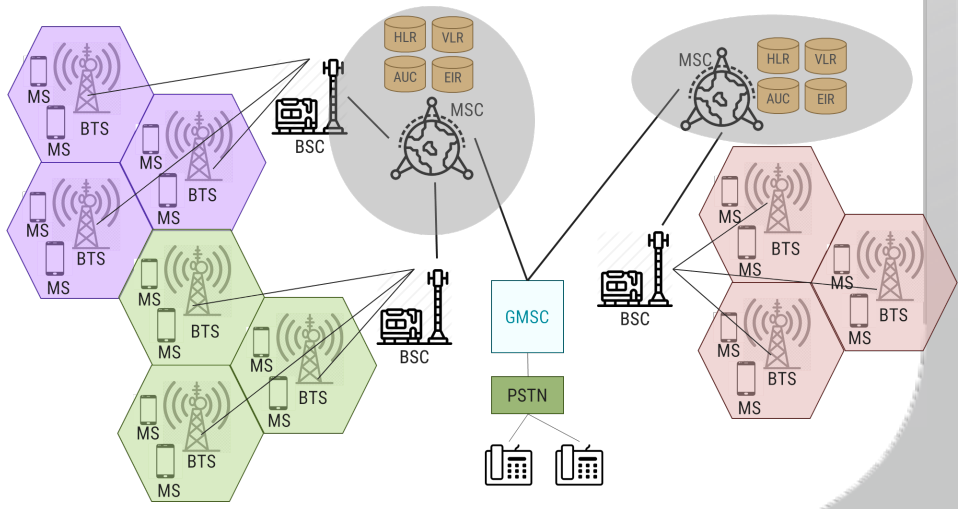
Call Routing in GSM



Call Routing in GSM

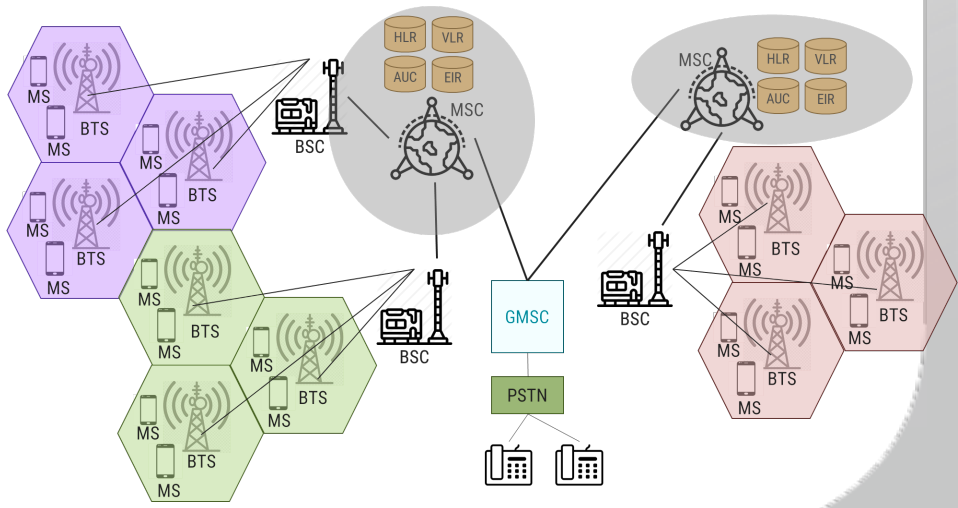
Call routing in GSM: Mobile Phone to PSTN

1. Mobile phone subscriber will dial a number on PSTN network
2. To identify the communicating network the MSC will receive the message of a call request through BTS and BSC respectively.
3. The MSC checks if the MS is authorized to access the destination network. If YES, then service of MS is activated, else the service will be denied.
4. MSC will ask the BSC to allocate a traffic channel (radio channel + time slot)
5. The BSC will allocates the traffic channel and pass the information to PSTN telephone.

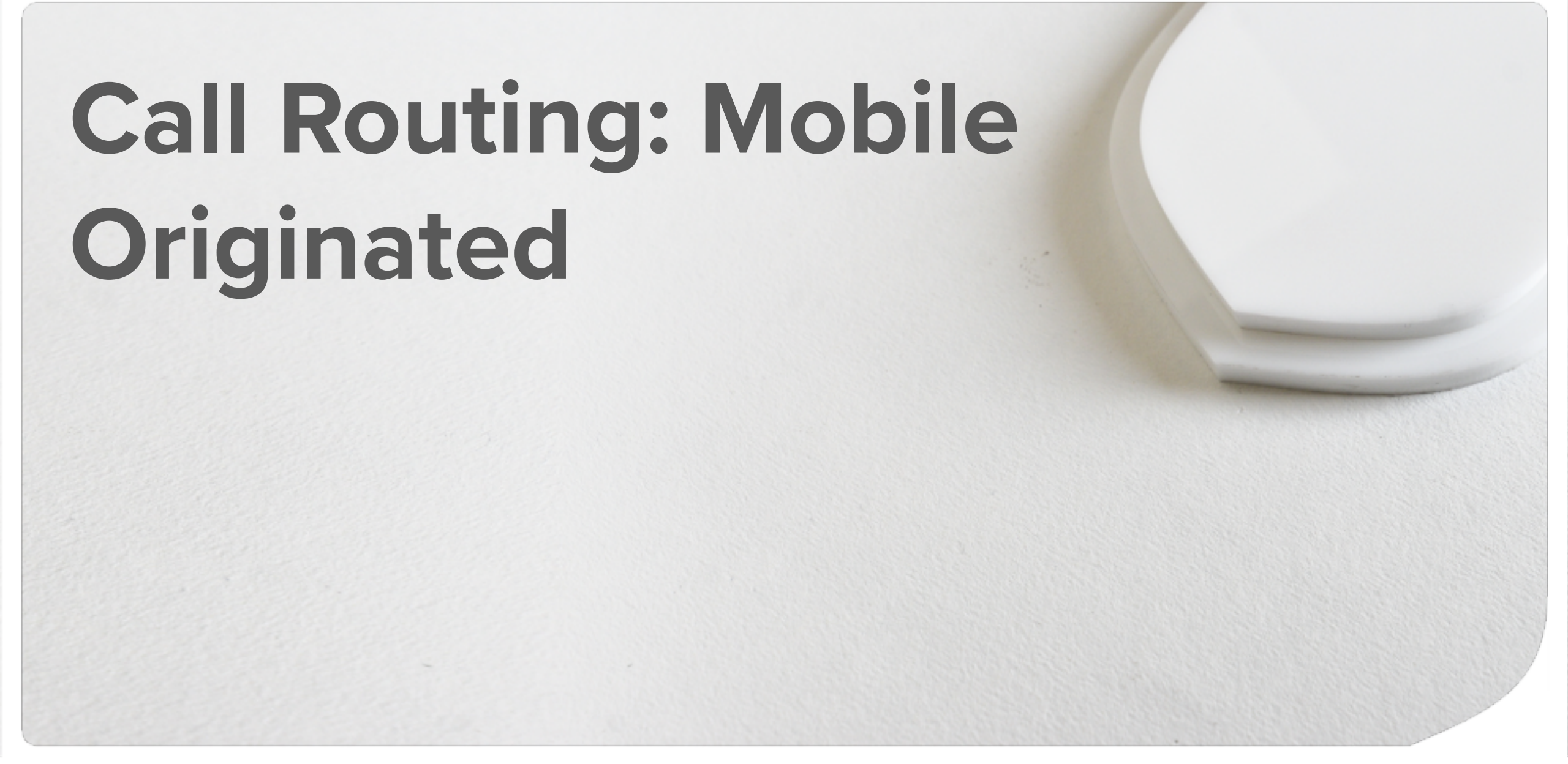


Call routing in GSM: Mobile Phone to PSTN

6. The called party answers the call and the conversation takes place.
7. The MS keeps on taking measurements of the radio channels in the present cell and the neighbouring cells and passes the information to the BSC.
8. The BSC decides if a handover is required.
9. If so, a new traffic channel is allocated to the mobile station and the handover takes place.
10. If handover is not required, the mobile station continues to transmit in the same frequency.

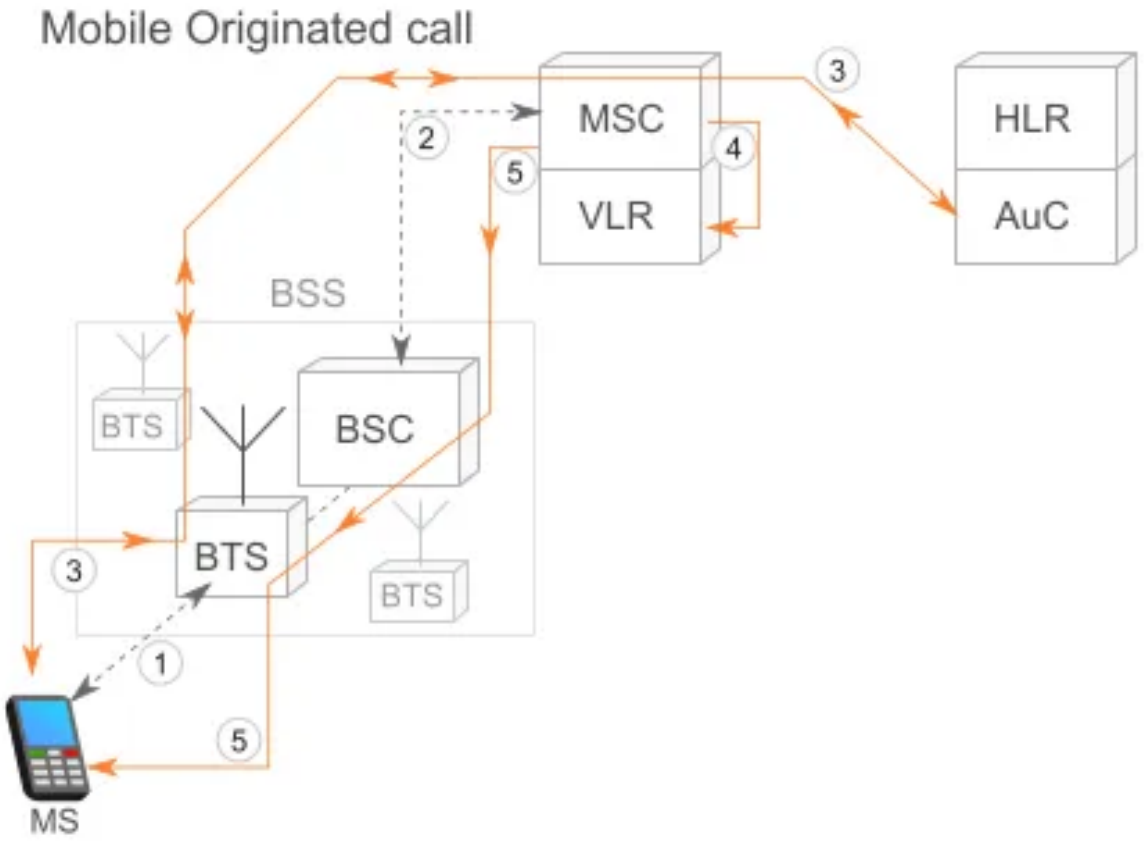


Call Routing: Mobile Originated



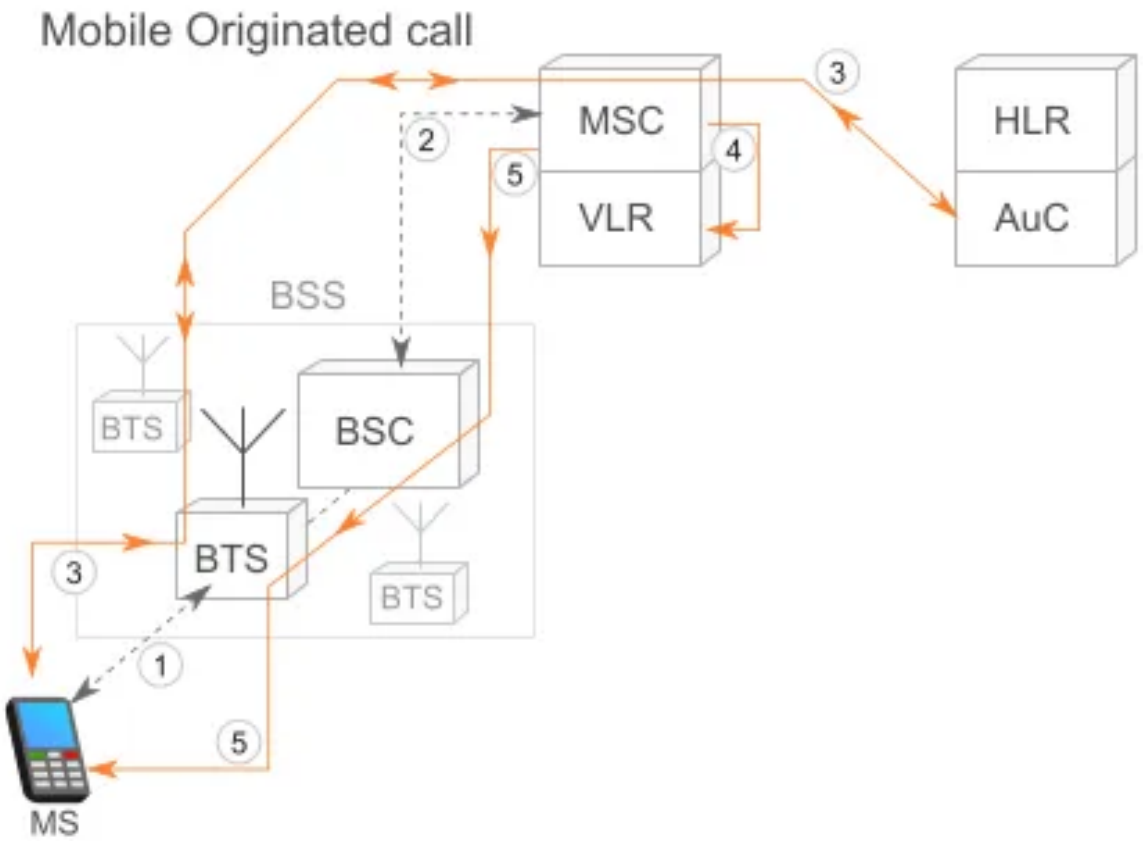
Mobile Originated Call

Step-1	To initiate a call, the MS request for radio resource allocation to the BSS, which mediates further connection to the Mobile Switching Center (MSC). The BSS assigns the MS a channel with a given frequency and time slot.
Step-2	BSS initiate the connection to the MSC.
Step-3	Now as MS had connected to the network, the subscriber needs to be authenticated. As IMSI number is stored in MS SIM card, AUC will verify subscriber's identity. Thus, MS and MSC are now connected. MSC initiates a ciphering procedure which is transmitted to the BTS, which in turn forwards the message to the MS. it will start the ciphered transmission of information, finalizing the encryption procedure.
Step-4	MSC verifies that the requested service is allowed for the subscriber. This information is available in VLR. Once the VLR confirms the service requested by the originating MS, the MSC starts the call setup.



Mobile Originated Call

Step-5	MSC allocates a voice channel between the MSC and the BSS. The MSC routes the call to the dialed number. When the call is received in the PSTN, the MSC is notified that the called subscriber is being alerted, at which point the originating MS receives a ring notification.
Step-6	To disconnect the call by either party, a disconnect message is sent to the MSC, which releases the communication channels created with the PSTN and the BSS

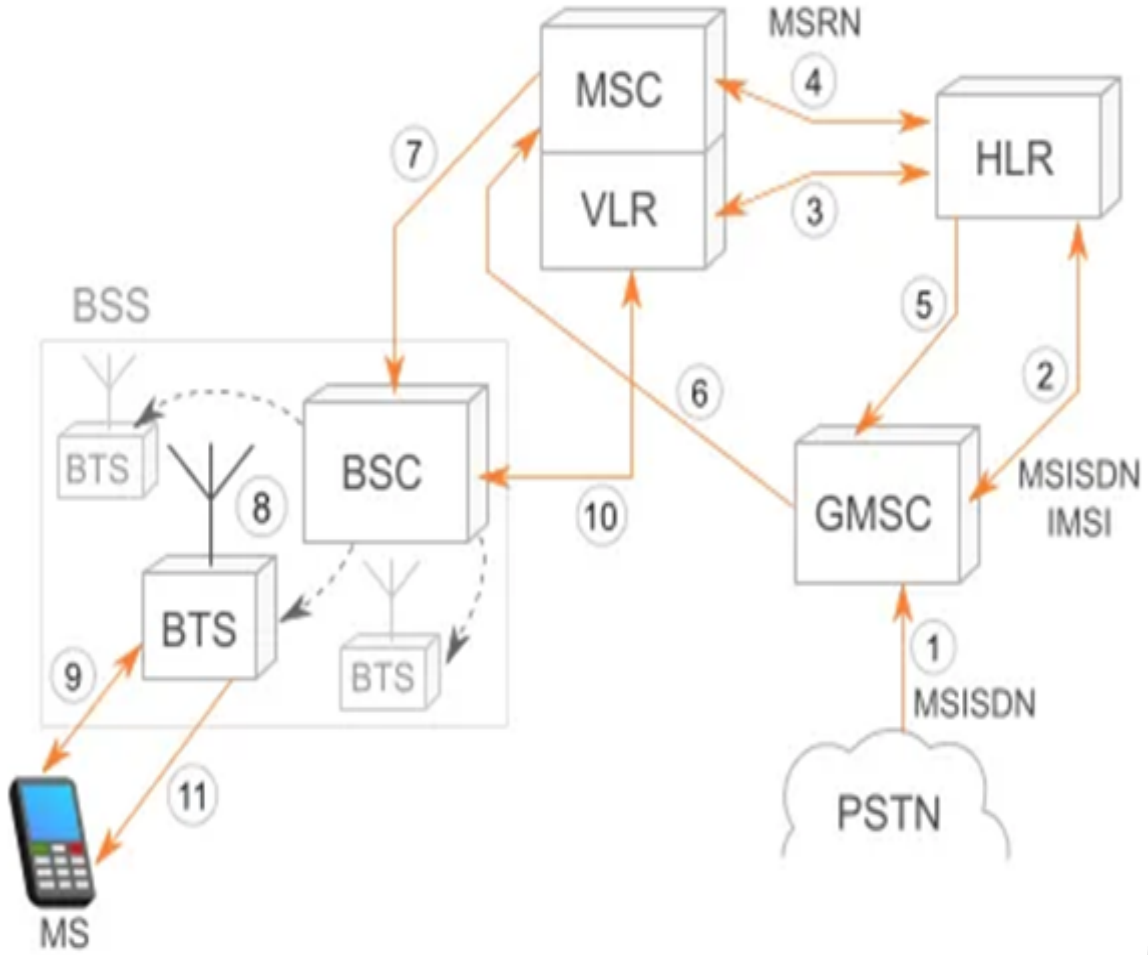


Marwadi University

Call Routing: PSTN Originated

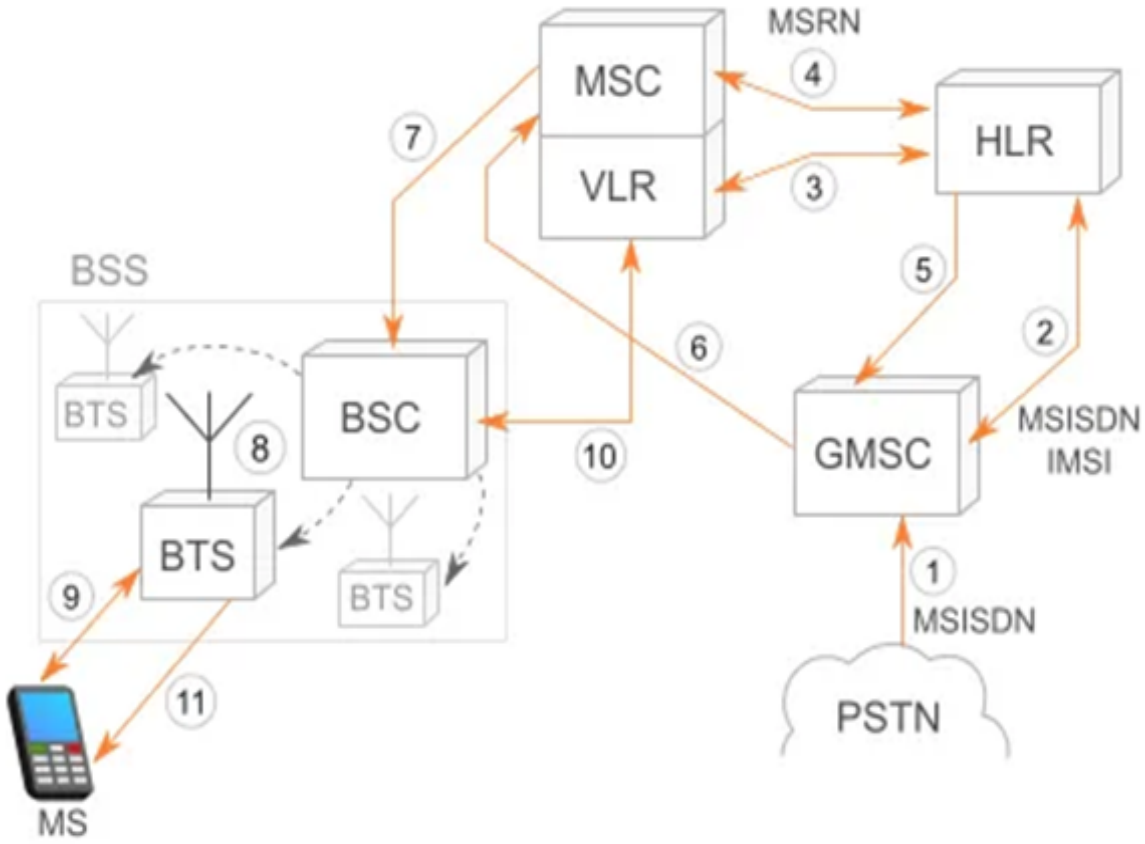
PSTN Originated Call

Step-1	When a call is placed from the PSTN, the PSTN uses the information in the phone number (country and if available, operator) to locate GMSC leading to the MSC where the subscriber is registered.
Step-2	GMSC can request information about the subscriber's core network and current location by interrogating the HLR.
Step-3	HLR constantly updates locations of the MS stored in the VLRs of the networks the MS visits. In the HLR, the subscriber MSISDN (phone number) is associated with the IMSI number of the SIM card, which was used to authenticate the subscriber in the visited network as they registered. HLR is aware of the visited MSC/ VLR of the MS at a given time.
Step-4	In order for the GMSC to pass the call to the MSC, the HLR asks a temporary roaming phone number(MSRN) from the MSC. (Mobile Station Roaming Number – MSRN).



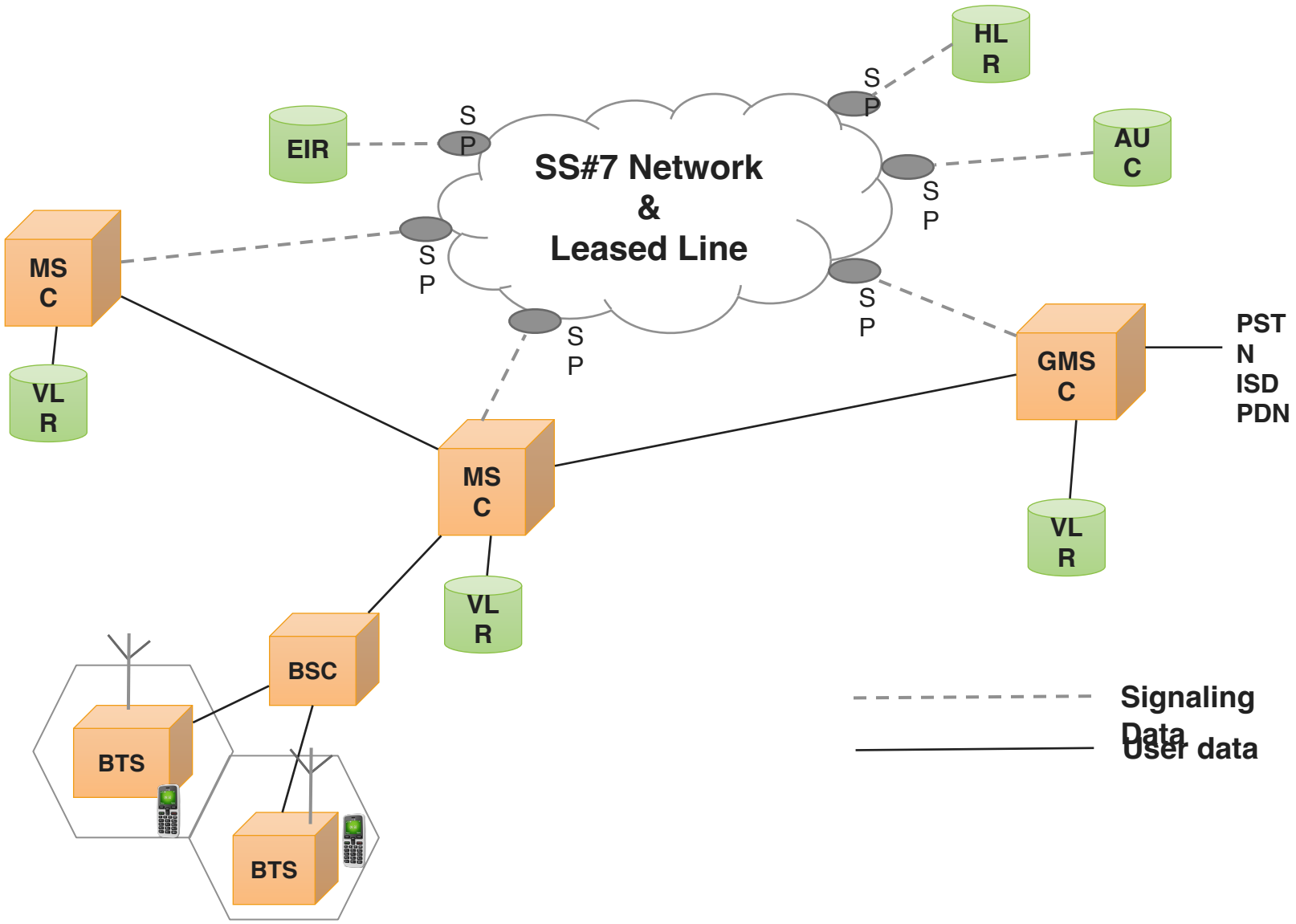
PSTN Originated Call

Step-5	MSRN is sent back from the HLR to the GMSC.
Step-6	GMSC forward the call to the MSC using the assigned MSRN.
Step-7	MSC pages all the BSCs in the area that it serves.
Step-8	Then BSC assigned page to the BTSs.
Step-9	Called MS responds to the paging from the BTS, asking to establish a radio channel to the BTS.
Step-10	Response is forwarded to the MSC, which, once notified, authenticates the MS and initiates the ciphering of the call
Step-11	MSC sends back to the radio network the call confirmation message, the called MS starts to ring.
Step-12	Then, MSC notifies the GMSC, which notifies the PSTN that the destination number is being alerted.



PLMN Interface

PLMN Interface

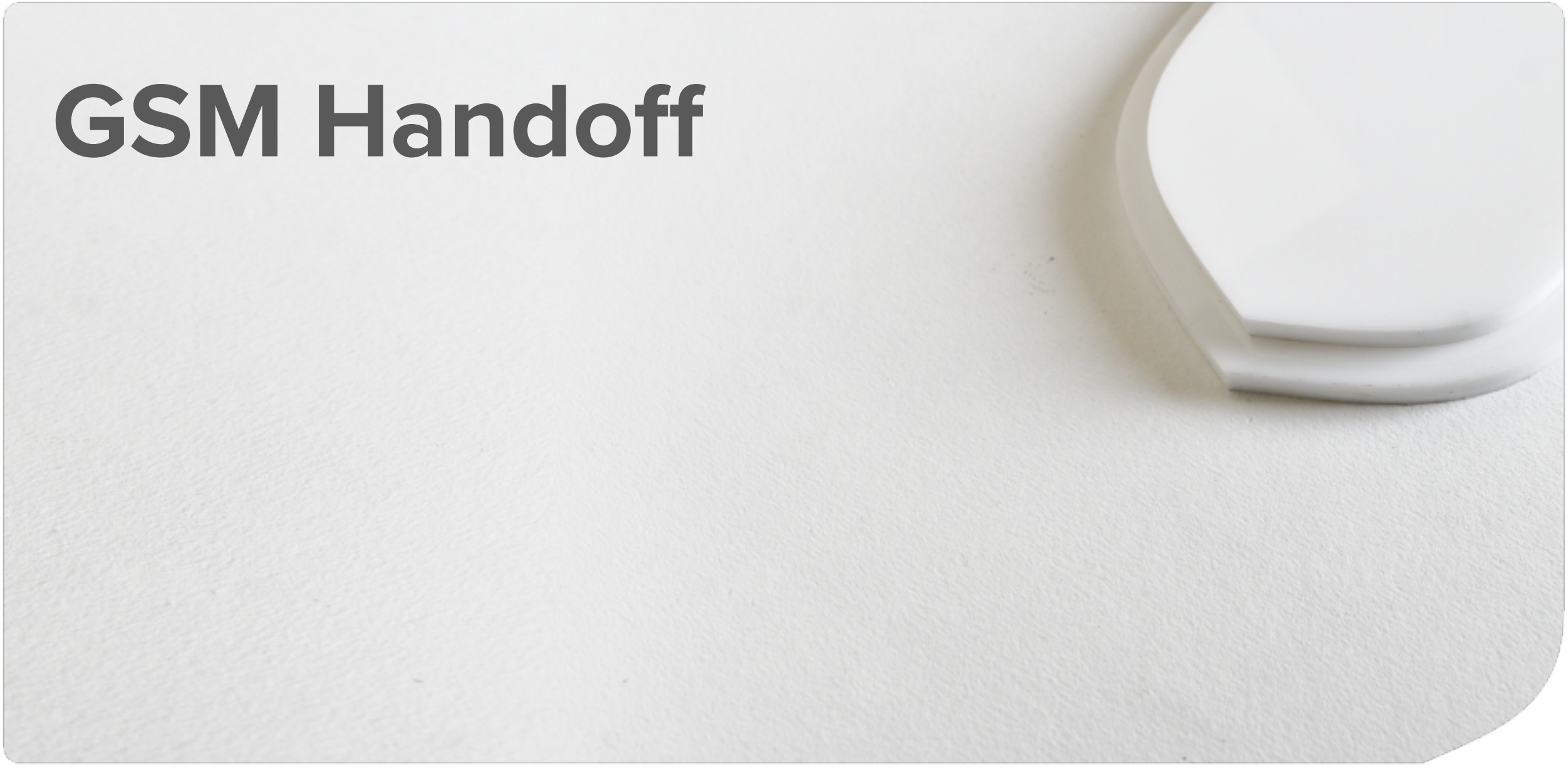


PLMN Interface

- PLMN: Public Land Mobile Network
- A basic configuration of a GSM network contains a central HLR and a central VLR, where
  - 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.
- Any data related to user call (connection establishment, teardown, etc.) processed with the SS7 protocol for signaling.
- For mobile specific signaling, a protocol stack called MAP (Mobile Application Part) used over the SS7 network which does all database transactions and handover/roaming transactions between the MSC.
- MSC uses registers known as SP – Signaling Point.
- SS7 is also widely used for signaling between wireless networks and the PSTN.
- In GSM networks, SS7 is also used for signaling between Base Station Controllers (BSC) and the Mobile Switching Center (MSC).

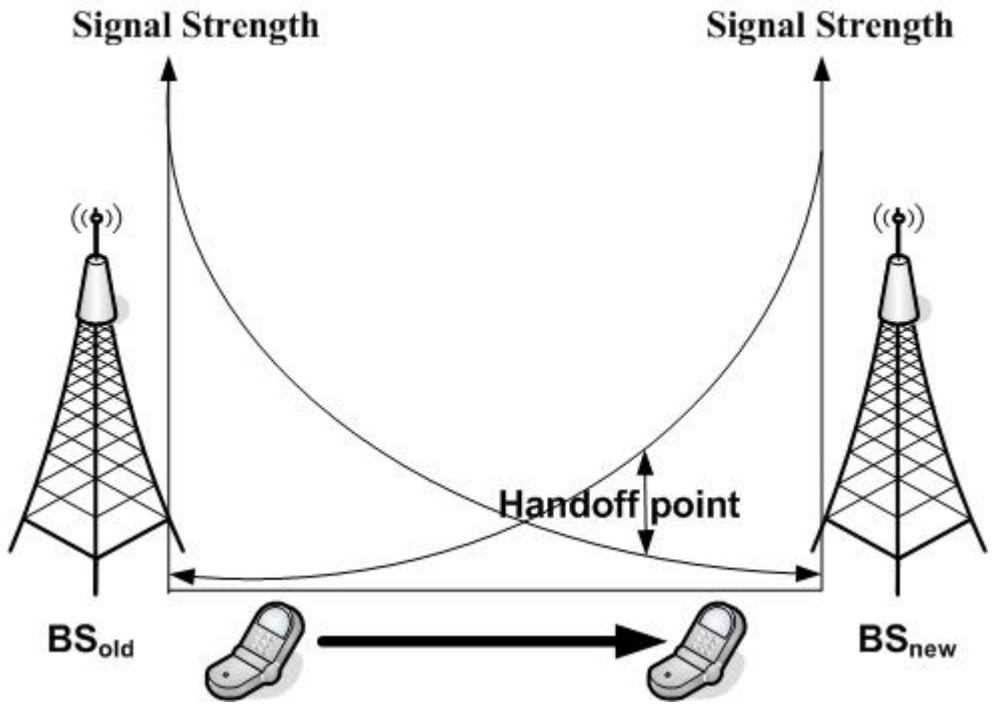
Marwadi University

GSM Handoff



Handoff

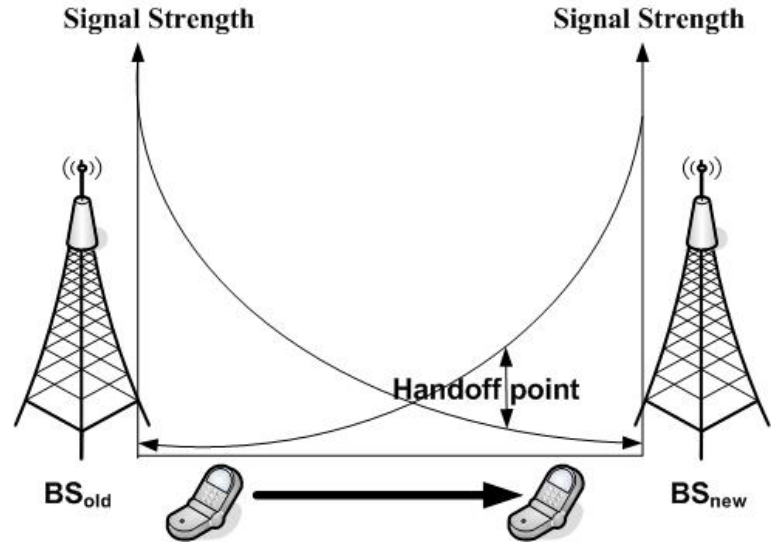
- In cellular communications, the terms **handover** or **handoff** refers to the process of transferring ongoing call or data connectivity from old Base Station to new Base Station.
- When a mobile moves into the different cell while the conversation is in progress then the MSC (Mobile Switching Centre) will transfer the call to a new channel belonging to the new Base Station.
- When a mobile user A moves from one cell to another cell then BTS 1 signal strength loses for the mobile User A and the signal strength of BTS 2 increases and thus ongoing calls or data connectivity for mobile user goes on without interrupting.



Handoff

Situations for triggering Handoff

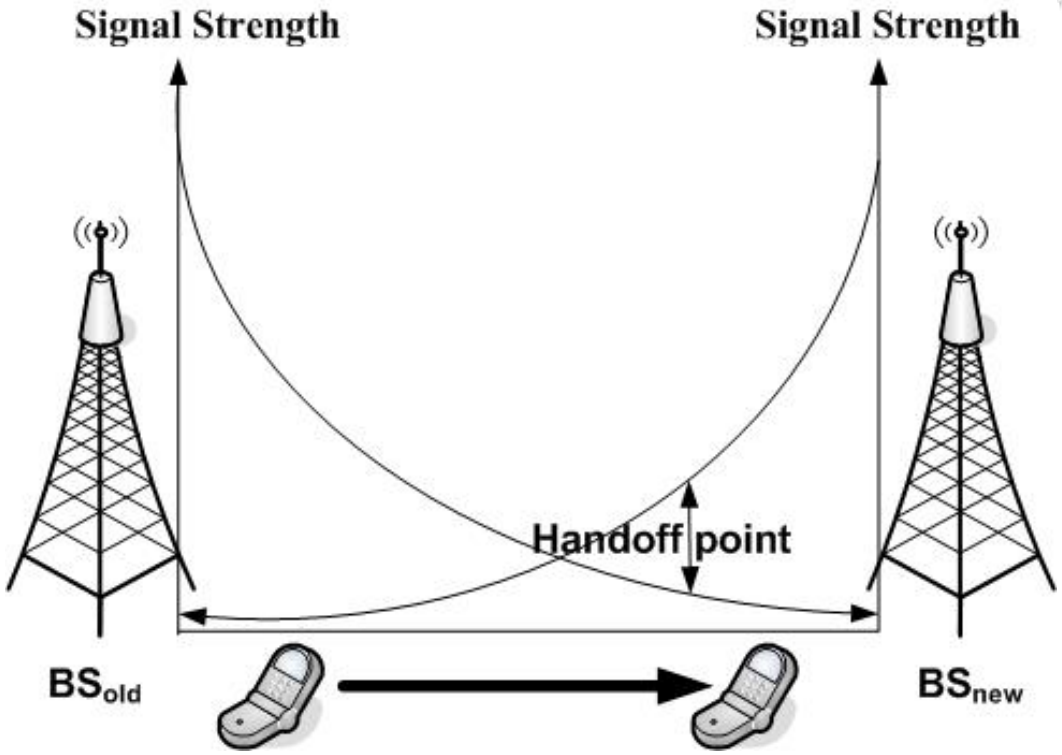
- Handoffs are triggered in any of the following situations –
- If a subscriber who is in a call or a data session moves out of coverage of one cell and enters coverage area of another cell, a handoff is triggered for a continuum of service. The tasks that were being performed by the first cell are delineating to the latter cell.
- Each cell has a pre-defined capacity, i.e. it can handle only a specific number of subscribers. If the number of users using a particular cell reaches its maximum capacity, then a handoff occurs. Some of the calls are transferred to adjoining cells, provided that the subscriber is in the overlapping coverage area of both the cells.
- Cells are often sub-divided into microcells. A handoff may occur when there is a transfer of duties from the large cell to the smaller cell and vice versa. For example, there is a traveling user moving within the jurisdiction of a large cell. If the traveler stops, then the jurisdiction is transferred to a microcell to relieve the load on the large cell.
- Handoffs may also occur when there is an interference of calls using the same frequency for communication.



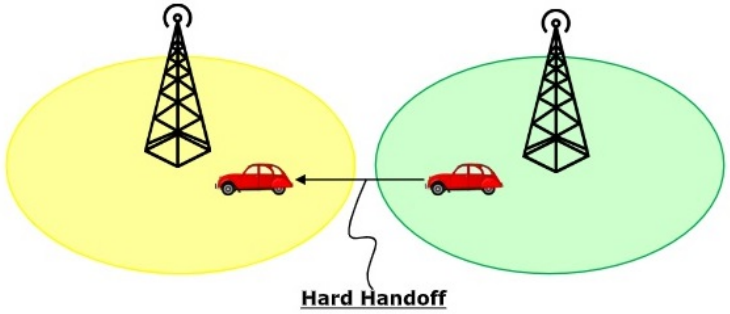
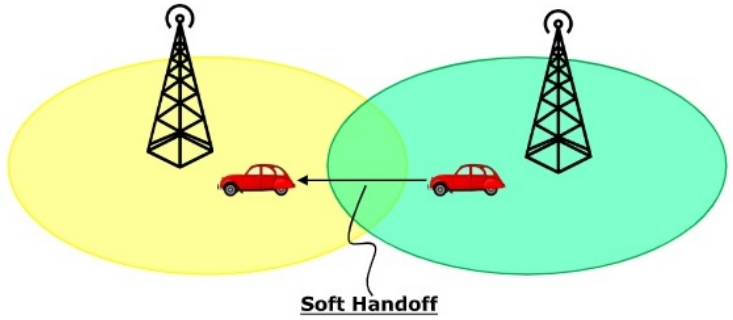
Why Handoff?

Two Reasons

- When The Radio Signal's quality and power decreases to necessary scores, the connection deliver to more powerful cell.
- When the Traffic Capacity approaches to maximum, the connection deliver to less density of traffic cell.

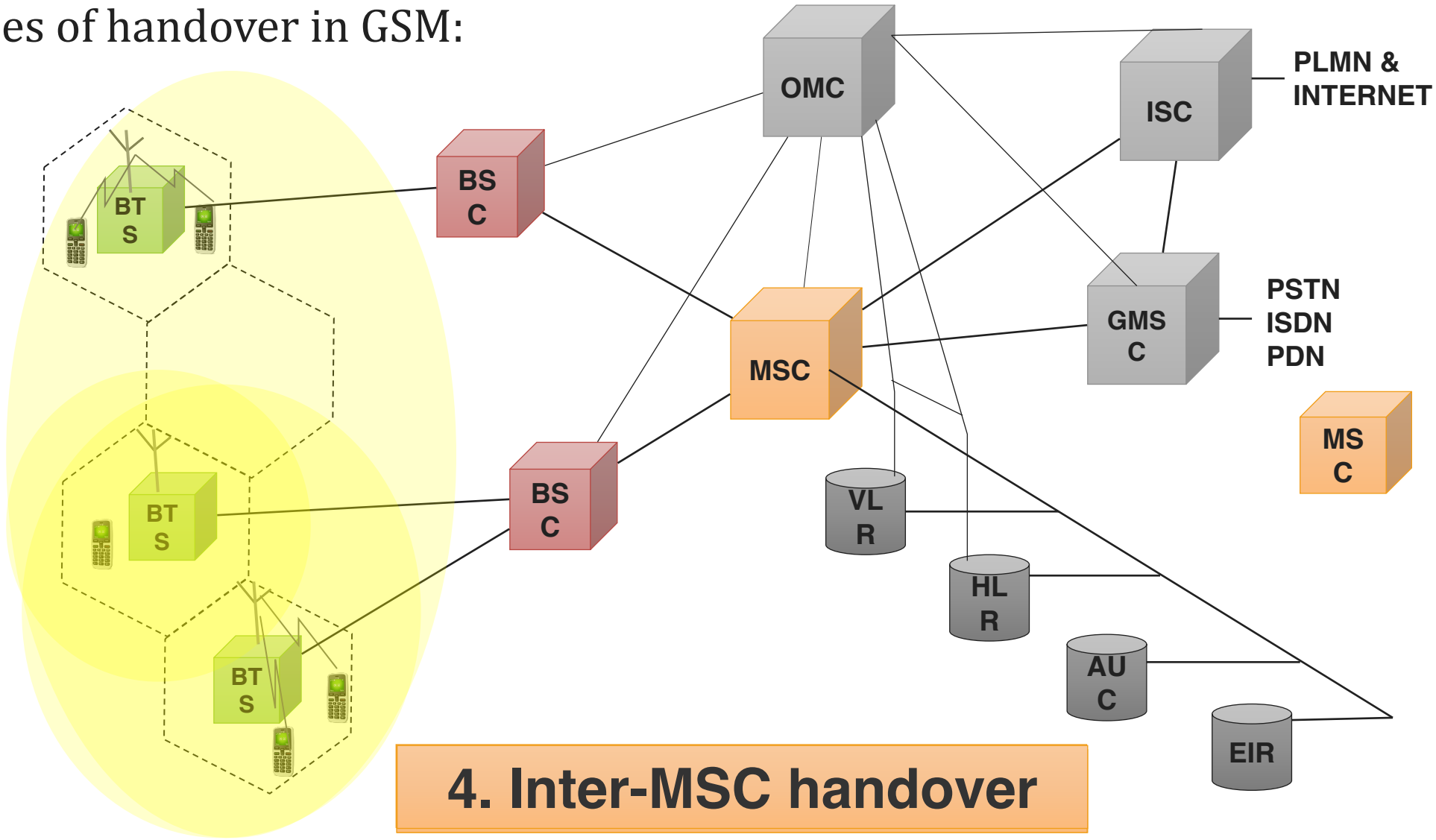


Handoff Types: Soft Handoff vs Hard Handoff

Hard Handoff	Soft Handoff
	
Break in the connection occurs while switching from one cell to another.	Break in the connection will not occur due to overlapping cells.
The radio links from the mobile station to the existing cell is broken before establishing a link with the next cell.	In soft handoff, at least one of the links is kept when radio links are added and removed to the mobile station.
It is a **"break before make"** policy.	It is a **"make before break"** policy.

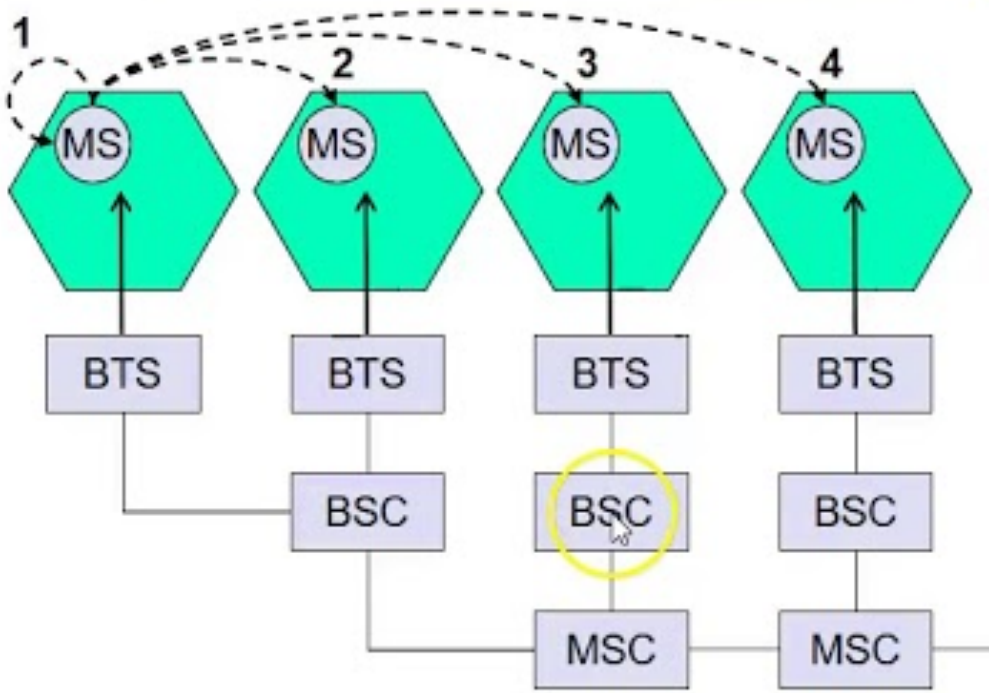
Types of Handover/Handoff

- Four types of handover in GSM:



4. Inter-MSC handover

Handoff Types



1. Intra-cell handover
2. Inter-cell, intra-BSC handover
3. Inter-BSC, intra-MSC handover
4. Inter MSC handover

Marwadi University

Network Aspect in GSM

Network Aspect in GSM: Signaling Protocol Structure

Marwadi University

Transmission of voice and data over the radio link is only a part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally.

This requires that registration, authentication, call routing and location updating functions are standardized across GSM networks. The geographical area covered by a network is divided into cells of small radius.
When a call is in progress and the user is on the move, there will be a handover mechanism from one cell to another. This is like a relay race where one athlete passes on the baton to another.

Though both roaming and handover functions are the basic characteristic of mobility, there is a difference between these functions.

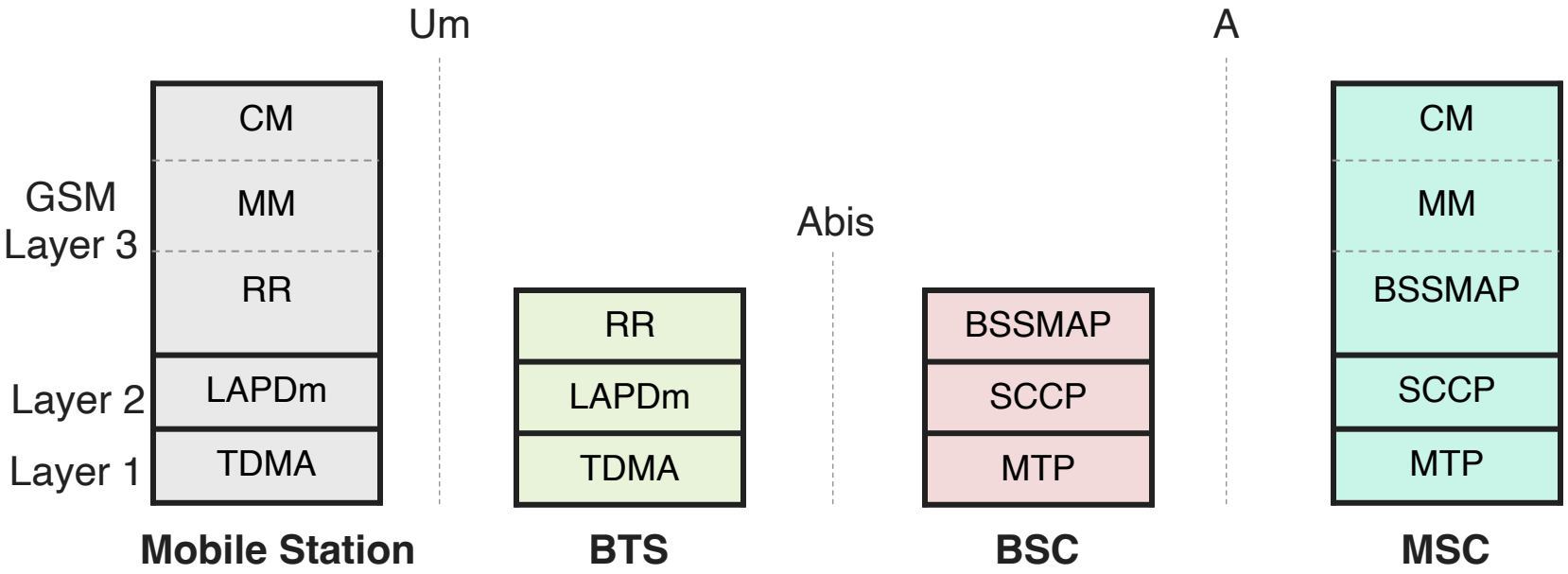
These functions are performed by the Network Subsystem, mainly using the **Mobile Application Part (MAP) built on top of the Signalling System # 7 (SS7)**

Network Aspect in GSM: Signaling Protocol Structure

Marwadi University

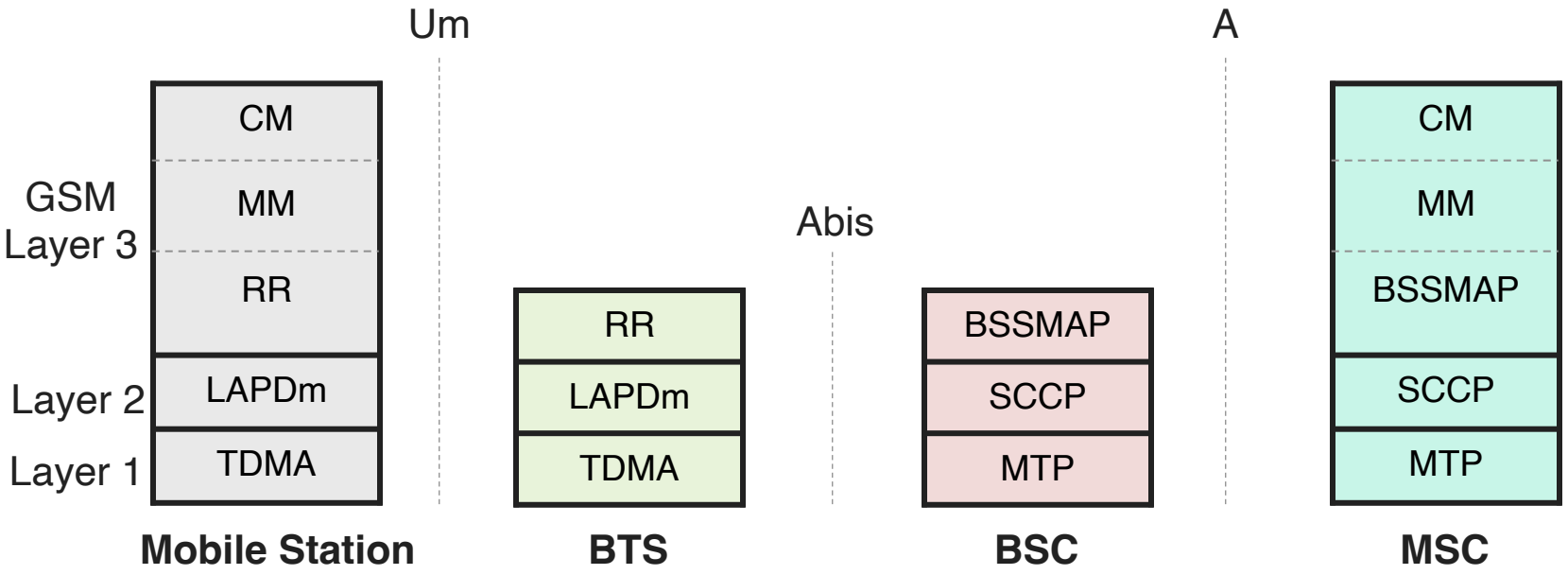
Network Aspect in GSM: Signaling Protocol Structure

- 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.



Network Aspect in GSM: Signaling Protocol Structure

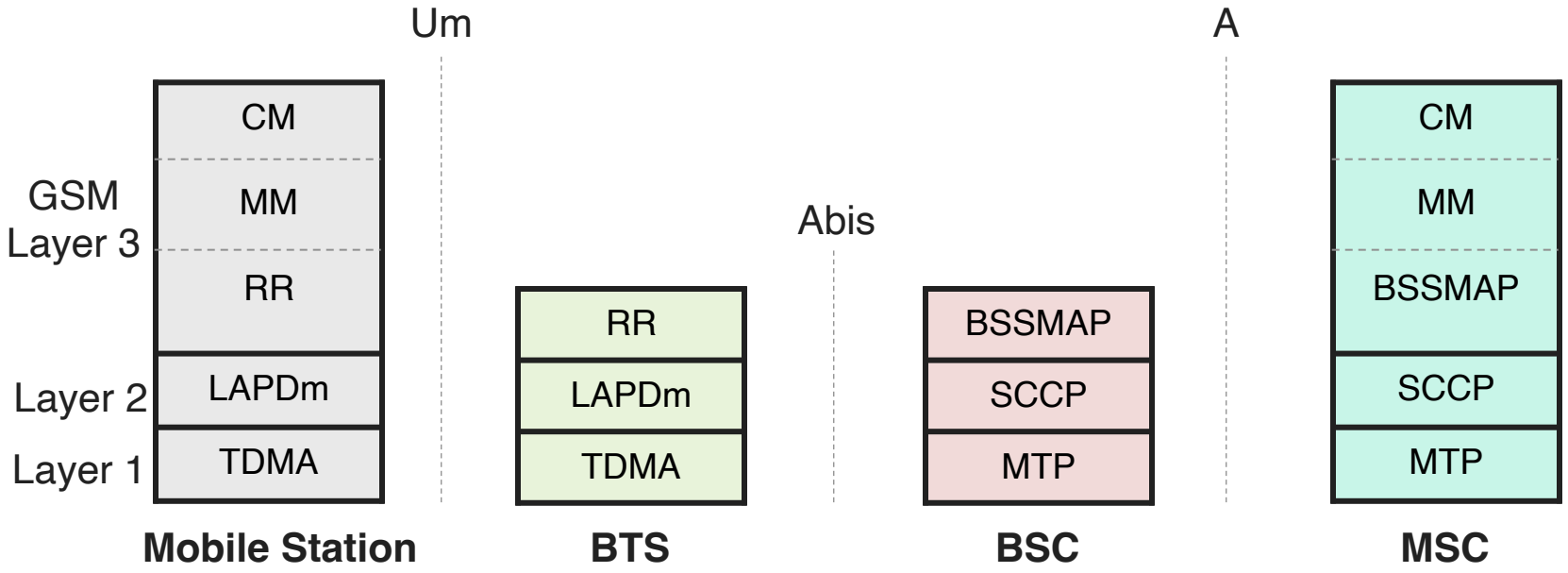
- GSM signalling protocol is categorized into three general layers:
- **Layer 1** - physical layer: It uses the channel structures over the air interface.
- **Layer 2** - The data-link layer: Across the Um interface, the data-link layer is a modified version of the Link access protocol for the D channel (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.



Network Aspect in GSM: Signaling Protocol Structure

The GSM signalling protocol is categorized into three general layers:

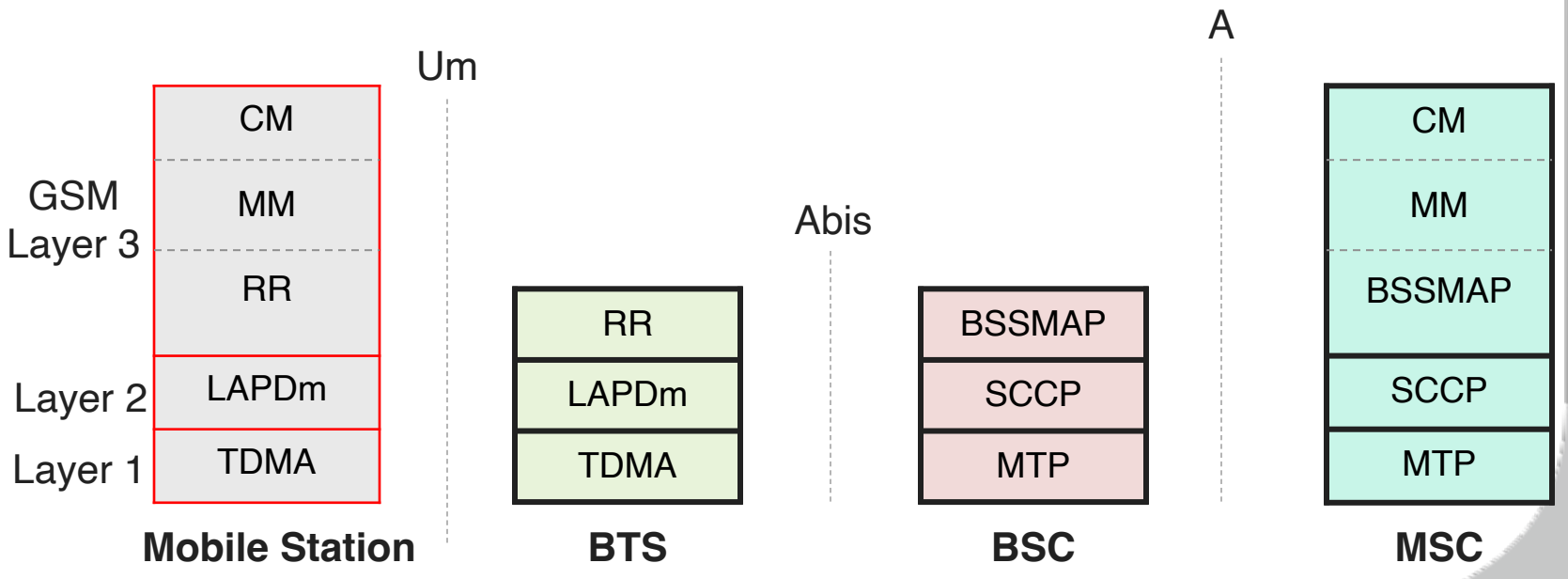
- **Layer 3** : GSM signalling protocol's third layer is divided into three sublayers:
  1. **Radio Resource Management (RR):** It controls the set-up, maintenance, and termination of radio channels, including handovers.
  2. **Mobility Management (MM):**It manages the location updating and registration procedures as well as security and authentication.
  3. **Connection Management (CM):** It handles general call control and manages Supplementary Services and the Short Message Service(SMS).



Network Aspect in GSM: Signaling Protocol Structure

MS to BTS Protocols

1. **RR layer :**
   - Manages a link, both radio and fixed, between the MS and the MSC
   - Manages the RR-session, the time when a mobile is in a dedicated mode, and the radio channels including the allocation of dedicated channels.
2. **MM layer:** Stacked above the RR layer
   - Handles the functions that arise from the mobility of the subscriber
   - Authentication and security aspects
   - Location management



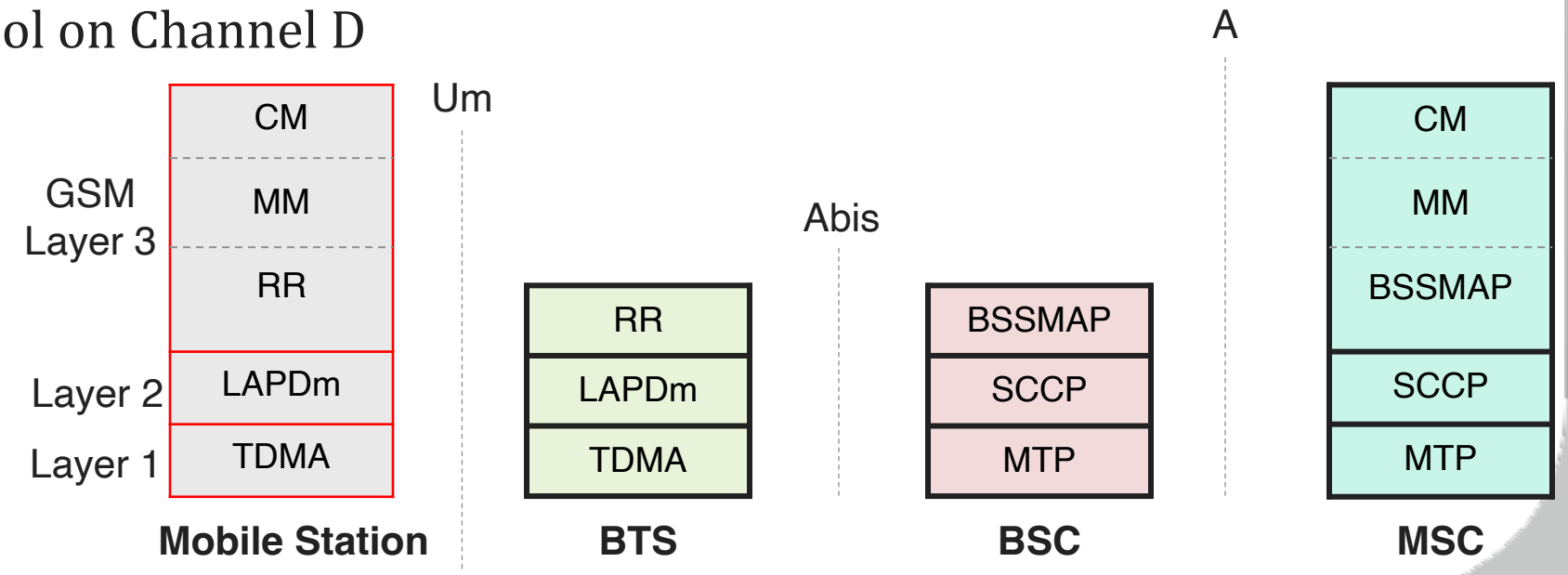
Network Aspect in GSM: Signaling Protocol Structure

Marwadi University

MS Protocols

3. **CM Layer:** Call Management(CM) is topmost layer of the GSM protocol stack
   - ➥ Responsible for Call Control, Supplementary Service Management, and Short Message Service Management.
   - ➥ Handles call establishment, selection of the type of service (including alternating between services during a call), and call release.

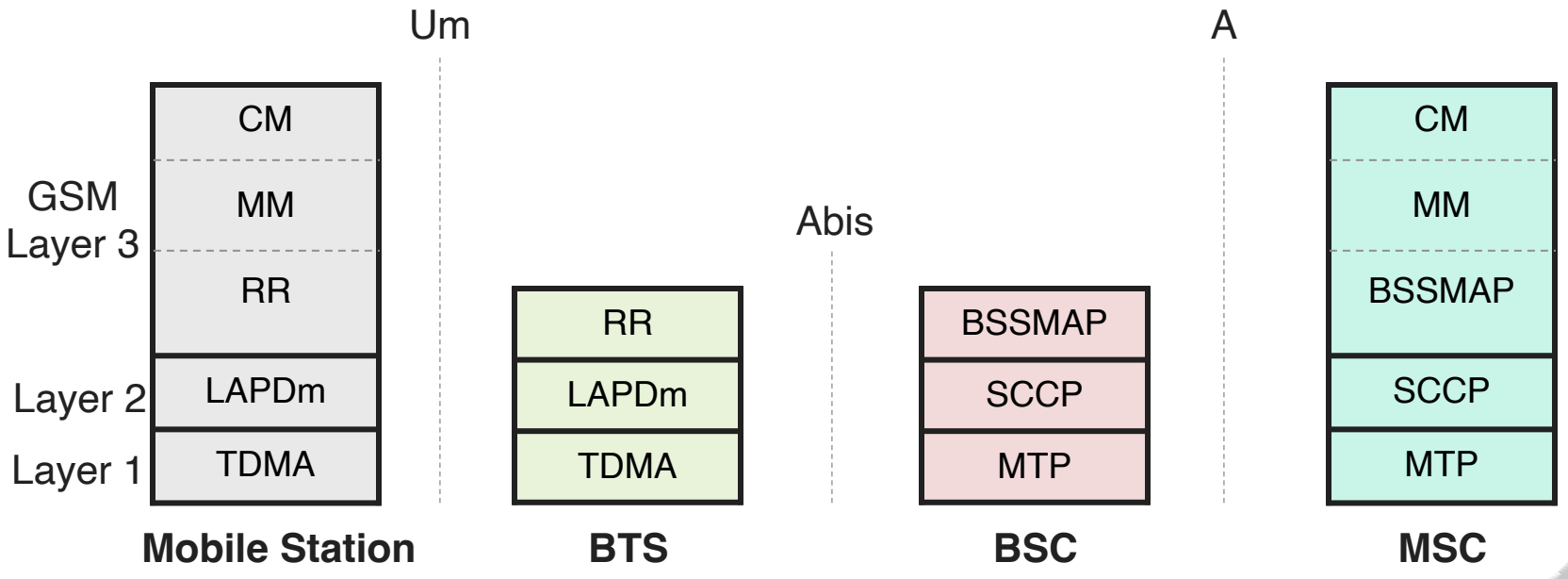
4. **LAPDm:** Link Access Protocol on Channel D
   - ➥ LAPDm is a data link layer **protocol** used in GSM cellular networks.
   - ➥ It is used in the radio link between the cellular network and the subscriber handset.



Network Aspect in GSM: Signaling Protocol Structure

Um interface

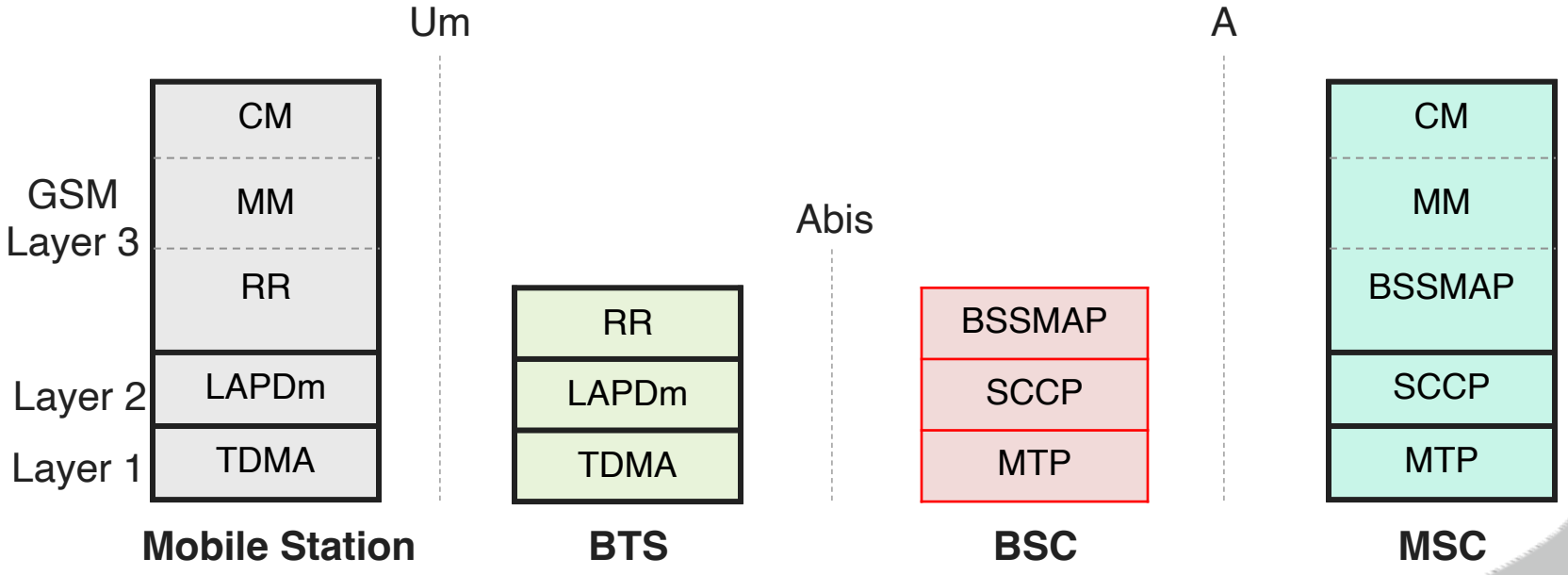
- The Um interface is the air interface of the GSM mobile telephone standard.
- It is the interface between the mobile station (MS) and the Base transceiver station (BTS).
- It is known as Um because it is the mobile analog to the U interface of ISDN.
- Um can also support GPRS packet-oriented communication.



Network Aspect in GSM: Signaling Protocol Structure

BSC Protocols: Uses a different set of protocols after receiving the data from BTS.

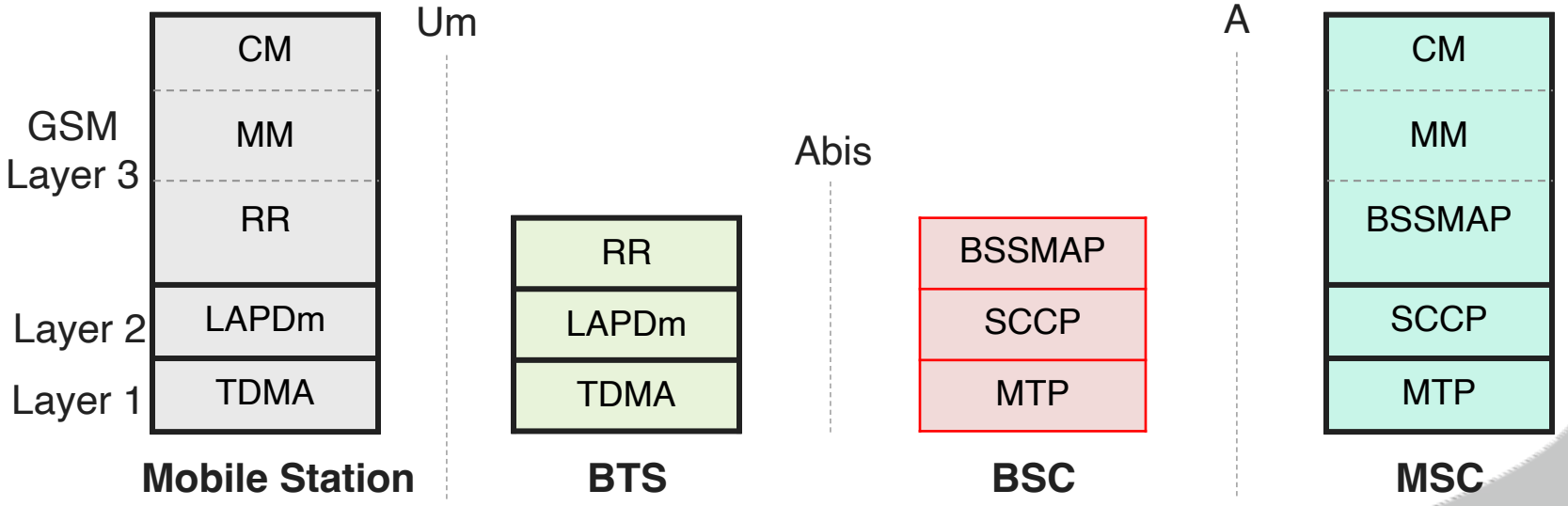
- **Abis interface**: Used between the BTS and BSC.
  - Allows control of the radio equipment and radio frequency allocation in the BTS.
- **BSSMAP:** Base Station System Management Application Part
  - Designed for signalling over the A interface
  - Supports both connectionless and connection-oriented services provided by the SCCP
  - Supports message transfer between the MSC and the MS



Network Aspect in GSM: Signaling Protocol Structure

BSC Protocols: Uses a different set of protocols after receiving the data from BTS.

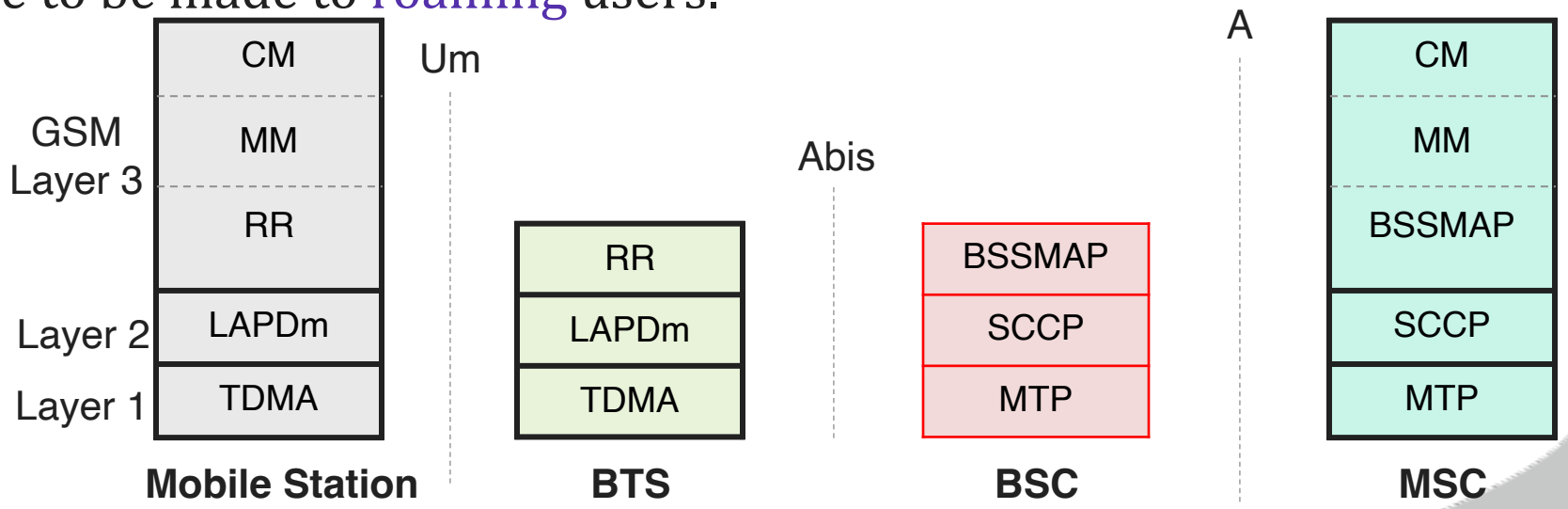
- **SCCP:** Signalling Connection Control Part (SSCP) is a network layer protocol
  - Provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities in Signaling System 7 (SS7) telecommunications networks.
  - SCCP relies on the services of MTP for basic routing and error detection.
- **MTP**: Message Transfer Part
  - Part of the Signalling System 7 (SS7) used for communication in Public Switched Telephone Networks (PSTN).
  - MTP is responsible for reliable, unduplicated and in-sequence transport of SS7 messages between communication partners.



Network Aspect in GSM: Signaling Protocol Structure

MSC Protocols

- **A interface:**
  - Used to provide communication between the BSC and the MSC.
  - The interface carries information to enable the channels, timeslots and the like to be allocated to the mobile equipment's being serviced by the BSSs.
- At the MSC, starting from the BSC, the information is mapped across the A interface to the MTP Layers 1 through 3.
- 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.



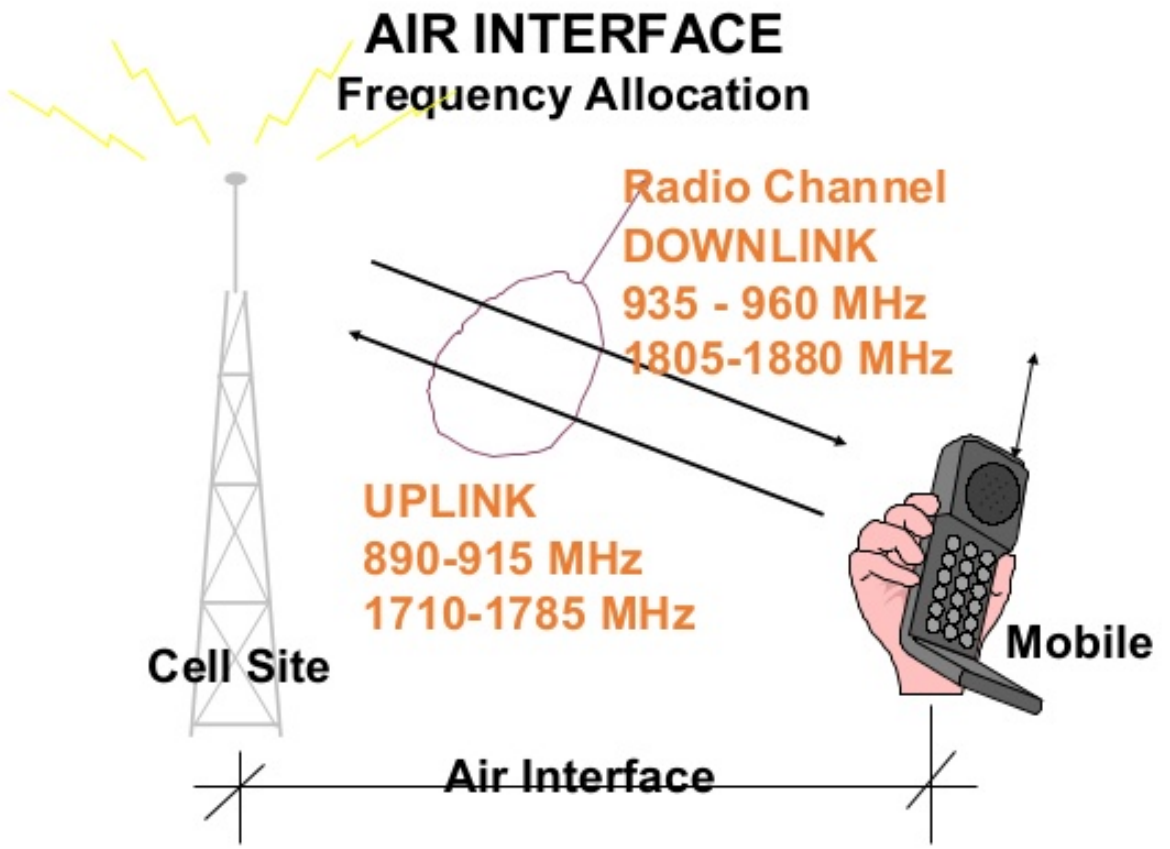
Marwadi University

GSM Frequency Allocation

GSM Frequency Allocation

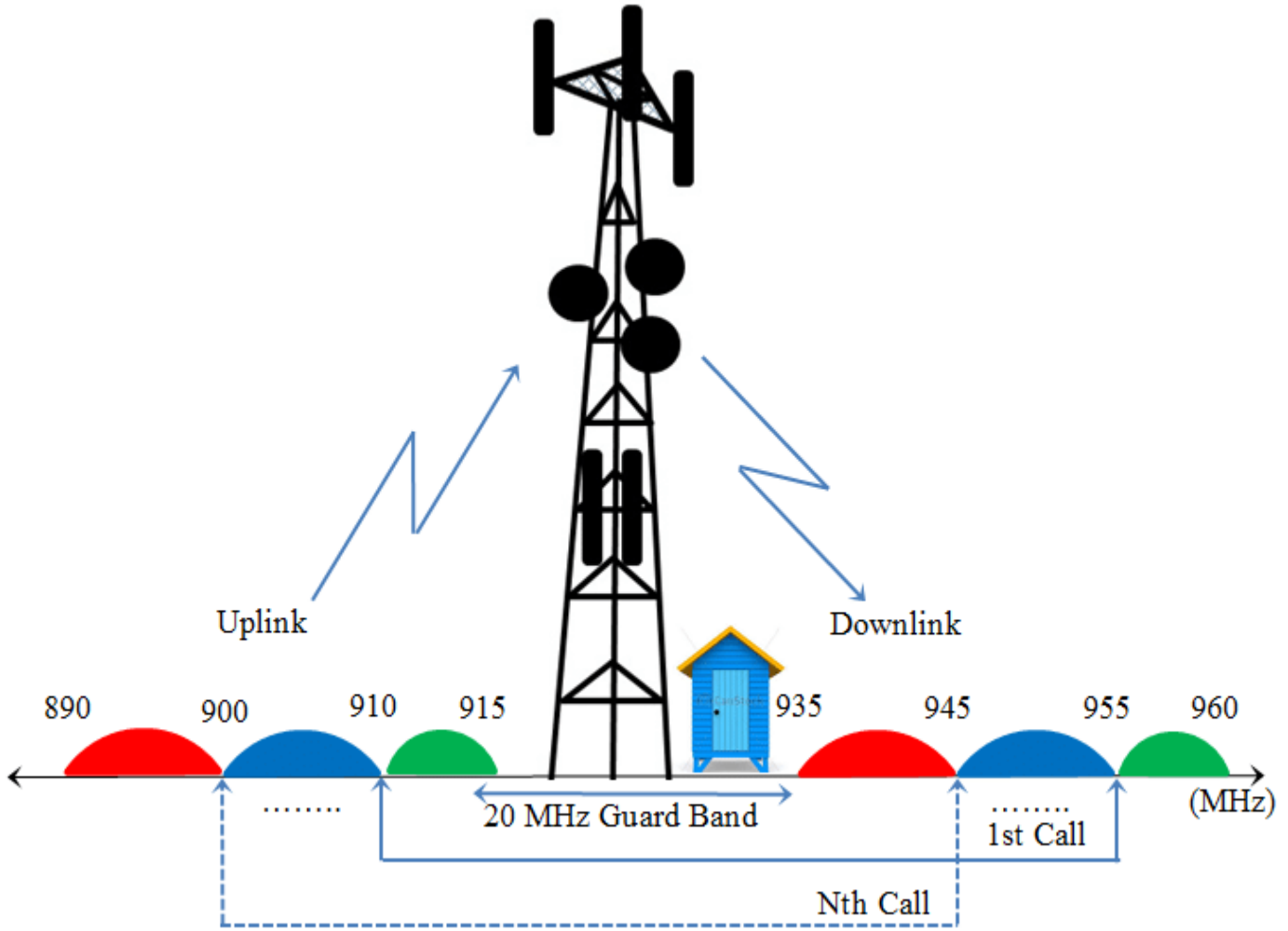
- Uplink: is a frequency transmission that links mobile handset to base station
- Downlink: is a frequency transmission that links base station to mobile handset
- There are 4 major GSM frequency bands
  1. 850 MHz
  2. 900 MHz
  3. 1800 MHz
  4. 1900 MHz
- Allocation of band

Country	Frequency Band
United States	850 MHz and 1900 MHz
Rest of the world (Europe, Middle East, Africa, Asia)	900 MHz and 1800 MHz



GSM Bands in India

- Each way the bandwidth for the GSM system is 25 MHz which provides 125 carriers uplink/ downlink each having a bandwidth of 200 kHz.
- For Uplink: 900 MHz of frequency is allocated.
  - **Range**: 890-915 MHz
- For Downlink: 900 MHz of frequency is allocated.
  - **Range**: 935-960 MHz



Authentication and Security

- Authentication involves two functional entities:
  1. SIM card in the mobile phone
  2. Authentication Center (AUC)
- For authentication; different algorithms used:
  1. MS algorithm A3
  2. Voice Privacy key algorithm A8
  3. Strong over-the-air voice privacy algorithm A5
- It used for ciphering and deciphering procedure for signaling, voice, and data.
- So, signal, voice, data, and SMS within GSM networks ciphered over the wireless radio interface.

Marwadi University

01CE0701 – Mobile Computing

Unit - 3 Telecommunication System (Part 2 – GPRS)

Prof. Chirag Bhalodia
Computer Engineering Department

Outline

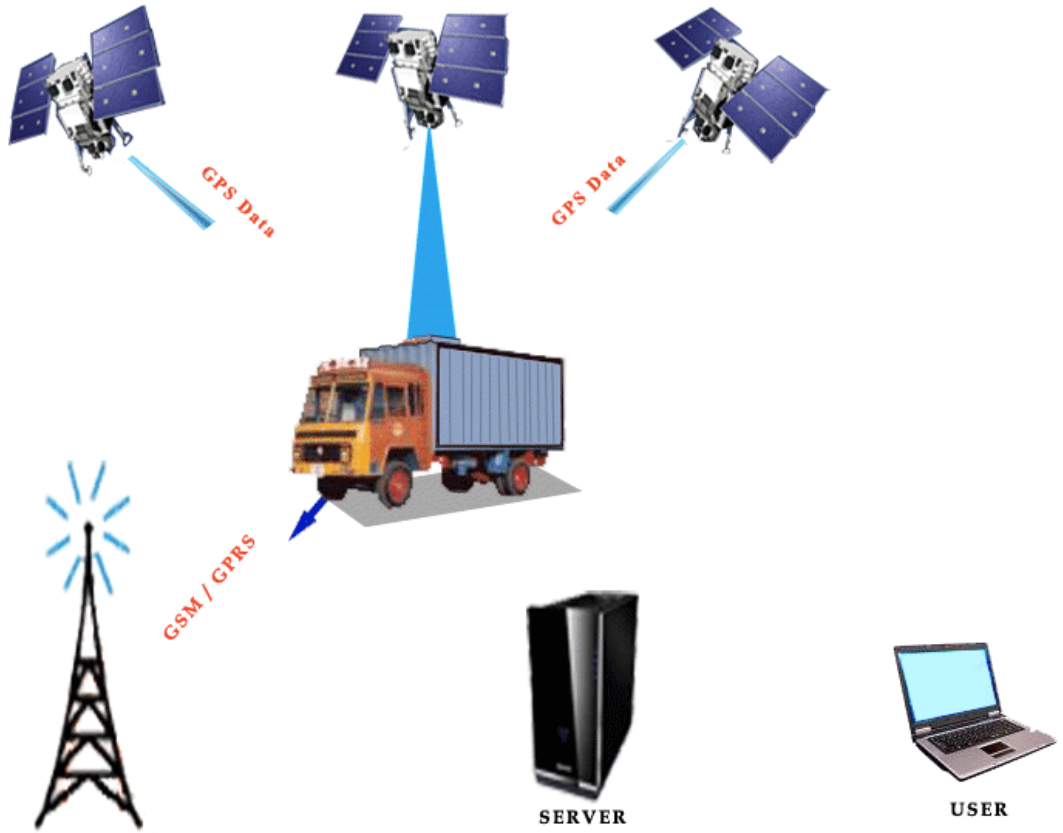
- **GPRS**
  - GPRS Architecture
  - Data services
  - Applications
  - Billing and charging

General Packet Radio Service - GPRS

- GPRS stands for General Packet Radio Service
- GPRS defined as an efficient transport high-speed data over the current GSM and TDMA-based wireless network infrastructures.
- GPRS was built up by European Telecommunications Standards Institute (ETSI).
- GPRS is also known as a third-generation step toward internet access.
- It is basically a packet-oriented mobile data standard on the 2G and 3G cellular communication.
- Used for mobile internet, MMS and other data communications.

General Packet Radio Service - GPRS

- Value added service to 2G to connect users to IP (Internet Protocol) -based data networks.
- GPRS offers for data speeds of 14.4 Kbps to 171.2 Kbps, which allow for Internet access.
- For example, e-mail and web browsing
- It is not the replacement of GSM but an extension of it.



GPRS Key Features

Marwadi University

There are 3 key features as follows:

1. **The always online feature** - Removes the dial-up process, making applications only one click away.
2. **An upgrade to existing systems** - Operators do not have to replace their equipment; rather, GPRS is added on top of the existing infrastructure.
3. **An integral part of future 3G systems** - GPRS is the packet data core network for 3G systems EDGE and WCDMA.

GPRS Characteristics

GPRS Characteristics

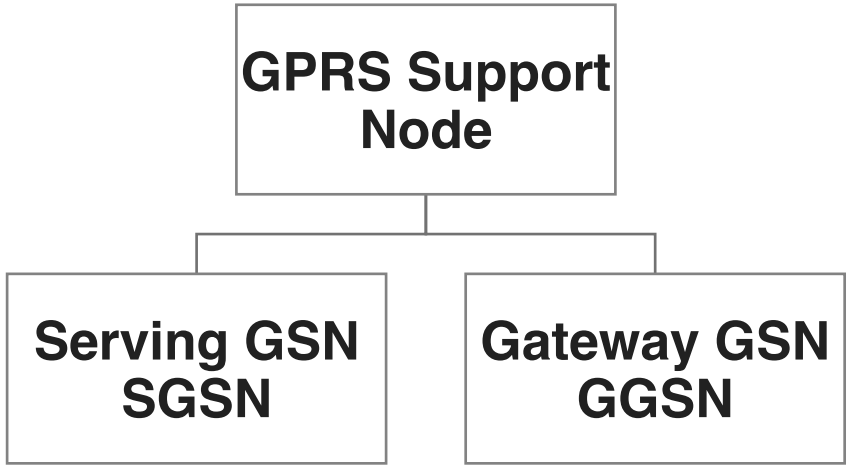
- Resource allocation
  - resources allocated only when data is to be sent/received
- Flexible channel allocation
  - one to eight time slots
  - available resources shared by active users
  - up and down link channels reserved separately
- Traffic characteristics suitable for GPRS
  - Intermittent, burst data transmissions
  - Frequent transmissions of small volumes of data
  - Infrequent transmission of larger volumes of data

Marwadi University

GPRS Architecture

GPRS Network Architecture

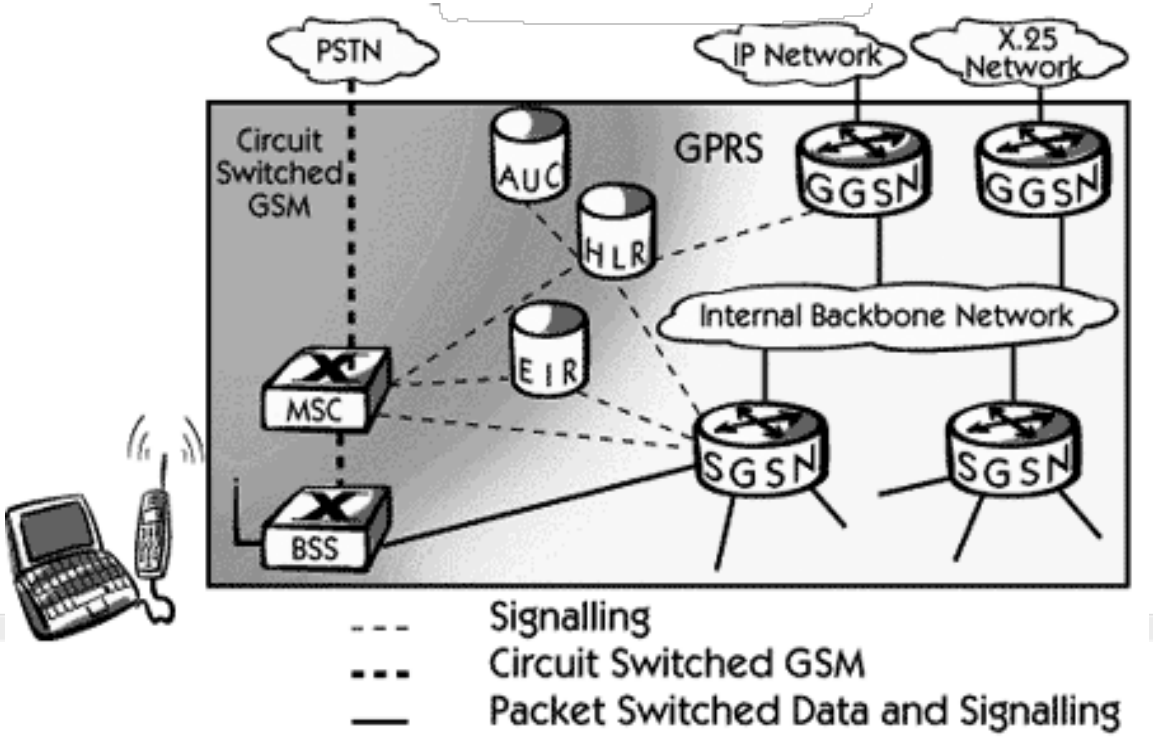
- GPRS uses the GSM architecture for voice.
- To offer packet data services through GPRS, a new class of network nodes called GPRS support nodes (GSN).
- GSNs are responsible for the delivery and routing of data packets between the mobile stations and the external packet data networks (PDN).



GPRS Network Architecture

GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission.

This data network overlaps a second-generation GSM network providing packet data transport at the rates from 9.6 to 171 kbps. Along with the packet data transport the GSM network accommodates multiple users to share the same air interface resources concurrently.



GPRS Network Architecture

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GPRS Network Architecture

GPRS attempts to reuse the existing GSM network elements as much as possible, but to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.

Therefore, GPRS requires modifications to numerous GSM network elements as summarized below:

GPRS Network Architecture

GSM Network Element	Modification or Upgrade Required for GPRS.
Mobile Station (MS)	New Mobile Station is required to access GPRS services. These new terminals will be backward compatible with GSM for voice calls.
BTS	A software upgrade is required in the existing Base Transceiver Station(BTS).
BSC	The Base Station Controller (BSC) requires a software upgrade and the installation of new hardware called the packet control unit (PCU). The PCU directs the data traffic to the GPRS network and can be a separate hardware element associated with the BSC.
GPRS Support Nodes (GSNs)	The deployment of GPRS requires the installation of new core network elements called the serving GPRS support node (SGSN) and gateway GPRS support node (GGSN).
Databases (HLR, VLR, etc.)	All the databases involved in the network will require software upgrades to handle the new call models and functions introduced by GPRS.

GPRS Network Architecture

Marwadi University

GPRS Mobile Stations

New Mobile Stations (MS) are required to use GPRS services because existing GSM phones do not handle the enhanced air interface or packet data.

A variety of MS can exist, including a high-speed version of current phones to support high-speed data access, a new PDA device with an embedded GSM phone, and PC cards for laptop computers.

These mobile stations are backward compatible for making voice calls using GSM.

GPRS Network Architecture

Marwadi University

GPRS Base Station Subsystem

Each BSC requires the installation of one or more Packet Control Units (PCUs) and a software upgrade. The PCU provides a physical and logical data interface to the Base Station Subsystem (BSS) for packet data traffic. The BTS can also require a software upgrade but typically does not require hardware enhancements.

When either voice or data traffic is originated at the subscriber mobile, it is transported over the air interface to the BTS, and from the BTS to the BSC in the same way as a standard GSM call.

However, at the output of the BSC, the traffic is separated; voice is sent to the Mobile Switching Center (MSC) per standard GSM, and data is sent to a new device called the SGSN via the PCU over a Frame Relay interface.

GPRS Network Architecture

Marwadi University

GPRS Support Nodes

Following two new components, called Gateway GPRS Support Nodes (GSNs) and, Serving GPRS Support Node (SGSN) are added:

Gateway GPRS Support Node (GGSN)

The Gateway GPRS Support Node acts as an interface and a router to external networks. It contains routing information for GPRS mobiles, which is used to tunnel packets through the IP based internal backbone to the correct Serving GPRS Support Node.

The GGSN also collects charging information connected to the use of the external data networks and can act as a packet filter for incoming traffic.

Serving GPRS Support Node (SGSN)

The Serving GPRS Support Node is responsible for authentication of GPRS mobiles, registration of mobiles in the network, mobility management, and collecting information on charging for the use of the air interface.

.

GPRS Network Architecture

Marwadi University

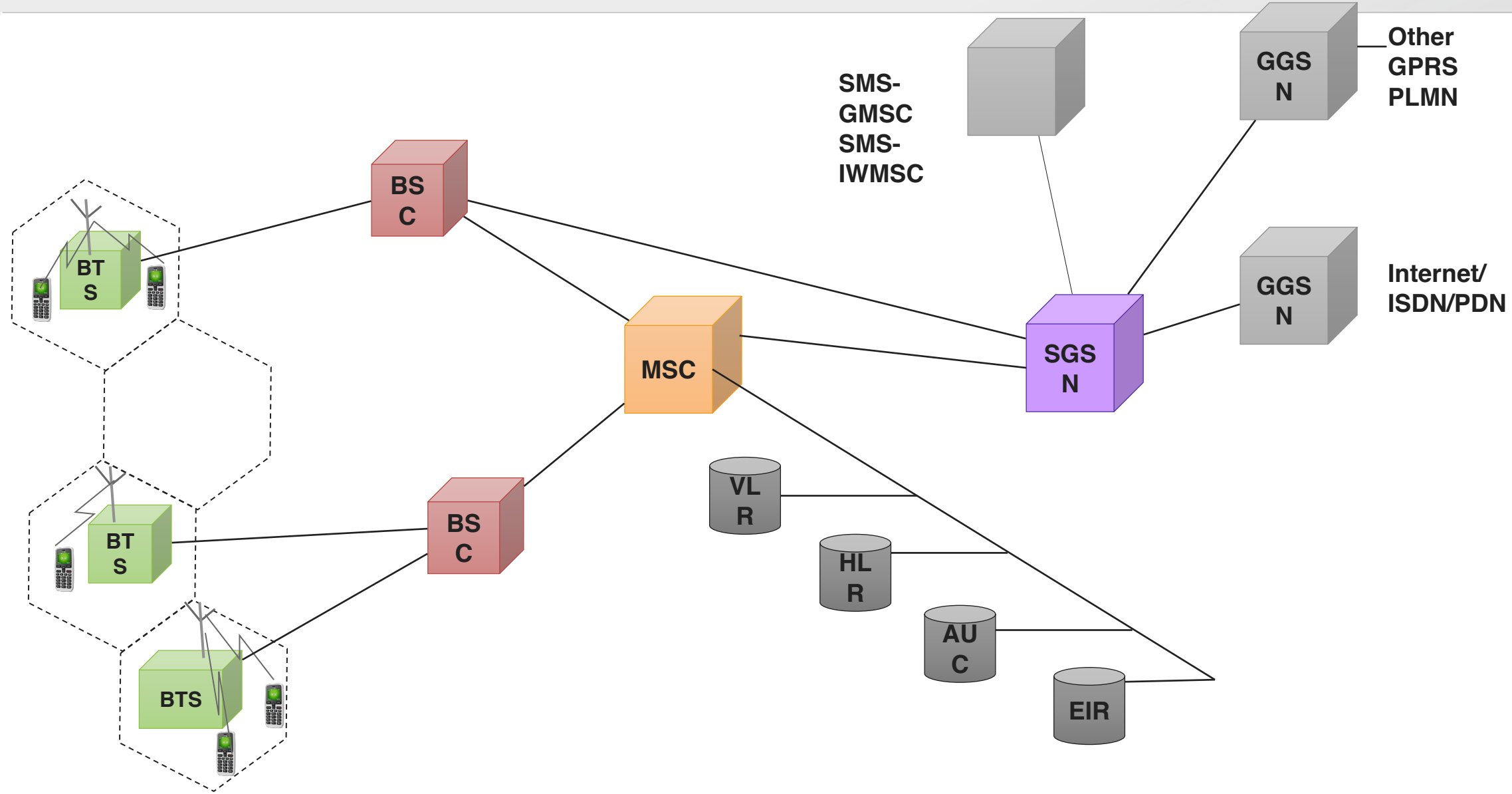
Internal Backbone

The internal backbone is an IP based network used to carry packets between different GSNs. Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network. Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

Routing Area

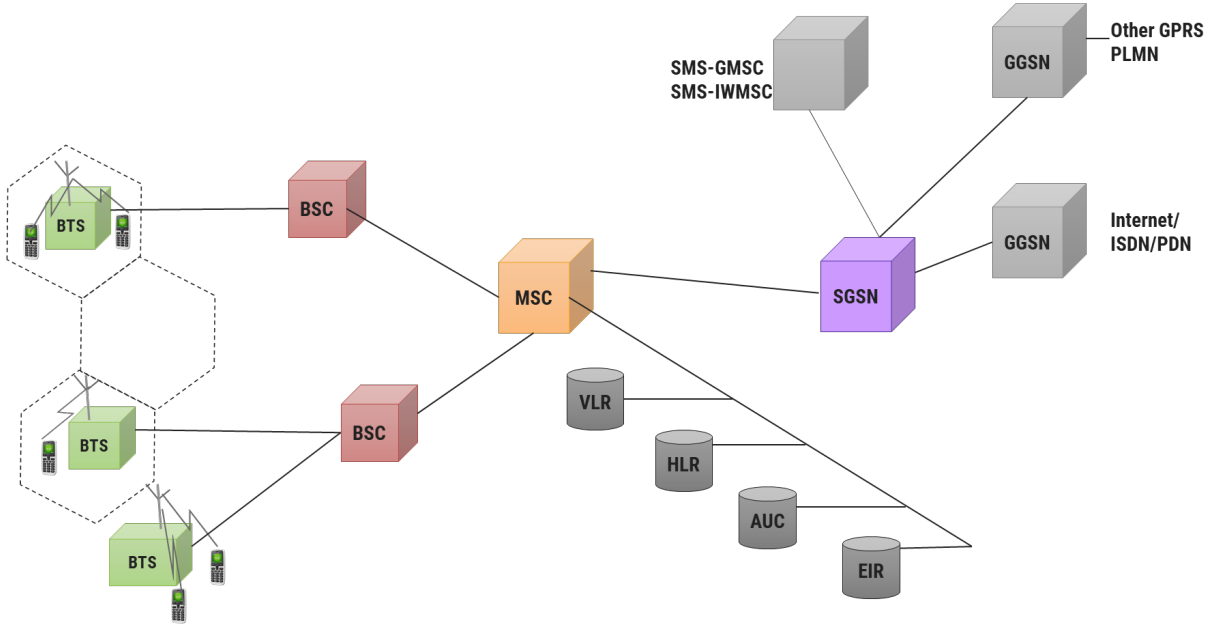
GPRS introduces the concept of a Routing Area. This concept is similar to Location Area in GSM, except that it generally contains fewer cells. Because routing areas are smaller than location areas, less radio resources are used While broadcasting a page message.

GPRS Architecture-In Details



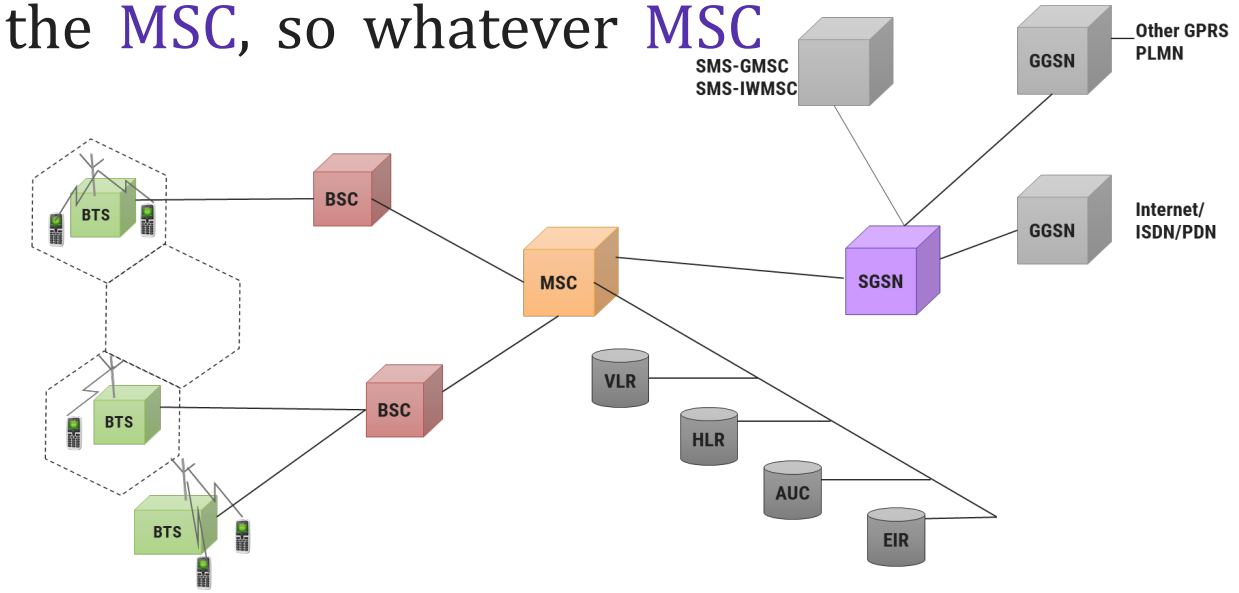
GPRS Architecture

- GPRS architecture works on the same procedure like GSM network, but, has additional entities that allow packet data transmission.
- Together with the packet data transport the GSM network accommodates multiple users to share the same resources simultaneously.
- GPRS reuse the existing GSM network.
- Moreover, to effectively build a packet-based mobile cellular network, some new network elements, interfaces, and protocols for handling packet traffic are required.



GPRS Architecture: SGSN

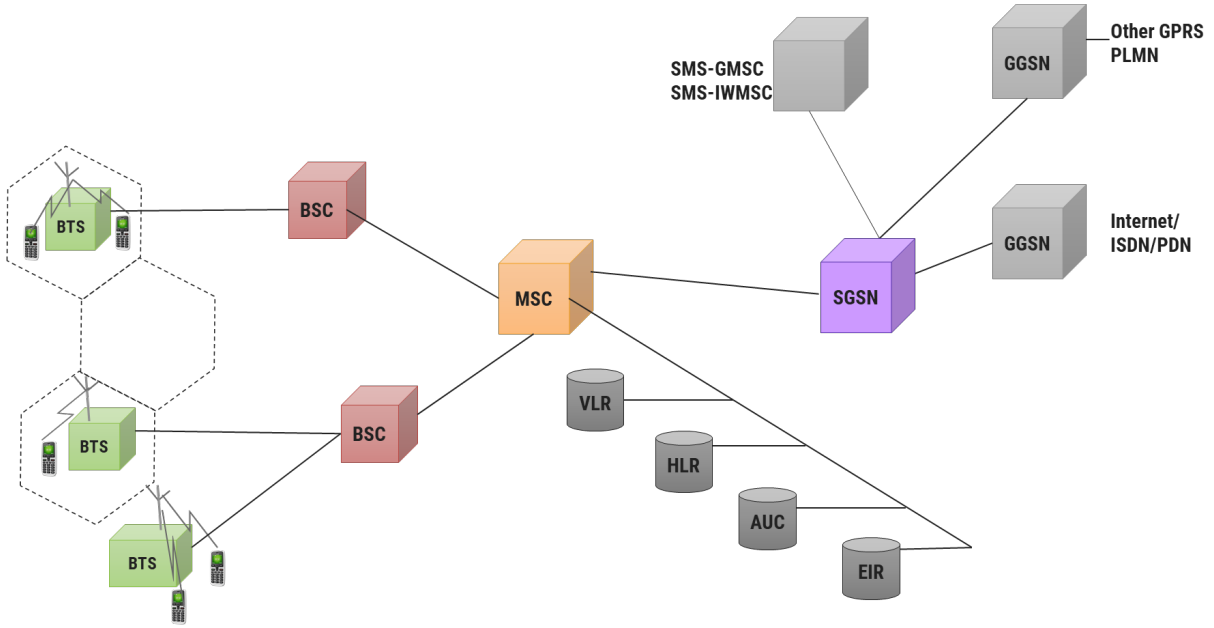
- Serving GPRS Support Node
- SGSN is at the same hierarchical level as the MSC, so whatever MSC does for voice, SGSN does for packet data.
- SGSN's tasks includes:
  - Packet switching
  - Routing and transfer
  - Mobility management
  - Logical link management
  - Authentication and Charging functions



- SGSN processes the registration of new mobile subscribers and keeps a record of their location within a given service area.
- Location register of the SGSN stores location information (like a current cell, current VLR, etc.) and user profiles of all GPRS users registered with this SGSN.
- SGSN sends queries to HLR to obtain profile data of GPRS subscribers.

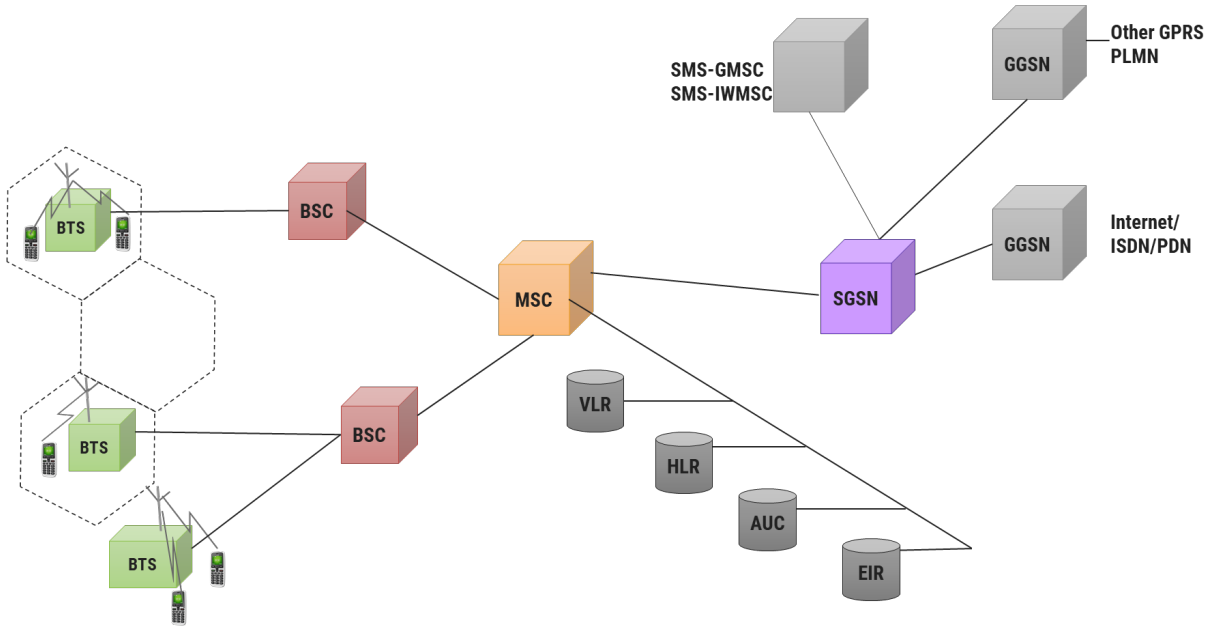
GPRS Architecture: GGSN

- Gateway GPRS Support Node
- GGSN acts as an interface between the GPRS backbone network and the external packet data networks.
- GGSN's functions are similar to the router in a Network.
- GGSN maintains routing information that is necessary to tunnel the Protocol Data Units (PDUs) to the SGSNs that service particular mobile stations.



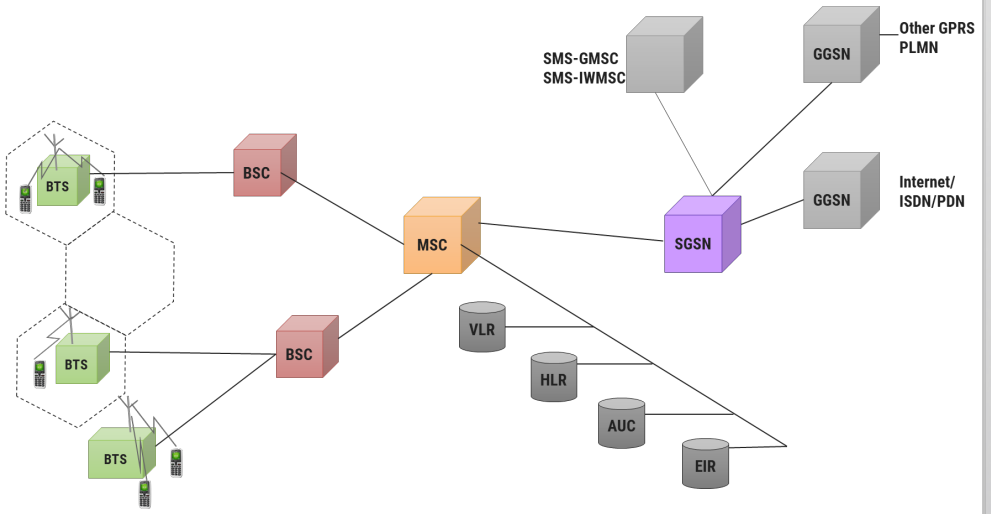
GPRS Architecture: GGSN

- GGSNs converts the GPRS packets coming from the SGSN into the appropriate packet data protocol (PDP) format for the data networks like the Internet.
- PDP sends these packets out on the corresponding packet data network.
- PDP receives incoming data packets from data networks and converts them to the GSM address of the destination user.
- GGSN stores the current SGSN address of the user and user's profile in its location register while performing authentication and charging functions related to data transfer.



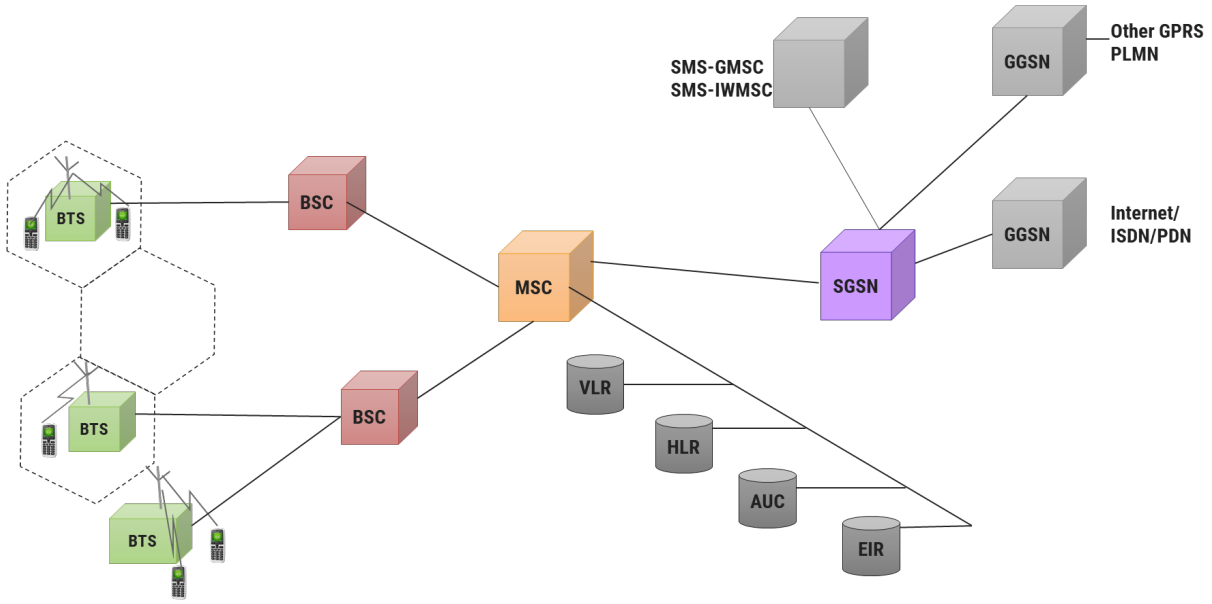
GPRS Architecture: GPRS Network Enhancement

- Base Station System (BSS) needs enhancement to recognize and send packet data.
  - BTS needs an upgrade to allow transportation of user data to the SGSN.
  - Also BTS needs to be upgraded to support packet data transportation between BTS and MS over the radio.
- HLR needs enhancement to register GPRS user profiles and respond to queries originating from GSNs regarding these profiles.
- MS (mobile station) for GPRS is different from that of GSM.
- SMS-GMSCs and SMS-IWMSCs(Internetworking MSC) are upgraded to support SMS transmission via the SGSN.



GPRS Architecture: Internal Backbone

- The internal backbone is an IP based network used to carry packets between different GSNs.
- Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network.
- Signalling from a GSN to a MSC, HLR or EIR is done using SS7.



Marwadi University

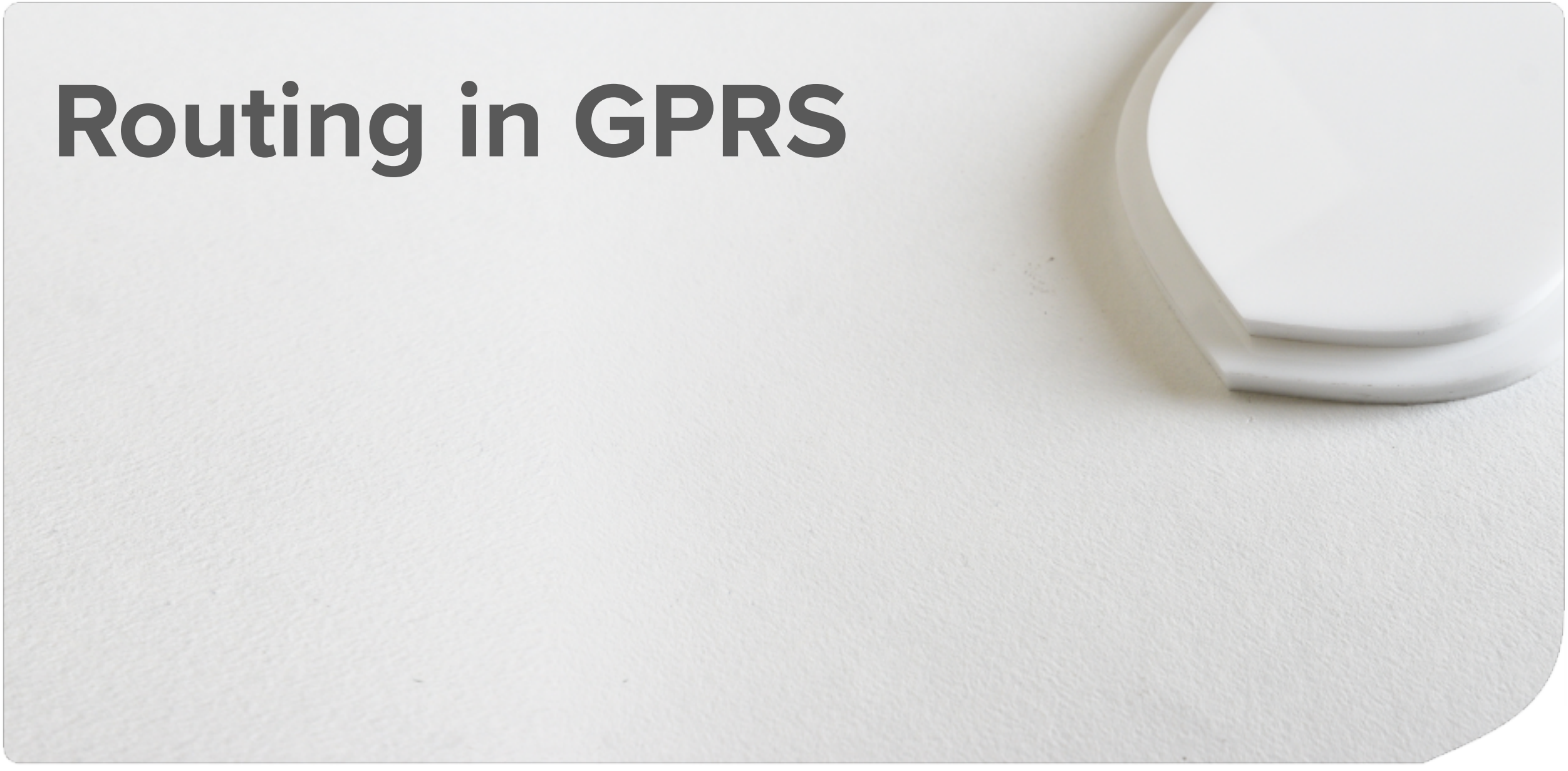
Security in GPRS

Security in GPRS

- GPRS security is similar to the existing GSM security.
- SGSN performs authentication and cipher setting procedures based on the same algorithms, keys and other criteria of GSM.
- GPRS uses a ciphering algorithm optimized for packet data transmission.

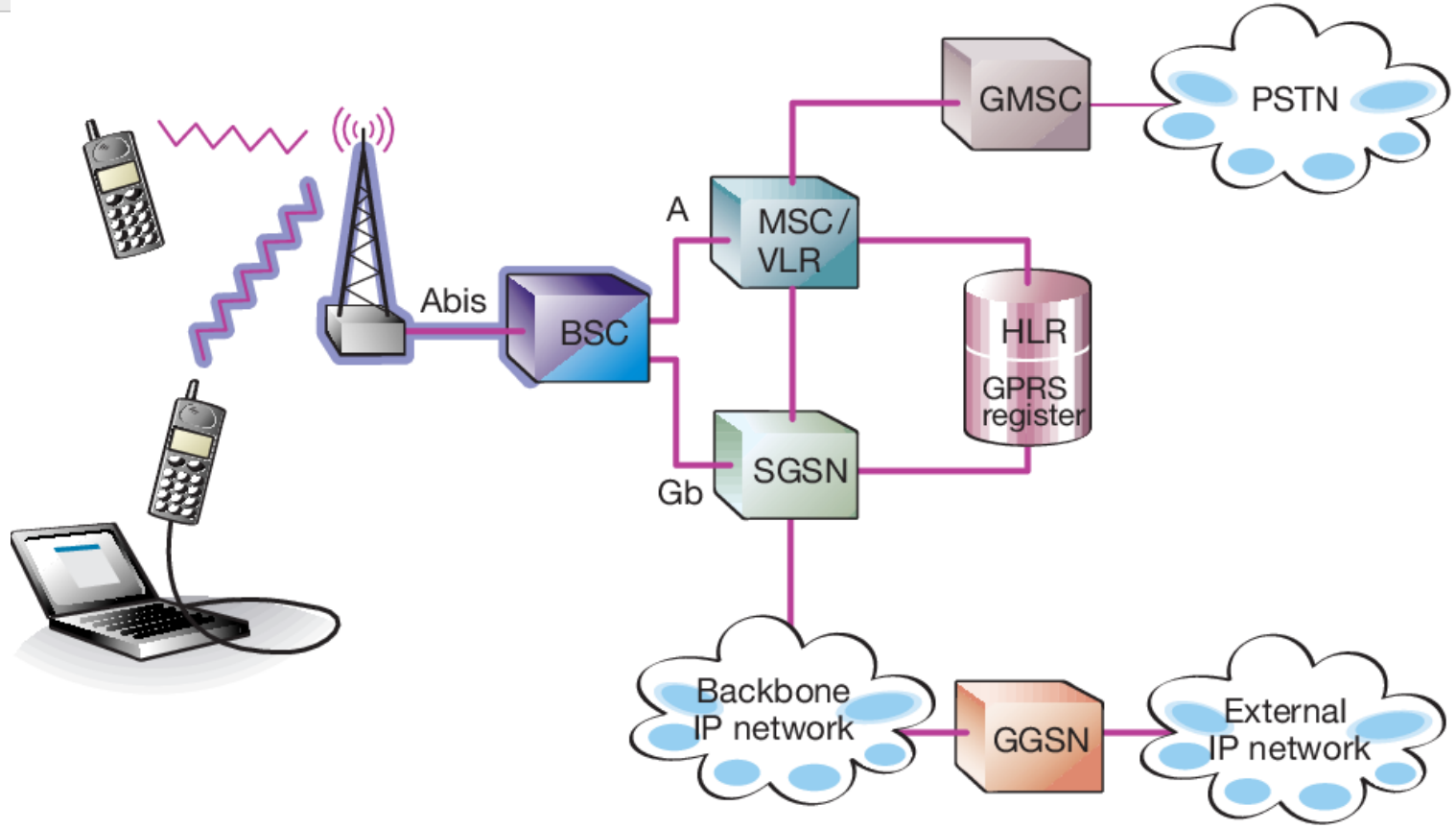
Marwadi University

Routing in GPRS



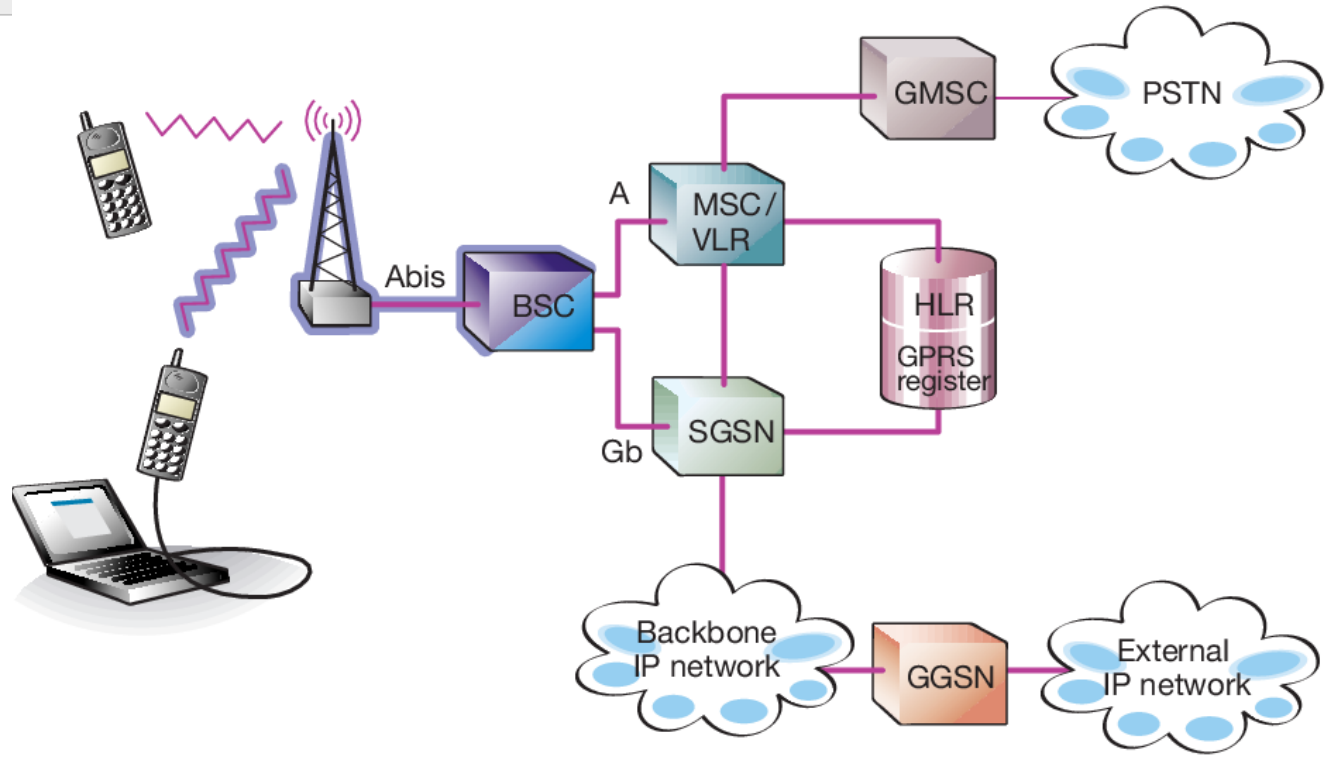
Routing in GPRS

- Data routing or routing of data packets to and from a mobile user, is one of the pivot requisites in the GPRS network.
- The requirement can be divided into two areas:
  1. Data packet routing
  2. Mobility management

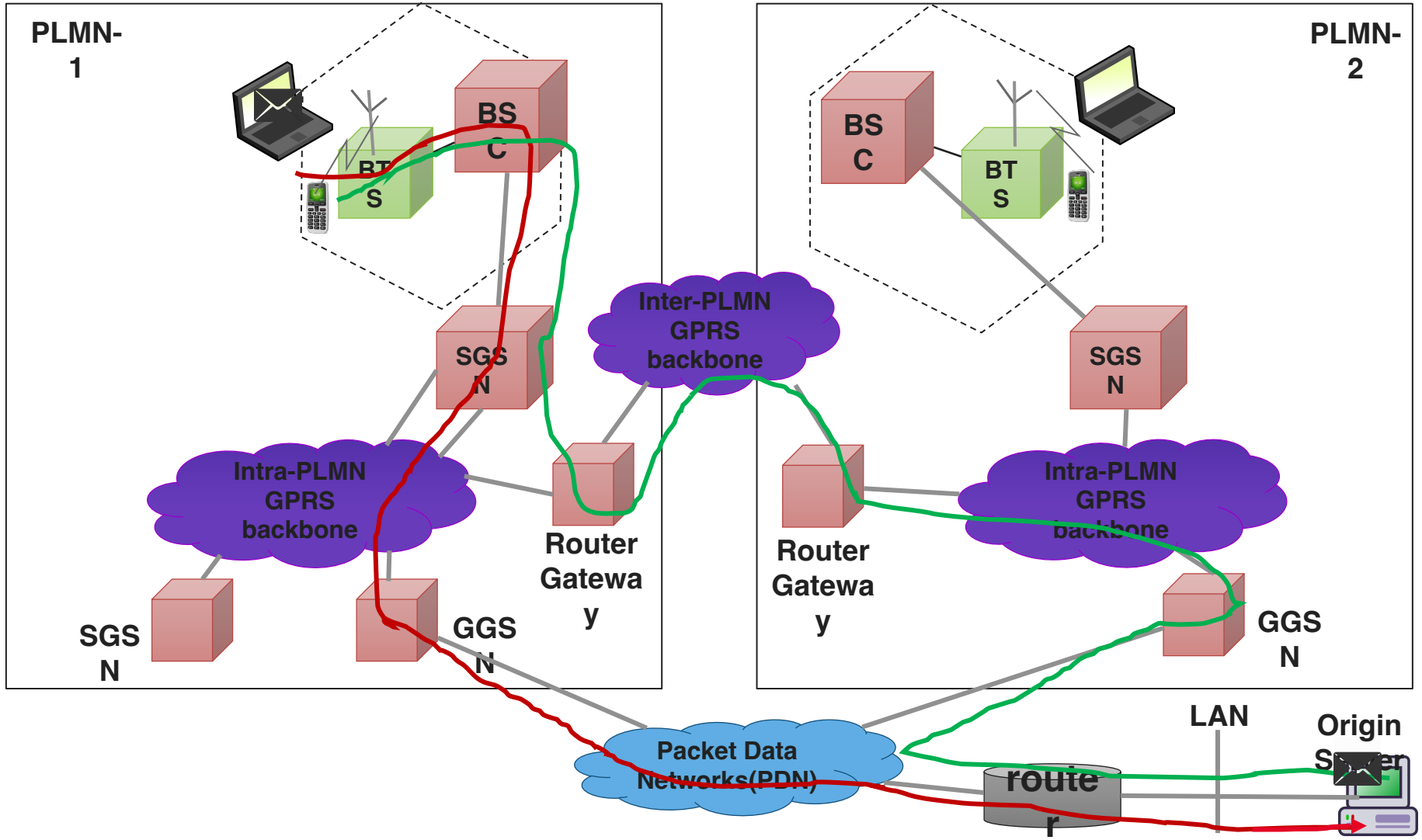


Routing in GPRS

- The important roles of GGSN involve synergy with the external data network.
- The GGSN updates the location directory using routing information supplied by the SGSNs about the location of an MS.
- GGSN routes the external data network protocol packet encapsulated over the GPRS backbone to the SGSN currently serving the MS.
- It also de-encapsulates and forwards external data network packets to the appropriate data network and collects charging data that is forwarded to a charging gateway (CG).



Routing in GPRS



It encapsulates the incon through the inter-PLMN GPRS backbone to t while the SGSN de-encapsulates the packets.

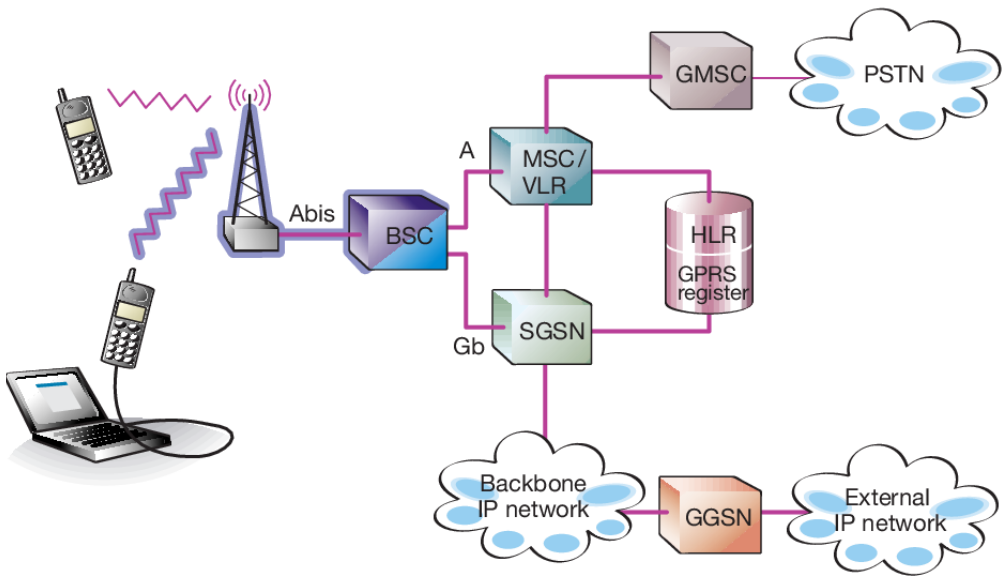
Finally delivers them to the MS.

Marwadi University

Data Services in GPRS

Data Services in GPRS

- Any user is likely to use either of the two modes of the GPRS network:
  1. **Application mode**
  2. **Tunneling mode**
- In application mode, the user uses the GPRS to access the applications running on the phone itself.
- The phone here acts as the end user device.
- In tunneling mode, user uses GPRS interface as an access to the network as the end user device would be a large device like laptop computer or a small device like PDA.
- The mobile phone will be connected to the device and used as a modem to access the wireless data network.



Bearers in GPRS

- Bearer services of GPRS offer end-to-end packet switched data transfer.
- GPRS supports two different kinds of data transport services:
  1. Point-to-point (PTP) services
  2. Point-to-multipoint (PTM) services
- GPRS continues to supports bearer services. (Same as the GSM)
- Wireless Application Protocol is a data bearer service over HTTP protocol.
- GPRS supports Multimedia Messaging Service.

Application of GPRS

Application in GPRS

1. **Communications** - E-mail, Chat, fax and intranet/internet access, etc.
2. **Value-added services** - Information services and games, etc.
3. **E-commerce** - Retail, ticket purchasing, banking and financial trading, etc.
4. **Location-based applications** - Navigation, traffic conditions, airline/rail schedules and location finder, etc.
5. **Vertical applications** - Freight delivery and fleet management.
6. **Advertising** - Advertising may be location sensitive. For example, a user entering a mall can receive advertisements specific to the stores in that mall.

Marwadi University

Benefits & Limitation of GPRS

Benefits of GPRS

- Resources are reserved only when needed and charged accordingly
- Connection setup times are reduced
- GPRS reuses existing GSM infrastructure, therefore deployment is easier
- Enables new service opportunities
- It provides seamless and instant connectivity with the internet
- Allows simultaneous use of both voice and data services. Thus user can have both voice call and data call together. Data call refers to use of internet by browsing or downloading or uploading data.

Limitation of GPRS

1. **Limited Cell Capacity for All Users:**
   - Only limited radio resources can be deployed for different uses. Both Voice and GPRS calls use the same network resources.
   - Network can be affected when more number of GPRS users in the same area utilize the GPRS services at the same time. This leads to congestion which results into slower data connection.

2. **Low Speed in Reality:**
   - Achieving the theoretical maximum GPRS data transmission speed of 172.2 kbps would require a single user taking over all eight time slots without any error protection.
   - GPRS is slower compare to latest wireless standards such as HSPA, LTE, LTE-advanced etc.

Marwadi University

Billing & Charging

Billing & Charging in GPRS

Minimum charging information that must be collected are:

- Usage of radio interface.
- Usage of external Packet Data Networks.
- Usage of general GPRS resources and location of the Mobile Station.

- Various business models exist for charging customers as billing of services can be based on:
  - The transmitted data volume
  - The type of service
- GPRS call records generated in the GPRS Service Nodes.
- Packet counts passed to a Charging Gateway that generates call detail records that sent to the billing system.

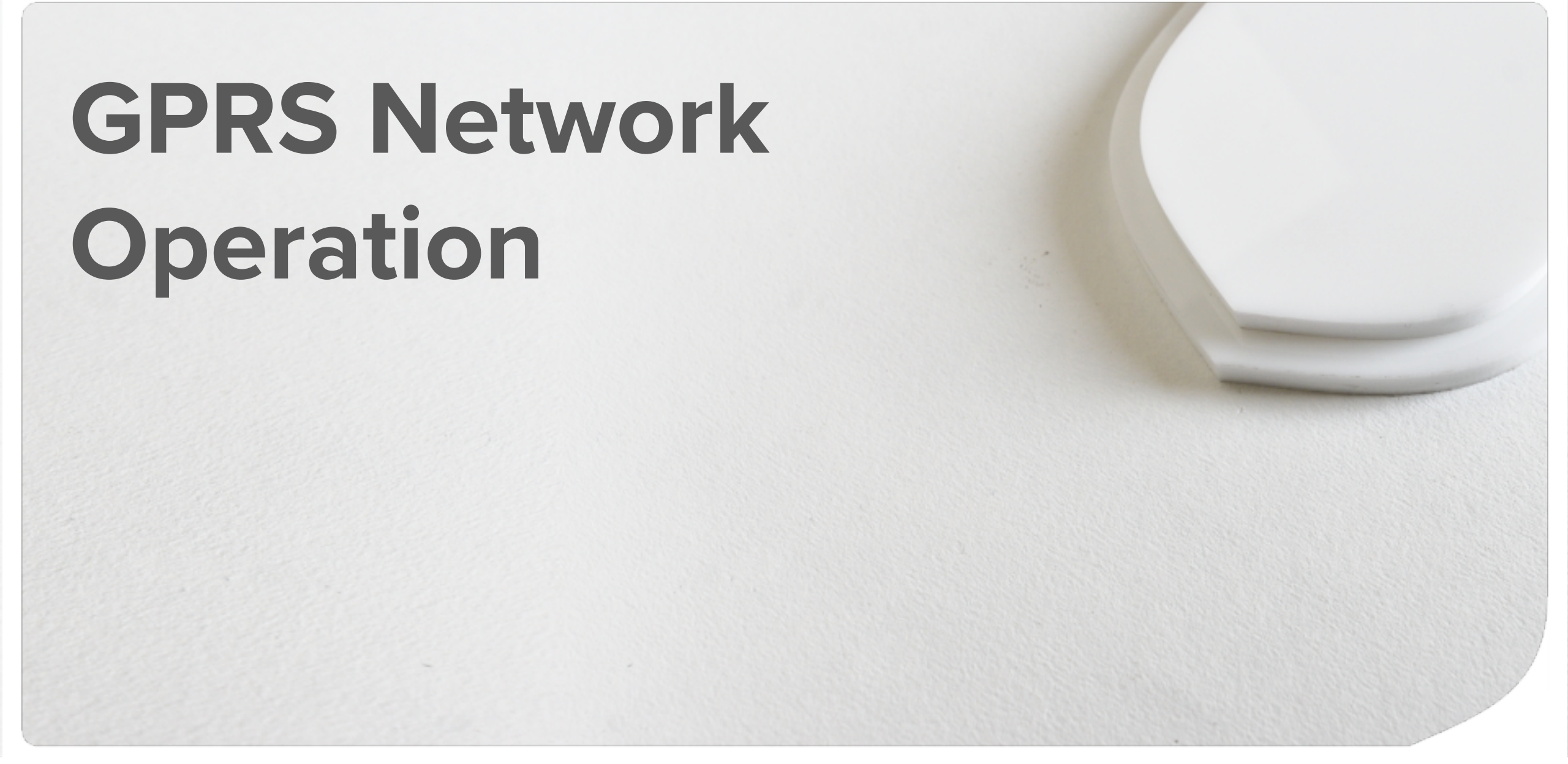
Billing & Charging in GPRS

- The SGSN and GGSN register all possible aspects of a GPRS user's behavior and generate billing information accordingly. This information is gathered in so-called Charging Data Records (CDR) and is delivered to a billing gateway.
- The GPRS billing parameters:

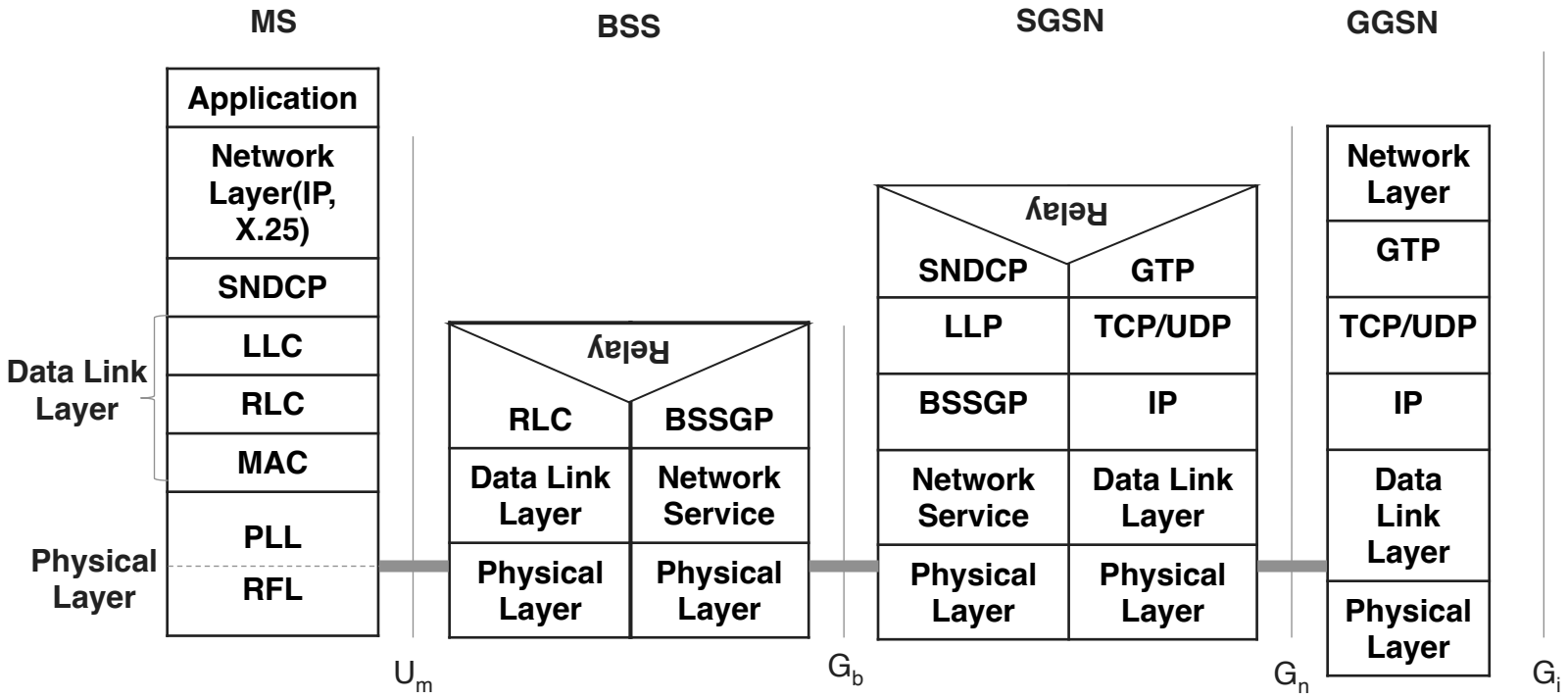
Volume	The amount of bytes transferred, i.e., downloaded & uploaded both
Duration	Duration of a PDP context session
Time	Date, time of day and day of the week information
Final destination	A subscriber could be charged for access to the specific network.
Location	Current location of the subscriber
Quality of Service	Pay high for higher network priority
Flat rate	A fixed monthly rate
Bearer service	Charging based on different bearer services (for an operator who has several networks, such as GSM900 and GSM1800, and who wants to promote usage of one of the networks).

Marwadi University

GPRS Network Operation



GPRS Network Operation: GPRS Protocol Stack



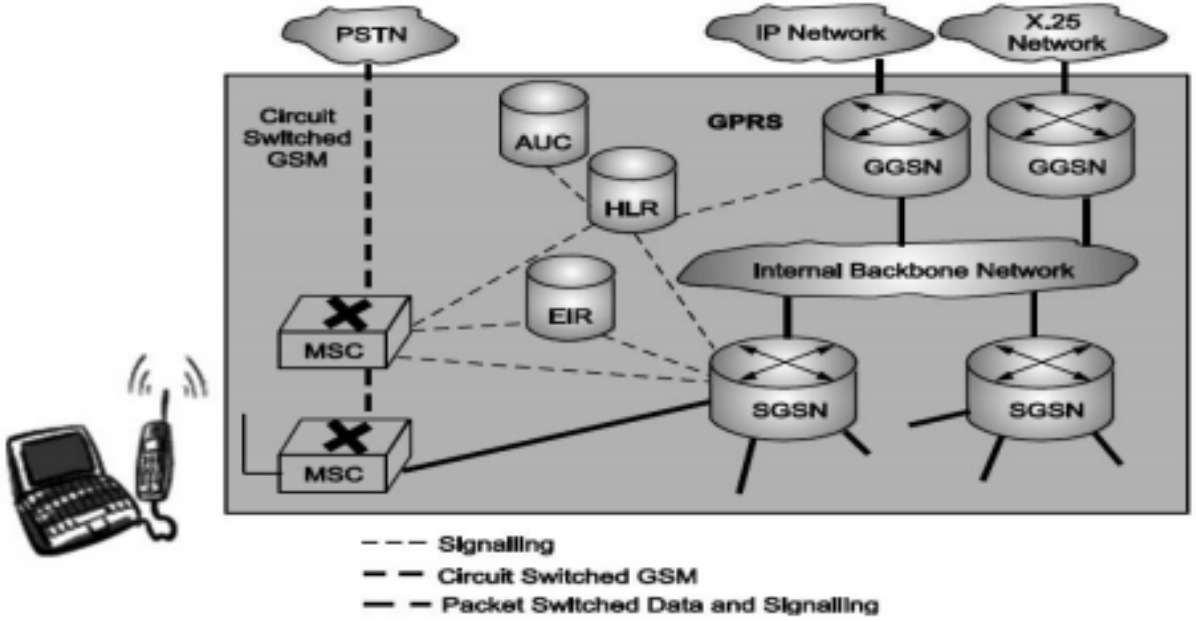
RFL	Radio Frequency Layer	SNDCP	Subnet Dependent Convergence Protocol
PLL	Physical Link Layer	BSSGP	BSS GPRS Application Protocol
MAC	Medium Access Control	GTP	GPRS Tunneling Protocol
RLC	Radio Link Control		
LLC	Logical Link Control		

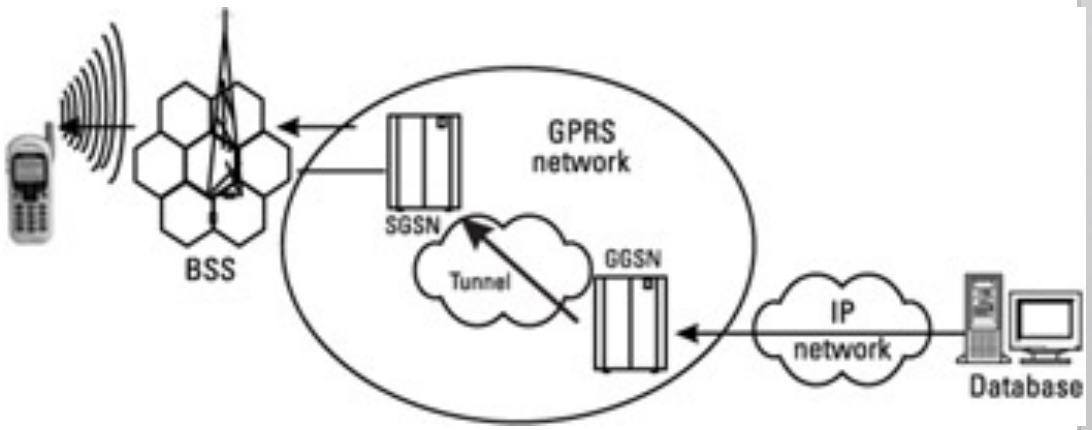
GPRS Network Operation: GPRS Protocol Stack

- **Protocol architecture** of the GPRS transmission signaling protocols for control and support of the functions.
- It includes:
  1. GPRS attach and detach
  2. PDP(Packet Data Protocol) context activation
  3. Control of routing paths
  4. Allocation of network resources

GPRS Network Operation: GPRS Internal Backbone

- The internal backbone is an IP based network used to carry packets between different GSNs.
- Tunnelling is used between SGSNs and GGSNs, so the internal backbone does not need any information about domains outside the GPRS network.
- Signalling from a GSN to a MSC, HLR or EIR is done using SS7.

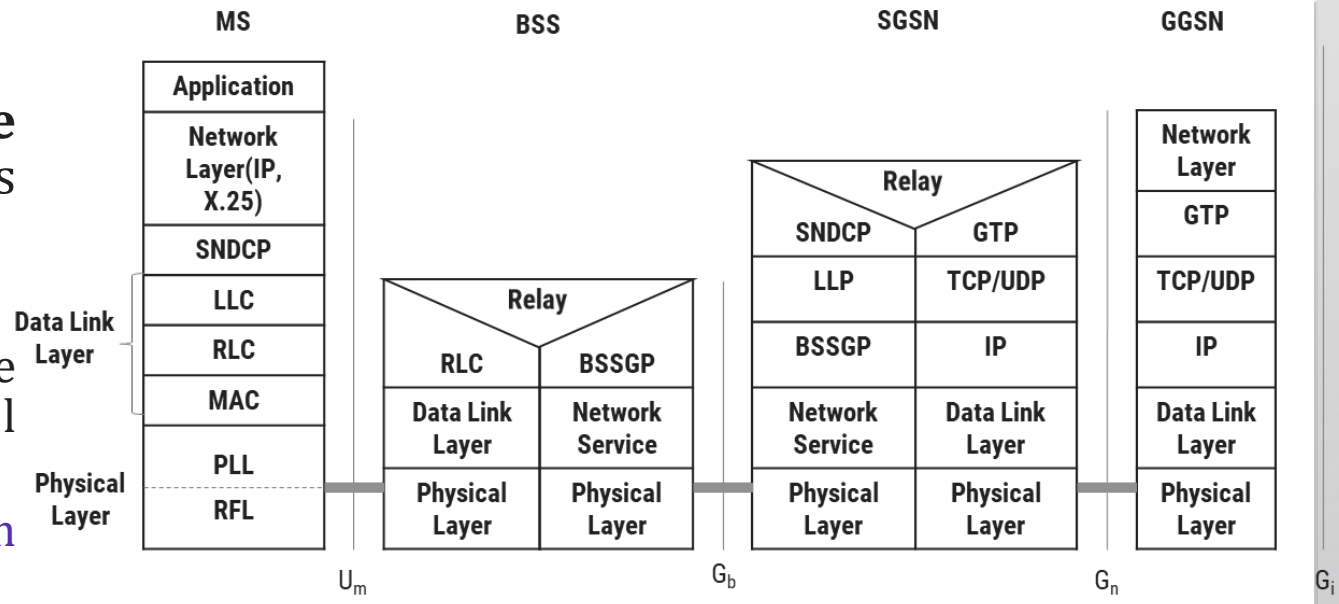


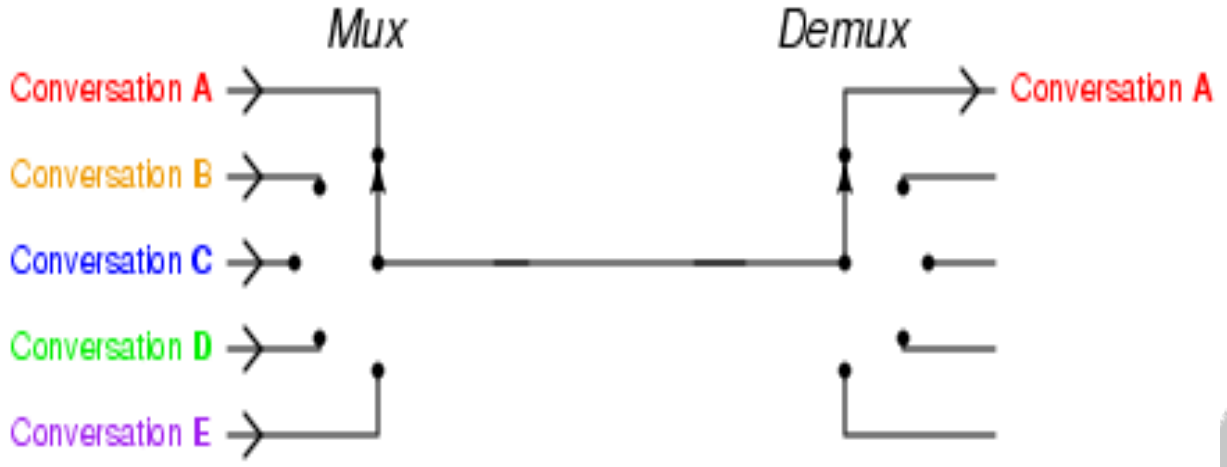


GPRS Network Operation: BSS-SGSN Interface

BSS-SGSN interface is divided into four layers:

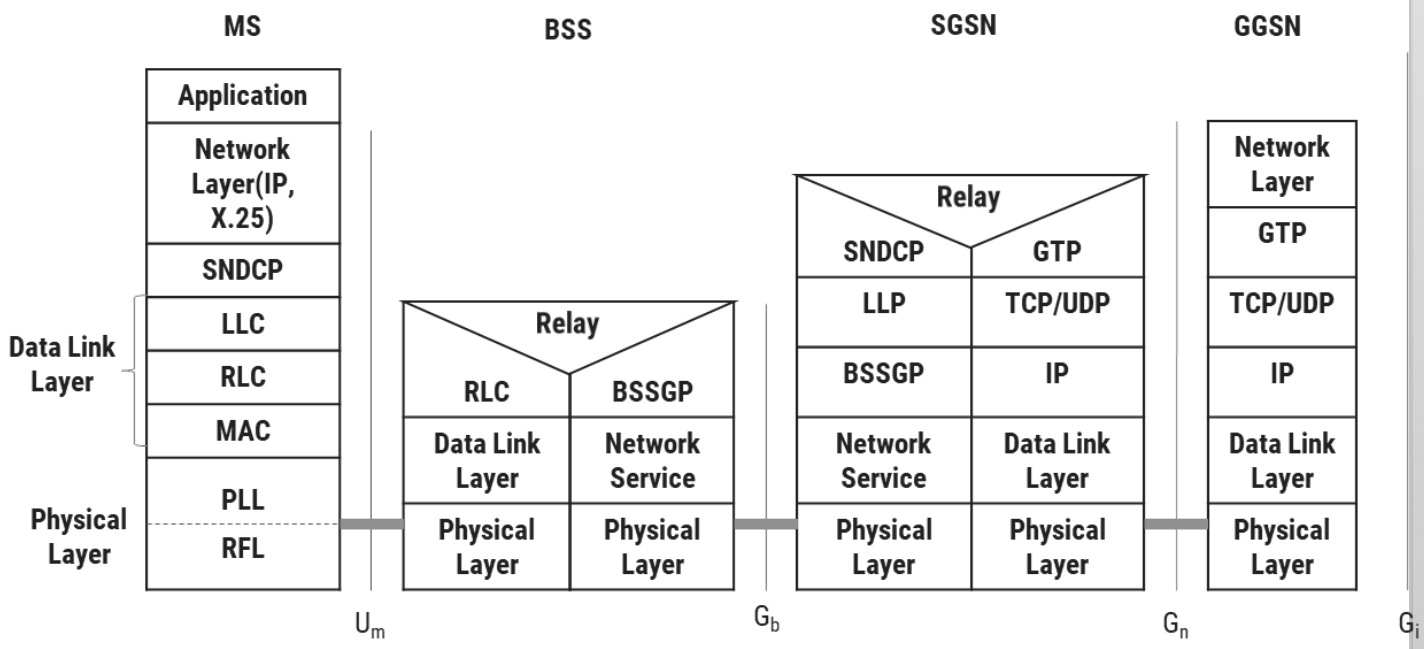
1. **Sub-Network Dependent Convergence Protocol (SNDCP)** which is used to transfers data packets between SGSN and MS.
   - ➥ Its functionality includes:
     - Multiplexes several connections of the network layer onto one virtual logical connection of the underlying LLC layer.
     - Segmentation, compression-decompression of user data.
2. **Logical Link Control (LLC)** is 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.





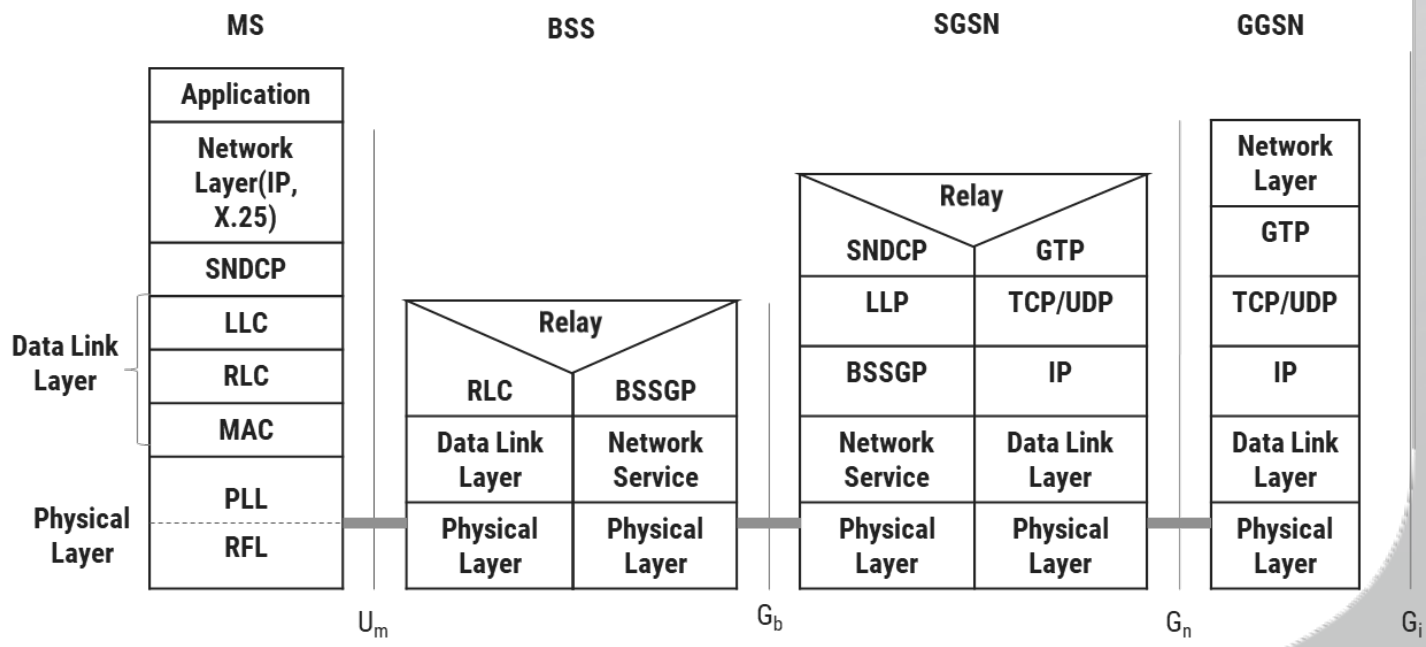
GPRS Network Operation: BSS-SGSN Interface

3. **Base Station System GPRS Protocol (BSSGP)** delivers routing and QoS related information between BSS and SGSN.
4. **Network Service layer** manages the convergence sub-layer that operates between BSSGP and Frame Relay.



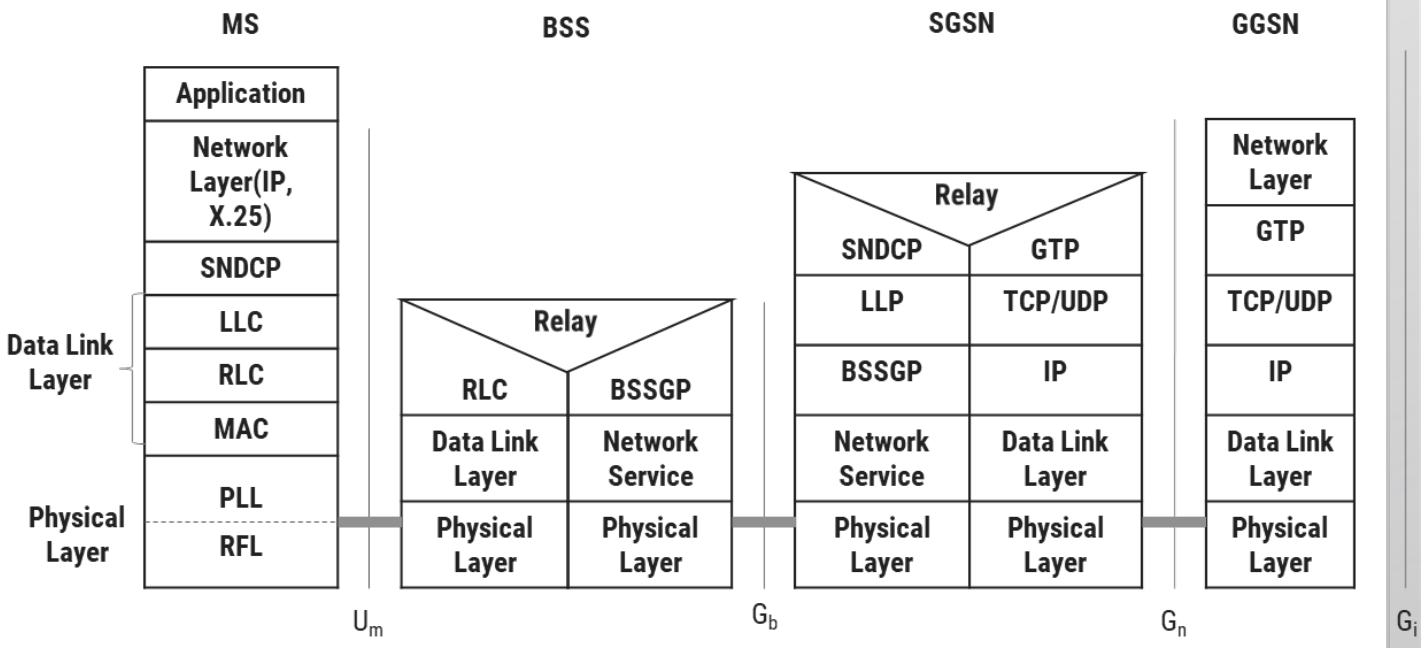
GPRS Network Operation: Air Interface

- Air interface of GPRS consists of data link layer and physical layer.
- Data link layer between MS and BSS divided into three sub-layers:
  1. Logical Link Control (LLC) layer
  2. Radio Link Control (RLC) layer
  3. Medium Access Control (MAC) layer
- Physical layer between MS and BSS divided into two sub-layers:
  1. Physical Link Layer (PLL)
  2. Physical RF Layer (RFL)



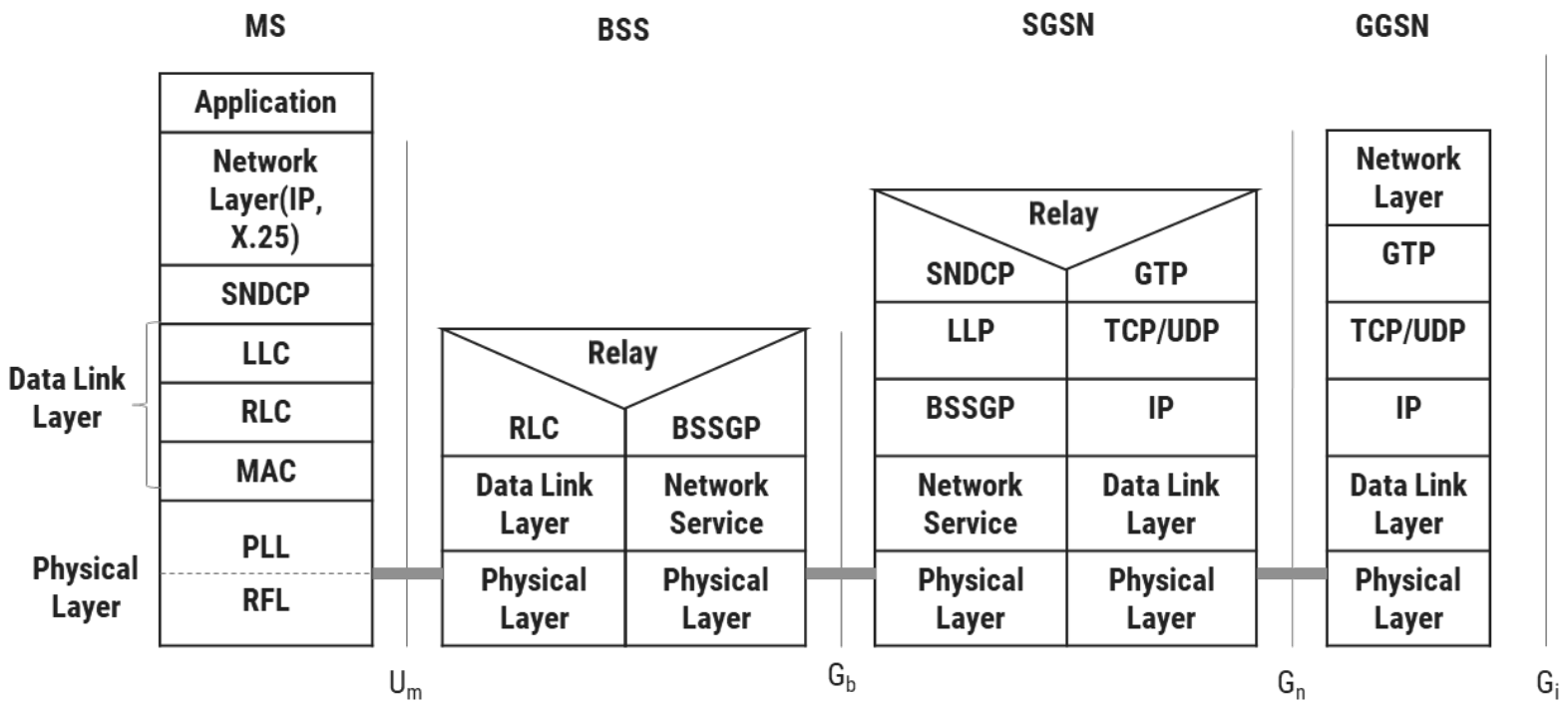
GPRS Network Operation: Logical Link Control (LLC) Layer

- 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.
- It includes:
  - Sequence control
  - In-order delivery Flow control
  - Detection of transmission errors and retransmissions
- Encryption is used in this interface to ensure data confidentiality.
- Variable frame lengths are possible. Both acknowledged and unacknowledged data transmission modes are supported.



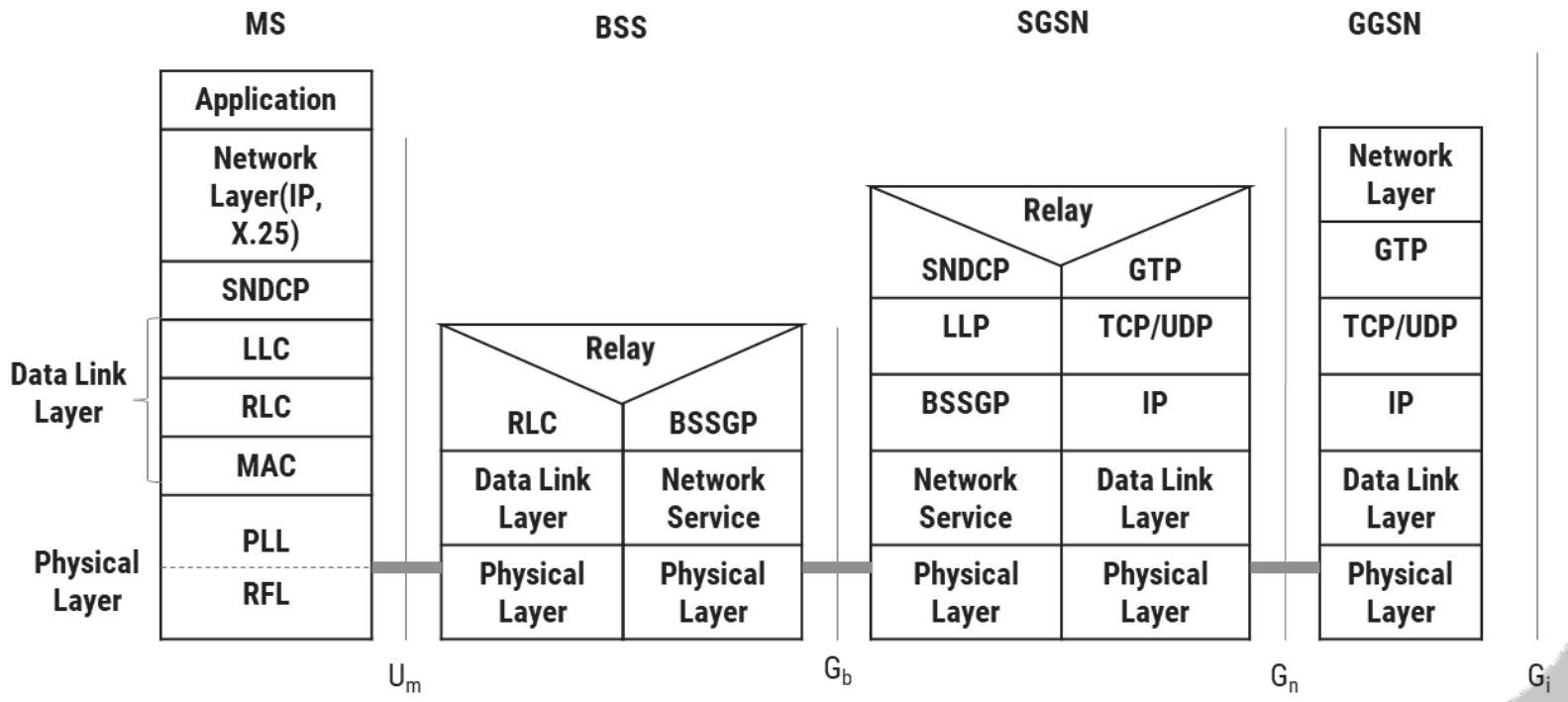
GPRS Network Operation: Radio Link Control Layer

- Radio Link Control (RLC) layer establishes a reliable link between MS and BSS.
- It also does segmentation and reassembly of LLC frames into RLC data blocks and ARQ of uncorrectable data.



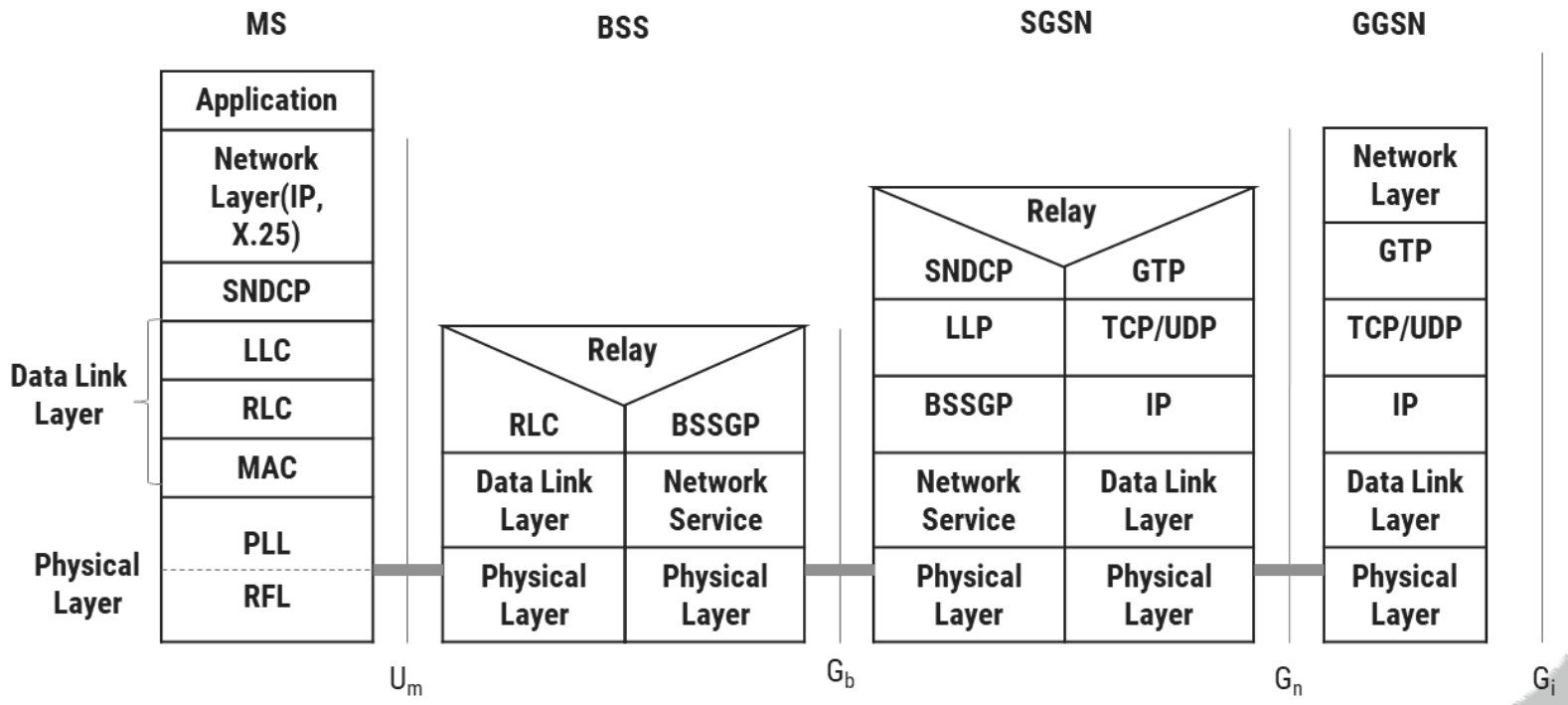
GPRS Network Operation: Medium Access Control (MAC) Layer

- **Medium Access Control (MAC)** layer controls the access attempts of an MS on the radio channel shared by several MSs.
- It employs algorithms for conflict resolution, multi-user multiplexing on a packet data traffic channel.



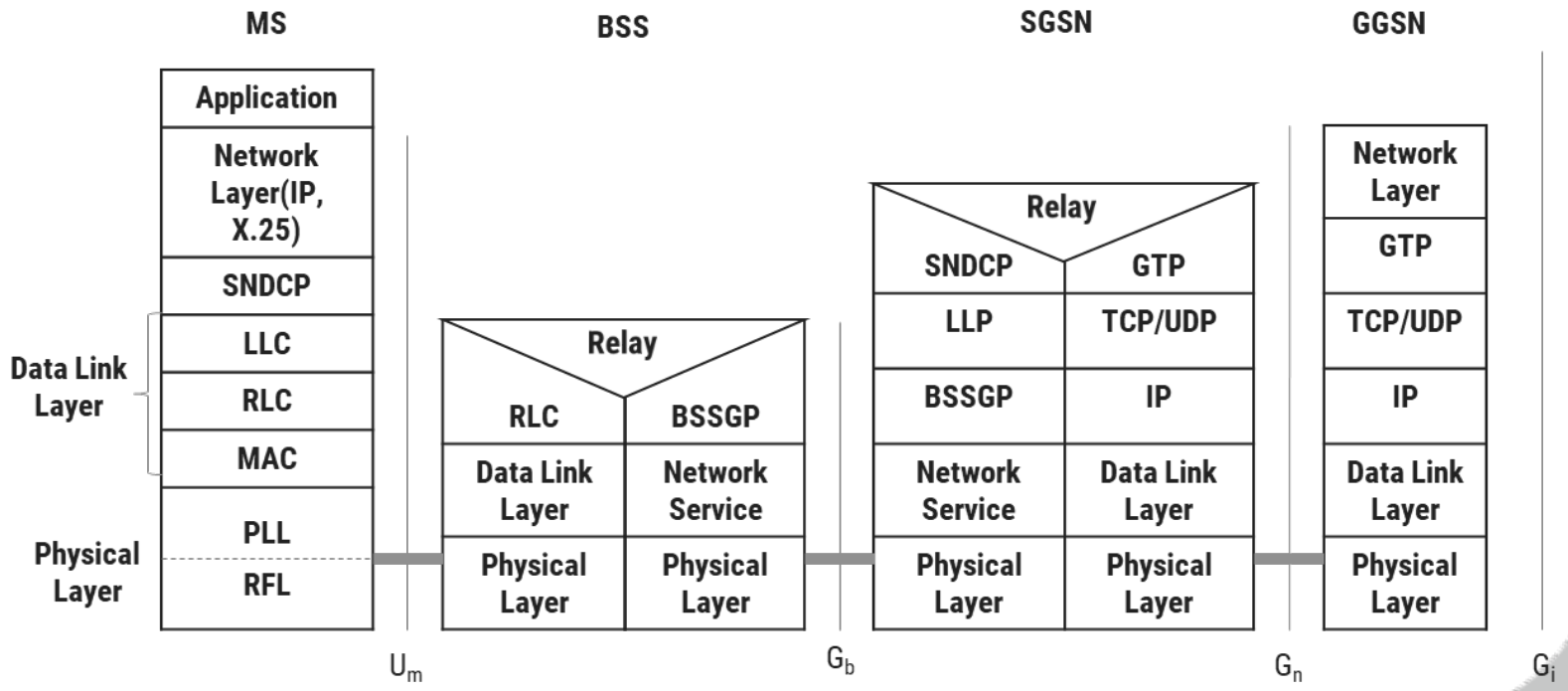
GPRS Network Operation: Physical Link Layer (PLL)

- **Physical Link Layer (PLL)** provides services for information transfer over a physical channel between the MS and the network.
- Its functions include
  - data unit framing,
  - data is encoded before data is transmitted



GPRS Network Operation: Physical RF Layer (RFL)

- **Physical RF Layer (RFL)** performs the modulation of the waveforms based on the sequence of bits received from the Physical Link Layer above.
- It also demodulates received wave forms into a sequence of bits that transferred to the Physical Link layer for interpretation.




Thank
You