2. Mobile Telecommunication System

1.Explain GSM architecture in detail.

GSM stands for **Global System for Mobile Communication**.
It is a **digital mobile network** used all over the world to make calls, send SMS, and transfer data.

- It combines **FDMA (Frequency Division Multiple Access)** and **TDMA (Time Division Multiple Access)**.
- It uses **4 frequency bands: 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz**.
- It divides one frequency into **8 time slots**, so many users can share the same channel.

GSM architecture is a network framework that enables wireless communication for mobile users.

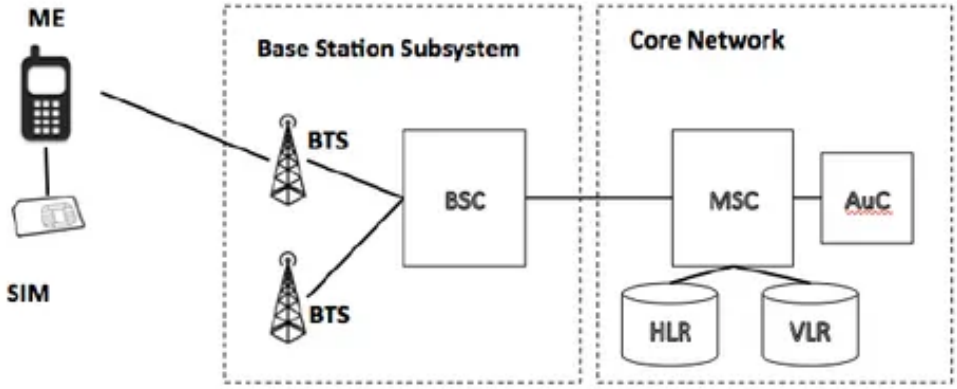
It consists of several subsystems that manage **radio communication, network switching, subscriber authentication, call setup, mobility management, and data services**.

GSM cells are areas covered by mobile towers. They come in different sizes:

1. **Macro Cell** – Large coverage (antenna on a tall tower/building).
2. **Micro Cell** – Smaller coverage (antenna below rooftop level).
3. **Pico Cell** – Very small (few meters, used in malls/offices).
4. **Umbrella Cell** – Fills coverage gaps between cells.

Main Features of GSM

- International roaming (use your phone in other countries).
- Good voice clarity.
- Works with many mobile devices.
- Low power consumption.
- Low cost of service.
- Easy to access and manage.
- Compatible with ISDN (old landline systems).
- Supports new services like SMS, call forwarding, etc.



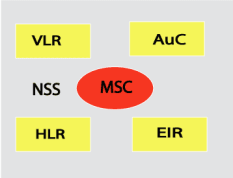
GSM Architecture

The GSM network has four main parts:

1. **Mobile Station (MS)**
    - Your mobile phone + SIM card.
    - SIM stores your identity and data (number, plan, contacts).
    - Communicates with towers using radio waves.

2. **Base Station Subsystem (BSS)**
    - Manages wireless communication between your phone and the core network.
    - Components:
        - **BTS (Base Transceiver Station):** The equipment on towers that sends/ receives signals.
        - **BSC (Base Station Controller):** Controls multiple BTSs, manages channels, and handovers.

3. **Network and Switching Subsystem (NSS)**



- The NSS is the **core of the GSM network** responsible for call routing, switching, subscriber data management, and mobility management.
- It connects the Base Station Subsystem (BSS) to external networks like PSTN, ISDN, and the Internet.

    - The brain of GSM — manages calls, messages, and mobility.
    - Components:
        - **MSC (Mobile Switching Center):** Routes calls/SMS and connects to landlines (PSTN).
        - **HLR (Home Location Register):** Stores permanent user data (plans, number, ID).
        - **VLR (Visitor Location Register):** Stores temporary location info when you travel.
        - **AUC (Authentication Center):** Checks if your SIM is real and allowed.
        - **EIR (Equipment Identity Register):** Keeps a list of allowed/blocked devices.
            1. **White list:** Allowed devices.
            2. **Black list:** Stolen/unauthorized devices.
            3. **Grey list:** Devices under observation.

4. **Operation Support Subsystem (OSS)**
    - Used by network operators to monitor, control, and maintain the network.
    - Contains **OMC (Operation & Maintenance Center)** for performance monitoring.

Interfaces in GSM

- **Air Interface (Um):** Between mobile and BTS.
- **Abis Interface:** Between BTS and BSC.
- **A Interface:** Between BSC and MSC

How GSM Works (Simple Flow)

1. Your phone (MS) connects to the nearest tower (BTS).
2. BTS sends your data to BSC.
3. BSC passes it to MSC for call/SMS setup.
4. MSC checks your details in HLR/VLR and authenticates using AUC.
5. If valid, your call/message is sent to the recipient via PSTN or another network

Applications of GSM

- Mobile calling & SMS
- Mobile banking
- Smart homes & IoT
- Alarms & surveillance systems
- VoIP integration

Advantages

- Works worldwide (high compatibility).
- Good security (authentication & encryption).
- Efficient bandwidth use.
- International roaming supported.
- Many features like voicemail, conference calls, etc.

Disadvantages

- Limited coverage in remote areas.
- Slower internet (compared to 3G/4G).
- Can get congested during peak hours.
- Still has some security loopholes.
- Limited data capacity.

2. GSM Services

1. Bearer Services (Data Services)

Bearer services allow the **transmission of data** (not just voice) between devices using the GSM network.

- **Purpose:** To transfer data (text, images, files, etc.).
- **Speed:** Original GSM supported up to **9.6 kbps** (later improved with GPRS/EDGE).
- **Examples:** Internet browsing, fax transmission, email.

Types of Bearer Services:

1. **Transparent Bearer Services**
    - Uses only the physical layer (basic connection).
    - No error correction — data sent as it is.
    - Constant delay and data rate if no transmission error occurs.
    - Example: Circuit-switched data.
2. **Non-Transparent Bearer Services**

- Uses higher layers (data link & network layers).
- Includes **error correction and flow control**.
- More reliable for unstable connections.
- Example: Data transmission with automatic retransmission.

2. Tele Services

These are the basic **voice and text communication services** in GSM.

Major Tele Services:

- **Voice Calls:**
  The main service of GSM — allows person-to-person voice communication.
- **Short Message Service (SMS):**
  Allows sending text messages up to 160 characters.
- **Multimedia Messaging Service (MMS):**
  Supports sending images, audio, and video (in advanced GSM with GPRS).
- **Fax Transmission:**
  Sending faxes through GSM.
- **Emergency Calls:**
  Can be made even without balance or SIM registration (e.g., 112, 100).

3. Supplementary Services

These are **extra features** that enhance tele and bearer services.

Common Supplementary Services:

- **Call Forwarding:**
  Redirects calls to another number when busy, unreachable, or out of coverage.
- **Call Waiting:**
  Notifies you of an incoming call while you're on another call.
- **Call Hold:**
  Lets you put an active call on hold to take another.
- **Conference Call:**
  Allows multiple users to talk together on a single call.
- **Caller ID (CLIP/CLIR):**
  Displays the number of the caller or hides your number.
- **Barring of Outgoing/Incoming Calls:**
  Blocks calls in certain conditions (e.g., international calls).

4. GSM Security Services

GSM Security

Security in GSM is designed to protect **user identity, communication, and network access**. It ensures that only valid users connect to the network and that their data is transmitted securely.

GSM security mainly involves **Authentication, Encryption, and Confidentiality**.

1. Authentication

- **Purpose:** To verify that the user trying to access the network is legitimate.

- **How it works:**
  - Each SIM has a unique **IMSI (International Mobile Subscriber Identity)** and a secret key called **Ki**.
  - When you try to connect, the network (AUC – Authentication Center) sends a random number (RAND) to your SIM.
  - SIM uses the secret key (Ki) to calculate a response (SRES).
  - The network checks if SRES matches its own calculation.
  - If they match → You are authenticated.

2. Encryption

- **Purpose:** To protect your calls, SMS, and data from eavesdropping during transmission.
- **How it works:**
  - After authentication, the network and SIM agree on an **encryption key (Kc)**.
  - This key is used to encrypt data between the Mobile Station (MS) and the Base Transceiver Station (BTS).
  - Even if someone intercepts the signal, they cannot easily decode it.

3. Confidentiality

- **Purpose:** To hide your **identity and location** from unauthorized access.
- **How it works:**
  - Instead of sending IMSI every time, GSM uses a **Temporary Mobile Subscriber Identity (TMSI)**.
  - This TMSI keeps changing, making it difficult to track the user.

4. SIM Security

- GSM provides **PIN (Personal Identification Number)** and **PUK (Personal Unblocking Key)** codes.
  - **PIN:** Protects your SIM from unauthorized use.
  - **PUK:** Unlocks your SIM if you enter the wrong PIN multiple times.

5. Equipment Security

- **EIR (Equipment Identity Register):** Maintains a list of valid, stolen, or blacklisted devices using their IMEI numbers.
  - White list: Allowed devices.
  - Black list: Blocked (stolen/illegal).
  - Grey list: Monitored devices.

Limitations of GSM Security

- Original GSM encryption algorithms (like A5/1, A5/2) are outdated and can be cracked.
- Data is encrypted only between **MS and BTS**, not across the entire network.
- Vulnerable to **IMSI catchers (fake base stations)**.

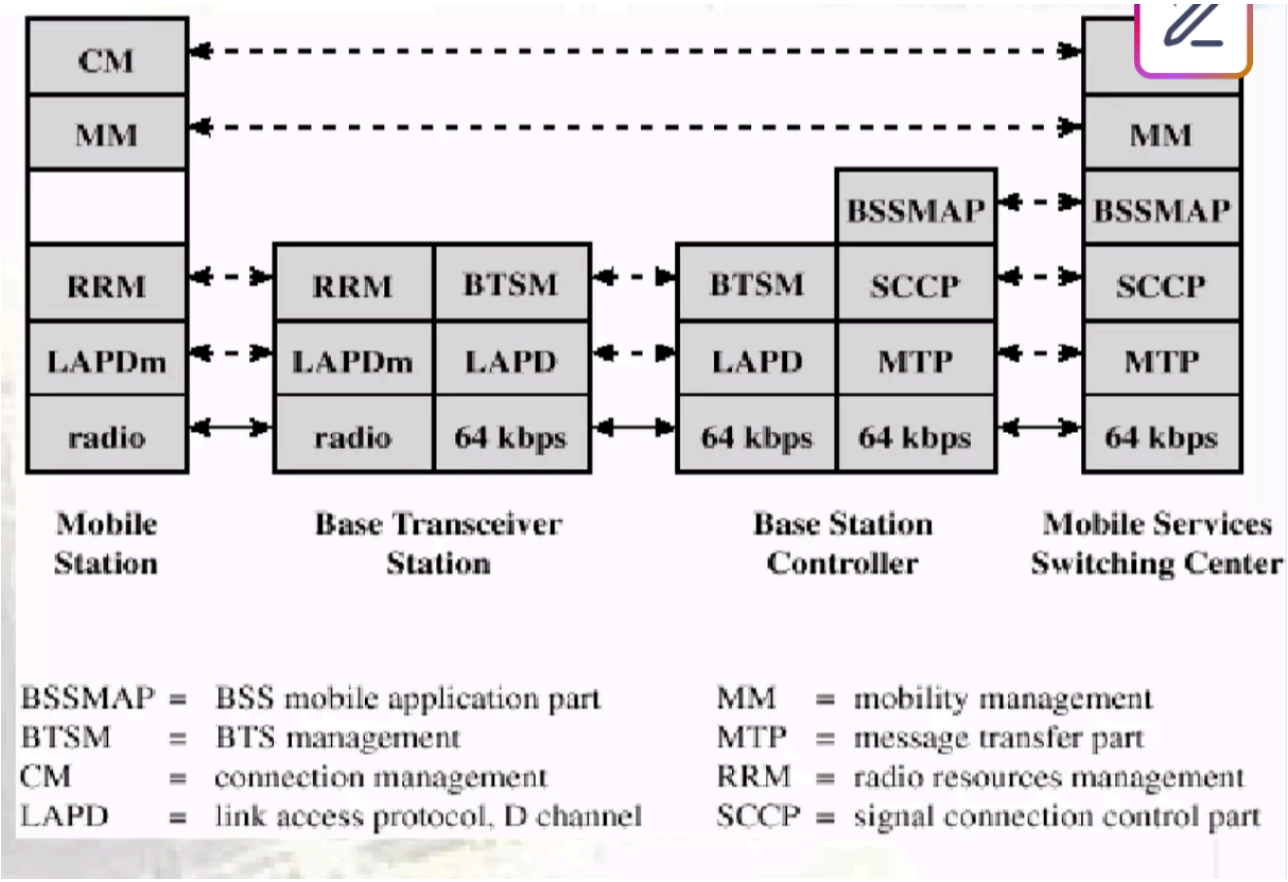
3.Protocol Architecture for Signaling in GSM

GSM uses a layered protocol structure to manage communication between mobile stations (MS), base stations (BSS), and the core network (NSS).

Signaling in GSM is mainly used for:

- Call setup and release
- Mobility management (location updates, handovers)
- SMS delivery
- Authentication and security procedures

The signaling protocols in GSM follow the **OSI (Open Systems Interconnection) reference model** but are adapted for GSM-specific needs.



Layers of GSM Signaling Protocol Architecture

1. Physical Layer (Layer 1)

- Responsible for the physical transmission of data over the radio interface.
- Uses **TDMA (Time Division Multiple Access)** and **FDMA (Frequency Division Multiple Access)**.
- Handles channel coding, modulation (GMSK), and synchronization.

2. Data Link Layer (Layer 2)

- Ensures reliable transmission over the physical link.
- Uses **LAPDm (Link Access Protocol for the Dm channel)**, derived from LAPD (used in ISDN).
- Functions: Error detection, correction, and flow control.

3. Network Layer (Layer 3)

This is divided into three sublayers:

1. **Radio Resource Management (RR)**
    - Manages allocation and release of radio channels.
    - Handles handovers between BTSs.
2. **Mobility Management (MM)**
    - Manages subscriber location, registration, authentication, and security.
    - Uses TMSI/IMSI for identification.
3. **Call Control (CC)**
    - Responsible for call setup, modification, and release.
    - Works with the MSC to manage calls.

GSM Signaling Channels

- **Control Channels (CCH):** Used for signaling (not voice/data).
    - Broadcast Control Channel (BCCH)
    - Common Control Channel (CCCH)
    - Standalone Dedicated Control Channel (SDCCH)
- **Traffic Channels (TCH):** Used for voice and user data.

Signaling Protocols Used

- **Signaling System No. 7 (SS7):** Used in the core network (MSC, HLR, VLR).
- **MAP (Mobile Application Part):** Manages mobility and database services (HLR/VLR).
- **BSSAP (BSS Application Part):** Communication between BSS and MSC.

4.Frequency Allocation in GSM

GSM uses specific frequency bands allocated for mobile communication. The allocation ensures interference-free communication between the Mobile Station (MS) and Base Station (BTS).

1. GSM Frequency Bands

GSM operates in different frequency bands based on region:

- **GSM 900 (Original band)**
    - Uplink (MS → BTS): **890–915 MHz**
    - Downlink (BTS → MS): **935–960 MHz**
    - Duplex spacing: **45 MHz**
- **GSM 1800 (DCS)**
    - Uplink: **1710–1785 MHz**
    - Downlink: **1805–1880 MHz**

    - Duplex spacing: **95 MHz**
- **GSM 850 and 1900 (used mainly in the Americas)**
    - GSM 850: Uplink 824–849 MHz, Downlink 869–894 MHz
    - GSM 1900: Uplink 1850–1910 MHz, Downlink 1930–1990 MHz

2. Channel Bandwidth and Division

- Each frequency band is divided into **25 MHz for uplink and 25 MHz for downlink** (for GSM 900).
- Each **carrier is 200 kHz wide**, allowing **124 carriers in GSM 900**.
- Each carrier supports **8 time slots using TDMA**, giving **8 voice channels per carrier**.

3. Frequency Reuse

- To increase capacity, frequencies are **reused in different cells**.
- Frequency reuse patterns (e.g., 3/9, 4/12) ensure minimal interference.

4. Duplexing Technique

- GSM uses **Frequency Division Duplex (FDD)**.
- Uplink and downlink are separated by a fixed frequency offset (e.g., 45 MHz for GSM 900).

5. Guard Bands

- Small frequency gaps at band edges prevent interference between adjacent bands.

6. Allocation by Regulatory Authorities

- Frequency bands are allocated by **national telecommunication authorities** (e.g., TRAI in India, FCC in USA).

5.GSM Mobility Management (MM)

Mobility Management is a core function of GSM that ensures a mobile user can **move freely across different cells, BSCs, MSCs, or even networks** without losing ongoing services (calls, SMS, or data).
It handles **location tracking, registration, authentication, and roaming**.

Objectives of Mobility Management

1. **To keep track of the user's location** (for incoming calls/SMS).
2. **To support seamless handover** during movement.
3. **To manage roaming** (domestic and international).
4. **To ensure secure and authenticated access** to the network.

Functions of Mobility Management

1. Location Management

- **Location Update (LU):** MS informs the network when moving between Location Areas (LAs).
- **HLR and VLR Coordination:**
  - HLR stores permanent subscriber data.
  - VLR stores temporary location info of users in its area.

2. Roaming Management

- Allows a subscriber to use services outside their home network.
- HLR communicates with foreign VLR to provide service.

3. Handover Management

- Ensures uninterrupted service during movement.
- Types:
  - Intra-cell (within the same BTS)
  - Inter-cell (between different BTS under the same BSC)
  - Inter-BSC (between different BSCs)
  - Inter-MSC (between different MSCs)

4. Authentication & Security

- Validates subscriber identity using IMSI and secret key (Ki).
- Uses **TMSI (Temporary Mobile Subscriber Identity)** to protect privacy.

Components Involved

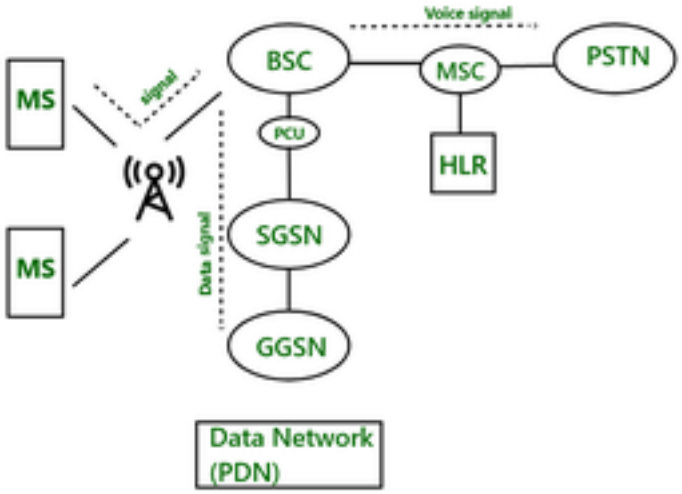
- **Mobile Station (MS):** Sends location updates.
- **Base Station Subsystem (BSS):** Detects signal strength for handover decisions.
- **Mobile Switching Center (MSC):** Coordinates handover and routing.
- **HLR & VLR:** Manage location and authentication data.

6. GPRS Architecture

GPRS (General Packet Radio Service) is an extension of GSM that enables **packet-switched data transmission**, allowing users to access the internet, send emails, and use multimedia services.

- **GPRS (General Packet Radio Service)** is an enhanced version of GSM that allows **packet-oriented mobile data communication**.
- Unlike GSM (which mainly carries voice), GPRS transmits **both voice and data** using the same physical radio channels but with a different logical structure.

GPRS builds on the existing GSM infrastructure with the addition of **GPRS Support Nodes (GSNs)**.



Main Components of GPRS Architecture

1. **Mobile Station (MS)**
    - Enhanced mobile devices capable of handling both GSM voice calls and GPRS data packets.
2. **Base Station Controller (BSC) + Packet Control Unit (PCU)**
    - BSC is part of GSM; GPRS adds **PCU** to route data signals to SGSN via the **FRI interface**.
3. **GPRS Support Nodes (GSN)**
    - **SGSN (Serving GPRS Support Node):** Handles packet delivery, mobility management, authentication, billing, and terminal registration.
    - **GGSN (Gateway GPRS Support Node):** Connects GPRS to external data networks (PDNs), stores user profiles, and manages data routing.
4. **Internal Backbone Network**
    - IP-based network enabling tunneling between SGSN and GGSN for secure data transfer.
5. **Mobility Support**
    - Includes **Attachment Procedure, Location Management, and Handoff Management**.
6. **Routing Area**
    - Smaller than GSM's location area, optimizing data routing.
7. **SMS in GPRS**
    - SMS works as in GSM but can be handled over GPRS for improved efficiency.

Benefits of GPRS

1. **Mobility:** Seamless voice and data communication on the move.
2. **Cost-Efficient:** Charges based on data usage, not time.
3. **Always-On Connectivity:** Immediate network access without repeated logins.
4. **Location-Based Services:** Provides localized content based on user position.
5. **Simple Billing:** Easier data-based billing compared to circuit-switched GSM.

Advantages of GPRS

1. **Always-on Connectivity:** Provides continuous data connection without repeated dial-up.
2. **High Data Rates:** Up to 171.2 kbps (higher than traditional GSM SMS or circuit-switched data).
3. **Efficient Spectrum Usage:** Uses packet-switching, only occupying bandwidth when data is sent.
4. **Cost-Effective:** Charges based on data volume (per KB/MB) rather than connection time.
5. **Supports Multimedia Services:** Enables MMS, WAP, mobile internet, and email.
6. **Backward Compatible:** Works with existing GSM infrastructure with minimal upgrades.
7. **Enables IoT/M2M Applications:** Used in early mobile IoT devices and telemetry systems.

Disadvantages of GPRS

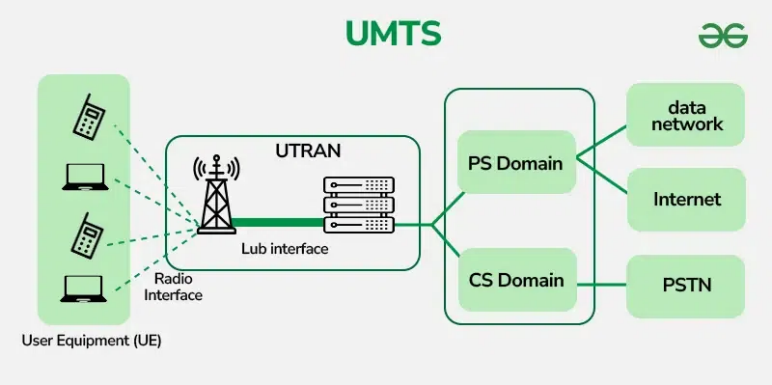
1. **Lower Data Speed:** Typical speed ranges between 56–114 kbps, much slower compared to modern 3G/4G networks.
2. **Variable Connection Quality:** Data transfer depends on network traffic and signal strength.
3. **Shared Bandwidth:** Multiple users share the same bandwidth, reducing individual speeds.
4. **High Latency:** Not suitable for real-time applications like high-quality video calls or online gaming.
5. **Limited Availability:** Cannot be used in areas without GSM infrastructure.
6. **Less Secure:** Vulnerable to certain security threats compared to newer technologies.
7. **No Guaranteed Data Delivery Time:** Because it is packet-switched, delays may occur

7. UMTS

- **UMTS (Universal Mobile Telecommunications System)** is a **third-generation (3G) mobile cellular system** based on the GSM standard.
- It provides **high-speed data transfer (up to 2 Mbps)** and supports **voice, video, and multimedia services** using **WCDMA (Wideband Code Division Multiple Access)** as its radio access technology.
- **Definition:** UMTS is a **third-generation (3G) mobile communication system** based on GSM, using **WCDMA technology** for high-speed voice, video, and data services.

- **Elements of UMTS:-**

UMTS consists of three major domains:



1. User Equipment (UE)

- Mobile device used by the subscriber.
- Contains:
  - **Mobile Equipment (ME):** The physical phone.
  - **USIM (Universal Subscriber Identity Module):** Stores user identity, authentication, and subscription details.

2. UMTS Terrestrial Radio Access Network (UTRAN)

- Manages the **radio interface** between the user equipment and the core network.
- Main components:
  - **Node B:** Similar to GSM Base Station, responsible for radio transmission/reception.
  - **RNC (Radio Network Controller):** Controls Node Bs, manages handover, admission control, and radio resource allocation.

3. Core Network (CN)

- Responsible for switching, routing, and connecting calls/data to external networks.
- Divided into:
  - **Circuit-Switched (CS) Domain:** Handles traditional voice services.
  - **Packet-Switched (PS) Domain:** Handles data services like internet browsing and multimedia.
  - **Databases:** HLR (Home Location Register), VLR (Visitor Location Register), AuC (Authentication Center), and EIR (Equipment Identity Register).

Applications of UMTS

- Streaming / Download (Video, Audio)
- Videoconferences.
- Fast Internet / Intranet.
- Mobile E-Commerce (M-Commerce)
- Remote Login
- Background Class applications
- Multimedia-Messaging, E-Mail
- FTP Access
- Mobile Entertainment (Games)

8.Routing in GSM

Routing in GSM refers to the **process of finding the path** for delivering calls, SMS, or data from the **calling party to the receiving subscriber** using GSM network components.

Steps in GSM Routing:

1. **Call Initiation:** When a call or message is initiated, the Mobile Switching Center (MSC) checks the **Home Location Register (HLR)** for subscriber details.
2. **HLR Query:** HLR provides the subscriber's location information by querying the **Visitor Location Register (VLR)** where the subscriber is currently registered.
3. **Routing Number Assignment:** The Gateway MSC (GMSC) obtains a **Mobile Station Roaming Number (MSRN)** from the VLR to establish the connection.
4. **Call Setup:** The MSC routes the call to the serving MSC/VLR where the subscriber is located.
5. **Delivery:** The call/SMS/data is delivered to the Base Station Subsystem (BSS), then to the Base Transceiver Station (BTS), and finally to the Mobile Station (MS).

Key Network Elements in Routing:

- **GMSC (Gateway MSC):** Entry point for calls/messages into the GSM network.
- **HLR:** Stores permanent subscriber information.
- **VLR:** Stores temporary location data of subscribers.
- **MSRN:** Temporary number for routing calls to roaming users.