UNIT 1

Mobile Computing Overview

Mobile Computing refers to the ability to use computing devices such as smartphones, tablets, laptops, and wearable technology while being mobile. It enables users to access data, applications, and services wirelessly from anywhere.

(OR)

Mobile Computing is an umbrella term used to describe technologies that enable People to access network services anyplace, anytime, and anywhere.

1. Key Components of Mobile Computing

1. **Mobile Devices** – Smartphones, tablets, laptops, PDAs, and wearable devices.
2. **Wireless Communication** – Technologies such as Wi-Fi, Bluetooth, cellular networks (3G, 4G, 5G), and satellite communication.
3. **Mobile Software** – Operating systems (Android, iOS, Windows), applications, and cloud computing services.

2. Characteristics of Mobile Computing

✅ **Portability** – Devices can be carried anywhere.
✅ **Ubiquity** – Access to computing resources from any location.
✅ **Connectivity** – Wireless access to the internet and networks.
✅ **Personalization** – Customized user experiences and settings.
✅ **Energy Efficiency** – Battery-powered operation with power-saving modes.

3. Technologies in Mobile Computing

🔹 **Wireless Communication Protocols** – Wi-Fi, Bluetooth, NFC (Near Field Communication).
🔹 **Cellular Networks** – 2G, 3G, 4G, 5G, LTE.
🔹 **Cloud Computing** – Data storage and computing services available remotely.
🔹 **IoT (Internet of Things)** – Connecting mobile devices to smart home appliances, vehicles, and other systems.
🔹 **Edge Computing** – Processing data near the source rather than relying on cloud computing.

4. Applications of Mobile Computing

📱 **Mobile Banking & Payments** – UPI, PayPal, Google Pay.
🚗 **Navigation & GPS Services** – Google Maps, Waze.
🎮 **Entertainment & Streaming** – Netflix, YouTube, Spotify.
📞 **Communication** – WhatsApp, Skype, Zoom.
🏥 **Healthcare & Telemedicine** – Remote patient monitoring, fitness apps.
🏦 **E-commerce & Online Shopping** – Amazon, Flipkart, eBay.

5. Advantages of Mobile Computing

✔️ **Increased Productivity** – Work from anywhere.
✔️ **Improved Communication** – Instant access to messaging and calls.
✔️ **Convenience & Accessibility** – Easy access to online services.
✔️ **Enhanced Learning** – E-learning platforms like Coursera, Udemy.

6. Challenges in Mobile Computing

❌ **Security Issues** – Hacking, malware, data breaches.
❌ **Battery Life** – Limited power supply.
❌ **Network Reliability** – Connectivity issues in remote areas.
❌ **Hardware Limitations** – Processing power and storage constraints.

APPLICATIONS OF MOBILE COMPUTING

In many fields of work, the ability to keep on the move is vital in order to utilize time efficiently. The importance of Mobile Computers has been highlighted in many fields of which a few are described below:

a. Vehicles:

Music, news, road conditions, weather reports, and other broadcast information are received via digital audio broadcasting (DAB) with 1.5 Mbit/s. For personal communication, a universal mobile telecommunications system (UMTS) phone might be available offering voice and data connectivity with 384 kbit/s. The current position of the car is determined via the global positioning system (GPS). Cars driving in the same area build a local ad-hoc network for the fast exchange of information in emergency situations or to help each other keep a safe distance. In case of an accident, not only will the airbag be triggered, but the police and ambulance service will be informed via an emergency call to a service provider. Buses, trucks, and trains are already transmitting maintenance and logistic information to their home base, which helps to improve organization (fleet management), and saves time and money.

b. Emergencies: An ambulance with a high-quality wireless connection to a hospital can carry vital information about injured persons to the hospital from the scene of the accident. All the necessary steps for this particular type of accident can be prepared and specialists can be consulted for an early diagnosis. Wireless networks are the only means of communication in the case of natural disasters such as hurricanes or earthquakes. In the worst cases, only decentralized, wireless ad-hoc networks survive.

c. Business: Managers can use mobile computers say, critical presentations to major customers. They can access the latest market share information. At a small recess, they can revise the presentation to take advantage of this information. They can communicate with the office about possible new offers and call meetings for discussing responds to the new proposals. Therefore, mobile computers can leverage competitive advantages. A travelling salesman today needs instant access to the company’s database: to ensure that files on his or her laptop reflect the current situation, to enable the company to keep track of all activities of their travelling employees, to keep databases consistent etc. With wireless access, the laptop can be turned into a true mobile office, but efficient and powerful synchronization mechanisms are needed to ensure data consistency.

d. Credit Card Verification: At Point of Sale (POS) terminals in shops and supermarkets, when customers use credit cards for transactions, the intercommunication required between the bank central computer and the POS terminal, in order to effect verification of the card usage, can take place quickly and securely over cellular channels using a mobile computer unit. This can speed up the transaction process and relieve congestion at the POS terminals.
e. Replacement of Wired Networks: wireless networks can also be used to replace wired networks, e.g., remote sensors, for tradeshows, or in historic buildings. Due to economic reasons, it is often impossible to wire remote sensors for weather forecasts, earthquake detection, or to provide environmental information. Wireless connections, e.g., via satellite, can help in this situation. Other examples for wireless networks are computers, sensors, or information displays in historical buildings, where excess cabling may destroy valuable walls or floors.

f. Infotainment: wireless networks can provide up-to-date information at any appropriate location. The travel guide might tell you something about the history of a building (knowing via GPS, contact to a local base station, or triangulation where you are) downloading information about a concert in the building at the same evening via a local wireless network. Another growing field of wireless network applications lies in entertainment and games to enable, e.g., ad-hoc gaming networks as soon as people meet to play together.

Limitations of Mobile Computing

Despite its numerous advantages, mobile computing has some limitations. These include:

1. Security Issues 🔒

- **Data Breaches & Hacking** – Wireless communication is more vulnerable to cyberattacks.
- **Unauthorized Access** – Lost or stolen devices can be misused.
- **Malware & Viruses** – Mobile applications can be infected with malicious software.

2. Battery Life 🔋

- Mobile devices rely on batteries, which have limited power.
- High-performance applications drain battery quickly.
- Charging facilities may not always be available.

3. Connectivity Problems 📶

- **Network Coverage Issues** – Poor signals in remote areas or inside buildings.
- **Latency & Speed Limitations** – Internet speed may vary depending on location and network congestion.
- **Interference** – Wireless signals can be affected by obstacles and weather conditions.

4. Limited Processing Power & Storage 🖥️

- Mobile devices have lower processing power compared to desktops.
- Limited RAM and storage restrict multitasking and large file processing.
- Heavy applications may slow down the device.

5. Small Screen Size & Input Limitations 📱

- Typing and data entry are difficult compared to a full-sized keyboard.
- Small screens can limit productivity and content visibility.
- Prolonged use may cause eye strain and discomfort.

6. Cost of Mobile Devices & Data Plans 💰

- High-end smartphones and tablets are expensive.
- Mobile data plans and roaming charges can be costly.
- Frequent upgrades and repairs add to expenses.

7. Compatibility Issues 🔄

- Not all mobile devices support the same applications or operating systems.
- Different screen sizes and hardware configurations create challenges for developers.

8. Environmental & Health Concerns 🌍

- E-waste generation due to frequent upgrading of mobile devices.
- Prolonged screen time can lead to health issues like eye strain and poor posture.
- Radiation concerns, though research is ongoing.

SIMPLIFIED REFERENCE MODEL IN MOBILE COMPUTING

A **Mobile Computing Reference Model** provides a structured way to understand how mobile systems function. A simplified version consists of **four main layers**:

1. User Layer (Application Layer) 👨‍💻

- **Interfaces & Apps** – Mobile applications (WhatsApp, YouTube, Maps, etc.).
- **User Interaction** – Touchscreens, voice commands, gestures.
- **Customization** – Settings, profiles, notifications.

🔹 **Example:** A user sends a message using WhatsApp.

2. Network Layer 📡

- **Wireless Communication** – Wi-Fi,
- , 4G, 5G, satellite.
- **Data Transmission** – How devices communicate over the internet.
- **Mobility Management** – Seamless switching between networks (Wi-Fi to mobile data).

🔹 **Example:** The message travels through Wi-Fi or mobile data to WhatsApp servers.

---

3. Middleware Layer 🔄

- **Cloud Services** – Data storage, backups, synchronization.
- **Security & Authentication** – Encryption, passwords, biometric authentication.
- **Resource Management** – Managing battery, processing power, and memory.

🔹 **Example:** WhatsApp encrypts and stores the message before sending it.

---

4. Hardware Layer 💻

- **Mobile Devices** – Smartphones, tablets, wearables.
- **Sensors & Processors** – GPS, accelerometer, fingerprint scanner.

- **Battery & Power Management** – Energy-efficient processing.

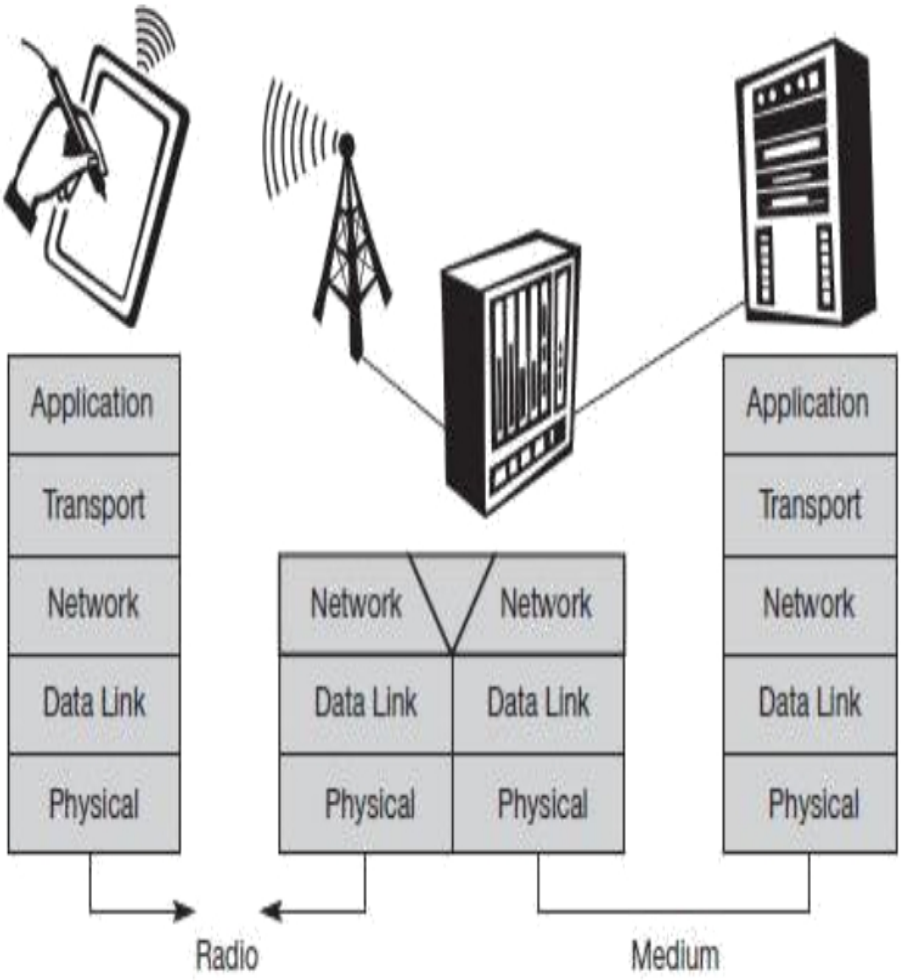
🔹 **Example:** The smartphone processes the message and sends it.

Summary Table

Layer	Function	Example
User Layer	Apps & User Interaction	WhatsApp, Google Maps
Network Layer	Wireless Communication	Wi-Fi, 4G, 5G
Middleware Layer	Security, Cloud, Authentication	Encryption, Cloud Storage
Hardware Layer	Mobile Devices & Sensors	Smartphones, GPS, Battery

How It Works Together?

❖ User sends a message (User Layer).
❖ Data is transmitted via the internet (Network Layer)
❖ Encryption & processing occur (Middleware Layer).
❖ The device hardware executes the process (Hardware Layer).



A Simplified Reference Model

● Physical layer:

❖ This is the lowest layer in a communication system and is responsible for the conversion of a stream of bits into signals that can be transmitted on the sender side. The physical layer of the receiver then transforms the signals back into a bit stream. For wireless communication, the physical layer is responsible for frequency selection, generation of the carrier frequency, signal detection (although heavy interference may disturb the signal), modulation of data onto a carrier frequency and (depending on the transmission scheme) encryption.

❖ ● Data link layer:

❖ The main tasks of this layer include accessing the medium, multiplexing of different data streams, correction of transmission errors, and synchronization (i.e., detection of a data frame). Altogether, the data link layer is responsible for a reliable point-to-point

❖ Connection between two devices or a point-to-multipoint connection between one sender and several receivers.

● Network layer:

❖ This third layer is responsible for routing packets through a network or establishing a connection between two entities over many other intermediate systems. Important functions are addressing, routing, device location, and handover between different networks.

❖ ● Transport layer:

This layer is used in the reference model to establish an end-to-end connection

❖

● Application layer:

Finally, the applications (complemented by additional layers that can support applications) are situated on top of all transmission oriented layers. Functions are service location, support for multimedia applications, adaptive applications that can handle the large variations in transmission characteristics, and wireless access to the world-wide web using a portable device.

Middleware Layer in Mobile Computing

The **Middleware Layer** acts as a bridge between the **hardware/network layers** and the **application/user layers**. It provides essential services like security, communication, resource management, and cloud integration, making mobile applications work efficiently across different devices and networks.

Key Functions of the Middleware Layer

1 Security & Authentication 🔐

- **Encryption & Decryption** – Protects data during transmission (e.g., end-to-end encryption in WhatsApp).
- **User Authentication** – Passwords, biometrics (fingerprint, facial recognition).
- **Access Control** – Determines who can access certain resources.

✅ **Example:** When logging into a banking app, the middleware verifies the user via fingerprint or OTP.

---

2 Data Synchronization & Cloud Services ☁️

- Ensures **real-time data updates** across multiple devices.
- Provides **cloud backup & storage** (Google Drive, iCloud).
- Manages **offline access** and updates when reconnected.

✅ **Example:** Google Docs allows users to edit offline and sync changes when back online.

---

3 Resource Management & Optimization ⚡

- **Manages power consumption** to extend battery life.
- Allocates **processing power and memory** efficiently.
- Controls **bandwidth usage** to optimize network performance.

✅ **Example:** A mobile game adjusts graphics quality based on the device's processing power.

---

4 Communication & Interoperability 🔄

- Allows **different applications and devices** to communicate.

- Supports **APIs** that enable apps to interact with services like Google Maps, PayPal, or Bluetooth devices.
- Provides **cross-platform compatibility** (Android, iOS, Windows).

✅ **Example:** A food delivery app integrates Google Maps for tracking.

Importance of Middleware in Mobile Computing

✔️ Enhances **security** and **data privacy**.
✔️ Improves **app performance** by managing resources.
✔️ Enables **seamless communication** between apps, devices, and networks.
✔️ Supports **cross-platform compatibility** for different operating systems.

The middleware layer is crucial in ensuring smooth, secure, and efficient mobile computing experiences

Radio in Mobile Computing

In mobile computing, **radio communication** plays a crucial role in enabling wireless connectivity between mobile devices and networks. Radios are embedded in smartphones, tablets, and other mobile devices to facilitate **data transmission** over various wireless technologies.

---

1. Types of Radio Technologies in Mobile Computing

1 Cellular Networks 📶

- **2G (GSM, CDMA)** – Basic voice and SMS services.
- **3G (UMTS, HSPA)** – Improved speed, video calling, and internet access.
- **4G (LTE, WiMAX)** – High-speed internet, HD video streaming.
- **5G** – Ultra-fast data, low latency, IoT connectivity.

✅ **Example:** Smartphones use LTE or 5G for internet access when Wi-Fi is unavailable.

---

2 Wi-Fi (Wireless Fidelity) 🌐

- Uses **radio waves (2.4 GHz, 5 GHz, and 6 GHz)** for wireless internet.
- Faster than cellular networks but limited to a specific area (hotspots).

✅ **Example:** Laptops and smartphones connect to the internet via home or public Wi-Fi.

---

3 Bluetooth 🔵

- Short-range **(10–100 meters)** wireless communication.
- Used for **file transfer, wireless headphones, IoT devices**.

✅ **Example:** Connecting wireless earbuds to a smartphone.

---

4 NFC (Near Field Communication) 📲

- Very short-range (a few centimeters) communication.
- Used in **contactless payments (Google Pay, Apple Pay), access control, data sharing**.

✅ **Example:** Paying for groceries using a smartphone at a contactless payment terminal.

---

5 Satellite Communication 🛰️

- Uses satellites to provide network access in **remote areas**.
- Common in **GPS navigation, military applications, disaster recovery**.

✅ **Example:** Google Maps uses GPS satellites for location tracking.

---

2. Role of Radio in Mobile Computing

- **Provides wireless communication** for mobile devices.
- **Ensures mobility** by enabling internet access anywhere.
- **Supports IoT & smart devices** by connecting them wirelessly.
- **Enables secure & fast data transmission** through encryption techniques.

---

3. Challenges of Radio Communication in Mobile Computing

❌ **Interference** – Signals can be affected by obstacles (walls, buildings, weather).
❌ **Limited Range** – Bluetooth and NFC work only within short distances.
❌ **Power Consumption** – Continuous use of Wi-Fi or mobile networks drains battery.
❌ **Security Risks** – Public Wi-Fi and Bluetooth connections are vulnerable to hacking.

Bluetooth in Mobile Computing

Bluetooth is a short-range wireless communication technology used in mobile computing to exchange data between devices. It operates on **radio waves** in the **2.4 GHz ISM (Industrial, Scientific, and Medical) band**, allowing devices to connect without cables.

1. Features of Bluetooth in Mobile Computing

✔️ **Short-Range Communication** – Typically **10 meters** (can extend up to 100 meters in some versions).
✔️ **Low Power Consumption** – Optimized for mobile devices to save battery.
✔️ **Wireless Connectivity** – Eliminates the need for physical cables.
✔️ **Secure Communication** – Uses encryption and authentication.
✔️ **Automatic Device Discovery** – Devices detect and pair with each other.

---

2. Bluetooth Versions & Data Speeds

Bluetooth Version	Speed (Mbps)	Range	Features
Bluetooth 1.0 & 1.2	1 Mbps	10 m	Basic wireless connectivity
Bluetooth 2.0 + EDR	3 Mbps	10 m	Faster data transfer
Bluetooth 3.0 + HS	24 Mbps	10 m	High-speed data transfer
Bluetooth 4.0	1 Mbps	50 m	Low Energy (BLE) support
Bluetooth 5.0	2 Mbps	200 m	Faster, longer range, IoT support
Bluetooth 5.1 & 5.2	2 Mbps	400 m	Location tracking, better energy efficiency
Bluetooth 5.3 & 5.4	2 Mbps	400 m	Improved security & reliability

3. Applications of Bluetooth in Mobile Computing

📡 1. Wireless Peripherals

- Connecting **keyboards, mice, printers, and game controllers** to mobile devices.
  ✅ **Example:** Using a Bluetooth mouse with a tablet.

🎧 2. Audio & Entertainment

- **Wireless headphones, speakers, car audio systems**.
  ✅ **Example:** Listening to music on AirPods connected via Bluetooth.

📲 3. File Transfer & Communication

- **Sharing files** between mobile devices (e.g., Android's Bluetooth sharing).
  ✅ **Example:** Sending a photo from one phone to another.

🏠 4. Smart Home & IoT Integration

- **Smart locks, lights, and thermostats** controlled via Bluetooth.
  ✅ **Example:** Unlocking a smart door lock using a mobile phone.

🚗 5. Automotive & Navigation

- Hands-free calling, music streaming, and car diagnostics.
  ✅ **Example:** Connecting a smartphone to a car's infotainment system.

---

4. Advantages of Bluetooth in Mobile Computing

✔️ **No Internet Required** – Works offline without Wi-Fi or mobile data.
✔️ **Energy Efficient** – Low-power Bluetooth (BLE) supports battery-powered IoT devices.
✔️ **Universal Compatibility** – Works across all major mobile operating systems (Android, iOS, Windows).
✔️ **Secure Connection** – Uses encryption and authentication for data safety.

---

5. Limitations of Bluetooth

❌ **Limited Range** – Typically **10–100 meters** depending on the version.
❌ **Slower Speed** – Compared to Wi-Fi or 5G, data transfer is slower.
❌ **Interference Issues** – Can be affected by other devices using the 2.4 GHz frequency (e.g., Wi-Fi).
❌ **Security Risks** – Vulnerable to hacking (e.g., Bluetooth-based attacks like "Bluejacking" and "Bluesnarfing").

---

6. Future of Bluetooth in Mobile Computing

🚀 **Bluetooth 5.4 & Beyond** – More power efficiency, better range, and enhanced security.
📡 **Bluetooth Mesh Networking** – Supports IoT networks for smart homes & industrial automation.
🔋 **Ultra-Low Power Devices** – Optimized for wearable tech and medical devices.

Bluetooth is a **critical wireless technology** in mobile computing, providing **seamless connectivity** between devices for communication, entertainment, and smart applications. Its continuous evolution enhances **speed, security, and efficiency**, making it an essential component of modern mobile technology.

GENERATION OF MOBILE SERVICES

The generation of mobile it is divided into five categories.

First generation (1G) TECHNOLOGY

It is the first generation of the wireless mobile communication where analogy signal were used to transmit data .it was introduced in 1980s designed for voice communication.

Characteristics of 1G.

1.Speed it was 2.4 kbps

2.poor voice

3.low betry life

Second generation(2G) TECHNOLOGY

It is the second generation which used digital signal for the first time.

It was launched in finland 1991 and used GSM technology.

Characteristics of 2G.

1.Data speed up to 64 kbps

2.text and multimedia messaging was innovated

3.Better quality than 1G

When GPRS TECHNOLOGY was introduced it enabled web browsing,email service and fast to uploading/download speed.

2G+GPRS=2.5G

3G TECHNOLOGY

It was advanced than 1G and 2G.

Characteristics of 3G

1.Data speed of 144kbps to 2Mbps

2.High speed of web browsing

3.running web based like video conferencing

4.fast and easy file and data transfer like video and audio.

5.3D gamming

4G technology

It was more advanced more the other generation,it has high quality and speed of data transfer.

The basic term used to describes the 4G is magic.

M Mobile multimedia

A Anytime Anywhere

G Global Mobility support

I Intergrated wireless solution

C Customised Personal service

Characteristics

1.speed of 100Mbps to 1Gbps

2.Mobile web access

3.High definition mobile Tv

4.Cloud computing

5.VOIp technology

5G technology

It is highly supportable to WWWW(wireless world wide web)

It is complete wireless communication with almost no limitation

Characteristics of 5G

1.High speed,high capacity of data transfer

2.providing large broadcasting of data in GBs

3.Multmedia,newpaper,watch tv programs with HD quality.

4.faster transmission,large phone memory

GSM PRINCIPLES AND ARCHITECTURE:-

GSM & ITS HISTORY

Global System for Mobile (GSM) is a second generation cellular standard developed to cater voice services and data delivery using digital modulation. It is a digital cellular technology used for transmitting mobile voice and data services. GSM is the most widely accepted standard in telecommunications and it is implemented globally. GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals. GSM provides basic to advanced voice and data services including roaming service. Roaming is the ability to use your GSM phone number in another GSM network. GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates. GSM digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own timeslot.

• The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.

• Conference of European Posts and Telegraph (CEPT) establishes a GSM group to widen the standards for a pan-European cellular mobile telephone system in 1982. GSM is named as "Global System for Mobile communication" in 1989. In year 2000, General Packet Radio Service (GPRS) came into existence.

• GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.

Presently GSM supports more than one billion mobile subscribers in more than 210 countries Through out the world.

GSM SERVICES

• Tele-services:- Telecommunication services that enable voice communication via mobile phones. Offered services like Mobile telephony & Emergency calling.

• Bearer or Data Services:- Include various data services for information transfer between GSM and other networks like PSTN, ISDN etc . Short Message Service (SMS) up to 160 character alphanumeric data transmission to/from the mobile terminal & Voice mailbox.

• Supplementary services:-

- Call Waiting- Notification of an incoming call while on the handset
- Call Hold- Put a caller on hold to take another call
- Call Barring- 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

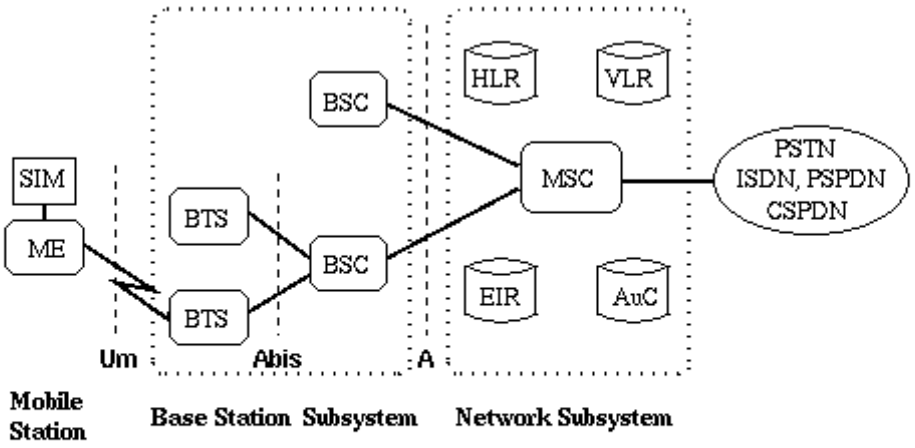
Listed below are the features of GSM that account for its popularity and wide acceptance.

Improved spectrum efficiency with High-quality speech & International roaming

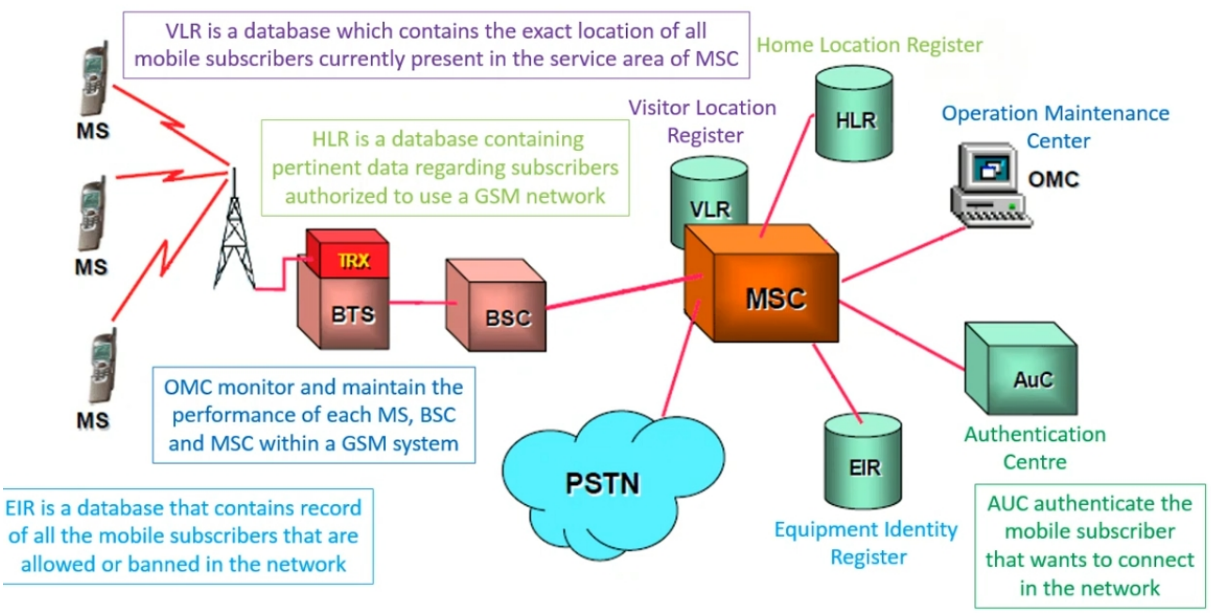
Low-cost mobile sets and base stations (BSs)

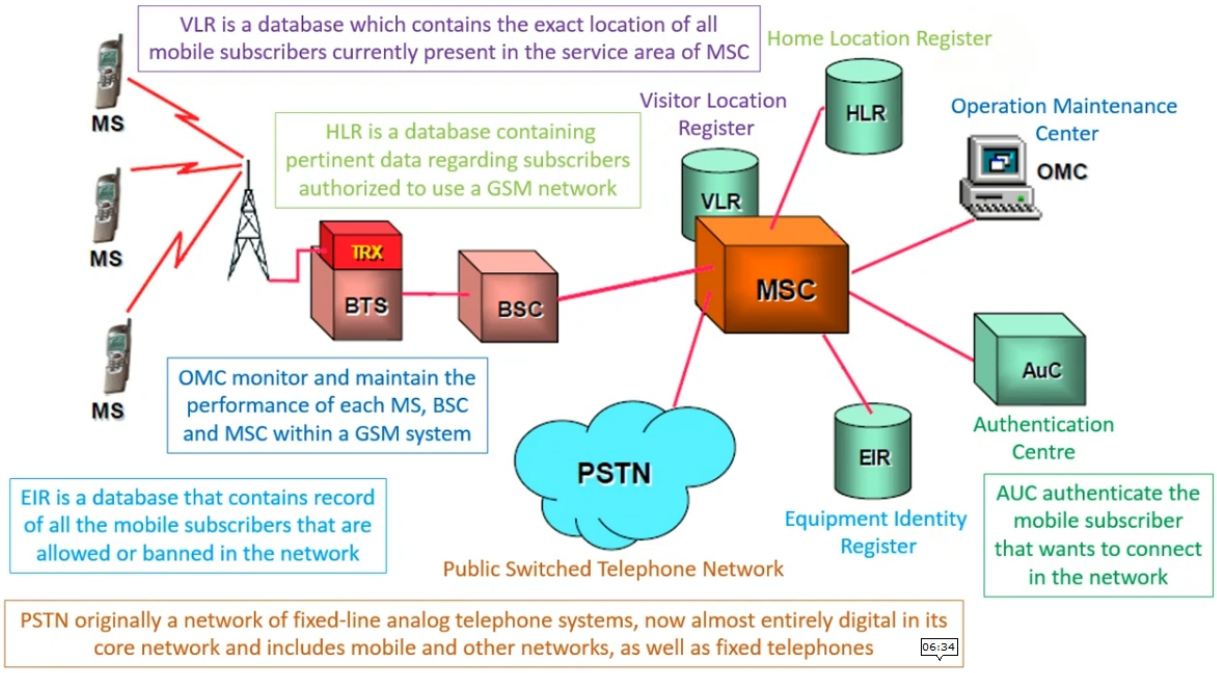
Compatibility with Integrated Services Digital Network (ISDN) and other telephone company services. Support for new services

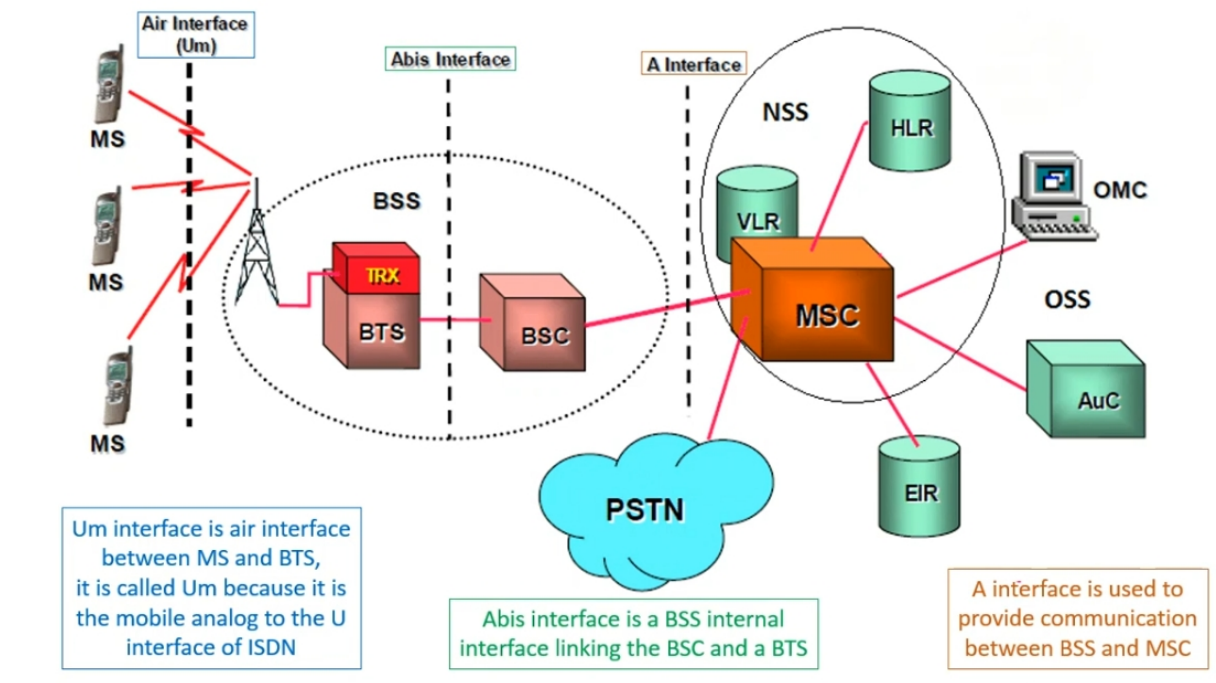
GSM SYSTEM ARCHITECTURE



SIM Subscriber Identity Module
ME Mobile Equipment
BTS Base Transceiver Station
BSC Base Station Controller
HLR Home Location Register
VLR Visitor Location Register
MSC Mobile services Switching Center
EIR Equipment Identity Register
AuC Authentication Center




VLR is a database which contains the exact location of all mobile subscribers currently present in the service area of MSC
Home Location Register
Visitor Location Register
HLR is a database containing pertinent data regarding subscribers authorized to use a GSM network
Operation Maintenance Center
OMC
MS
MS
MS
TRX
BTS
BSC
VLR
HLR
MSC
AuC
Authentication Centre
OMC monitor and maintain the performance of each MS, BSC and MSC within a GSM system
PSTN
EIR
Equipment Identity Register
EIR is a database that contains record of all the mobile subscribers that are allowed or banned in the network
Public Switched Telephone Network
AUC authenticate the mobile subscriber that wants to connect in the network
PSTN originally a network of fixed-line analog telephone systems, now almost entirely digital in its core network and includes mobile and other networks, as well as fixed telephones
06:34


Air Interface (Um)
Abis Interface
A Interface
MS
MS
MS
BSS
TRX
BTS
BSC
NSS
HLR
VLR
MSC
OMC
OSS
AuC
EIR
PSTN
Um interface is air interface between MS and BTS, it is called Um because it is the mobile analog to the U interface of ISDN
Abis interface is a BSS internal interface linking the BSC and a BTS
A interface is used to provide communication between BSS and MSC

The GSM network architecture consists of three major subsystems:-
Mobile Station (MS)
- Mobile Equipment (ME)
- Subscriber Identity Module (SIM)

Base Station Subsystem (BSS)
- Base Transceiver Station (BTS)
- Base Station Controller (BSC)

Network Switching Sub system(NSS)
- Mobile Switching Center (MSC)
- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Authentication Center (AUC)
- Equipment Identity Register (EIR)

In a GSM network, the following areas are defined:

Cell : Cell is the basic service area; one BTS covers one cell. Each cell is given a Cell Global Identity (CGI), a number that uniquely identifies the cell.

Location Area : A group of cells form a Location Area (LA). This is the area that is paged when a subscriber gets an incoming call. Each LA is assigned a Location Area Identity (LAI). Each LA is served by one or more BSCs.

MSC/VLR Service Area : The area covered by one MSC is called the MSC/VLR service area.

PLMN : The area covered by one network operator is called the Public Land Mobile Network (PLMN). A PLMN can contain one or more MSCs.

The wireless link interface between the MS and the Base Transceiver Station (BTS), which is a part of BSS. Many BTSs are controlled by a Base Station Controller (BSC). BSC is connected to the Mobile Switching Center (MSC), which is a part of NSS. Above Figure shows the key functional elements in the GSM network architecture.

1. Mobile Station (MS):

A mobile station communicates across the air interface with a base station transceiver in the same cell in which the mobile subscriber unit is located. The MS communicates the information with the user and modifies it to the transmission protocols if the air-interface to communicate with the BSS. The user’s voice information is interfaced with the MS through a microphone and speaker for the speech, keypad, and display for short messaging, and the cable connection for other data terminals. The MS has two elements. The Mobile Equipment (ME) refers to the physical device, which comprises of transceiver, digital signal processors, and the antenna. The

second element of the MS is the GSM is the Subscriber Identity Module (SIM). The SIM card is unique to the GSM system. It has a memory of 32 KB.

2. Base Station Subsystem (BSS):

A base station subsystem consists of a base station controller and one or more base transceiver station. Each Base Transceiver Station defines a single cell. A cell can have a radius of between 100m to 35km, depending on the environment. A Base Station Controller may be connected with a BTS. It may control multiple BTS
units and hence multiple cells. There are two main architectural elements in the BSS – the Base Transceiver Subsystem (BTS) and the Base Station Controller (BSC). The interface that connects a BTS to a BSC is called the A-bis interface. The interface between the BSC and the MSC is called the A interface, which is standardised within GSM.

3. Network and switching subsystem (NSS):

The NSS is responsible for the network operation. It provides the link between the cellular network and the Public switched telecommunicates Networks (PSTN or ISDN or Data Networks). The NSS controls handoffs between cells in different BSSs, authenticates user and validates their accounts, and includes functions for enabling worldwide roaming of mobile subscribers. The MSC basically performs the switching function of the system by controlling calls to and from other telephone and data systems. It includes functions such as network interfacing and common channel signalling. The NSS has one hardware, Mobile switching center and four software database element: Home location register (HLR), Visitor location Register (VLR), Authentications center (Auc) and Equipment Identity Register (EIR). In particular the switching subsystem consists of:

- Mobile switch center (MSC)
- Home location register (HLR)
- Visitor location Register (VLR)
- Authentications center (Auc)
- Equipment Identity Register (EIR)
- Interworking Functions (IWF)

HLR: The HLR is database software that handles the management of the mobile subscriber account. It stores the subscriber address, service type, current locations, forwarding address, authentication/ciphering keys, and billings information. In addition to the ISDN telephone number for the terminal, the SIM card is identified with an International Mobile Subscribes Identity (IMSI) number that is totally different from the ISDN telephone number. The HLR is the reference database that permanently stores data related to subscribers, including subscriber's service profile, location information, and activity status.

VLR: The VLR is temporary database software similar to the HLR identifying the mobile subscribers visiting inside the coverage area of an MSC. The VLR assigns a Temporary mobile subscriber Identity (TMSI) that is used to avoid using IMSI on the air. The visitor location register maintains information about mobile subscriber that is currently physically in the range covered by the switching center. When a mobile subscriber roams from one LA (Local Area) to another, current location is automatically updated in the VLR. When a mobile station roams into a new MSC area, if the old and new LA's are under the control of two different VLRs, the VLR connected to the MSC will request data about the mobile stations from the HLR.

The entry on the old VLR is deleted and an entry is created in the new VLR by copying the database from the HLR.
AuC: The AuC database holds different algorithms that are used for authentication and encryptions of the mobile subscribers that verify the mobile user's identity and ensure the confidentiality of each call. The AuC holds the authentication and encryption keys for all the subscribers in both the home and visitor location register.
EIR: The EIR is another database that keeps the information about the identity of mobile equipment such the International mobile Equipment Identity (IMEI) that reveals the details about the manufacturer, country of production, and device type. This information is used to prevent calls from being misused, to prevent unauthorised or defective MSs, to report stolen mobile phones or check if the mobile phone is operating according to the specification of its type.
White list: This list contains the IMEI of the phones who are allowed to enter in the network.
Black list: This list on the contrary contains the IMEI of the phones who are not allowed to enter in the network, for example because they are stolen.
Grey list: This list contains the IMEI of the phones momentarily not allowed to enter in the network, for example because the software version is too old or because they are in repair.
IWF- It is a system in the PLMN that allows for non speech communication between the GSM and the other networks. The tasks of an IWF are particularly to adapt transmission parameters and protocol conversions. The physical manifestations of an IWF may be through a modem which is activated by the MSC dependent on the bearer service and the destination network. The OSS (Operational Support Systems) supports operation and maintenance of the system and allows engineers to monitor, diagnose, and troubleshoot every aspect of the GSM network.

IMEI (International Mobile Equipment Identity)

IMEI (International Mobile Equipment Identity) is a **unique 15-digit identifier** assigned to each mobile device. It is used to identify, track, and authenticate mobile devices on a network.

---

1. IMEI Structure (15 Digits)

IMEI is divided into several parts:

Section	Digits	Description
TAC (Type Allocation Code)	First 8 digits	Identifies the device model and manufacturer.
SN (Serial Number)	Next 6 digits	Unique identifier for the device.
Check Digit	Last 1 digit	Used for validation (Luhn algorithm).

✅ **Example IMEI:** `359420055432177`

- **TAC:** `35942005` → Identifies the phone model.
- **SN:** `543217` → Unique to this phone.
- **Check Digit:** `7` → Used for verification.

---

2. How to Find IMEI on a Mobile Device

📱 **Dial Code:** `*#06#` (Displays IMEI on most phones).
📱 **Settings:** Go to `Settings > About Phone > IMEI`.
📱 **On Device:** Printed inside the battery compartment or SIM tray.

---

3. Functions of IMEI

1 Device Identification

- Networks use IMEI to **identify a device model and origin**.
- Helps in managing **warranty and support** services.

2 Security & Anti-Theft Protection

- **Blacklisting:** If a phone is **stolen**, its IMEI can be **blocked** by networks, making it unusable.
- **Tracking:** Law enforcement can use IMEI to track lost or stolen phones.

✅ **Example:** If a stolen phone's IMEI is blacklisted, it won't work on any network worldwide.

3 🔒SIM-Locking & Unlocking

- Carriers lock devices to a network using IMEI.
- Unlocking requires **IMEI-based authorization** from the carrier.

✅ **Example:** If you switch from AT&T to T-Mobile, you may need an IMEI unlock code.

---

4. IMEI vs. IMSI

IMEI (Device ID)	IMSI (Subscriber ID)
Identifies the **device**.	Identifies the **SIM card (user)**.
Stored in the **phone hardware**.	Stored in the **SIM card**.
Cannot be changed easily.	Can change when SIM is replaced.

5. IMEI Tampering & Legal Issues

❌ **IMEI Spoofing (Illegal in many countries)** – Changing IMEI to avoid blacklisting.
❌ **IMEI Cloning** – Copying a valid IMEI onto another device (used in phone fraud).
❌ **IMEI Tracking & Privacy** – Governments and agencies can track devices using IMEI.

✅ **Solution:** Use official carriers and report lost/stolen devices immediately.

Conclusion

IMEI is a **critical security and identification tool** in mobile computing. It helps **track stolen devices, prevent fraud, and authenticate mobile phones** on global networks.

GPRS Transmission Plane Protocol Reference Model

GPRS (General Packet Radio Service) is an **extension of GSM** that enables packet-switched data transmission for mobile internet access. The **GPRS transmission plane** deals with the actual **data transfer process**, ensuring that packets move efficiently across the network.

---

1. GPRS Protocol Reference Model

GPRS follows a layered architecture similar to GSM but includes **packet-switching capabilities**. It consists of **two planes**:

- **Control Plane** – Manages signaling, session establishment, and mobility.
- **Transmission (User) Plane** – Handles actual data transfer (IP packets).

The **Transmission Plane Protocol Stack** consists of **five key layers**:

---

2. GPRS Transmission Plane Layers

Layer	Protocol	Function
Application Layer	HTTP, FTP, Email	User services like web browsing, email, file transfers.
Transport Layer	TCP/UDP	Ensures reliable (TCP) or fast (UDP) data delivery.
Network Layer	IP (IPv4/IPv6)	Routes data packets between mobile devices and servers.
GPRS Tunneling Protocol (GTP-U)	GTP-U	Tunnels user data over the core network.
Link Layer	LLC, RLC	Error correction, segmentation, retransmission.
Physical Layer	GSM Radio	Transmits data over radio frequencies.

3. Explanation of Each Layer

1 Application Layer (HTTP, FTP, Email)

- Provides **internet services** (browsing, messaging, file transfers).
  ✅ **Example:** Accessing a website using mobile internet.

2 Transport Layer (TCP/UDP)

- **TCP:** Ensures **error-free delivery** for reliable data (e.g., emails, file downloads).
- **UDP:** Provides **faster, connectionless** delivery (e.g., live streaming).
  ✅ **Example:** TCP is used for a secure banking transaction, UDP for watching a video.

3 Network Layer (IP)

- Assigns **IP addresses** to mobile devices.
- Routes packets between **mobile users and internet servers**.
  ✅ **Example:** When a mobile user opens Google, the request is routed via an IP address.

4 GPRS Tunneling Protocol (GTP-U)

- **GTP-U (User Plane):** Transfers user data through the **GPRS core network**.
- **Tunnels packets** between network elements (SGSN & GGSN).
  ✅ **Example:** A user streaming a video sends data through a GTP tunnel to the internet.

5 Link Layer (LLC, RLC, MAC)

- **LLC (Logical Link Control):** Manages encryption & error handling.
- **RLC (Radio Link Control):** Splits data into smaller packets for transmission.
- **MAC (Medium Access Control):** Manages wireless channel access.
  ✅ **Example:** If there's interference, RLC retransmits lost packets.

6 Physical Layer (GSM Radio)

- Converts digital data into **radio signals** for transmission over GPRS.
  ✅ **Example:** A smartphone sends data via **radio waves** to the nearest cell tower.

---

4. Data Flow in GPRS Transmission Plane

1. A user **requests a webpage** (Application Layer).
2. The request is **packetized** and assigned an **IP address** (Network Layer).
3. The **GTP-U tunnel** sends the data through the **GPRS core network**.
4. The **link layer** handles **error detection** and **retransmissions** if needed.
5. The **physical layer** transmits the data via radio waves to the base station.
6. The request reaches the internet, and the **webpage is loaded** on the mobile device.

---

5. Advantages of GPRS Transmission Plane

✔️ **Packet-Switched Technology** – Efficient use of network resources.
✔️ **Always-On Connectivity** – Users don't need to dial in (like circuit-switched data).
✔️ **Supports Multiple Applications** – Browsing, email, streaming, gaming.
✔️ **Global Reach** – Works on GSM networks worldwide.

---

6. Limitations of GPRS Transmission Plane

❌ **Lower Speed (56–114 Kbps)** – Much slower than 3G, 4G, and 5G.
❌ **Latency Issues** – Not suitable for real-time applications.
❌ **Shared Bandwidth** – Speed depends on network congestion.

Conclusion

The **GPRS transmission plane protocol reference model** defines how data is transferred efficiently using a **layered approach**. It uses **packet-switching, tunneling (GTP-U), and error correction** to provide mobile internet over GSM networks.

‘A base staton subsystem GPRS protocol (BSSGP) is used to convey routing and QoS-related informaton between the BSS and SGSN. BSSGP does not perform error correction and works on top of a frame relay (FR) network. Finally, radio link dependent protocols are needed to transfer data over the U_m interface. The radio link protocol (RLC) provides a reliable link, while the MAC controls access with signaling procedures for the radio channel and the mapping of LLC frames onto the GSM physical channels. The radio interface at U_m needed for GPRS does not require fundamental changes compared to standard GSM.

Quality of Service (QoS) in Mobile Computing

Quality of Service (QoS) refers to the ability of a mobile network to **prioritize and manage traffic** efficiently, ensuring that different types of data receive appropriate levels of **performance, speed, and reliability**.

In mobile computing, QoS is crucial for applications such as **voice calls, video streaming, gaming, and cloud computing**, where delays or data loss can degrade the user experience.

---

1. Key Parameters of QoS

QoS Parameter	Definition	Impact on Mobile Computing
Bandwidth	Maximum data transfer rate (measured in Mbps/Gbps).	Higher bandwidth enables faster internet speeds.
Latency (Delay)	Time taken for a data packet to travel from sender to receiver.	Low latency is critical for real-time applications (e.g., video calls, gaming).
Jitter	Variation in packet arrival times.	High jitter affects voice and video quality (causing lag and buffering).
Packet Loss	Percentage of data packets lost in transmission.	Packet loss leads to dropped calls, video freezes, and slow loading times.
Throughput	Actual data transmission rate at a given time.	Higher throughput improves browsing, downloads, and streaming.
Reliability	Consistency of network performance over time.	Essential for mission-critical applications like online banking and IoT.

2. QoS in Different Mobile Networks

Network Type	QoS Characteristics
GSM (2G)	Basic voice and SMS; no high-speed internet.
GPRS/EDGE (2.5G)	Low-speed mobile data (56–384 Kbps).
3G (UMTS, HSPA)	Moderate-speed internet (up to 42 Mbps).
4G (LTE, LTE-A)	High-speed data, HD video streaming, VoLTE.
5G	Ultra-low latency, high bandwidth, IoT and AI support.

3. QoS Mechanisms in Mobile Networks

1 Traffic Prioritization & Differentiation.

- **Voice & video traffic** get higher priority than background downloads.
- **Streaming services** use adaptive bit-rate (ABR) to adjust quality dynamically.

✅ **Example:** Video calls on 4G/5G use **VoLTE (Voice over LTE)** for **better quality** and **low latency**.

---

2 QoS Classes in GPRS, 3G, 4G, and 5G

QoS Class	Traffic Type	Delay Sensitivity	Example Application
Conversational	Real-time, two-way	Very sensitive	Voice calls, video conferencing
Streaming	One-way, continuous	Moderately sensitive	YouTube, Netflix
Interactive	User-driven	Somewhat sensitive	Web browsing, online gaming
Background	Low-priority	Not sensitive	Email, software updates

3 Packet Scheduling & Traffic Shaping

- Ensures that **real-time services (voice, video) get lower delays**.
- **Load balancing** prevents network congestion by distributing traffic.

✅ **Example: 5G networks** use **Network Slicing** to create **customized QoS levels** for different users (e.g., ultra-reliable IoT vs. HD gaming).

---

4. QoS Challenges in Mobile Computing

❌ **Network Congestion** – High traffic can degrade performance.
❌ **Handover Delays** – Switching between towers affects QoS.
❌ **Interference** – Obstacles, weather, and other signals impact signal quality.
❌ **Power Constraints** – Mobile devices have limited battery life.

---

5. QoS Optimization Techniques

🚀 **Traffic Prioritization:** Assigns higher priority to important applications.
🚀 **Bandwidth Management:** Allocates resources dynamically based on network load.
🚀 **Edge Computing:** Reduces latency by processing data closer to users.
🚀 **5G Network Slicing:** Creates dedicated virtual networks for different services.

QoS is essential for **delivering smooth and efficient mobile computing experiences**. It ensures **fast, reliable, and secure** data transmission for various applications, from **voice calls and streaming to IoT and cloud computing**.