GSM System Architecture Overview

GSM (Global System for Mobile Communication) is a technology used for mobile phones. Think of it like a big system that helps your phone make calls, send texts, and connect to the internet. It works using radio frequencies and is divided into three main parts: the Base Station Subsystem (BSS), Network Switching Subsystem (NSS), and Operational Support Subsystem (OSS). There's also the Mobile Station (MS), which is your phone.

1. Mobile Station (MS)

Your phone is a Mobile Station. It's divided into two parts:

A. **Mobile Equipment (ME)**:

- **Example**: Your smartphone.
- It's the device you hold in your hand, uniquely identified by an IMEI number (like a unique ID for your phone).
- It lets you make calls, send texts, and connect to the internet. It also checks the signal strength to give you the best connection.

B. **Subscriber Identity Module (SIM)**:

- **Example**: The SIM card inside your phone.
- It's a small card that holds your phone number and other important details.
- It lets you make and receive calls and use mobile services. You can move your SIM card to another phone if needed.

2. Base Station Subsystem (BSS)

This part handles the communication between your phone and the rest of the network.

A. **Base Transceiver Station (BTS)**:

- **Example**: A cell tower.
- It sends and receives signals from your phone.
- It handles the technical stuff like encoding and encrypting the signals.

B. **Base Station Controller (BSC)**:

- **Example**: The manager of multiple cell towers.
- It manages the radio resources for the BTS.
- It assigns frequencies and time slots to your phone and handles call setup and handovers (when you move from one cell tower to another).

3. Network Switching Subsystem (NSS)

This part manages the main switching functions and connects your calls to other networks.

A. **Mobile Switching Centre (MSC)**:

- **Example**: The heart of the network.
- It connects your call to another person's phone, whether they are on the same network or a different one.
- It handles call setup, routing, and mobility management (like registration and location updates).

B. **Home Location Register (HLR)**:

- **Example**: A permanent database of subscribers.
- It stores information about you, like your phone number and services you use.

C. **Visitor Location Register (VLR)**:

- **Example**: A temporary database.
- It stores information about your phone when you're in a different area, making sure you can still receive calls and texts.

D. **Authentication Centre (AuC)**:

- **Example**: A security system.
- It protects your phone's connection from intruders by checking your identity.

E. **Equipment Identity Register (EIR)**:

- **Example**: A list of phones.
- It tracks phones using their IMEI number and can blacklist stolen phones.

4. Operational Support Subsystem (OSS)

This part supports the operation and maintenance of the GSM network.

- **Example**: The tech support team.
- It helps engineers monitor and troubleshoot the network.
- It manages billing, hardware maintenance, and overall network performance.

Putting It All Together

Imagine you're calling your friend. Here's how it works:

1. Your phone (MS) uses the SIM card to connect to the nearest cell tower (BTS).
2. The cell tower (BTS) communicates with the Base Station Controller (BSC) to manage the connection.
3. The call is routed through the Mobile Switching Centre (MSC) to connect to your friend's phone.
4. The HLR and VLR databases ensure your phone is registered and authenticated.
5. The OSS monitors the entire process to make sure everything runs smoothly.

This system ensures that you can make calls, send texts, and use mobile data seamlessly wherever you are.

What is a Satellite?

A satellite is a small object that orbits around a larger object in space. The moon, which orbits the Earth, is an example of a natural satellite.

What is Satellite Communication?

Satellite communication is when two stations on Earth communicate with each other using a satellite. This involves sending data (like audio, video, or text) through electromagnetic waves between Earth and the satellite.

Why Do We Need Satellite Communication?

Before satellites, we used two types of communication:

1. **Ground Wave Propagation**:
   - **Example**: AM radio signals.
   - Suitable for frequencies up to 30 MHz.
   - Uses the Earth's troposphere for signal transmission.
2. **Sky Wave Propagation**:
   - **Example**: Shortwave radio.
   - Suitable for frequencies between 30–40 MHz.
   - Uses the Earth's ionosphere to bounce signals.

Both methods have a limitation: they can only cover distances up to 1500 km due to the Earth's curvature. Satellite communication overcomes this limitation, allowing long-distance communication far beyond the line of sight.

Key Components and Terms

- **Repeater**: A device that boosts a received signal and sends it again.
- **Transponder**: A device in the satellite that changes the frequency of the received signal before sending it back.

Frequencies

- **Uplink Frequency**: The frequency at which signals are sent from an Earth station to the satellite.
- **Downlink Frequency**: The frequency at which the satellite sends signals back to an Earth station.

How Satellite Communication Works

1. **Uplink Process**:
    - **Example**: Sending a TV broadcast.
    - The process starts at an Earth station (like a big satellite dish).
    - The Earth station sends data to the satellite using high-powered, high-frequency signals (in the GHz range).
2. **Transponder Function**:
    - The satellite receives these signals with its transponder.
    - The transponder changes the signal's frequency to avoid interference with the uplink frequency.
    - It then amplifies the signal and prepares it for sending back to Earth.
3. **Downlink Process**:
    - The satellite sends the modified signal back to Earth at the downlink frequency.
    - Another Earth station, within the satellite's coverage area, receives this signal.

Example of Satellite Communication

Think about how TV broadcasting works via satellite:

1. A TV station sends its broadcast signal to a satellite (uplink).
2. The satellite's transponder changes the signal's frequency and amplifies it.
3. The satellite sends the signal back down to Earth (downlink), where your satellite dish receives it, allowing you to watch TV.

This system allows us to communicate over long distances, even across continents, making satellite communication essential for global broadcasting, internet connectivity, and more

GEO: Geostationary Earth Orbit

- **Distance from Earth**: About 36,000 km above the Earth's surface.
- **Orbital Period**: 24 hours (matches the Earth's rotation).
- **Key Feature**: These satellites appear to stay fixed over one spot on Earth because they move at the same speed as the Earth's rotation.
- **Usage**:
    - **Example**: TV and satellite radio broadcasting.
    - Ideal for constant communication because they stay over the same area.
- **Limitations**:
    - One satellite cannot cover the entire Earth; it takes at least three geostationary satellites to cover the whole planet.
    - Expensive to launch and maintain; requires fuel for small adjustments to stay in position.

MEO: Medium Earth Orbit

- **Distance from Earth**: About 5,000 to 12,000 km above the Earth's surface.
- **Visibility**: Satellites in this orbit are visible for longer periods (2 to 8 hours) compared to LEO satellites.
- **Coverage**: Larger coverage area than Low Earth Orbit satellites.
- **Usage**:
    - **Example**: Navigation systems like GPS.

LEO: Low Earth Orbit

- **Distance from Earth**: About 500 to 1,200 km above the Earth's surface.
- **Orbital Period**: 95 to 120 minutes.
- **Speed**: Very fast, about 20,000 to 25,000 km/h.
- **Visibility**: Each satellite is visible from Earth for about 10 minutes.
- **Key Feature**: Provides global radio coverage.
- **Usage**:
    - **Example**: Satellites for weather monitoring, Earth observation, and some communication networks.

WAP Architecture (Wireless Application Protocol)

Wireless Application Protocol (WAP) is a technical standard for accessing information over a mobile wireless network. It enables mobile devices to access web services and Internet content. Here's a simplified explanation of the WAP architecture:

Overview

WAP architecture is designed to bring Internet content and advanced services to mobile devices such as smartphones and tablets. The architecture is made up of several layers, each performing specific functions to facilitate communication between the mobile device and the web server.

Components of WAP Architecture

1. **Mobile Device**: The user's mobile device (such as a smartphone or tablet) that accesses WAP services.
   - **Example**: Smartphones accessing news websites.
2. **WAP Client**: The software on the mobile device that communicates with the WAP gateway/server.
   - **Example**: A WAP browser.
3. **WAP Gateway**: This acts as an intermediary between the mobile device and the Internet. It translates WAP requests from the mobile device into HTTP requests for web servers and vice versa.
   - **Example**: A gateway server that converts WAP requests to standard web requests.
4. **Web Server**: The server that hosts the web content and services.
   - **Example**: A news website's server.

Layers of WAP Architecture

1. **Application Layer (WAE - Wireless Application Environment)**:
   - This layer contains the applications and services accessible via WAP.
   - **Example**: WML (Wireless Markup Language) applications that present content similar to HTML on the web.
2. **Session Layer (WSP - Wireless Session Protocol)**:
   - Manages the sessions between the WAP client and WAP gateway.
   - **Example**: Keeps track of the session state for continuous interaction.
3. **Transaction Layer (WTP - Wireless Transaction Protocol)**:
   - Ensures reliable communication by providing transaction support (requests and responses).
   - **Example**: Handling secure transactions for mobile banking services.
4. **Security Layer (WTLS - Wireless Transport Layer Security)**:
   - Provides security features such as encryption, authentication, and data integrity.
   - **Example**: Securing login credentials for online banking.
5. **Transport Layer (WDP - Wireless Datagram Protocol)**:
   - Facilitates the transmission of data over various wireless networks (like GSM, CDMA).
   - **Example**: Sending and receiving data packets over the mobile network.

Working of WAP Architecture

1. **Request**:
   - The user enters a URL or clicks a link in the WAP browser on the mobile device.
   - The WAP client sends the request to the WAP gateway.
2. **Processing**:
   - The WAP gateway translates the WAP request into a standard HTTP request.
   - The gateway forwards the request to the appropriate web server.
3. **Response**:
   - The web server processes the request and sends the content (often in WML format) back to the WAP gateway.
   - The WAP gateway converts the HTTP response into a WAP response.
4. **Display**:
   - The WAP client on the mobile device receives the WAP response.
   - The content is then displayed to the user in the WAP browser.

Example of WAP Usage

Example: A user wants to check the weather on their mobile phone.

- The user opens the WAP browser and enters the URL for a weather service.
- The WAP client sends the request to the WAP gateway.
- The WAP gateway converts the request to HTTP and sends it to the weather service's web server.
- The server processes the request and sends the weather information back to the gateway.
- The WAP gateway converts the HTTP response to WAP format and sends it back to the mobile device.

- The WAP browser displays the weather information to the user.

Goals of WAP/advantages of WAP

1. **Access Internet on Mobile**:
   - **Goal**: Let users access web services from their mobile phones.
2. **Optimize for Wireless**:
   - **Goal**: Make web content work well with slow and limited wireless networks.
3. **Work on Any Device**:
   - **Goal**: Ensure web services work on various mobile devices and networks.
4. **Support Many Services**:
   - **Goal**: Allow a wide range of mobile applications and services.
5. **Save Data**:
   - **Goal**: Use data efficiently to keep mobile data usage low.
6. **Secure Communication**:
   - **Goal**: Protect user data during transmission.
7. **Easy to Use**:
   - **Goal**: Provide a user-friendly interface for small mobile screens.
   - In short, WAP aims to make the internet accessible and usable on mobile devices, even with their limitations.

Disadvantages of WAP

1. **Limited Functionality**:
   - **Disadvantage**: Early WAP versions had limited capabilities compared to full web browsers.
2. **Performance Issues**:
   - **Disadvantage**: Can experience slow performance due to limited bandwidth and network constraints.
3. **Complex Development**:
   - **Disadvantage**: Developing WAP applications required specific skills and knowledge of WML (Wireless Markup Language), which could be complex.
4. **Obsolescence**:
   - **Disadvantage**: WAP has become outdated with the advent of more advanced technologies like mobile web browsers and 4G/5G networks.
5. **Compatibility Issues**:
   - **Disadvantage**: Variations in WAP implementations could lead to compatibility issues across different devices and networks.

ad hoc network

An **ad hoc network** is a type of wireless network where devices connect directly to each other without relying on a central network or fixed infrastructure. These networks are created spontaneously and can adapt to changes, such as devices moving in and out of range. They are often used in situations where a traditional network setup is not available or practical.

Key Features

1. **Decentralized**:
   - **Explanation**: There is no central server or router. Each node communicates directly with other nodes.
   - **Example**: In a military field operation, soldiers' devices can form an ad-hoc network to share information without needing a central communication hub.
2. **Dynamic Topology**:
   - **Explanation**: Nodes can move freely, and the network topology changes constantly. This requires the network to adapt quickly.
   - **Example**: In a disaster recovery scenario, rescue teams can set up a temporary ad-hoc network with their devices to coordinate efforts as they move around the disaster area.
3. **Self-Organizing**:
   - **Explanation**: Nodes automatically form connections and maintain the network without manual configuration.
   - **Example**: When you connect several smartphones in close proximity for a file-sharing app, they form an ad-hoc network automatically.
4. **Peer-to-Peer Communication**:
   - **Explanation**: Nodes communicate directly with each other, functioning as both clients and servers.
   - **Example**: In a group of friends playing a multiplayer game on their smartphones, they might use an ad-hoc network to interact directly with each other.

Types of Ad-Hoc Networks

1. **Mobile Ad-Hoc Networks (MANETs)**:
   - **Description**: These networks are composed of mobile nodes that change their positions frequently.
   - **Use Case**: Vehicular networks where cars communicate with each other for navigation and traffic updates.
2. **Wireless Sensor Networks (WSNs)**:
   - **Description**: Networks consisting of many sensor nodes that collect and transmit data.
   - **Use Case**: Environmental monitoring where sensor nodes collect data on temperature, humidity, and pollution levels.
3. **Delay-Tolerant Networks (DTNs)**:
   - **Description**: Designed to handle networks with intermittent connections where nodes may be disconnected for periods.
   - **Use Case**: Space communication or rural areas where connectivity is sporadic.

Routing Protocols

Routing in ad-hoc networks involves finding and maintaining paths between nodes as the network topology changes. Key types of routing protocols include:

1. **Proactive Routing Protocols**:
   - **Example**: **Destination-Sequenced Distance Vector (DSDV)**
   - **How It Works**: Continuously updates routing tables to ensure routes are always known.
   - **Advantage**: Immediate route availability.
   - **Disadvantage**: High overhead due to constant updates.
2. **Reactive Routing Protocols**:
   - **Example**: **Ad-Hoc On-Demand Distance Vector (AODV)**
   - **How It Works**: Finds routes only when needed through a route discovery process.
   - **Advantage**: Reduces overhead by discovering routes as required.
   - **Disadvantage**: May introduce delays during route discovery.
3. **Hybrid Routing Protocols**:
   - **Example**: **Zone Routing Protocol (ZRP)**
   - **How It Works**: Combines proactive and reactive methods, using proactive routing within a local zone and reactive routing outside it.
   - **Advantage**: Balances overhead and efficiency.
   - **Disadvantage**: Complexity in protocol design.

Advantages

1. **Flexibility**:
   - **Advantage**: Can quickly set up networks in areas without existing infrastructure.
2. **Cost-Effective**:
   - **Advantage**: No need for expensive infrastructure.
3. **Scalability**:
   - **Advantage**: Can accommodate a varying number of nodes.
   - **Example**: Expanding the network as more sensors are added to a monitoring system.

Disadvantages

1. **Scalability Issues**:
   - **Disadvantage**: Performance can degrade as the number of nodes increases due to routing overhead.
2. **Security Risks**:
   - **Disadvantage**: Lack of central control makes it challenging to implement robust security measures.
3. **Dynamic Topology Challenges**:
   - **Disadvantage**: Frequent topology changes can complicate routing and network stability.

DSDV

Destination-Sequenced Distance Vector (DSDV) is a proactive routing protocol used in mobile ad-hoc networks (MANETs). It is designed to maintain up-to-date routing tables for all nodes in the network to facilitate immediate route discovery. Here's an overview of how DSDV works:

Key Features

1. **Proactive Nature**:
   - **Description**: DSDV continuously updates its routing tables, ensuring that route information is always current. This means routes are known before they are needed.
2. **Distance Vector Protocol**:
   - **Description**: Each node maintains a table that lists the shortest path to every other node in the network. The table includes the destination, the next hop, and the distance (cost) to the destination.
3. **Sequence Numbers**:
   - **Description**: Each route entry in the routing table is associated with a sequence number provided by the destination node. This helps differentiate between old and new routing information.

How It Works

1. **Routing Table Updates**:
   - **Description**: Nodes periodically broadcast updates containing their routing tables to their neighbors. This update includes the sequence numbers to indicate the freshness of the information.
   - **Process**: When a node receives a routing update, it checks the sequence number to determine if the information is more recent than its current table entries. If it is, the node updates its own table accordingly.
2. **Route Discovery**:
   - **Description**: Since DSDV proactively maintains route information, routes are available immediately when a node needs to send data.
   - **Process**: Nodes use their routing tables to find the next hop towards the destination and send data packets accordingly.
3. **Handling Topology Changes**:
   - **Description**: When nodes move or network topology changes, nodes generate new routing updates to reflect these changes.
   - **Process**: Nodes that detect topology changes broadcast updated route information, which propagates through the network to keep all nodes informed.

Advantages

1. **Immediate Route Availability**:
   - **Benefit**: Routes are known and available at all times, which minimizes delay in route establishment.
2. **Simplicity**:
   - **Benefit**: The protocol is relatively simple to implement, as it is based on distance vector principles and sequence numbers.

Disadvantages

1. **High Overhead**:
   - **Disadvantage**: Constant updates and broadcasts can lead to high control message overhead, especially in large or highly dynamic networks.
2. **Scalability Issues**:
   - **Disadvantage**: As the number of nodes increases, the size of routing tables and the frequency of updates can become problematic.

File Systems

File System: A file system is a method and data structure that an operating system uses to manage and organize files on a storage device, such as a hard drive or SSD.

- **Purpose**: It helps in storing, retrieving, and organizing files so that the operating system can access and manage them efficiently.
- **Components**: Includes directories (folders), files, and metadata (information about the files, like their size and creation date).

Databases

Database: A database is an organized collection of data that can be easily accessed, managed, and updated. It uses structured formats to store data efficiently and allows users to perform operations such as querying and updating.

- **Purpose**: To store large amounts of data in a structured way, enabling efficient retrieval and management.
- **Components**: Typically includes tables (in relational databases), records (rows), and fields (columns).
- **Types**: Relational databases (e.g., MySQL, PostgreSQL) and NoSQL databases (e.g., MongoDB, Cassandra).

WWW (World Wide Web)

WWW (World Wide Web): The WWW is a system of interlinked hypertext documents and multimedia content accessible via the internet using web browsers.

- **Purpose**: To provide a global platform for accessing and sharing information through websites and web applications.
- **Components**: Includes web pages, websites, hyperlinks, and web servers.
- **Protocols**: Uses protocols like HTTP (HyperText Transfer Protocol) and HTTPS (HTTP Secure) to enable communication between web browsers and servers.

Mobility

Mobility: Mobility refers to the ability to move freely and access resources, services, or networks from various locations, often through mobile devices like smartphones and laptops.

- **Purpose**: To allow users to stay connected and productive regardless of their physical location.
- **Components**: Includes wireless technologies (like Wi-Fi and cellular networks), mobile applications, and portable devices.
- **Aspects**: Can involve features like roaming (accessing network services outside your home area) and seamless connectivity (switching between different networks without losing service).

Example: Using your smartphone to check emails or navigate maps while traveling is an example of mobility, as it allows you to stay connected and access information on the go.

Multiplexing

Multiplexing is a technique used in communication systems to combine multiple signals or data streams into a single transmission channel. The purpose is to optimize the use of available bandwidth and to efficiently transmit multiple signals over a single communication medium.

Types of Multiplexing

1. **Time Division Multiplexing (TDM)**:
   - **Description**: Divides the time into slots and allocates each slot to a different signal or data stream.
2. **Frequency Division Multiplexing (FDM)**:
   - **Description**: Allocates different frequency bands to each signal or data stream. Each signal is transmitted simultaneously over its own frequency band.
3. **Wavelength Division Multiplexing (WDM)**:
   - **Description**: Similar to FDM but used in optical fiber communication, where different wavelengths (colors) of light are used to transmit multiple signals.
4. **Code Division Multiplexing (CDM)**:
   - **Description**: Uses unique codes to distinguish between different signals transmitted over the same frequency band.

Modulation

Modulation is the process of varying a carrier signal's characteristics (such as amplitude, frequency, or phase) to transmit information. This allows the signal to be transmitted over a communication channel and received accurately.

Types of Modulation

1. **Amplitude Modulation (AM)**:
   - **Description**: Varies the amplitude of the carrier signal in proportion to the amplitude of the modulating signal.
2. **Frequency Modulation (FM)**:
   - **Description**: Varies the frequency of the carrier signal in proportion to the amplitude of the modulating signal.
3. **Phase Modulation (PM)**:
   - **Description**: Varies the phase of the carrier signal according to the modulating signal

Difference Between FDMA, CDMA and TDMA

FDMA	TDMA	CDMA
FDMA stands for Frequency Division Multiple Access.	TDMA stands for Time Division Multiple Access.	CDMA stands for Code Division Multiple Access.
Each user gets a separate frequency band.	Bandwidth is shared by allocating different time slots to each user.	Bandwidth and time are shared among users.
There is no need of any codeword.	There is no need of any codeword.	Codeword is necessary.
In this, there is only need of guard bands between the adjacent channels are necessary.	In this, guard time of the adjacent slots are necessary.	In this, both guard bands and guard time are necessary.
Synchronization is not required.	Synchronization is required.	Synchronization is not required.
The rate of data is low.	The rate of data is medium.	The rate of data is high.
Mode of data transfer is continuous signal.	Mode of data transfer is signal in bursts.	Mode of data transfer is digital signal.
It is little flexible.	It is moderate flexible.	It is highly flexible.