MOBILE COMPUTING (TOE 811)
UNIT-1 NOTES

Mobile computing refers to the use of portable computing devices such as smartphones, tablets, and laptops that are designed to be easily transported and used while on the go. The rise of mobile computing has been a game−changer in today's world.

It has transformed the way people communicate, access information, and perform tasks. With mobile devices becoming increasingly powerful and ubiquitous, it's no surprise that businesses such as Apple and Samsung have invested significantly in this area.

Mobile computing is defined as any technology that allows wireless communication between devices or people on−the−go. It is an umbrella term for various technologies like laptops, smartphones, wearables which allow convenient access to information from anywhere and anytime. These devices are designed to be lightweight with long battery lives making them portable.

Issues in Mobile Computing

Despite its numerous advantages, mobile computing faces several challenges, including:

1. **Limited Battery Life** – Mobile devices rely on battery power, which may drain quickly due to high processing demands and continuous connectivity.
2. **Security and Privacy Concerns** – Wireless networks are susceptible to cyber threats, including hacking, phishing, and data breaches.
3. **Network Connectivity Issues** – Mobile computing depends on network coverage, and poor or unstable internet connections can disrupt communication and data access.
4. **Data Synchronization** – Ensuring seamless synchronization of data across multiple devices and cloud services can be complex.
5. **Hardware Limitations** – Mobile devices often have limited processing power, storage, and memory compared to desktop computers.
6. **User Interface Constraints** – Smaller screens and touch-based navigation can impact productivity and usability.
7. **Cost of Mobile Data** – High data usage in mobile computing can lead to expensive network charges, especially in roaming scenarios.
8. **Device Compatibility** – Variations in operating systems, software, and hardware configurations may lead to compatibility issues.
9. **Environmental Factors** – Mobile devices can be affected by weather conditions, physical damage, or loss/theft.

Overview of Wireless Telephony: Cellular Concept

Wireless telephony refers to the transmission of voice and data over wireless communication networks, enabling mobile communication without the need for physical wires. The **cellular**

concept is the foundation of modern wireless telephony and is used in mobile communication systems such as **2G, 3G, 4G, and 5G** networks.

Cellular Concept

The **cellular concept** is a system design that divides a geographic area into smaller regions called **cells**, each served by a base station (cell tower). These cells collectively provide seamless coverage and enable efficient frequency reuse, increasing network capacity.

Key Components of the Cellular Concept

1. **Cells** – Small geographical areas that form a cellular network, each served by a base station.
2. **Base Station (BTS - Base Transceiver Station)** – A tower that transmits and receives signals, connecting mobile users to the network.
3. **Mobile Switching Center (MSC)** – The central hub that connects multiple base stations and manages call routing and handovers.
4. **Frequency Reuse** – Each cell is assigned a specific set of frequencies, which can be reused in non-adjacent cells to avoid interference and optimize spectrum usage.
5. **Handoff (Handover)** – When a mobile user moves from one cell to another, the call or data session is transferred to the new base station without interruption.
6. **Cell Splitting** – To handle high traffic demand, large cells can be divided into smaller cells to increase capacity.
7. **Sectoring** – Each cell can be divided into multiple sectors with directional antennas to reduce interference and improve efficiency.

Advantages of the Cellular Concept

✔ **Efficient Spectrum Utilization** – Enables frequency reuse to maximize network capacity.
✔ **Wide Coverage Area** – Supports mobile users over large geographical regions.
✔ **Scalability** – Can accommodate more users by adding new cells or splitting existing ones.
✔ **Improved Call Quality** – Reduces interference and enhances signal strength.
✔ **Support for Mobility** – Ensures seamless communication even when users are moving.

GSM:Air Interface

The **GSM (Global System for Mobile Communications)** air interface defines how mobile devices communicate wirelessly with base stations. It is the link between mobile phones and the GSM network, using **radio frequencies, multiple access techniques, and modulation schemes** to transmit voice and data.

- **Radio Frequencies**

GSM operates in different frequency bands depending on the region:

- **900 MHz (GSM-900)** and **1800 MHz (DCS-1800)** (Europe, Asia, Africa)
- **850 MHz (GSM-850)** and **1900 MHz (PCS-1900)** (North America)

- **Multiple Access Technique**

GSM uses **TDMA (Time Division Multiple Access)** combined with **FDMA (Frequency Division Multiple Access)** to enable multiple users to share the same frequency band:

- **FDMA**: Divides the available frequency spectrum into channels.

- **TDMA**: Further divides each frequency channel into time slots, allowing multiple users to share the same frequency by transmitting in different time slots.

- **Time Slot and Frame Structure**

  - Each frequency is divided into **8 time slots**, forming a **TDMA frame**.
  - A mobile user gets assigned one time slot per frame for communication.

- **Modulation Scheme**

GSM uses **Gaussian Minimum Shift Keying (GMSK)** modulation, which:

  - Reduces signal bandwidth, improving efficiency.
  - Provides better noise resistance and signal quality.

- **Logical Channels**

The GSM air interface consists of two main types of channels:

  - **Traffic Channels (TCH)** – Carry voice and data.
  - **Control Channels (CCH)** – Handle signaling and network management.

GSM Channel Structure

In **GSM (Global System for Mobile Communications)**, the channel structure is designed to efficiently manage voice, data, and signaling information over the air interface. The GSM network uses **radio channels**, which are divided into **physical channels** and **logical channels**.

A. Traffic Channels (TCH)

These channels carry user data, such as voice or SMS.

- **Full-Rate Traffic Channel (TCH/F)** – Allocates a full time slot for a voice call.
- **Half-Rate Traffic Channel (TCH/H)** – Uses half a time slot, allowing two calls per slot.
- **Data Traffic Channels (TCH/F and TCH/H for data)** – Carry circuit-switched data (e.g., internet or fax).

B. Control Channels (CCH)

Control channels handle network management, call setup, and mobility. They are divided into:

1. Broadcast Channels (BCH) – Downlink only

- **Broadcast Control Channel (BCCH)** – Sends network information (e.g., cell identity, frequency list).
- **Synchronization Channel (SCH)** – Provides timing information for synchronization.
- **Frequency Correction Channel (FCCH)** – Helps mobile devices tune to the correct frequency.

2. Common Control Channels (CCCH) – Uplink and downlink

- **Paging Channel (PCH)** – Notifies a mobile user of an incoming call or SMS.
- **Random Access Channel (RACH)** – Used by mobile devices to request network access (uplink only).

- **Access Grant Channel (AGCH)** – Assigns a mobile device to a dedicated channel after an **access request.**

3. Dedicated Control Channels (DCCH) – For call setup and handovers

- **Stand-alone Dedicated Control Channel (SDCCH)** – Used for call setup, SMS transmission, and registration.
- **Slow Associated Control Channel (SACCH)** – Maintains connection status, signal strength updates.
- **Fast Associated Control Channel (FACCH)** – Used during handover to quickly switch cells.

GSM Frame Structure Overview

- **1 TDMA Frame** = 8 time slots.
- **26 TDMA Frames** = 1 Multiframe (used for traffic).
- **51 TDMA Frames** = 1 Multiframe (used for signaling).

GSM - Architecture

The GSM network can be broadly divided into –

- The Mobile Station (MS)
- The Base Station Subsystem (BSS)
- The Network Switching Subsystem (NSS)
- The Operation Support Subsystem (OSS)

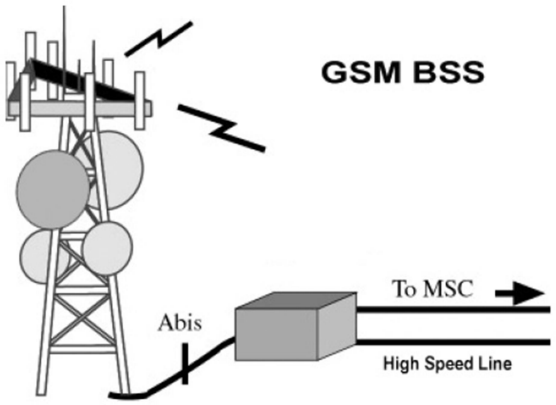
The **MS c**onsists of the physical equipment, such as the radio transceiver, display and digital signal processors, and the SIM card. It provides the air interface to the user in GSM networks. The **MS** also provides the receptor for SMS messages, enabling the user to toggle between the voice and data use.

MS also provides access to the various data services available in a GSM network.

- X.25 packet switching through a synchronous or asynchronous dial-up connection to the PAD at speeds typically at 9.6 Kbps.
- General Packet Radio Services (GPRSs) using either an X.25 or IP based data transfer method at the speed up to 115 Kbps.
- High speed, circuit switched data at speeds up to 64 Kbps.

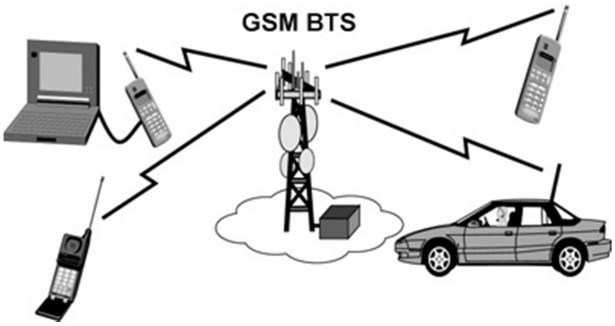
The Base Station Subsystem (BSS): The BSS is composed of two parts –

- The Base Transceiver Station (BTS)
- The Base Station Controller (BSC)



The Base Transceiver Station (BTS)

The BTS houses the radio transceivers that define a cell and handles the radio link protocols with the MS. In a large urban area, a large number of BTSs may be deployed.



The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between 1 and 16 transceivers, depending on the density of users in the cell. Each BTS serves as a single cell. It also includes the following functions −

- Encoding, encrypting, multiplexing, modulating, and feeding the RF signals to the antenna
- Transcoding and rate adaptation
- Time and frequency synchronizing
- Voice through full- or half-rate services
- Decoding, decrypting, and equalizing received signals
- Random access detection
- Timing advances
- Uplink channel measurements.

The Base Station Controller (BSC)

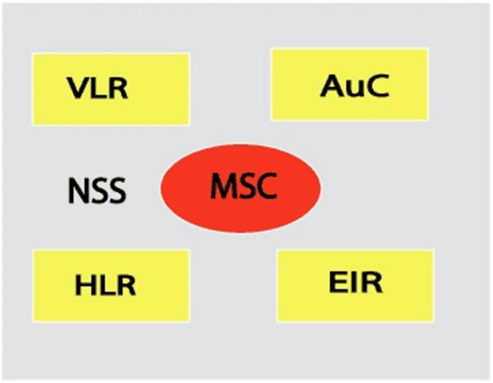
The BSC manages the radio resources for one or more BTSs. It handles radio channel setup, frequency hopping, and handovers. The BSC is the connection between the mobile and the MSC. The BSC also translates the 13 Kbps voice channel used over the radio link to the standard 64 Kbps channel used by the Public Switched Telephone Network (PSDN) or ISDN.

The functions include–

- Control of frequency hopping
- Performing traffic concentration to reduce the number of lines from the MSC
- Providing an interface to the Operations and Maintenance Center for the BSS

GSM - The Network Switching Subsystem (NSS)

The Network switching system (NSS), the main part of which is the Mobile Switching Center (MSC), performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as authentication.



The switching system includes the following functional elements –

Home Location Register (HLR)

The HLR is a database used for storage and management of subscriptions. The HLR is considered the most important database, as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription in the form of SIM, then all the information about this subscription is registered in the HLR of that operator.

Mobile Services Switching Center (MSC)

The central component of the Network Subsystem is the MSC. The MSC performs the switching of calls between the mobile and other fixed or mobile network users, as well as the management of mobile services such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. It also performs such functions as toll ticketing, network interfacing, common channel signaling, and others. Every MSC is identified by

Visitor Location Register (VLR)

The VLR is a database that contains temporary information about subscribers that is needed by the MSC in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about the mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

Authentication Center (AUC)

The Authentication Center is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel. The AUC protects network operators from different types of fraud found in today's cellular world.

Equipment Identity Register (EIR)

The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where its International Mobile Equipment Identity (IMEI) identifies each MS. An IMEI is marked as invalid if it has been reported stolen or is not type approved.

GSM - The Operation Support Subsystem (OSS)

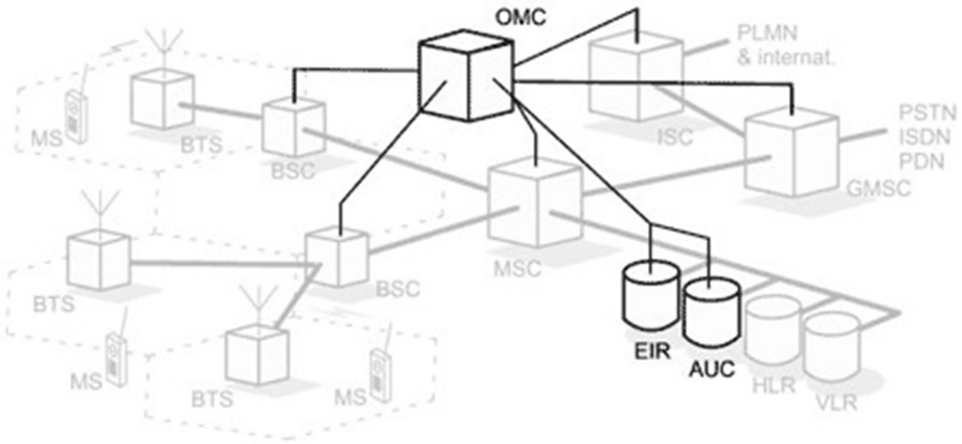
The operations and maintenance center (OMC) is connected to all equipment in the switching system and to the BSC. The implementation of OMC is called the operation and support system (OSS).

Here are some of the OMC functions−

- Administration and commercial operation (subscription, end terminals, charging, and statistics).
- Security Management.
- Network configuration, Operation, and Performance Management.
- Maintenance Tasks.

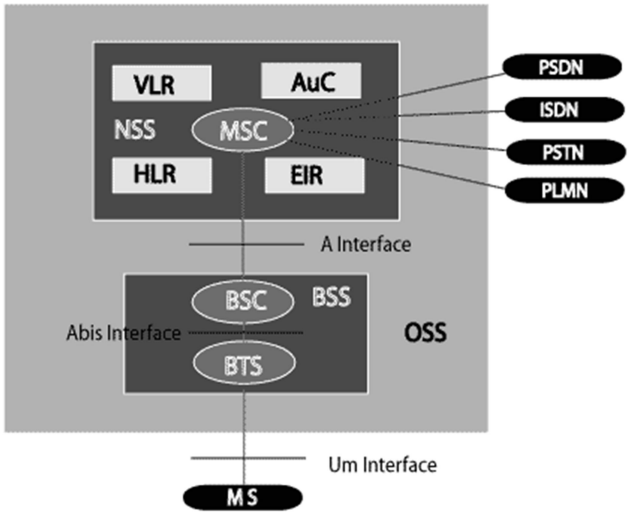
The operation and Maintenance functions are based on the concepts of the Telecommunication Management Network (TMN), which is standardized in the ITU-T series M.30.

Following is the figure, which shows how OMC system covers all the GSM elements.



The OSS is the functional entity from which the network operator monitors and controls the system. The purpose of OSS is to offer the customer cost-effective support for centralized, regional, and local operational and maintenance activities that are required for a GSM network.

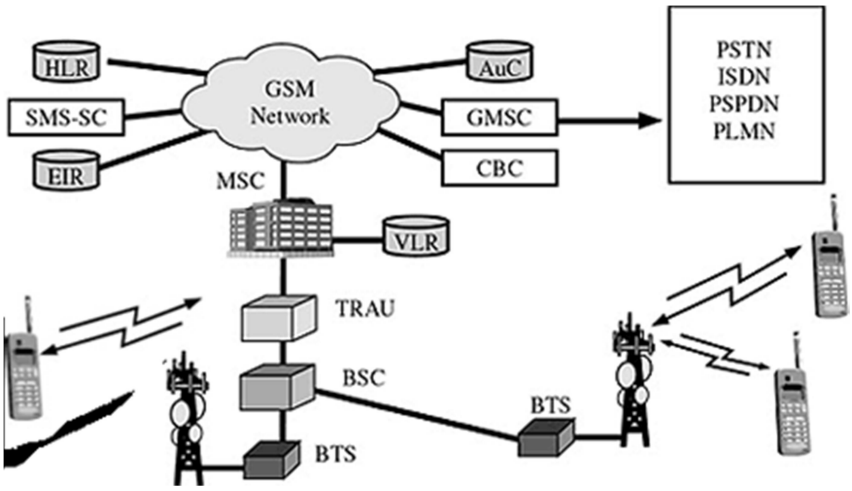
A simple pictorial view of the GSM architecture is given below −



The additional components of the GSM architecture comprise of databases and messaging systems functions −

- Home Location Register (HLR)
- Visitor Location Register (VLR)
- Equipment Identity Register (EIR)
- Authentication Center (AuC)
- SMS Serving Center (SMS SC)
- Gateway MSC (GMSC)
- Chargeback Center (CBC)
- Transcoder and Adaptation Unit (TRAU)

The following diagram shows the GSM network along with the added elements −



The MS and the BSS communicate across the Um interface. It is also known as the *air interface* or the *radio link*. The BSS communicates with the Network Service Switching (NSS) center across the *A* interface.

GSM network areas

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.

Location Management in GSM: HLR and VLR

Location management in GSM ensures that a mobile device can be tracked and reached for calls, SMS, and data services while moving across different areas. This is achieved using two key database systems:

- **HLR (Home Location Register)**
- **VLR (Visitor Location Register)**

These databases help the network keep track of a mobile user's location and facilitate call routing and handovers.

1. Home Location Register (HLR)

The **HLR** is a central database that stores **permanent subscriber information** and helps manage user authentication and location updates.

Functions of HLR

✔ **Stores subscriber details** – IMSI (International Mobile Subscriber Identity), MSISDN (Mobile Number), and service subscriptions.
✔ **Keeps track of location** – Stores the last known **VLR location** of the subscriber.
✔ **Manages authentication** – Provides security details (Ki, A3/A8 algorithms) for user authentication.
✔ **Handles call and SMS routing** – Directs incoming calls/messages to the correct VLR.

Location Update Process in HLR

1. When a mobile device moves to a new location, it registers with the nearest **VLR**.
2. The **VLR** updates the **HLR** with the new location.
3. The **HLR** deletes the old location information and stores the new one.

2. Visitor Location Register (VLR)

The **VLR** is a temporary database that stores **current subscriber information** for users visiting its area. Each **Mobile Switching Center (MSC)** has an associated **VLR**.

Functions of VLR

✔ **Temporarily stores subscriber data** – Retrieved from HLR when a mobile enters a new area.
✔ **Manages call setup** – Assigns temporary identifiers (TMSI) to users to reduce signaling load.
✔ **Handles location updates** – Registers the mobile device when it moves to a new location.
✔ **Supports handovers** – Assists in call continuation when moving between cells.

Location Update Process in VLR

1. When a mobile enters a new **VLR** area, it sends a **location update request**.
2. The **VLR** contacts the **HLR** to retrieve the subscriber's details.
3. The **VLR** assigns a **TMSI (Temporary Mobile Subscriber Identity)** for security.
4. If the subscriber moves out, the **VLR** deletes the user's data.

HLR vs. VLR: Key Differences

Feature	HLR (Home Location Register)	VLR (Visitor Location Register)
Data Type	Permanent subscriber data	Temporary subscriber data
Function	Stores user details & current VLR location	Manages call setup & location updates
Location	Centralized (one per network)	Distributed (one per MSC)
Update Frequency	Infrequent	Frequent (as users move)

Cellular networks use a well-organized **hierarchical structure**, efficient **handoff mechanisms**, and optimized **channel allocation** techniques to ensure seamless communication for mobile users.

1. Hierarchical Cellular Structure

To efficiently manage network resources, cellular systems are structured into a **hierarchical architecture**. This hierarchy consists of different levels of cells, each serving specific purposes:

Types of Cells in a Hierarchical Network

1. **Macrocell** – Covers large areas (10–30 km), used in highways and rural areas.
2. **Microcell** – Covers smaller urban areas (1–2 km), reducing congestion in cities.
3. **Picocell** – Small coverage (200–500 m), used inside buildings, malls, airports.
4. **Femtocell** – Very small coverage (10–50 m), used in homes and offices.

Advantages of a Hierarchical Structure

✔ **Efficient Frequency Reuse** – Smaller cells allow frequency reuse without interference.
✔ **Load Balancing** – Offloads traffic from macrocells to smaller cells.
✔ **Improved Call Quality** – Reduces congestion and call drops.
✔ **Power Efficiency** – Lower power consumption in smaller cells.

2. Handoffs in Cellular Systems

A **handoff (handover)** occurs when a mobile device moves from one cell to another while maintaining an active call or data session.

Types of Handoffs

1. **Hard Handoff (Break-Before-Make)**
   - Used in **GSM, 2G networks**.
   - The connection is **broken** before switching to a new base station.
   - Can cause call drops if the new channel is unavailable.
2. **Soft Handoff (Make-Before-Break)**
   - Used in **CDMA, 3G networks**.
   - The device connects to a new base station **before disconnecting** from the old one.
   - Provides seamless transition and better call quality.
3. **Handoff Between Different Networks**
   - **Horizontal Handoff** – Between cells of the same network (e.g., LTE to LTE).
   - **Vertical Handoff** – Between different technologies (e.g., Wi-Fi to 4G, 4G to 5G).

Handoff Process

1. **Signal Measurement** – The mobile device continuously measures signal strength.
2. **Handoff Decision** – The network decides when to switch the connection.

3. **Resource Allocation** – The target cell allocates a new channel.
4. **Connection Transfer** – The mobile switches to the new cell without disruption.

3. Channel Allocation in Cellular Systems

Channel allocation is the process of assigning frequency channels to different cells in a cellular network.

Types of Channel Allocation

1. **Fixed Channel Allocation (FCA)**
   - Each cell gets a fixed number of channels.
   - Simple but inefficient in high-traffic conditions.
2. **Dynamic Channel Allocation (DCA)**
   - Channels are assigned based on real-time demand.
   - More efficient but requires complex algorithms.
3. **Hybrid Channel Allocation (HCA)**
   - Combines FCA and DCA.
   - Some channels are fixed, and some are dynamically assigned.

Frequency Reuse in Channel Allocation

- Each cell is assigned a group of frequencies that are reused in non-adjacent cells.
- **Frequency Reuse Factor (N)** defines how frequently a frequency is reused (e.g., N = 7 means a frequency is reused every 7 cells).

CDMA

code Division Multiple Access system is very different from time and frequency multiplexing. In this system, a user has access to the whole bandwidth for the entire duration. The basic principle is that different CDMA codes are used to distinguish among the different users.

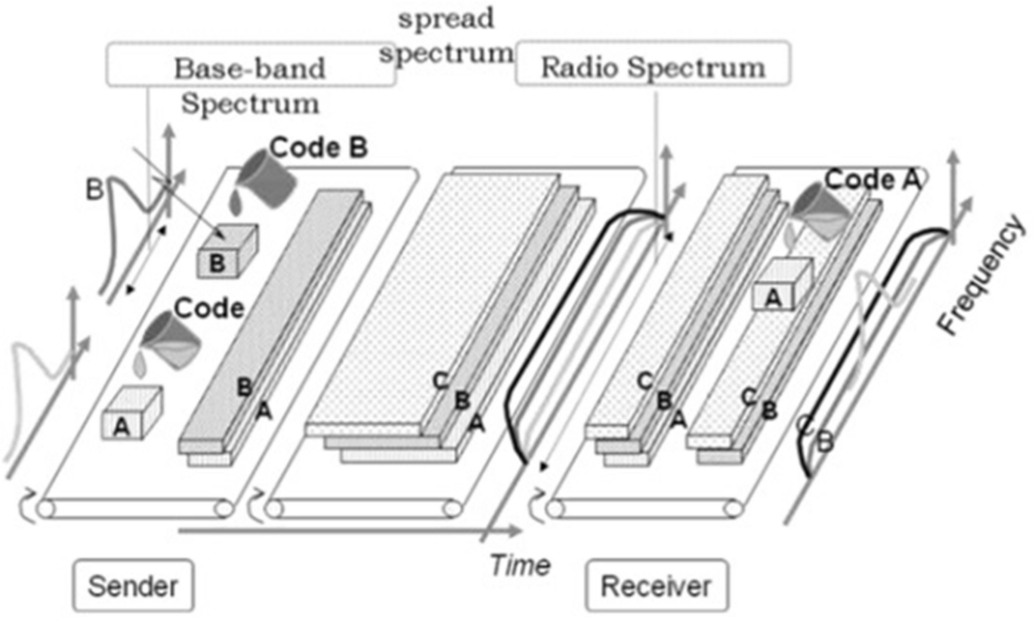
Techniques generally used are direct sequence spread spectrum modulation (DS-CDMA), frequency hopping or mixed CDMA detection (JDCDMA). Here, a signal is generated which extends over a wide bandwidth. A code called **spreading code** is used to perform this action. Using a group of codes, which are orthogonal to each other, it is possible to select a signal with a given code in the presence of many other signals with different orthogonal codes.

Working:

CDMA allows up to 61 concurrent users in a 1.2288 MHz channel by processing each voice packet with two PN codes. There are 64 Walsh codes available to differentiate between calls and theoretical limits. Operational limits and quality issues will reduce the maximum number of calls somewhat lower than this value.

In fact, many different "signals" baseband with different spreading codes can be modulated on the same carrier to allow many different users to be supported. Using different orthogonal codes, interference between the signals is minimal. Conversely, when signals are received from several mobile stations, the base station is capable of isolating each as they have different orthogonal spreading codes.

Structure:



CDMA Capacity

The factors deciding the CDMA capacity are –

- Processing Gain
- Signal to Noise Ratio
- Voice Activity Factor
- Frequency Reuse Efficiency

Capacity in CDMA is soft, CDMA has all users on each frequency and users are separated by code. This means, CDMA operates in the presence of noise and interference.

Centralized Methods

- The band used in CDMA is 824 MHz to 894 MHz (50 MHz + 20 MHz separation).
- Frequency channel is divided into code channels.
- 1.25 MHz of FDMA channel is divided into 64 code channels.

Processing Gain

CDMA is a spread spectrum technique. Each data bit is spread by a code sequence. This means, energy per bit is also increased. This means that we get a gain of this.

P (gain) = 10log (W/R)

W is Spread Rate

R is Data Rate

For CDMA P (gain) = 10 log (1228800/9600) = 21dB

This is a gain factor and the actual data propagation rate. On an average, a typical transmission condition requires a signal to the noise ratio of 7 dB for the adequate quality of voice.

Translated into a ratio, signal must be five times stronger than noise.

Actual processing gain = P (gain) - SNR

= 21 – 7 = 14dB

CDMA uses variable rate coder

The Voice Activity Factor of 0.4 is considered = -4dB.

Hence, CDMA has 100% frequency reuse. Use of same frequency in surrounding cells causes some additional interference.

In CDMA frequency, reuse efficiency is 0.67 (70% eff.) = -1.73dB

Advantages of CDMA

CDMA has a soft capacity. The greater the number of codes, the more the number of users. It has the following advantages –

- CDMA requires a tight power control, as it suffers from near-far effect. In other words, a user near the base station transmitting with the same power will drown the signal latter. All signals must have more or less equal power at the receiver
- Rake receivers can be used to improve signal reception. Delayed versions of time (a chip or later) of the signal (multipath signals) can be collected and used to make decisions at the bit level.
- Flexible transfer may be used. Mobile base stations can switch without changing operator. Two base stations receive mobile signal and the mobile receives signals from the two base stations.
- Transmission Burst – reduces interference.

Disadvantages of CDMA

The disadvantages of using CDMA are as follows –

- The code length must be carefully selected. A large code length can induce delay or may cause interference.
- Time synchronization is required.
- Gradual transfer increases the use of radio resources and may reduce capacity.
- As the sum of the power received and transmitted from a base station needs constant tight power control. This can result in several handovers.

GPRS

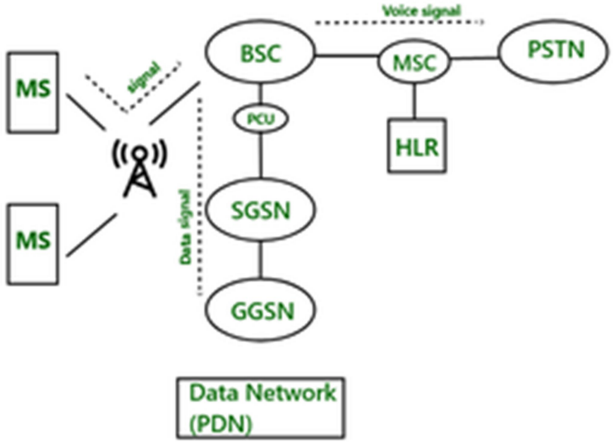
GPRS (General Packet Radio Service) is an expansion of GSM (Global System for Mobile Communications) networks that offer packet-switched data services. The GPRS architecture consists of different network components and interfaces that work together to provide data services.

GPRS stands for **General Packet Radio Service.** It is the modified version of GSM architecture. GPRS is a packet-oriented mobile data mechanism, that can carry data packets as well. In GSM architecture, only voice signals can be transported, so being an enhanced version GPRS can transmit voice as well as data packets. It uses the same physical radio channel as GSM does, the only difference is it has a new logic defined for the radio channel.

GPRS Network Architecture

GPRS tries to make maximum use of the existing physical structure of GSM. It has introduced a new entity named GPRS support nodes(GSN) whose responsibility is to route and deliver a data packet. GSN is of two types:

- Serving GPRS Support Node (SGSN)
- Gateway GPRS Support Node (GGSN)



Components of GPRS Architecture

1. Mobile Station(MS)

GPRC requires enhanced mobile stations, as existing mobile stations were designed according to the GSM network, and they were unable in handling enhanced data packets. A variety of high-speed mobile stations are available to support enhanced data packets. These mobile stations are also capable of handling the GSM architecture to make voice calls.

2. Base Station Controller (BSC)

In GSM architecture there is one component called BSC. But in GPRS there is one component is added to BSC called PCU. PCU stands for Packet Control Unit. If the signal comes to BSC and that signal contains data, then PCU routes to the SGSN. The interface is used between BSC and PCU is the FRI interface. After the signal comes to SGSN, it delivers the data packet to the GGSN. GGSN routes the data packet to the data network (PDN- Predefined Data Network).

3. GPRS Support Nodes

GPRS support nodes are of two types:

(a) **Serving GPRS Support Node (SGSN)**: It is responsible for the following tasks:

- Packet Delivery
- Mobility management
    - apply/ sign off of terminals
    - localization
- LLC (Logical Link Control) management
- Authentication
- Billing

(b) Gateway GPRS Support Node (GGSN): It is responsible for the following tasks:

- Mediator between GPRS between backbone and external data networks.
- Saves current data for the SGSN address of the participant as well as their profile and data for authentication and invoice.

4. Internal Backbone Network

It is an IP-based network that is used to support the working of GPRS and this is responsible to carry new packets between different GSNs. The tunneling is used between SGSNs and GGSNs to exchange information without informing the internal backbone.

5. Mobility Support

GPRS has the following mechanism to support mobility in the network:

- Attachment Procedure
- Location and Handoff Management

6. Routing Area

This is similar to the location area in GSM the only difference is routing area use fewer cells as routing areas are smaller than the location area.

7. SMS in GSM

GSM introduced a mechanism of Short Messaging Service(SMS) which is similar to peer-to-peer Instant messaging.

Benefits Of GPRS

- **Mobility:** The capacity to keep up consistent voice and information interchanges while moving.
- **Cost Efficient:** Communication via GPRS is cheaper than through the regular GSM network.
- **Immediacy:** Allows customers to obtain connectivity when needed, regardless of location and without a lengthy login session.
- **Localization:** Enables customers to acquire data applicable to their present area.
- **Easy Billing:** GPRS packet transmission offers an easier to use billing than that offered by circuit switched administrations.

Unit-02 Notes

Wireless Networking:

Wireless networking refers to the communication between devices using radio waves or infrared signals instead of physical cables. It enables mobility, flexibility, and connectivity across various applications, such as **Wi-Fi, Bluetooth, cellular networks, and satellite communication**.

1. Key Features of Wireless Networking

✔ **Mobility** – Users can move freely while staying connected.
✔ **Scalability** – Easily expands without additional cabling.
✔ **Cost-Effective** – Reduces the need for wired infrastructure.
✔ **Flexibility** – Supports different devices and applications.

2. Types of Wireless Networks

A. Wireless Local Area Networks (WLAN)

- Uses **Wi-Fi (IEEE 802.11)** technology.

- Provides connectivity within **homes, offices, and public hotspots**.

B. Wireless Metropolitan Area Networks (WMAN)

- Covers larger areas such as cities.
- Uses technologies like **WiMAX (IEEE 802.16)**.

C. Wireless Wide Area Networks (WWAN)

- Supports long-range communication using **cellular networks (2G, 3G, 4G, 5G)**.
- Used for mobile internet and telecommunication.

D. Wireless Personal Area Networks (WPAN)

- Short-range communication, such as **Bluetooth (IEEE 802.15) and Zigbee**.
- Used in smart devices, wearables, and IoT applications.

3. Wireless Networking Technologies

A. Wi-Fi (IEEE 802.11)

- Standard for **wireless LANs** with high-speed internet access.
- Operates on **2.4 GHz and 5 GHz** frequency bands.

B. Bluetooth

- Short-range communication for **connecting devices like phones, speakers, and smartwatches**.

C. Cellular Networks (2G, 3G, 4G, 5G)

- Provides **mobile communication and data services** over a large area.

D. Satellite Communication

- Used in **remote areas, GPS, and global connectivity**.

4. Advantages of Wireless Networking

 No Cables – Reduces infrastructure costs.
 Easy Installation – Quick deployment in homes and businesses.
 Supports Mobility – Connects users on the move.
 Broad Coverage – Expands connectivity beyond wired networks.

Wireless LAN Overview: MAC issues

Wireless LANs (WLANs), primarily based on **IEEE 802.11 (Wi-Fi)**, use **radio waves** instead of wired connections. However, due to the shared nature of wireless communication, **Medium Access Control (MAC) issues** arise, affecting performance and reliability.

1. Role of MAC in Wireless LANs

The **MAC layer** in WLANs is responsible for controlling access to the wireless medium and ensuring **efficient and fair data transmission** among multiple devices. It prevents **collisions** and manages **data transmission and reception**.

Key Functions of MAC in WLAN

✔ **Channel Access Control** – Decides when a device can transmit data.
✔ **Collision Avoidance** – Prevents data packet collisions.
✔ **Packet Framing & Addressing** – Ensures correct delivery of packets.
✔ **Retransmissions & Error Handling** – Manages lost or corrupted packets.

2. MAC Issues in Wireless LANs

A. Hidden Node Problem

Issue:

- Occurs when two devices cannot detect each other but are both communicating with the same access point.
- Results in **collisions** because nodes think the channel is free and transmit at the same time.

Solution:

- **RTS/CTS (Request to Send / Clear to Send) Mechanism**:
  - The sender sends an **RTS signal** to the access point.
  - The access point responds with a **CTS signal**, instructing other devices to wait before transmitting.

B. Exposed Node Problem

Issue:

- A node **unnecessarily** refrains from transmitting because it senses another nearby transmission, even when it wouldn't cause interference.
- Reduces **network throughput** and efficiency.

Solution:

- Using **spatial reuse** techniques to allow parallel transmissions.

C. Hidden Terminal Collisions

Issue:

- When two distant devices send data to the access point at the same time, causing **collisions** at the receiver.
- The devices are **unaware of each other's transmissions**.

Solution:

- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**:
  - Before transmitting, a device listens to the channel to check if it's free.
  - If the channel is free, it transmits data; otherwise, it waits and retries later.

D. Near-Far Problem

Issue:

- A **stronger signal from a nearby device** can overpower a weaker signal from a distant device, causing **packet loss** at the receiver.

Solution:

- **Power control mechanisms** adjust transmission power to balance signal strength.

E. Channel Contention & Congestion

Issue:

- Multiple devices competing for access to the same wireless channel can cause **delays, packet loss, and reduced performance**.

Solution:

- **Quality of Service (QoS) mechanisms** such as IEEE **802.11e**, which prioritizes traffic based on application needs (e.g., voice vs. data).

---

3. Solutions to MAC Issues in WLAN

MAC Issue	Solution
Hidden Node	RTS/CTS Mechanism
Exposed Node	Spatial Reuse Techniques
Hidden Terminal Collisions	CSMA/CA Protocol
Near-Far Problem	Power Control Mechanism
Channel Contention	QoS Mechanisms (802.11e)

The **IEEE 802.11** standard defines the **protocols for Wireless Local Area Networks (WLANs)**, commonly known as **Wi-Fi**. It specifies how wireless devices communicate over radio waves, ensuring **interoperability, security, and efficiency** in wireless networking.

---

1. IEEE 802.11 Architecture

A. Key Components of a WLAN

1. **Stations (STAs):** Devices with wireless interfaces (laptops, smartphones, etc.).
2. **Access Points (APs):** Connects wireless stations to the wired network.
3. **Basic Service Set (BSS):** A group of devices communicating with the same AP.
4. **Extended Service Set (ESS):** Multiple BSSs connected via a distribution system.

B. Modes of Operation

 Infrastructure Mode: Devices connect to an AP, which manages traffic.
 Ad-Hoc Mode: Devices communicate directly without an AP (peer-to-peer).

---

2. IEEE 802.11 Standards and Variants

Standard	Frequency	Max Speed	Range	Features
802.11 (Legacy)	2.4 GHz	2 Mbps	20m indoors	First WLAN standard
802.11a	5 GHz	54 Mbps	35m indoors	Less interference, shorter range
802.11b	2.4 GHz	11 Mbps	40m indoors	Low cost, more interference
802.11g	2.4 GHz	54 Mbps	40m indoors	Backward compatible with 802.11b
802.11n (Wi-Fi 4)	2.4 & 5 GHz	600 Mbps	70m indoors	MIMO (Multiple Input Multiple Output)
802.11ac (Wi-Fi 5)	5 GHz	6.9 Gbps	35m indoors	Beamforming, MU-MIMO
802.11ax (Wi-Fi 6)	2.4 & 5 GHz	9.6 Gbps	50m indoors	OFDMA, Better efficiency & speed

---

3. Key Technologies in IEEE 802.11

A. CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)

- Prevents data collisions by **listening** before transmitting.
- Uses **ACK (Acknowledgment) packets** to confirm successful transmissions.

B. MIMO (Multiple Input Multiple Output) – 802.11n & later

- Uses **multiple antennas** to improve speed and range.

C. Beamforming – 802.11ac & later

- Directs signals toward specific devices for **better connectivity**.

D. OFDMA (Orthogonal Frequency-Division Multiple Access) – 802.11ax

- Improves efficiency by **dividing channels** into smaller sub-channels for multiple users.

---

4. Security in IEEE 802.11

 WEP (Wired Equivalent Privacy) – Weak encryption, easily hacked.
 WPA (Wi-Fi Protected Access) – Improved security but still vulnerable.
 WPA2 (AES Encryption) – Stronger security, widely used.
 WPA3 – Enhanced encryption and protection against attacks.

---

5. Advantages of IEEE 802.11

✔ **Wireless Convenience** – No need for cables.
✔ **High-Speed Data Transfer** – Up to **9.6 Gbps (Wi-Fi 6)**.
✔ **Wide Adoption** – Used in homes, offices, and public spaces.
✔ **Backward Compatibility** – Newer Wi-Fi versions support older devices.

Bluetooth is used for short-range wireless voice and data communication. It is a Wireless Personal Area Network (WPAN) technology and is used for data communications over smaller distances. This generation changed into being invented via Ericson in 1994. It operates within the unlicensed, business, scientific, and clinical (ISM) bands from 2.4 GHz to 2.485 GHz.

Bluetooth stages up to 10 meters. Depending upon the version, it presents information up to at least 1 Mbps or 3 Mbps. The spreading method that it uses is FHSS (Frequency-hopping unfold spectrum). A Bluetooth network is called a piconet and a group of interconnected piconets is called a scatter net.

Key Features of Bluetooth

- The transmission capacity of Bluetooth is 720 kbps.
- Bluetooth is a wireless technology.
- Bluetooth is a Low-cost and short-distance radio communications standard.
- Bluetooth is robust and flexible.
- The basic architecture unit of Bluetooth is a piconet.

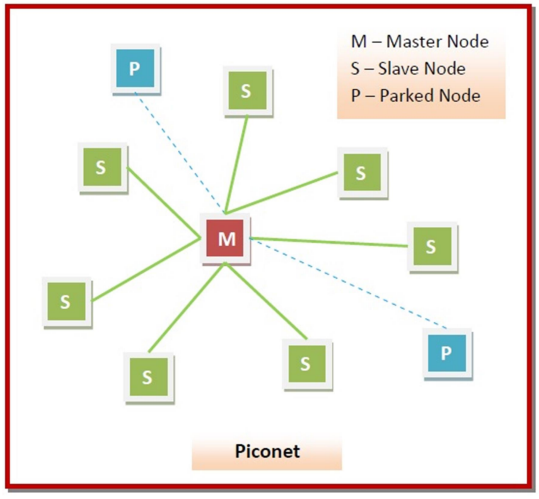
Architecture of Bluetooth

The architecture of Bluetooth defines two types of networks:

Piconet

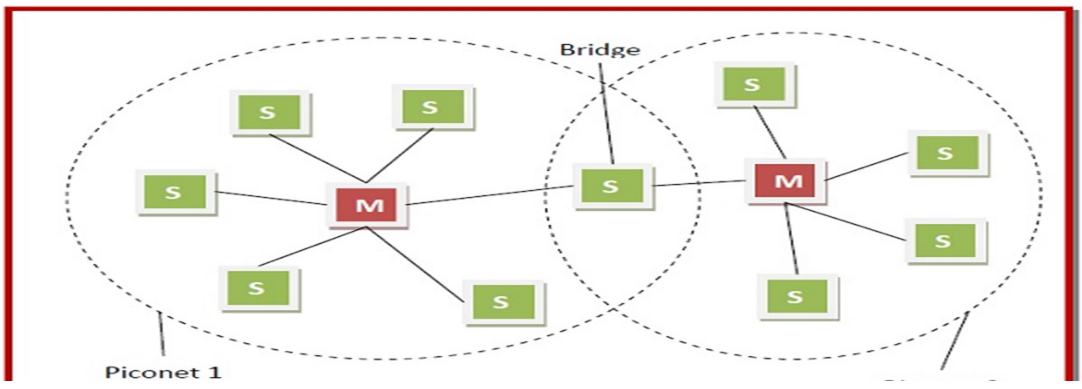
Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters.

The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.



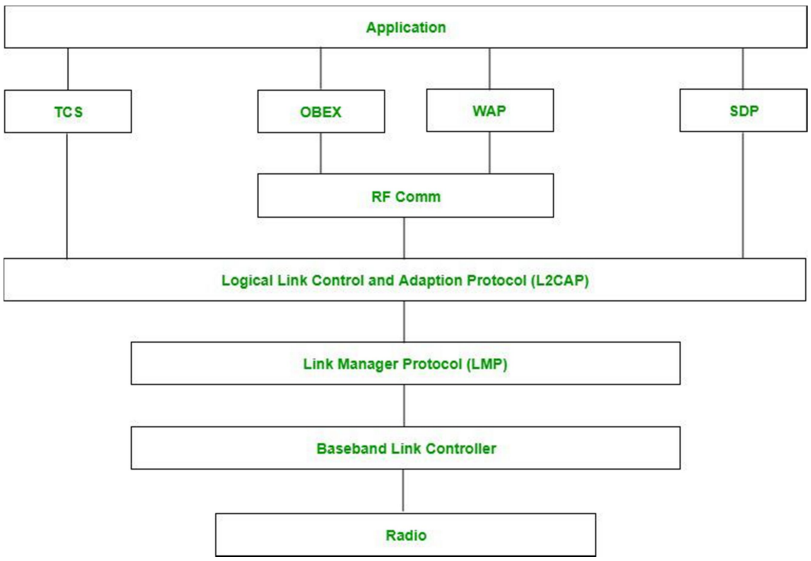
Scatternodes

A **scatternet** is an interconnected collection of two or more piconets. They are formed when a node in a piconet, whether a master or a slave, acts as a slave in another piconet. This node is called the bridge between the two piconets, which connects the individual piconets to form the scatternet.



Bluetooth Protocol Stack

- **Radio (RF) Layer:** It specifies the details of the air interface, including frequency, the use of frequency hopping and transmit power. It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.
- **Baseband Link Layer:** The baseband is the digital engine of a Bluetooth system and is equivalent to the MAC sublayer in LANs. It performs the connection establishment within a piconet, addressing, packet format, timing and power control.
- **Link Manager Protocol Layer:** It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.
- **Logical Link Control and Adaption (L2CAP) Protocol Layer:** It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and multiplexing.
- **Service Discovery Protocol (SDP) Layer:** It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.
- **RF Comm Layer:** It is a cabal replacement protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.
- **OBEX:** It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.
- **WAP:** It is short for Wireless Access Protocol. It is used for internet access.
- **TCS:** It is short for Telephony Control Protocol. It provides telephony service. The basic function of this layer is call control (setup & release) and group management for the gateway serving multiple devices.
- **Application Layer:** It enables the user to interact with the application.



Types of Bluetooth

Various types of Bluetooth are available in the market nowadays. Let us look at them.

- **In-Car Headset:** One can make calls from the car speaker system without the use of mobile phones.
- **Stereo Headset:** To listen to music in car or in music players at home.
- **Webcam:** One can link the camera with the help of Bluetooth with their laptop or phone.
- **Bluetooth-Equipped Printer:** The printer can be used when connected via Bluetooth with mobile phone or laptop.
- **Bluetooth Global Positioning System (GPS):** To use Global Positioning System (GPS) in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

Applications of Bluetooth

- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wireless to a mobile phone.
- It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
- It is used in the sectors of Medical healthcare, sports and fitness, Military.

Advantages

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Multiple Access Protocols are methods used in computer networks to control how data is transmitted when multiple devices are trying to

communicate over the same network. These protocols ensure that data packets are sent and received efficiently, without collisions or interference.

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk.

1. Random Access Protocol

In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

ALOHA

It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

Pure ALOHA

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

```
Vulnerable Time = 2* Frame transmission time
Throughput =  G exp{-2*G}
Maximum throughput = 0.184 for G=0.5
```

Slotted ALOHA

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

```
Vulnerable Time =  Frame transmission time
Throughput =  G exp{-*G}
Maximum throughput = 0.368 for G=1
```

CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay.

if station A wants to send data, it will first sense the medium. If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA Access Modes

- **1-Persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-Persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-Persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

CSMA/CA

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred.

CSMA/CA Avoids Collision

Interframe Space: Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS

- **Contention Window:** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.

- **Acknowledgement:** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access

Controlled access protocols ensure that only one device uses the network at a time. Think of it like taking turns in a conversation so everyone can speak without talking over each other.

3. Channelization

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA) –** The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA) –** In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.

Code Division Multiple Access (CDMA) – One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time.

- **Orthogonal Frequency Division Multiple Access (OFDMA) –** In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.
    - **Spatial Division Multiple Access (SDMA) –** SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Features of Multiple Access Protocols

Contention-Based Access: Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel.

- **Carrier Sense Multiple Access (CSMA):** CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.

- **Collision Detection (CD):** CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.
- **Collision Avoidance (CA):** CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.

Token Passing: Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel.

Bandwidth Utilization: Multiple access protocols can affect the overall bandwidth utilization of a network.

The **Transmission Control Protocol (TCP)** is a reliable transport-layer protocol designed for wired networks. However, in **wireless networks**, TCP faces several **challenges** due to factors like packet loss, congestion, and mobility. To improve performance, various **optimizations** are applied.

1. Challenges of TCP in Wireless Networks

A. High Packet Loss (Not Due to Congestion)

 Issue:

- TCP assumes **packet loss is due to congestion** and **reduces transmission speed**.
- In wireless networks, packet loss can be due to **signal fading, interference, or mobility**.

 Solution:
✔ Use **Selective Acknowledgment (SACK)** to retransmit only lost packets instead of reducing speed.
✔ Use **Explicit Loss Notification (ELN)** to inform TCP that packet loss is due to wireless issues, not congestion.

B. High Latency and Variable Delay

 Issue:

- Wireless links can have **variable latency** due to interference or handoffs.
- TCP interprets delays as **network congestion** and reduces its sending rate.

 Solution:
✔ Use **Adaptive Retransmission Timers** that adjust to variable delays.
✔ Implement **Delayed ACK** to reduce unnecessary acknowledgments.

C. Handoff Issues in Mobile Networks

□ **Issue**:

- In **mobile networks (Wi-Fi, 4G, 5G)**, devices switch from one base station to another.
- This can cause **packet loss and delay**, affecting TCP performance.

□ **Solution**:
✔ Use **Fast Retransmit and Fast Recovery** to quickly recover lost packets.
✔ Implement **Mobile IP** to maintain connectivity during handoff.

D. Bandwidth Variability

□ **Issue**:

- Wireless bandwidth fluctuates due to **network congestion, interference, and mobility**.
- TCP's congestion control mechanisms **fail to adapt quickly** to changing bandwidth.

□ **Solution**:
✔ Use **Bandwidth Estimation Techniques** to adjust transmission rates dynamically.
✔ Implement **TCP Westwood**, which adapts to bandwidth variations.

---

2. Optimized TCP Variants for Wireless Networks

TCP Variant	Key Feature	Use Case
TCP Reno	Standard TCP with fast recovery	Basic wired/wireless networks
TCP New Reno	Improves recovery from multiple losses	Wireless networks with high packet loss
TCP SACK	Selective retransmissions to avoid unnecessary data loss	Mobile and satellite networks
TCP Vegas	Congestion control based on delay measurements	High-latency wireless networks
TCP Westwood	Adapts to variable bandwidth in wireless links	Cellular and Wi-Fi networks

---

3. Solutions for Improving TCP Performance Over Wireless

☑**Split-TCP Approach** – Splits the TCP connection into wired and wireless segments to optimize transmission.
☑**Link-Layer Retransmission (ARQ)** – Wireless networks retransmit lost packets without TCP intervention.
☑**Explicit Congestion Notification (ECN)** – Informs TCP whether congestion or wireless issues are causing packet loss.
☑**Proxy-Based Solutions** – Intermediary nodes handle TCP optimizations for wireless networks.

Wireless applications, data broadcasting:

Wireless technology is widely used in **various industries** for communication, automation, and real-time data access.

A. Categories of Wireless Applications

Category	Example Applications
Mobile Communication	Smartphones, VoIP, Messaging Apps
Wireless Internet Access	Wi-Fi, 4G, 5G, Satellite Internet
IoT & Smart Devices	Smart Homes, Smart Cities, Industrial IoT
Healthcare & Telemedicine	Remote Patient Monitoring, Wearable Devices
Transportation & GPS	Navigation Systems, Vehicle Tracking
Military & Defense	Secure Communication, Drone Surveillance
Entertainment & Multimedia	Streaming Services, Wireless Gaming

---

B. Key Wireless Technologies Used in Applications

 Wi-Fi (802.11) – High-speed wireless internet.
 Bluetooth – Short-range communication (headsets, wearables).
 NFC (Near Field Communication) – Contactless payments.
 Zigbee & Z-Wave – Smart home automation.
 5G Networks – Ultra-fast data transfer, low latency.

Data casting or Data Broadcasting:

Data broadcasting (data broadcasting) refers to broadcasting data over an outsized area through radio waves. It usually refers to the supplementary information sent by TV stations and digital TV, but it also can be applied to digital signals on analog TV or broadcasting. It always doesn't apply to the inherent data of the media that outline virtual channels for DTV or direct broadcast satellite systems; or things like cable modems or satellite modems, which use completely independent data channels.

Data broadcasting usually provides news, weather, traffic, stock exchange and other information, which can or might not be associated with the program carried. It also can be interactive, like games, shopping or education.

Data broadcasting requirements:

Due to the limited bandwidth of mobile systems, data should be organized and provided to users according to data needs.

Data broadcasting can be used to manage the interest in sending (pushing) the same data to listening clients without prior request (or locking). The server continuously broadcasts data to the MU.

• Scalability: The cost does not depend on the number of users listening.

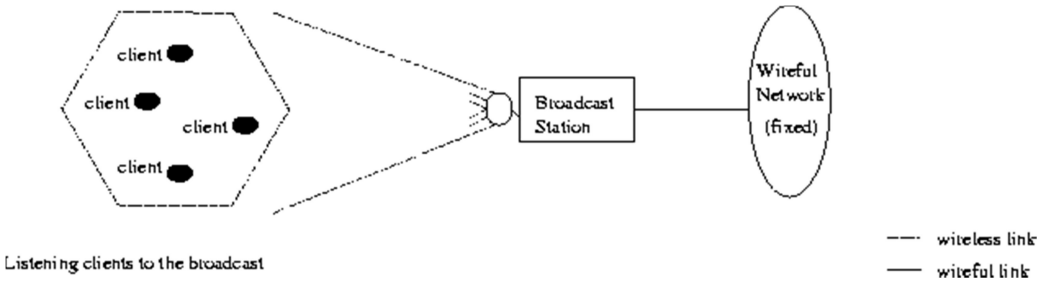
• The mobile unit may/may not be cached. • Facilitate data access during disconnection.

• Allow access to location-related data.

• There is no need to predict future data requirements with 100% accuracy.

Broadcast according to access probability.

• Broadcast all data regularly.



Listening clients to the broadcast

MOBILE IP (Problem situation):

The host's address consists of two parts: (1) The high-order bits of the address determine the n/w where the host is located (2), and the remaining low-order bits determine the host number. IP determines the next hop by determining network information based on the destination IP address of the data packet. On the other hand, higher layers like TCP maintain information about the connection, which is indexed by a four-tuple containing the IP address and port number of the endpoint. Therefore, when trying to support mobility on the Internet under the existing protocol suite, we are faced with two conflicting requirements:

Whenever a mobile node changes its connection point, it must change its IP address in order to correctly route data packets destined for that node.

To maintain an existing TCP connection, the IP address of the mobile node must remain unchanged. Changing the IP address will cause disconnection and loss of connection.

Computer mobility in heterogeneous networks.

Relocation between different IP subnets.

Goal: Transparent migration and localization, compatibility with IP, no changes to existing routers.

Idea: Introduce temporary/actual IP addresses (also known as "care-of address", COA);

Use localization technology to map permanent IP addresses to temporary IP addresses.

Motivation:

Mobile IP may be a proposed standard protocol, which is predicated on the web protocol, and realizes packet routing and delivery by making mobility transparent to applications and higher-level protocols (such as TCP).

Due to the big variety of wireless devices that provide IP connectivity (such as PDAs, handheld devices, and digital cellular phones), people's views on the web have changed.

Routing:

- Based on IP destination address, network prefix (for example, 129.13.42).
- Determine the physical subnet.
- The change of the physical subnet means changing the IP address to possess the right topological address (standard IP) or a special entry must be added to the routing table.

The specific route to the ultimate system?

- Change all routing table entries to forward the packet to the right destination.
- Cannot follow the rise within the number of mobile hosts and frequent changes in location, security issues.

Change IP address? : A simple solution is to let the mobile host change its address when entering a new network.

- Adjust the host IP address according to the current location.
- DNS update almost takes a long time to find the mobile system.
- TCP connection is interrupted, security issues.
- Without specific support, the mobile node cannot deliver from its local IP subnet (because of the routing based on the network prefix and destination IP address).
- The IP address cannot be changed when moving to a new IP subnet (because TPT/higher level connections cannot be maintained).

Use DHCP to obtain a new address to associate it with the new network. This method has several disadvantages.

- The configuration file will need to be changed
- Every time a computer moves from one network to another, it must be restarted.
- The DNS table needs to be modified so that all other hosts on the Internet are aware of the change.

- If the host roams from one N/W to another N/W during transmission, the data exchange will be interrupted. This is because the port and IP address of the client and server must remain unchanged during the connection.

MOBILE IP: Introduction:

Mobile IP was developed to enable a computer to take care of an online connection while moving from one Internet connection point to a different Internet connection point. It is an online Engineering Task Force (IETF) standard communication protocol designed to permit mobile device users to move from one network to a different while retaining a permanent IP address. Provide an efficient and scalable mechanism to roam within the web.

- Using mobile IP, a node can change its connection point with the web without changing its IP address. This permits them to take care of transmission and high-level connections while on the move.
- Don’t assume "base stations" are everywhere.
- Simple
- The communication host doesn't got to understand mobility
- Suitable for changing domain and network interface
- Although suitable for wired environments, it's especially suitable for wireless environments
- In "mobile connection": keep the connection, in "mobile connection": establish a replacement connection after each move.

Requirements to Mobile IP (RFC 2002):

Compatibility:

- Support the same layer 2 protocol as IP.
- No need to change the current terminal system and router.
- Mobile terminal system can communicate with fixed system.

Transparency:

- The mobile terminal system reserves its IP address.
- Possibility to continue communication after the link is interrupted.
- Can change the connection point with the fixed network.

Efficiency and scalability:

- Only a few additional messages to the mobile system.
- (Usually connected via a low-bandwidth radio link).
- Support for a large number of mobile systems worldwide.

Safety:

- Verify all registration messages.

Mobile IP: Terminology:

Home network: In terms of its IP address, it's the subnet to which the MN belongs. No mobile IP support is required within the home network.

External network: this is often the present subnet visited by the MN, not the local network.

Mobile Node (MN): A node that moves throughout the network without changing its IP address.

Communication node (CN): MN and its corresponding host (TCP).

Home Agent (HA):

- The host within the MN's home network, usually a router.
- Maintain the mobility binding table, where each entry is identified by the tuple. The aim of this table is to map the house address of the mobile node with its COA and forward data packets accordingly.
- Register the situation of the MN, and transmit the IP data packet to the COA through the tunnel.

Foreign Agent (FA):

- The host within the current external network of MN, usually a router.
- Maintain a visitor list that contains information about the mobile nodes currently visiting that n/w. Each entry within the visitor list is identified by the tuple.
- Forward tunnel packets to MN, usually the default router of MN.

Care of address (COA):

- MN's current tunnel endpoint address (in FA or MN).
- View the particular location of MN from an IP perspective.