MOBILE COMPUTING

UNIT-2

- **Mobile System**

A mobile system refers to a combination of hardware, software, and network infrastructure that enables communication and computing on mobile devices such as smartphones, tablets, and laptops. Mobile systems rely on wireless networks to provide seamless connectivity and mobility.

Key Components of a Mobile System:

1. Mobile Devices – Smartphones, tablets, and other portable devices.

2. Operating Systems – Android, iOS, Windows Mobile.

3. Applications – Apps that run on mobile devices.

4. Network Infrastructure – Cellular networks (4G, 5G), Wi-Fi, and Bluetooth.

5. Cloud & Backend Services – Cloud computing, databases, APIs supporting mobile apps.

- **Wireless Network:**

A wireless network is a communication system that enables devices to connect and exchange data without physical cables. Wireless networks use radio waves, infrared signals, or satellite communications for data transmission.

Types of Wireless Networks:

1. Cellular Networks – 2G, 3G, 4G, 5G for mobile communication.

2. Wi-Fi – Local wireless networking for internet access.

3. Bluetooth – Short-range communication between devices.

4. Satellite Communication – Used for GPS, remote area connectivity.

5. IoT Networks – Zigbee, LoRaWAN, and NB-IoT for smart devices.

- **Relationship between Mobile Systems and Wireless Networks**

• Mobile systems rely on wireless networks to enable communication and data transfer.

• Wireless networks provide mobility and flexibility, reducing reliance on wired infrastructure.

• The growth of mobile technology (smartphones, wearables, IoT) is driving advancements in wireless networks (5G, Wi-Fi 6).

GSM

GSM stands for **G**lobal **S**ystem for **M**obile Communication. It is a digital cellular technology used for transmitting mobile voice and data services. Important facts about the GSM are given below −

- The concept of GSM emerged from a cell-based mobile radio system at Bell Laboratories in the early 1970s.
- GSM is the name of a standardization group established in 1982 to create a common European mobile telephone standard.
- GSM is the most widely accepted standard in telecommunications and it is implemented globally.
- GSM is a circuit-switched system that divides each 200 kHz channel into eight 25 kHz time-slots. GSM operates on the mobile communication bands 900 MHz and 1800 MHz in most parts of the world. In the US, GSM operates in the bands 850 MHz and 1900 MHz.

- GSM owns a market share of more than 70 percent of the world's digital cellular subscribers.
- GSM makes use of narrowband Time Division Multiple Access (TDMA) technique for transmitting signals.
- GSM was developed using digital technology. It has an ability to carry 64 kbps to 120 Mbps of data rates.
- Presently GSM supports more than one billion mobile subscribers in more than 210 countries throughout the world.
- 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 digitizes and compresses data, then sends it down through a channel with two other streams of user data, each in its own timeslot.

- **Why GSM?**

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

• Improved spectrum efficiency

• International roaming

• Low-cost mobile sets and base stations (BSs)

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

1. Global System for Mobile Communications (GSM)

GSM (Global System for Mobile Communications) is a **2G (second-generation)** digital mobile network standard that enables voice and data communication. It was developed to replace analog cellular networks and became the most widely used mobile communication standard globally.

Key Features of GSM

✓ **Digital Technology** – Uses digital signals for better call quality and security.
✓ **International Roaming** – Allows users to connect across different countries.
✓ **SIM Card-Based System** – Mobile services are linked to a SIM card, not the device.
✓ **Efficient Frequency Usage** – Uses Frequency Division Multiple Access (FDMA) and Time Division Multiple Access (TDMA) to maximize network capacity.
✓ **Supports Data Services** – Enables SMS, MMS, and mobile internet (GPRS, EDGE).

GSM Architecture

GSM consists of multiple components that work together to provide seamless mobile communication. The architecture is divided into the following subsystems:

1. Mobile Station (MS)

The **Mobile Station** is the device used by the user, consisting of:

- **Mobile Equipment (ME)** – The physical phone or mobile device.
- **Subscriber Identity Module (SIM)** – A smart card that stores user identity, phone number, and network details.

2. Base Station Subsystem (BSS)

Responsible for communication between mobile devices and the network. Includes:

- **Base Transceiver Station (BTS)** – Handles radio communication with mobile devices.
- **Base Station Controller (BSC)** – Manages multiple BTS, handles handovers, and allocates resources.

3. Network and Switching Subsystem (NSS)

Manages call routing, authentication, and mobility. Includes:

- **Mobile Switching Center (MSC)** – Routes calls and messages between mobile and landline networks.
- **Home Location Register (HLR)** – Stores permanent user information (e.g., SIM details, services).
- **Visitor Location Register (VLR)** – Temporarily stores user data when they roam into a new area.

- **Authentication Center (AuC)** – Provides security by authenticating users and encrypting data.
- **Equipment Identity Register (EIR)** – Maintains a list of valid and stolen mobile devices.

4. Operation and Support System (OSS)

- Monitors and manages the entire GSM network.
- Ensures network performance, maintenance, and troubleshooting.

GSM Network Interfaces

GSM operates using different interfaces to facilitate smooth communication:

- **Um Interface** – Connects Mobile Station (MS) with Base Transceiver Station (BTS).
- **Abis Interface** – Connects BTS with Base Station Controller (BSC).
- **A Interface** – Connects BSC with Mobile Switching Center (MSC).

GSM Services

GSM provides various services, including:

1. Telephony Services

Voice Calls – Supports high-quality mobile-to-mobile and mobile-to-landline calls.
Short Message Service (SMS) – Allows text messaging.
Multimedia Messaging Service (MMS) – Supports image and video messaging.

2. Data Services

GPRS (2.5G) – Basic internet access (up to 171 Kbps).
EDGE (2.75G) – Enhanced speed for internet and multimedia services (up to 384 Kbps).

3. Supplementary Services

Call Forwarding, Call Waiting, Call Holding
Caller ID, Call Blocking, Voicemail

Advantages of GSM

✓ **Global Standard** – Used in over 200 countries.
✓ **Better Call Quality** – Digital transmission reduces noise and interference.
✓ **SIM Card Flexibility** – Allows users to switch devices easily.
✓ **Secure Communication** – Uses encryption for data protection.

Disadvantages of GSM

❌ **Limited Data Speed** – Slower internet compared to modern technologies like 4G/5G.
❌ **Signal Interference** – Can be affected by buildings and environmental factors.
❌ **Higher Latency** – Slight delay in voice transmission compared to newer networks.

📶 CDMA – Code Division Multiple Access

CDMA stands for **Code Division Multiple Access**, which is a **digital cellular technology** used for transmitting voice, data, and signaling between mobile devices and base stations. Unlike GSM (which uses Time Division), CDMA allows **multiple users to occupy the same frequency band at the same time**, but separates them using **unique codes**. It is based on **spread-spectrum technology**, which spreads the signal over a wide frequency band, making it more secure and efficient.

🌐 How CDMA Works

In CDMA, all users **share the same frequency range simultaneously**, but each user is assigned a **unique code** known as a **pseudorandom code**. When a user sends data, their data is **encoded with this unique code**. On the receiving end, the system decodes the signal using the same code to extract the data meant for a specific user.

- Each user's signal is spread across the entire bandwidth.
- The receiver filters out all signals except the one with the correct code.
- It's similar to multiple people speaking different languages in the same room — you only understand the one speaking your language (code).

📊 Key Features of CDMA

- **Efficient spectrum usage:** All users share the same frequency band.
- **Resistance to interference:** Spread spectrum makes it robust against jamming and interference.
- **Improved capacity:** More users per MHz than GSM.
- **Soft handoff:** Smooth transfer between base stations, reducing dropped calls.
- **Secure communication:** Difficult to intercept due to code-based access.

🔧 CDMA Architecture Components

CDMA architecture includes:

1. **Mobile Station (MS):** The user device.
2. **Base Station Subsystem (BSS):**
    - **Base Transceiver Station (BTS)**
    - **Base Station Controller (BSC)**
3. **Mobile Switching Center (MSC):** Handles call routing and mobility.
4. **Databases:** HLR, VLR, AuC, EIR (same as GSM)
5. **PDSN (Packet Data Serving Node):** Supports internet/data services in CDMA2000 networks.

📡 CDMA Technologies

- **IS-95 (cdmaOne):** First CDMA standard, used in 2G.
- **CDMA2000:** Enhanced version, supports 3G services.
- **WCDMA (used in UMTS):** Used in 3G GSM evolution (not the same as IS-95).

✅ Advantages of CDMA

- Higher user capacity
- Better call quality and lower dropped calls
- Strong privacy and security
- Efficient use of bandwidth
- Supports soft handoff

⚠️ Disadvantages of CDMA

- Complex system design
- Difficult to allocate unique codes as the network grows
- Limited international roaming (compared to GSM)
- Gradually being replaced by newer technologies like 4G LTE and 5G

📘 Summary

CDMA is a multiple access technology that allows many users to share the same frequency by assigning each a unique code. It is known for its **efficiency, security**, and **capacity**, and was widely used in the U.S. and parts of Asia. Though it is being phased out in favor of LTE/5G, CDMA played a key role in the development of modern mobile communication systems.

📡 FDMA – Frequency Division Multiple Access

FDMA stands for **Frequency Division Multiple Access**. It is one of the **earliest and simplest multiple access techniques** used in wireless communication systems, especially in **1G (first generation)** mobile networks like analog cellular systems (e.g., AMPS in the USA).

🧠 What is FDMA?

In FDMA, the **available frequency band is divided into multiple smaller frequency channels**, and **each user is assigned a unique frequency** during a call or transmission session. These channels are **separated by guard bands** to avoid overlapping and interference.

- Think of it like a multi-lane highway: each car (user) stays in its own lane (frequency band), avoiding collisions.
- If 30 users are talking at the same time, each will be given a separate channel to transmit and receive.

🔁 How FDMA Works

- The **total bandwidth** is divided into **fixed frequency channels**.
- Each **call or session** is given **one frequency channel** for the full duration.
- Once the call ends, that frequency is freed and can be assigned to another user.
- A **guard band** (small unused bandwidth) is placed between channels to prevent interference.

🧱 FDMA System Components

1. **Frequency Allocator:** Divides and assigns the frequencies.
2. **Multiplexer/Demultiplexer:** Combines and separates multiple signals.
3. **Transmitter/Receiver:** Uses the assigned frequency for communication.

✅ Advantages of FDMA

- **Simple implementation**
- **Low latency**: Since each user has a dedicated channel
- **No interference** between users (if guard bands are properly maintained)

- Good for **analog voice communication**

⚠️ Disadvantages of FDMA

- **Inefficient spectrum usage** – fixed channels can remain unused during idle times.
- **Limited scalability** – number of users is restricted by number of frequency channels.
- **Requires large bandwidth** and guard bands.
- Not suitable for **high-speed data** or multimedia services.

📘 Summary

FDMA is a multiple access technique in which **each user is assigned a separate frequency channel** for communication. It was widely used in **1G analog systems** but is no longer used in modern cellular networks due to **inefficient use of spectrum** and limited capacity. Newer technologies like **TDMA, CDMA, and OFDMA** offer better performance and are preferred in digital and high-speed data systems.

⏱️ TDMA – Time Division Multiple Access

TDMA (Time Division Multiple Access) is a **digital multiple access technique** used in wireless communication systems, where **multiple users share the same frequency channel**, but **each user is assigned a unique time slot**. It was widely used in **2G cellular systems**, including **GSM**, **IS-136**, and others.

🧠 What is TDMA?

In TDMA, the total available frequency is **divided in time** rather than in frequency (like FDMA). Each user transmits in **rapidly alternating time slots**, and although only one user transmits at a time, the switching happens so quickly that all users **appear to have continuous communication**.

📌 Example: Think of TDMA like a round-robin meeting where each person speaks one at a time, but quickly and repeatedly, so it feels like everyone is speaking continuously.

🔁 How TDMA Works

- The **frequency channel is divided into time slots** (e.g., 8 slots per channel in GSM).
- Each user is **assigned one or more time slots**.
- Users take turns to transmit/receive in their slot.
- A **synchronization mechanism** ensures that users stick to their assigned slots to avoid collisions.
- Unused slots can remain idle or be dynamically reassigned.

🧱 TDMA System Architecture

1. **Base Transceiver Station (BTS):** Allocates and manages time slots.
2. **Mobile Station (MS):** Communicates only during its time slot.
3. **Timing Control Unit:** Synchronizes user access.
4. **Time Slot Scheduler:** Ensures smooth switching between users.

📶 TDMA in GSM

- In **GSM**, each 200 kHz channel is divided into **8 time slots**.
- So, **8 users can share a single frequency**.
- It supports **digital voice**, **SMS**, and **low-speed data**.

✅ Advantages of TDMA

- **Efficient use of bandwidth**: Multiple users on one frequency.

- **Reduced power consumption**: Devices transmit only during their time slot.
- **Simple implementation** in digital systems.
- Supports **encryption and error correction**.

⚠️ Disadvantages of TDMA

- **Synchronization needed**: Accurate timing is critical.
- **Time slot collision** possible if not managed properly.
- **Limited data rate per user**: Depends on slot size.
- **Latency** can be higher compared to CDMA.

📘 Summary

TDMA is a digital access method in which **multiple users share the same frequency** by transmitting in different **time slots**. It was widely used in **2G systems like GSM**, offering better bandwidth usage and digital quality over FDMA. However, it has been largely replaced by more advanced technologies like **CDMA, OFDMA, and LTE**, which provide higher data speeds and scalability.

FDMA vs. TDMA vs. CDMA

Feature	FDMA	TDMA	CDMA
Access Method	Frequency Division	Time Division	Code Division
Channel Allocation	Fixed frequency per user	Time slots per user	Unique code per user
Interference	Low (due to separate frequencies)	Medium (due to time-sharing)	High (if overloaded)
Spectrum Efficiency	Low	Higher than FDMA	Very high
Synchronization Needed?	No	Yes	Yes
Used In	1G Networks, Satellite Systems	2G (GSM)	3G, 4G, 5G

Wireless networking:

Wireless Networking

Wireless Networking refers to a type of communication where devices connect and exchange data without physical cables, using **radio waves, infrared signals, or satellite links**. It enables seamless communication between computers, smartphones, IoT devices, and other networked systems.

Key Features of Wireless Networking

✅ **No Physical Cables** – Uses radio waves instead of wires.
✅ **Mobility & Flexibility** – Devices can move freely while staying connected.
✅ **Scalability** – Easy to add new devices without additional cabling.
✅ **Cost-Effective** – Reduces installation and maintenance costs.
✅ **Remote Connectivity** – Supports long-distance communication via satellites and cellular networks.

Types of Wireless Networks

Wireless networks are categorized based on their coverage area and technology:

1. Wireless Local Area Network (WLAN)

- Connects devices within a **small area** (home, office, campus).
- Uses **Wi-Fi (802.11 standards)** for internet and local connectivity.
- Example: Home Wi-Fi, Office Networks.

2. Wireless Metropolitan Area Network (WMAN)

- Covers a **city-wide** area.
- Uses technologies like **WiMAX (Worldwide Interoperability for Microwave Access)**.
- Example: Citywide Wi-Fi, Public WiMAX Services.

3. Wireless Wide Area Network (WWAN)

- Covers a **large geographical area** (nationwide or globally).
- Uses **cellular networks (3G, 4G, 5G) or satellite communication**.
- Example: Mobile Networks, GPS, Satellite Internet.

4. Wireless Personal Area Network (WPAN)

- Short-range communication for personal devices.
- Uses technologies like **Bluetooth, Zigbee, NFC (Near Field Communication)**.
- Example: Bluetooth headsets, Smartwatches, Home Automation.

Wireless Networking Technologies

🚀 **Wi-Fi (Wireless Fidelity)** – Standard for WLANs, used in homes, offices, and public hotspots.
📶 **Cellular Networks (2G, 3G, 4G, 5G)** – Used for mobile communication and internet access.
📡 **Bluetooth** – Short-range communication for personal devices.
🔗 **Zigbee & Z-Wave** – Used in IoT and smart home applications.
🌍 **Satellite Communication** – Provides internet and GPS services worldwide.
📻 **Infrared Communication** – Used in remote controls and some IoT applications.

Advantages of Wireless Networking

✓ **Easy Installation** – No need for physical cables.
✓ **Mobility** – Users can connect from anywhere within the network range.
✓ **Scalability** – Easy to expand by adding more devices.
✓ **Cost-Effective** – Reduces infrastructure and maintenance costs.
✓ **Remote Access** – Enables cloud computing and remote working.

Disadvantages of Wireless Networking

✗ **Security Risks** – More vulnerable to hacking, eavesdropping, and unauthorized access.
✗ **Interference Issues** – Affected by physical obstacles and other wireless devices.
✗ **Limited Speed & Range** – Slower than wired networks, especially at long distances.
✗ **Power Consumption** – Wireless devices need constant power and battery management.

Wireless Networking vs. Wired Networking

Feature	Wireless Networking	Wired Networking
Medium	Radio Waves	Ethernet Cables
Mobility	High	Limited
Installation	Easy	Complex
Speed	Moderate (Wi-Fi 6 can reach high speeds)	Very High (Fiber Optic, Ethernet)
Security	Less secure (prone to hacking)	More secure
Cost	Lower setup costs	Higher due to cabling

What is Wireless LAN (WLAN)?

A **Wireless Local Area Network (WLAN)** is a type of local area network that uses wireless communication to connect devices within a limited geographical area, such as a home, office, or campus. Instead of using physical cables (like Ethernet cables), WLAN relies on radio waves or infrared signals to enable devices to communicate with each other and connect to the internet.

Key Components of WLAN

1. **Wireless Access Point (WAP)**
    - Acts like a hub or switch in a wired LAN.
    - Provides a wireless communication point for devices to connect.
    - Connects to a wired network (like Ethernet) to bridge wired and wireless devices.
2. **Wireless Network Interface Cards (NICs)**
    - Installed in client devices (laptops, smartphones, tablets).
    - Allows the device to communicate over wireless signals.
3. **Wireless Router**
    - Combines the functions of a router and access point.
    - Often used in home or small office WLAN setups.
    - Connects multiple devices wirelessly and manages network traffic.
4. **Clients/Stations**
    - Devices such as laptops, smartphones, tablets, printers that connect to WLAN.

How WLAN Works

- Devices equipped with wireless NICs send and receive data using radio frequencies.
- The WAP or wireless router receives data wirelessly and passes it to the wired network or the internet.
- WLANs use protocols defined by the IEEE 802.11 family (e.g., 802.11a/b/g/n/ac/ax).

WLAN Standards (IEEE 802.11)

- **802.11b**: Early standard operating at 2.4 GHz, speeds up to 11 Mbps.
- **802.11a**: Operates at 5 GHz with speeds up to 54 Mbps.
- **802.11g**: Operates at 2.4 GHz, speeds up to 54 Mbps.
- **802.11n**: Uses both 2.4 GHz and 5 GHz bands, speeds up to 600 Mbps.
- **802.11ac**: Operates primarily at 5 GHz, speeds up to several Gbps.
- **802.11ax (Wi-Fi 6)**: Latest standard, improved speed, efficiency, and capacity.

WLAN Frequency Bands

- **2.4 GHz Band**:
    - Longer range but more susceptible to interference (from microwaves, Bluetooth, cordless phones).
    - Supports fewer channels, which can cause congestion.
- **5 GHz Band**:
    - Shorter range but less interference and more channels.
    - Supports higher data rates.

WLAN Topologies

1. **Infrastructure Mode**
    - Devices communicate through an access point.
    - Centralized control.
    - Common in offices and homes.
2. **Ad-Hoc Mode (Peer-to-Peer)**
    - Devices communicate directly without an access point.
    - Temporary setup for quick communication.

WLAN Security

Since WLANs use wireless signals, they are more vulnerable to security threats like eavesdropping and unauthorized access. Common security mechanisms include:

- **WEP (Wired Equivalent Privacy)** – Older and less secure.
- **WPA (Wi-Fi Protected Access)** and **WPA2** – Improved encryption and security.
- **WPA3** – The latest, stronger security features.
- **MAC Address Filtering** – Restricts devices allowed to connect.
- **SSID Broadcasting Control** – Hides the network name.
- **Authentication Protocols** – Like 802.1X and RADIUS for enterprise-level security.

Advantages of WLAN

- **Mobility**: Users can move freely within the network coverage area.
- **Ease of Installation**: No need for complex cabling.
- **Flexibility**: Easy to add new devices.
- **Cost-Effective**: Saves wiring costs in certain environments.

Limitations of WLAN

- **Security Risks**: Wireless signals can be intercepted.
- **Interference**: Other wireless devices or physical barriers can affect performance.
- **Range Limitations**: Coverage is limited by distance and obstacles.
- **Speed**: Typically slower than wired LAN.

Typical Applications of WLAN

- Corporate offices for employee mobility.
- Homes for internet access on multiple devices.
- Public hotspots (cafes, airports).
- Educational campuses.
- Industrial environments for wireless control and monitoring.

🔷 Bluetooth:

Bluetooth is a **short-range wireless communication technology** that enables devices to exchange data over short distances using **radio frequency (RF)** in the **2.4 GHz ISM band** (Industrial, Scientific, and Medical). It was originally developed as a wireless alternative to RS-232 data cables.

Bluetooth is ideal for personal area networks (PANs), connecting devices like:

- Smartphones
- Headphones
- Laptops
- Keyboards
- Smartwatches
- IoT devices

📡 How Bluetooth Works

Bluetooth works by using **frequency hopping spread spectrum (FHSS)**. This means:

- Devices switch frequencies rapidly (up to 1,600 times per second) among 79 channels (in classic Bluetooth).
- This reduces interference and allows multiple devices to share the same frequency band.

Devices communicate via **piconets** and **scatternets**:

- **Piconet**: A small network with one master and up to 7 active slaves.
- **Scatternet**: Multiple interconnected piconets.

📐 Bluetooth Architecture

1. **Master Device**
    - Controls the communication link.
    - Initiates and manages connections.
2. **Slave Devices**
    - Respond to the master's commands.
3. **Bluetooth Stack**
    - A set of protocols that manage everything from signal transmission to application-level operations.
    - Key layers:
        - **Radio Layer**
        - **Baseband Layer**
        - **L2CAP (Logical Link Control and Adaptation Protocol)**
        - **RFCOMM** (Serial Port Emulation)
        - **SDP (Service Discovery Protocol)**

🛡️ Bluetooth Security

Bluetooth uses several techniques for secure communication:

1. **Pairing**: Devices authenticate using PIN codes or numeric comparison.
2. **Encryption**: Data is encrypted during transmission.
3. **Authentication**: Verifies the identity of communicating devices.
4. **Secure Simple Pairing (SSP)**: Introduced in Bluetooth 2.1 for improved security.

Risks:

1. **Bluejacking**: Sending unsolicited messages.
2. **Bluesnarfing**: Unauthorized access to information.
3. **Bluebugging**: Taking control of a device.

⚙️ Bluetooth Profiles (Use Cases)

Bluetooth profiles define possible applications:

1. **A2DP** – Advanced Audio Distribution Profile (e.g., wireless audio)
2. **AVRCP** – Audio/Video Remote Control Profile
3. **HSP/HFP** – Headset/Hands-Free Profile (e.g., calls)
4. **OBEX/OPP** – Object Push Profile (file transfer)
5. **PBAP** – Phone Book Access Profile
6. **GATT** – Generic Attribute Profile (for BLE devices)
7. **HID** – Human Interface Device (keyboards, mice)

🟢 Bluetooth Low Energy (BLE) vs Classic Bluetooth

Feature	Classic Bluetooth	BLE
Use Case	Audio, file transfer	IoT, fitness trackers
Data Rate	Up to 3 Mbps	1 Mbps
Power Usage	High	Very low
Connection Time	Longer	Faster
Profiles	Many classic profiles	GATT-based

🔁 Bluetooth Applications

- **Wireless audio** (headphones, speakers)
- **Peripheral connectivity** (keyboard, mouse)
- **File transfer**
- **Health and fitness** (heart rate monitors, fitness bands)
- **Home automation** (smart lights, locks)
- **Location tracking** (asset trackers, beacons)
- **Automotive** (hands-free calling, media)

✅ Advantages of Bluetooth

- Easy to use and pair
- Low power consumption (especially BLE)
- No need for line-of-sight
- Wide support across devices and platforms
- Inexpensive and compact hardware

❌ Limitations of Bluetooth

- Limited range compared to Wi-Fi
- Lower data transfer speeds
- Potential for interference in crowded 2.4 GHz band
- Security vulnerabilities if not properly configured

📡 Wireless Multiple Access Protocols – Overview

In wireless networks, **multiple access protocols** manage how multiple devices share the same communication medium (radio waves) **without interference** or collision. Since there's no physical wire (like in Ethernet), controlling access is more complex.

These protocols ensure:

- Efficient **channel sharing**
- **Collision avoidance**
- **Fairness** among devices
- **High throughput** and **low latency**

🎯 Why Are They Important in Wireless Networks?

Unlike wired networks:

- Wireless devices can't **always detect each other** (hidden node problem).
- **Collisions are harder to detect**.
- Bandwidth is more limited and **shared**.

Hence, special **media access control (MAC) protocols** are needed.

Categories of Wireless Multiple Access Protocols:

1. **Random Access Protocols:**

   - ALOHA: One of the earliest protocols, where devices transmit whenever they have data, leading to potential collisions. Variants include Pure ALOHA and Slotted ALOHA, with the latter reducing collision chances by dividing time into slots.

   -Carrier Sense Multiple Access (CSMA): Devices sense the medium before transmitting. If the medium is idle, they proceed; if busy, they wait, reducing the likelihood of collisions.

2. Controlled Access Protocols:

- Reservation-Based: Devices reserve a time slot for transmission in advance, ensuring exclusive access during that period.

- Polling: A central controller polls devices in a predetermined order, granting them permission to transmit.

- Token Passing: A token circulates among devices; only the device possessing the token can transmit, preventing collisions.

3. Channelization Protocols:

a) TDMA (Time Division Multiple Access)

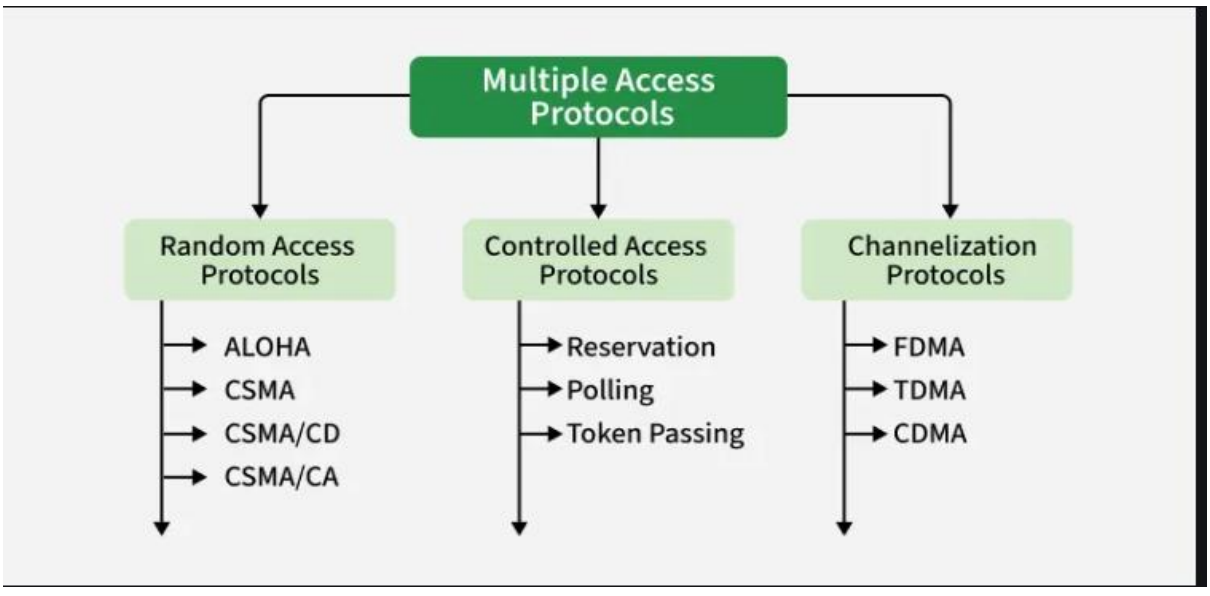
1. Time is divided into slots.
2. Each device is assigned a specific time slot.
3. Efficient but requires synchronization.
4. Used in GSM mobile networks.

b) FDMA (Frequency Division Multiple Access)

1. Frequency band is divided into channels.
2. Each user/device gets a separate frequency.
3. Used in analog cellular systems.

c) CDMA (Code Division Multiple Access)

1. Devices transmit over the same frequency at the same time.
2. Each has a unique code to spread the signal.
3. Allows multiple users to share the channel with minimal interference.
4. Used in 3G mobile systems.



➢TCP Over Wireless:

The Transmission Control Protocol (TCP) is a cornerstone of reliable data transmission over the Internet, ensuring ordered and error-checked delivery of data between applications. However, when operating over wireless networks, TCP faces unique challenges that can degrade its performance.

Layers in the TCP/IP Suite-

Physical Layer

TCP/IP does not define any specific protocol for the physical layer. It supports all of the standard and proprietary protocols.

- At this level, the communication is between two hops or nodes, either a computer or router. The unit of communication is a **single bit**.
- When the connection is established between the two nodes, a stream of bits is flowing between them. The physical layer, however, treats each bit individually.

The responsibility of the physical layer, in addition to delivery of bits, matches with what mentioned for the physical layer of the OSI model, but it mostly depends on the underlying technologies that provide links.

Data Link Layer

TCP/IP does not define any specific protocol for the data link layer either. It supports all of the standard and proprietary protocols.

- At this level also, the communication is between two hops or nodes. The unit of communication however, is a packet called a **frame**.
- A **frame** is a packet that encapsulates the data received from the network layer with an added header and sometimes a trailer.
- The head, among other communication information, includes the source and destination of frame.
- The **destination address** is needed to define the right recipient of the frame because many nodes may have been connected to the link.
- The **source address** is needed for possible response or acknowledgment as may be required by some protocols.

LAN, Packet Radio and Point-to-Point protocols are supported in this layer

Network Layer

At the network layer, TCP/IP supports the Internet Protocol (IP). The Internet Protocol (IP) is the transmission mechanism used by the TCP/IP protocols.

- IP transports data in packets called **datagrams**, each of which is transported separately.
- Datagrams can travel along different routes and can arrive out of sequence or be duplicated.

IP does not keep track of the routes and has no facility for reordering datagrams once they arrive at their destination.

Transport Layer

There is a main difference between the transport layer and the network layer. Although all nodes in a network need to have the network layer, only the two end computers need to have the transport layer.

- The network layer is responsible for sending individual datagrams from computer A to computer B; the transport layer is responsible for delivering the whole message, which is called a **segment**, from A to B.
- A segment may consist of a few or tens of **datagrams**. The segments need to be broken into datagrams and each datagram has to be delivered to the network layer for transmission.
- Since the Internet defines a different route for each datagram, the datagrams may arrive out of order and may be lost.
- The transport layer at computer B needs to wait until all of these datagrams to arrive, assemble them and make a segment out of them.

Traditionally, the transport layer was represented in the TCP/IP suite by two protocols: **User Datagram Protocol (UDP)** and **Transmission Control Protocol (TCP)**.

A new protocol called **Stream Control Transmission Protocol (SCTP)** has been introduced in the last few years.

Application Layer

The application layer in TCP/IP is equivalent to the combined session, presentation, and application layers in the OSI model.

- The application layer allows a user to access the services of our private internet or the global Internet.
- Many protocols are defined at this layer to provide services such as electronic mail file transfer, accessing the World Wide Web, and so on.
- The protocols supported in this layer are **TELNET, FTP** and **HTTP**.

Problems with TCP in Wireless Networks

The performance of TCP is generally lower in wireless networks than in fixed. This is explained by the fact that TCP cannot distinguish problems that typically occur in wireless networks from congestion. The congestion control algorithms in TCP are based on the assumptions that data is lost mainly due to congestion and that data loss due to transmission errors is rare. Therefore, data loss is interpreted as a signal of congestion in the network. Even in a wireless network, where data loss may not be related to congestion, data loss still signals congestion to the sender. TCP segments may be lost if the radio conditions are poor and the link layer protocol provides a low reliability. After some retransmission attempts the link layer protocol gives up and leaves further error recovery to TCP. Handover events may also lead to data loss. A whole window of data may be lost due to handover. Data loss due to an unreliable link layer or a handover, may cause a timeout event followed by slow start or fast retransmit and fast recovery. In either case, the congestion control action taken by TCP is unnecessary. Directly after the loss event, the radio quality may become high again, and after handover data may be transmitted without problems to the new base station.

TCP may also misinterpret a sudden increase in the round trip time as data loss. If the delay is long enough for the retransmission timer to expire before an acknowledgment is received, then TCP misinterprets the delay as an indication of data loss due to congestion. The delayed data is unnecessarily retransmitted and TCP enters slow start. A highly variable round trip time can also lead to a large RTO, since the RTO is based both on estimates of the round trip time and on variations in the round trip time. If the RTO is large, then TCP reacts slowly to data loss. Variations in the round trip time can be caused by link level retransmissions of a wireless link. If the link layer frames that contain a TCP segment must be retransmitted because of a poor radio environment, then the whole segment is delayed. Round trip time variations may also be caused by handover or competing traffic. Queuing in routers, base stations, and other intermediate nodes may also lead to a long round trip time. A long round trip time may cause low throughput and underutilization of the network, since it takes a number of round trip times before the congestion window reaches the capacity of the network. TCP performance is degraded, especially for short lived flows, which transmits a small amount of data.

Topic: Wireless applications

Wireless applications encompass a broad spectrum of technologies and services that utilize wireless communication to transmit data, voice, and multimedia content without the need for physical connections. These applications have become integral to various sectors, enhancing mobility, efficiency, and accessibility.

Key Categories of Wireless Applications:

1. **Mobile Communication:**
   - **Cellular Networks:** Enable voice and data communication over extensive areas through technologies like 4G LTE and 5G.
   - **Satellite Communication:** Provides connectivity in remote regions where terrestrial networks are unavailable.
2. **Personal Area Networks (PAN):**
   - **Bluetooth:** Facilitates short-range communication between devices such as smartphones, headphones, and wearable technology.
   - **Near Field Communication (NFC):** Allows contactless data exchange, commonly used in payment systems and access control.
3. **Local Area Networks (LAN):**
   - **Wi-Fi:** Offers wireless internet connectivity within homes, offices, and public hotspots, enabling devices to connect to local networks and the internet.
4. **Wide Area Networks (WAN):**
   - **WiMAX:** Provides wireless broadband access over long distances, suitable for metropolitan area networks.
5. **Internet of Things (IoT):**
   - **Smart Home Devices:** Include thermostats, security systems, and appliances that can be controlled remotely.

- **Wearable Devices:** Such as fitness trackers and smartwatches that monitor health metrics and provide notifications.

6. **Industrial and Enterprise Applications:**
   - **Wireless Sensor Networks:** Monitor environmental conditions, machinery status, and other parameters in industrial settings.
   - **Asset Tracking Systems:** Utilize wireless technology to monitor the location and status of goods and equipment.
7. **Public Safety and Emergency Services:**
   - **Emergency Response Systems:** Employ wireless communication for coordination during disasters and critical events.
   - **Surveillance Systems:** Use wireless cameras and sensors to monitor public areas and infrastructure.

Emerging Trends in Wireless Applications:

- **5G Technology:** Offers enhanced speed, reduced latency, and the capacity to connect a vast number of devices, facilitating advancements in autonomous vehicles, smart cities, and augmented reality applications.
- **Wi-Fi 7:** The upcoming standard aims to provide faster data rates and improved performance in dense environments, supporting high-bandwidth applications like 4K/8K streaming and virtual reality.
- **NearLink:** A new short-range wireless technology developed to offer lower latency and higher reliability compared to traditional Bluetooth, enhancing applications like wireless audio and real-time data transfer.
- **Auracast:** An innovation in Bluetooth technology that enables audio broadcasting to multiple devices simultaneously, transforming experiences in public venues and personal sharing scenarios.

The continuous evolution of wireless applications is reshaping how we interact with technology, driving innovation across industries, and enhancing the quality of life by providing seamless, efficient, and versatile connectivity solutions.

Topic: Data broadcasting

Data broadcasting, also known as data casting, refers to the transmission of digital data to multiple recipients simultaneously over a wide area using radio waves. This method is commonly employed to deliver supplemental information alongside traditional broadcast content, such as television or radio programs. The transmitted data can include news updates, weather forecasts, traffic reports, stock market information, and more, enhancing the value of standard broadcasts.

Key Applications of Data Broadcasting:

1. **Enhanced Television Services:** Television stations can transmit additional data alongside their regular programming, providing viewers with interactive services like electronic program guides, real-time news updates, and weather information.
2. **Educational Content Delivery:** Data broadcasting has been utilized to bridge the digital divide by delivering instructional materials to students in areas with limited internet access. For instance, Indiana Public Broadcasting Stations have implemented datacasting to provide educational content to students without reliable internet connections.
3. **Public Safety Communications:** Datacasting is employed to disseminate critical information during emergencies, such as natural disasters or public safety incidents, ensuring that vital data reaches a broad audience promptly.

Advantages of Data Broadcasting:

- **Efficiency:** By transmitting data to multiple recipients simultaneously, data broadcasting efficiently utilizes available bandwidth, making it ideal for disseminating information to large audiences without overburdening the network.
- **Reliability:** Broadcasting data over established radio or television frequencies ensures that information can reach recipients even in areas with limited or no internet connectivity.
- **Scalability:** Data broadcasting systems can accommodate a vast number of receivers without a significant increase in transmission costs or complexity.

Technological Standards and Protocols:

Several standards and protocols have been developed to facilitate data broadcasting:

- **Digital Video Broadcasting (DVB):** A suite of internationally accepted open standards for digital television, which includes provisions for data broadcasting.
- **IP Datacasting (IPDC):** A standard for delivering IP-based services over digital broadcast networks, enabling the transmission of multimedia content to various devices.
- **Broadcast Markup Language (BML):** An XML-based standard developed in Japan for data broadcasting, allowing for the integration of multimedia content and interactive services into digital broadcasts.

In summary, data broadcasting serves as a versatile and efficient method for delivering a wide range of information to large audiences. Its applications span from enhancing traditional broadcast services to providing critical information during emergencies, making it a valuable tool in modern communication infrastructures.

📱 What is Mobile IP?

Mobile IP (Mobile Internet Protocol) is a communication protocol that allows mobile devices (like smartphones, laptops, etc.) to move across different networks while maintaining a permanent IP address. s. It ensures that the communication will continue without the user's sessions or connections being dropped.

🚗 Why Do We Need Mobile IP?

In traditional IP networks:

- An IP address is associated with a specific **network location**.
- If a device moves to another network, its IP address **must change**.
- This causes **session interruption** (like a dropped video call or broken download).

👉 **Mobile IP solves this problem** by allowing a device to **roam between networks** without changing its **home IP address**, ensuring **continuous connectivity**.

🧠 Key Terminologies in Mobile IP:

Term	Description
Mobile Node (MN)	The device that moves from one network to another (e.g., smartphone).
Home Network	The original network where the mobile node's permanent IP address is assigned.
Foreign Network	The network the mobile node is visiting.
Home Agent (HA)	A router on the home network that keeps track of the mobile node's current location.
Foreign Agent (FA)	A router on the foreign network that helps the mobile node communicate with the home agent.
Care-of Address (CoA)	A temporary IP address assigned to the mobile node while it is in a foreign network.

⚙️ How Mobile IP Works: Step-by-Step

1. Agent Discovery

- Mobile Node (MN) listens for advertisements from **Foreign Agents (FA)** or requests them.
- These agents send messages about their presence and available services.

2. Care-of Address Assignment

- MN gets a **Care-of Address** (CoA), which can be:
  - The IP address of the **Foreign Agent**, or
  - A **co-located CoA** assigned directly to the MN.

3. Registration

- MN registers its CoA with its **Home Agent (HA)** through the Foreign Agent.
- The HA records the binding between the MN's **home address** and its **current CoA**.

4. Tunneling and Communication

- When a **correspondent node** (like a web server) sends data to the mobile node's **home address**, the data first goes to the **Home Agent**.
- The HA **tunnels** (forwards) the data to the **Care-of Address** using **IP-in-IP encapsulation**.
- The FA (or MN itself) receives and delivers the data to the MN.

5. Reverse Communication

- When the MN sends data, it can send it directly to the destination (route optimization), or via the HA.

✅ Advantages of Mobile IP:

- Supports **seamless mobility** across networks.
- Maintains **ongoing sessions** even when changing networks.
- Works with **existing IP infrastructure**.
- Useful in **mobile data networks**, **military**, **transport systems**, etc.

❌ Disadvantages of Mobile IP:

- **Triangular routing problem**: Data always goes through the HA, increasing delay.
- Security risks due to **IP spoofing** and **session hijacking**.
- Higher complexity due to **registration and tunneling** mechanisms.

Topic: Wireless Application Protocol (WAP) in Mobile Computing

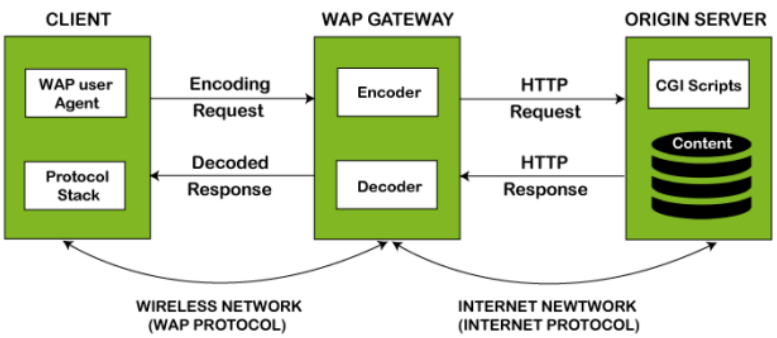
Wireless Application Protocol or WAP is a programming model or an application environment and set of communication protocols based on the concept of the World Wide Web (WWW), and its hierarchical design is very much similar to TCP/IP protocol stack design. See the most prominent features of Wireless Application Protocol or WAP in Mobile Computing:

- WAP is a De-Facto standard or a protocol designed for micro-browsers, and it enables the mobile devices to interact, exchange and transmit information over the Internet.
- WAP is based upon the concept of the World Wide Web (WWW), and the backend functioning also remains similar to WWW, but it uses the markup language Wireless Markup Language (WML) to access the WAP services while WWW uses HTML as a markup language. WML is defined as XML 1.0 application.
- In 1998, some giant IT companies such as Ericson, Motorola, Nokia and Unwired Planet founded the WAP Forum to standardize the various wireless technologies via protocols.
- After developing the WAP model, it was accepted as a wireless protocol globally capable of working on multiple wireless technologies such as mobile, printers, pagers, etc.
- In 2002, by the joint efforts of the various members of the WAP Forum, it was merged with various other forums of the industry and formed an alliance known as Open Mobile Alliance (OMA).
- WAP was opted as a De-Facto standard because of its ability to create web applications for mobile devices.

Working of Wireless Application Protocol or WAP Model

The following steps define the working of Wireless Application Protocol or WAP Model:

- The WAP model consists of 3 levels known as Client, Gateway and Origin Server.
- When a user opens the browser in his/her mobile device and selects a website that he/she wants to view, the mobile device sends the URL encoded request via a network to a WAP gateway using WAP protocol.
- The request he/she sends via mobile to WAP gateway is called as encoding request.
- The sent encoding request is translated through WAP gateway and then forwarded in the form of a conventional HTTP URL request over the Internet.
- When the request reaches a specified Web server, the server processes the request just as it would handle any other request and sends the response back to the mobile device through WAP gateway.
- Now, the WML file's final response can be seen in the browser of the mobile users.



- **WAP PROTOCOL STACK:**

1. **Application Layer:**
   This layer contains the *Wireless Application Environment (WAE)*. It contains mobile device specifications and content development programming languages like WML.
2. **Session Layer:**
   This layer contains *Wireless Session Protocol (WSP)*. It provides fast connection suspension and reconnection.
3. **Transaction Layer:**
   This layer contains *Wireless Transaction Protocol (WTP)*. It runs on top of UDP (User Datagram Protocol) and is a part of TCP/IP and offers transaction support.
4. **Security Layer:**
   This layer contains *Wireless Transaction Layer Security (WTLS)*. It offers data integrity, privacy and authentication.
5. **Transport Layer:**
   This layer contains *Wireless Datagram Protocol*. It presents consistent data format to higher layers of WAP protocol stack.

While both Mobile IP and WAP were instrumental in the evolution of mobile computing, advancements in technology have led to more sophisticated protocols and standards. Modern mobile devices now utilize protocols that offer higher data rates, enhanced security, and seamless mobility support, rendering earlier technologies like Mobile IP and WAP largely obsolete