UNIT II

📡 Media Access Control (MAC) in Mobile Computing.

Media Access Control (MAC) is a critical **sub-layer of the Data Link Layer** (Layer 2) in the **OSI model**. It is responsible for controlling how devices in a **network environment share the communication medium**, especially when multiple devices try to access the same medium (like Wi-Fi or mobile networks).

In **mobile computing**, MAC plays an especially important role because of:

- **Mobility of devices**
- **Wireless communication**
- **Limited bandwidth**
- **High error rates**

🔑 Key Functions of MAC in Mobile Computing:

Function	Description
Channel Access Control	Determines how devices share the wireless medium (e.g., which device can transmit at what time).
Collision Avoidance	Helps prevent data collisions in wireless communication.
Addressing	Assigns unique MAC addresses to devices for identification.
Frame Delimiting and Error Checking	Ensures correct formatting and checks for transmission errors.
Security and Access Control	Limits access to the network using authentication and encryption (e.g., WPA in Wi-Fi).

🧠 Types of MAC Protocols in Mobile Computing:

1. **Contention-Based Protocols**
   - Devices **compete** for the channel.
   - **Example**: **CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)** used in Wi-Fi (IEEE 802.11).
   - Suitable for **ad hoc** and **infrastructureless** networks.
2. **Reservation-Based Protocols**
   - Devices **reserve the channel** before transmitting.
   - Reduces collision
   - Example: **TDMA (Time Division Multiple Access)** in GSM networks.
3. **Hybrid MAC Protocols**
   - Combine contention and reservation methods.

- Provide **flexibility** and **better efficiency** in mobile environments.

🛰️ MAC in Wireless Technologies:

Technology	MAC Protocol Used	Features
Wi-Fi (802.11)	CSMA/CA + RTS/CTS (optional)	Collision avoidance, ACK-based retransmissions
Bluetooth	Frequency Hopping + TDMA	Master-slave architecture
GSM/3G/4G/5G	TDMA/CDMA/OFDMA	Centralized scheduling by base stations
Zigbee (802.15.4)	Slotted CSMA/CA	Energy-efficient, used in IoT and sensor networks

⚙️ Challenges of MAC in Mobile Computing:

- **Dynamic topology**: Devices move in and out of coverage areas.
- **Variable link quality**: Due to fading, interference, and obstacles.
- **Power constraints**: Mobile devices need energy-efficient MAC protocols.
- **Latency sensitivity**: Real-time applications need timely data transmission.

💡 Example: MAC in Wi-Fi (802.11)

- **CSMA/CA**: A device listens before sending data. If the channel is clear, it sends. If busy, it waits.
- **RTS/CTS (Request to Send / Clear to Send)**: Optional mechanism to further reduce collision risks in noisy environments.
- **ACK**: The receiver sends an acknowledgment after receiving data, ensuring reliable delivery.

🔐 Security Role of MAC in Mobile Computing

- MAC layer security includes **authentication**, **encryption**, and **access control**.
- In Wi-Fi networks, protocols like **WPA2** and **WPA3** operate partly at the MAC layer.
- MAC address filtering is a basic method to control which devices can join the network.

📝 Summary:

Aspect	MAC in Mobile Computing
Main Goal	Efficient and fair access to shared wireless medium
Challenges	Mobility, interference, limited energy
Techniques	CSMA/CA, TDMA, CDMA, OFDMA
Used In	Wi-Fi, Bluetooth, Cellular networks
Security Features	MAC address filtering, encryption, authentication

✅ Media Access Control (MAC) Techniques

Media Access Control (MAC) techniques determine **how multiple devices share and access a communication medium**, especially in **wireless** or **shared networks**. These techniques help **avoid collisions**, **organize transmission**, and **maximize efficiency** in data communication.

Types of MAC Techniques

MAC techniques are generally classified into **three categories**:

---

1. Contention-Based (Random Access) Techniques

Devices **compete** for access to the medium. These methods work well when **traffic is light**, but collisions can occur.

a. ALOHA

- **Pure ALOHA**: Send whenever you want. If collision occurs, resend after a random delay.
- **Slotted ALOHA**: Divides time into slots. Send only at slot start.
- **Used In**: Satellite communication, early wireless networks.

b. CSMA (Carrier Sense Multiple Access)

- **CSMA**: Listen before transmitting. If the medium is free, send; else, wait.
- **CSMA/CD (Collision Detection)**: Used in Ethernet (wired); detects collisions and stops.
- **CSMA/CA (Collision Avoidance)**: Used in Wi-Fi; avoids collisions using RTS/CTS handshake.

c. Polling

- Central controller **polls each device** to ask if it wants to send data.
- Reduces collision but introduces delay.
- Used in some **Bluetooth** and **industrial networks**.

---

2. Controlled Access (Scheduled/Deterministic) Techniques

The system **controls when each device can transmit**. These are better for **real-time**, **predictable**, and **collision-free** communication.

a. TDMA (Time Division Multiple Access)

- Each device gets a **time slot** to transmit.
- Used in **GSM mobile networks**.

b. FDMA (Frequency Division Multiple Access)

- Each device gets a **separate frequency**.
- Common in **analog systems** and satellite links.

c. CDMA (Code Division Multiple Access)

- Devices transmit **simultaneously** over the same frequency using **unique codes**.
- Used in **3G mobile systems**.

d. OFDMA (Orthogonal Frequency Division Multiple Access)

- Breaks bandwidth into **subcarriers**, assigns them to users.
- Used in **4G LTE** and **5G**.

---

3. Hybrid Techniques

Combine contention and controlled access for **better performance**.

Example:

WiMAX uses **TDMA + OFDMA**, and **Wi-Fi** uses **CSMA/CA with optional TDMA** in newer standards.

🧠 Summary Table

Technique	Type	Used In	Features
ALOHA	Contention-Based	Satellite, early wireless	Simple, high collision rate
CSMA/CD	Contention-Based	Ethernet (wired)	Detects and handles collisions
CSMA/CA	Contention-Based	Wi-Fi	Avoids collisions, uses RTS/CTS
TDMA	Controlled	GSM, LTE	Time slots, efficient scheduling
FDMA	Controlled	Satellite, analog	Frequency-based separation
CDMA	Controlled	3G	Code-based sharing, simultaneous users
OFDMA	Controlled	4G, 5G	Divides frequency into subcarriers

🚦 Motivation for Specialized MAC Protocols in Wireless Networks

🧩 Challenges in Wireless MACMobile Ad hoc NETworks (MANETs) are wireless networks which are characterized by dynamic topologies and no fixed infrastructure. Each node in a MANET is a computer that may be required to act as both a host and a router and, as much, may be required to forward packets between nodes which cannot directly communicate with one another. Each MANET node has much smaller frequency spectrum requirements that that for a node in a fixed infrastructure network. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes

1. Hidden Terminal Problem

- **Definition**: Occurs when two nodes are **not within range of each other** but both are within range of a **common receiver**.
- **Issue**: They may transmit simultaneously, causing **collisions** at the receiver.
- **Example**: Node A and Node C both send to Node B but can't hear each other.
- **Solution**: Use protocols like **RTS/CTS** (Request to Send / Clear to Send) in **CSMA/CA** to avoid collisions.

2. Exposed Terminal Problem

- **Definition**: A node is **unnecessarily prevented** from sending data because it senses the medium is busy, even though its transmission wouldn’t cause interference.
- **Example**: Node B wants to send to C, but hears A sending to D. It stays silent, although B → C wouldn’t interfere with A → D.
- **Impact**: **Underutilization** of the channel.
- **Solution**: Smarter MAC strategies or directional antennas.

3. Near-Far Terminal Problem

- **Definition**: A **nearer device** to a receiver can **overpower** a signal from a farther device.
- **Impact**: Receiver can't hear the weaker signal properly.
- **Solution**: Power control, adaptive transmission strategies, CDMA with power equalization.

📡 Specialized MAC Techniques

Technique	Full Form	Core Idea	Used In
SDMA	Space Division Multiple Access	Divide users **by physical space** using **beamforming** or sector antennas.	5G, Satellite, WiMAX
FDMA	Frequency Division Multiple Access	Assign **different frequency bands** to different users.	Analog systems, GSM
TDMA	Time Division Multiple Access	Divide the medium into **time slots**; each user gets one in a round-robin way.	GSM, LTE (with OFDMA)
CDMA	Code Division Multiple Access	All users transmit on the **same frequency**, separated by **unique codes**.	3G, GPS, some 4G uses

🎯 Summary of Access Techniques

Method	Division Factor	Strengths	Weaknesses
SDMA	Space	Efficient spatial reuse, reduces interference	Needs advanced antennas, high cost
FDMA	Frequency	Simple, no time synchronization needed	Inefficient use of bandwidth, rigid
TDMA	Time	Predictable timing, avoids collisions	Needs precise time synchronization
CDMA	Code	High capacity, secure, resistant to interference	Complex receiver design, near-far problem

🌺 ALOHA Protocol

ALOHA was developed at the **University of Hawaii** in the 1970s to allow wireless communication between islands. It's a **contention-based MAC protocol** used to control how data is sent over a shared communication channel.

🔄 Types of ALOHA

Type Description

1. Pure ALOHA

- Devices **transmit whenever they have data** to send.
- **No checking** of whether the channel is busy.
- If there's a **collision**, the device **waits for a random time** and resends the data.

Vulnerability: High chance of collisions.

- **Efficiency**: ~18% (only 18% of the time is used successfully).

---

2. Slotted ALOHA

- Time is divided into **equal time slots**.
- Devices can **only send at the beginning of a time slot**.
- Reduces the chance of collisions by synchronizing transmissions.
- **Efficiency**: ~36% (double that of Pure ALOHA).

⚙️ How it Works (Slotted ALOHA Example)

1. Time is divided into fixed slots.
2. A device with data waits until the next time slot starts.
3. It transmits the data packet.
4. If **ACK (Acknowledgment)** is received → success.
5. If not → collision occurred → wait a random time and retry.

💥 Pros and Cons

Pros	Cons
Simple and easy to implement	High collision rate (especially in Pure ALOHA)
Works well in low traffic conditions	Low efficiency as traffic increases
Doesn’t need coordination	Not suitable for high-load environments

📶 ALOHA Is Used In:

- Early satellite and wireless systems
- Some versions of **LoRaWAN** (IoT networks)
- **RFID systems** (to avoid tag collisions)

📱 MOBILE NETWORK LAYER

📌 Mobile IP

Mobile IP is a protocol that enables **mobile devices** (like smartphones, laptops) to move from one network to another **while maintaining the same IP address**.

🎯 Goals of Mobile IP

- Provide **seamless mobility** for devices across different networks.
- Maintain **ongoing connections** even when changing networks.
- Ensure **interoperability** with the existing Internet infrastructure.

Assumptions

- The Internet uses **IP-based communication**.
- Mobile nodes frequently **change their point of attachment**.
- Applications should **not need to know** a device is moving.

👥 Entities & Terminology

Term	Role
Mobile Node (MN)	A device that changes location (e.g., phone, laptop).
Home Agent (HA)	A router on the home network that forwards packets to the MN.
Foreign Agent (FA)	A router on the visited network that assists in delivery.
Care-of Address (CoA)	Temporary IP address for MN in a foreign network.

📦 IP Packet Delivery in Mobile IP

1. **Correspondent Node (CN)** sends packets to the **Home Address** of the MN.

2. **Home Agent** intercepts the packet and **forwards** it to the **Care-of Address** via **tunneling**.
3. FA or MN decapsulates and delivers it to the mobile device.

📢 Agent Advertisement and Discovery

- Agents (HA & FA) **broadcast messages** to announce their presence.
- MN uses this to **detect its current location**.
- MN can send a **solicitation** message to speed up the process.

📝 Registration Process

1. MN detects it is in a **foreign network**.
2. MN sends a **Registration Request** to FA → HA.
3. HA **authorizes** and replies with a **Registration Reply**.
4. Now HA will **forward packets** to MN via CoA.

🧊 Tunneling & Encapsulation

- HA creates a **tunnel** to the CoA.
- Uses **IP-in-IP encapsulation**:
  - **Outer header**: Source = HA, Destination = CoA
  - **Inner packet**: Original data from CN to MN

⚡ Optimizations

Optimization	Description
Route Optimization	CN sends packets directly to CoA (not via HA).
Fast Handover	Reduces delay during network switching.
Hierarchical Mobile IP	Reduces signaling load by using a regional agent.
Mobile IPv6	Built-in route optimization, no need for FAs.

📜 DHCP (Dynamic Host Configuration Protocol)

DHCP is a protocol that **dynamically assigns IP addresses** and other network configuration info to devices.

🔧 Main Functions

- **Assign IP address**
- **Assign gateway and DNS**
- **Lease time**: Temporary IP address assignment
- **Automatic configuration** of new devices

🔁 DHCP Workflow (DORA Process)

Step	Message	Description
1 Discover	DHCP Discover	Client broadcasts to find DHCP server
2 Offer	DHCP Offer	Server offers an IP address and config
3 Request	DHCP Request	Client requests the offered IP
4 Acknowledge	DHCP ACK	Server confirms the lease

💡 Difference Between Mobile IP & DHCP:

Mobile IP	DHCP
Supports **mobility**	Assigns IPs **in static locations**
Maintains **same IP**	IP may **change** across networks
Focus on **roaming**	Focus on **configuration**

Tunneling and Encapsulation in Mobile IP

Tunneling and encapsulation are key techniques used in **Mobile IP** to forward packets from the **Home Agent (HA)** to the **Mobile Node (MN)** when it's away from its home network.

📦 What is Encapsulation?

Encapsulation means **wrapping an original IP packet inside another IP packet** so it can be routed through the tunnel.

📩 Encapsulation Process (IP-in-IP)

1. A **Correspondent Node (CN)** sends a packet to the **Home Address** of the MN.
2. The **Home Agent (HA)** intercepts the packet.
3. HA **encapsulates** the original packet:
    - Adds a **new IP header**.
    - Source: HA's IP
    - Destination: CoA (Care-of Address of MN)
4. The encapsulated packet is sent through the **tunnel**.
5. The **Foreign Agent (FA)** or MN **decapsulates** it and processes the original packet.

🧱 Structure of an Encapsulated Packet

```
markdown
CopyEdit
Outer IP Header (HA → CoA)
---------------------------
Inner IP Header (CN → MN)
---------------------------
Payload (actual data)
```

🔁 Types of Encapsulation

Type	Description
IP-in-IP	Standard for Mobile IP. Full IP header added.
Minimal Encapsulation	Reduces overhead by using only essential fields.
GRE (Generic Routing Encapsulation)	Used for advanced tunneling (e.g., VPNs).

✅ Benefits

- Maintains **ongoing sessions** even when the MN changes location.
- **Transparency** to the correspondent node—no need to know MN's current location.
- **Flexible and scalable** for large mobile environments.

📡 Mobile Ad Hoc Networks (MANETs)

📘 Overview

A **Mobile Ad Hoc Network (MANET)** is a **self-configuring**, **infrastructure-less** network of **mobile devices** connected **wirelessly**.

- Each node acts as both a **host and a router**.
- Can be rapidly deployed in **dynamic environments**.
- No fixed routers or access points.

Or

Mobile Ad hoc NETworks (MANETs) are wireless networks which are characterized by dynamic topologies and no fixed infrastructure. Each node in a MANET is a computer that may be required to act as both a host and a router and, as much, may be required to forward packets between nodes which cannot directly communicate with one another. Each MANET node has much smaller frequency spectrum requirements that that for a node in a fixed infrastructure network. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes

---

🔍 Properties of a MANET

Property	Description
Dynamic Topology	Nodes move freely; the network changes rapidly.
Infrastructure-less	No central control or fixed infrastructure.
Multi-hop Communication	Data is forwarded through intermediate nodes.
Energy-constrained	Nodes often run on battery.
Scalability	Must scale to large and small networks.
Limited Bandwidth	Wireless links are less reliable than wired.

MANETs can operate across a **broad spectrum of wireless technologies**, such as:

- **Bluetooth** (short-range, low energy)
- **Wi-Fi (802.11)** (medium range, higher bandwidth)
- **Zigbee** (low power, sensor networks)
- **Cellular interfaces** (used in hybrid networks)
- **Satellite links** (for wide-area ad hoc coverage)

🧭 Applications of MANETs

Domain	Use Case
Military	Tactical battlefield communication.
Disaster Recovery	Emergency rescue when infrastructure is damaged.
IoT / Smart Homes	Wireless sensors communicating without a central router.
Vehicular Networks	Communication between moving vehicles (VANETs).
Remote Areas	Providing internet access or communication in rural zones.

📌 Routing in MANETs

Since topology changes frequently, routing is a major challenge.

🛤️ Routing Categories

1. **Proactive (Table-Driven)**
   - Maintains fresh lists of routes.
   - Example: **DSDV (Destination-Sequenced Distance Vector)**
2. **Reactive (On-Demand)**
   - Finds route only when needed.
   - Example: **AODV (Ad hoc On-Demand Distance Vector)**, **DSR (Dynamic Source Routing)**
3. **Hybrid**
   - Combines proactive + reactive.
   - Example: **ZRP (Zone Routing Protocol)**

📊 Popular MANET Routing Protocols

Protocol	Type	Feature
DSDV	Proactive	Updates routing tables periodically.
AODV	Reactive	Discovers route only when needed.
DSR	Reactive	Uses route caching and source routing.
OLSR	Proactive	Optimized for low latency, uses MPRs.
TORA	Reactive	Good for highly dynamic environments.

🔐 Security in MANETs

Security is complex in MANETs due to:

- **Open medium**
- **Lack of centralized authority**
- **Dynamic topology**

🚨 Common Security Threats

- **Eavesdropping**
- **Impersonation**
- **Wormhole attacks**
- **Blackhole and grayhole attacks**
- **Denial of Service (DoS)**

🔐 Security Solutions

Technique	Purpose
Encryption	Ensure confidentiality (e.g., AES, RSA).
Authentication	Verify identity using keys or certificates.
Intrusion Detection Systems (IDS)	Detect abnormal behavior in routing.
Trust-based Models	Trust levels determine whether nodes are secure.
Secure Routing Protocols	SAODV, ARAN, SRP, etc.