📘 Lecture 1 – Computer Networks

---

1. How Networks Developed

What is a Network?

A **network** is a group of computers or devices that are connected to share data and resources.

How It Started (1980s)

- In the **1980s**, four universities were connected using **Ethernet cables**.
- These connections formed a **chain**, and that chain became the early form of a **computer network**.
- With time, more devices were added and the concept of a **global network → the Internet** began to evolve.

Why Networks Were Needed?

- To share information quickly.
- To reduce the use of physical storage (like floppy disks).
- To communicate across long distances.

Daily Life Example

- Using WhatsApp, Instagram, or Google on your phone → all depend on networks.

---

2. Internet vs Intranet

Internet

- The **Internet** is a *public* network.
- It allows **global data sharing**.
- Anyone connected to the network can access public information.

Intranet

- The **Intranet** is a *private* network.
- Used inside companies or organizations.
- Only authorized people can access private data.

Daily Life Example

- **Internet**: Browsing YouTube.
- **Intranet**: Employees in a company accessing internal HR portal.

---

3. Types of Networks

1. LAN (Local Area Network)

- Small area: home, office, school.
- Very fast and inexpensive.

Example: Wi-Fi in your house.

---

2. MAN (Metropolitan Area Network)

- Covers a **city or large campus**.
- Boundary is *not fixed* (depends on the city/organization).

Example: Internet service provider (ISP) network inside a city.

---

3. WAN (Wide Area Network)

- Covers **countries or continents**.
- Largest type of network.

Example: The global Internet is a WAN.

Difference: MAN vs WAN

Feature	**MAN**	**WAN**
Coverage	City level	Country or world level
Speed	Faster	Slower due to long distance
Ownership	Usually one organization/ISP	Shared by many companies
Boundaries	Not strictly fixed	Can span across nations

---

4. IP Address

What is an IP Address?

- A unique **logical / virtual address** given to each device in a network.
- It identifies your device on the Internet.

Why is IP Address Used?

- To identify your device.
- To send/receive data to the correct destination (like a postal address).

How to Check IP/MAC Address

- **Get MAC Address:**
  getmac (in Command Prompt)
- **Get IP Address:**
  ipconfig /all

---

5. MAC Address

What is MAC Address?

- A **physical** address burned into the network card.
- Unique for every device.

- Used by switches to deliver data.

Example: Like a unique fingerprint of your device.

---

6. Network Devices

A. Router

What is it?

- A router **routes** (directs) data packets between networks.
- Connects private network to public Internet.

How it Works?

- Checks the **destination IP** of each packet.
- Sends it through the correct path like a GPS.

Why Used?

- To connect multiple networks.
- To provide Internet access.
- To manage traffic and security.

Daily Life Example

- Your home Wi-Fi router that connects your phone/laptop to the Internet.

B. Switch

What is it?

- An **intelligent device** used inside local networks (LAN).

How it Works?

- Creates a **MAC address table**.
- When a device sends data:
    - The switch learns **Sender MAC + Sender IP**.

    - When data comes back, the switch checks **Destination MAC**.
    - Sends data to the correct device **only**.

This process is called **MAC Learning**.

Why Used?

- To reduce network traffic.
- To improve security.
- Faster communication.

Daily Life Example

- Office computers connected to a switch for internal communication.

C. Hub

What is it?

- A **non-intelligent** device.
- Sends data to **all connected devices**, not just the correct one.

Why It's Problematic?

- Causes **privacy issues**.
- Creates **unnecessary traffic**.
- Very slow.

Daily Life Example

- Like a delivery boy going to **every house** in a society asking "Is this your parcel?"
  → Privacy is breached.

Current Use

- Hardly used today; replaced by **switches**.

D. Firewall

What is it?

- A **security device/software** that filters network traffic.
- Decides which data packets are allowed or blocked.

How it Works?

- Uses rules to check:
  - Source IP
  - Destination IP
  - Port number
  - Protocol

Why Used?

- To protect against hackers, malware, and attacks.
- To allow only safe connections.

Daily Life Example

- Blocking harmful websites on school or office networks.