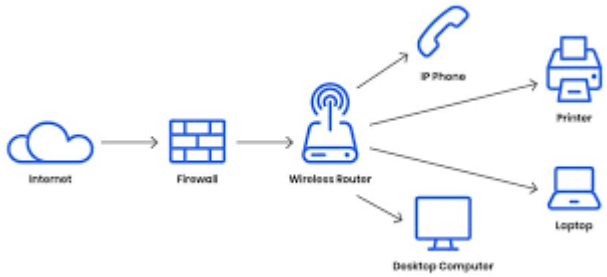
DAY 2 **DATE:29/04/2025**

27739 – Annie John

TITLE: COMPUTER NETWORKING

- **Computer networking** involves connecting two or more computing devices to enable communication, data sharing, and resource sharing.

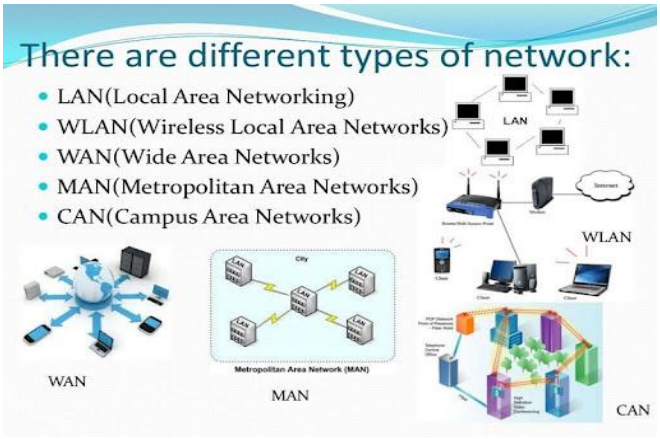


- **Working of Computer network?**
  - Devices like computers, routers, or printers (called **nodes**) are connected through **links.** These links can be cables or Wi-Fi signals. They act like roads for the data to travel. When you send something (like a message or file), it's broken into small pieces called packets. These packets move from one node to another using routers or switches, which help find the best path. At the receiving end, the device puts the packets back together and shows you the full message or file. All devices follow some rules (called protocols) so they understand each other and avoid confusion.
- **Fundamental components of Networking**
  1. Nodes (Devices) - These are the things that connect to the network.

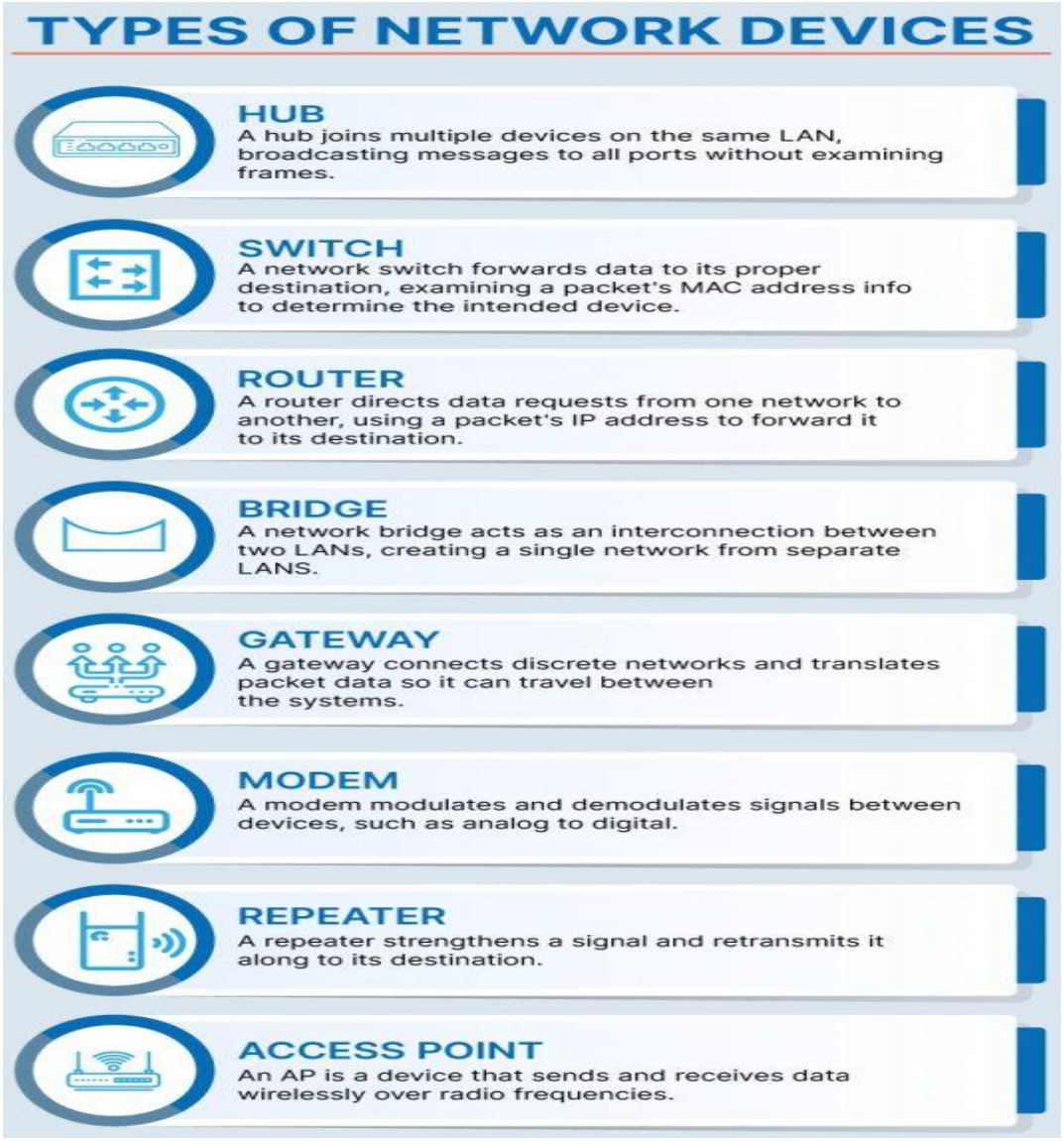
     Examples: Computers, phones, printers, routers. They send or receive data.
  2. Links (Connections) - These are the paths that connect the devices. Can be wires (like Ethernet cables) or wireless (like Wi-Fi). They carry the data between devices.

3. NIC (Network Card) - Each device has a network card inside. It lets the device talk to other devices on the network. *Like a phone's SIM card but for networking.*
4. Protocols (Rules) - These are the rules that devices follow to share information. Example: TCP/IP, used on the internet. Like a common language that all devices understand.
5. Router and Switch - Router: Connects your home network to the internet. Switch: Connects multiple devices inside the same network. They help move data to the right place.

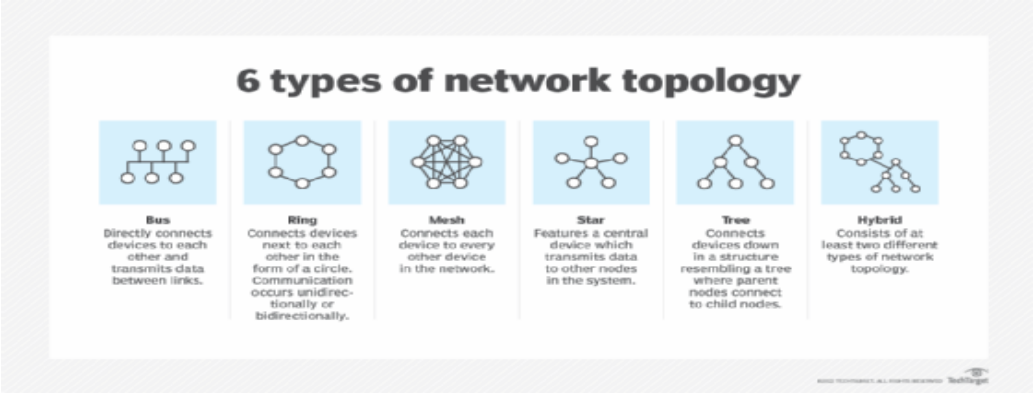
- **Types of Networks**



- **Cloud Network** - Cloud networking means using the internet (the cloud) to manage, store, and access network resources like servers, routers, firewalls, and data — instead of using physical hardware at your home or office.eg: **Amazon (AWS), or Microsoft (Azure)**.



- **Network Topology**



- A **network protocol** is like a set of rules that devices (like computers, phones, or servers) follow to communicate with each other over a

network.Classified into Network communication, network management and network security.

- **Network Communication Protocols**
  HTTP – Loads websites (insecure).
  HTTPS – Secure version of HTTP using SSL/TLS.
  UDP – Fast, connectionless, no error check (used in streaming).
  TCP – Reliable, ordered data delivery (used in web, email).
  ARP – Finds MAC address from IP address.
- **Network Management Protocols**
  ICMP – Sends error and status messages (used in ping).
  FTP – Transfers files between systems.
  Telnet – Remote access via command line (not secure).
- **Network Security Protocols**
  SSL – Encrypts data between devices (older version).
  TLS – More secure and modern version of SSL.
  HTTPS – HTTP + SSL/TLS = Secure web browsing.

- **NIC (Network Interface Card)**
  A **NIC** is a **hardware component** inside your computer or laptop that lets it **connect to a network**.
  There are two types:
  - **Wired NIC** – uses Ethernet cables
  - **Wireless NIC (Wi-Fi card)** – connects via Wi-FI

  Purpose: Acts like a **passport** for your device to join a network (like LAN or the internet).
  Example: If your laptop connects to Wi-Fi, it's using its wireless NIC.

- **Network Troubleshooting** is a way to maintain your computer network, ensuring optimal performance, and addressing issues that may disrupt connectivity. when any problems arise, network administrators and IT professionals use tools such as Ping, Traceroute, and PathPing to identify and solve a problem.
  - **Ping** is a command that sends a small packet of data to any network device and waits for its response.
  - **Traceroute** traces the route from source to destination and it helps identify any delay or bottleneck.
  - **PathPing** combines the functionality of both Ping and Traceroute commands to troubleshoot the network

- In networking, a **routing table** is a data structure, often visualized as a table, that routers use to determine the best path for sending data packets to their destination.
- **IP Address Basics**

  • Definition: An IP address is a numerical label assigned to each device connected to a network that uses the Internet Protocol for communication. It serves two main purposes:

  o Identification: Identifies a device on a network.

  o Location Addressing: Provides the location of the device in the network, facilitating data routing.

  • Format: IP addresses come in two main versions:
    - IPv4 (Internet Protocol version 4): Uses 32-bit addresses, typically represented in decimal format as four octets separated by periods (e.g., 192.168.1.1).
    - IPv6 (Internet Protocol version 6): Uses 128-bit addresses, represented in hexadecimal format as eight groups of four hexadecimal digits separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
    - IPv6 addresses are typically written in hexadecimal format and can include shorthand notations to simplify

  • Classes: IPv4 addresses are divided into classes based on the first octet. Each class has a different range and purpose:

  o Class A: 1.0.0.0 to 126.0.0.0 (Large networks)

  o Class B: 128.0.0.0 to 191.0.0.0 (Medium-sized networks)

  o Class C: 192.0.0.0 to 223.0.0.0 (Small networks)

  o Class D: 224.0.0.0 to 239.0.0.0 (Multicast addresses)

  o Class E: 240.0.0.0 to 255.0.0.0 (Experimental)
- **A subnet, or subnetwork**, is a logical division of a larger IP network into smaller, more manageable networks.
- A **firewall** is a network security system that acts as a barrier between a trusted internal network and untrusted external networks, such as the internet.
- **How Firewalls Manage Incoming and Outgoing Traffic**
  - **Incoming Traffic**: Data coming from the internet to your device (e.g., someone trying to access your system).
    Firewall checks if it's safe → allows or blocks it.

- **Outgoing Traffic**: Data your device sends out (e.g., browsing, sending emails).
  Firewall ensures your data goes to safe destinations.

- **Two Types of firewalls**

- **Server-Level Firewall -** A server-level firewall protects a single server. Installed directly on the server (like a host-based firewall). Controls which services/ports are open or blocked. Filters incoming and outgoing traffic to and from that specific server.
  Example: A web server may allow only port **80 (HTTP)** and **443 (HTTPS)**, and block everything else.
- **Subnet-Level Firewall** - A subnet-level firewall protects an entire group of devices within a subnet (a smaller part of a larger network). Positioned between subnets or network zones. Filters traffic going between different subnets (e.g., from a guest network to a private network). Used in corporate or cloud networks to isolate and protect sensitive areas.
  Example: In a company, a firewall might block access from the guest Wi-Fi subnet to the internal company subnet.