Computer Networking

A computer network is a group of connected computers and devices that share information and resources, like files and internet access. It allows devices to communicate with each other, either through cables or wirelessly.

Types of networks

1. Local Area Network (LAN)

A LAN connects devices within a limited geographic area, such as a single building or campus. It typically uses Ethernet cables, switches, routers, and Wi-Fi access points.
Example: A college computer lab network.

2. Wide Area Network (WAN)

A WAN covers a large geographic area, connecting multiple LANs through public networks or leased lines. It uses routers, modems, fiber-optic cables, and satellites for communication.
Example: The Internet.

3. Metropolitan Area Network (MAN)

A MAN spans a city or a large campus, offering higher speeds than a WAN but covering a smaller area. It uses fiber-optic cables, routers, and switches to interconnect buildings.
Example: A citywide Wi-Fi network.

4. Personal Area Network (PAN)

A PAN covers a small area, typically around a single user, connecting personal devices like smartphones, laptops, and tablets. It uses Bluetooth, USB, and infrared for connectivity.
Example: Connecting a smartphone to a laptop via Bluetooth.

Core Network Devices

1. Router

Use: Connects your home or office network to the internet.

How it works: It helps devices like your phone or laptop communicate with the internet by finding the best path for data to travel.

Example: The router in your home that connects all your devices to the internet.

2. Switch

Use: Connects multiple devices (like computers) in the same network.

How it works: It sends data only to the right device in your network, making communication faster and more efficient.

Example: The switch in an office that connects all the computers to each other.

3. Hub

Use: Connects multiple devices in the same network, but not very efficiently.

How it works: It sends data to all connected devices, which can slow down the network.

Example: An old device that connects computers together in a small office but is less efficient than a switch.

4. Modem

Use: Brings the internet to your network.

How it works: It changes the internet data from your ISP into a form that your devices can use, like turning digital signals into analog for the phone line.

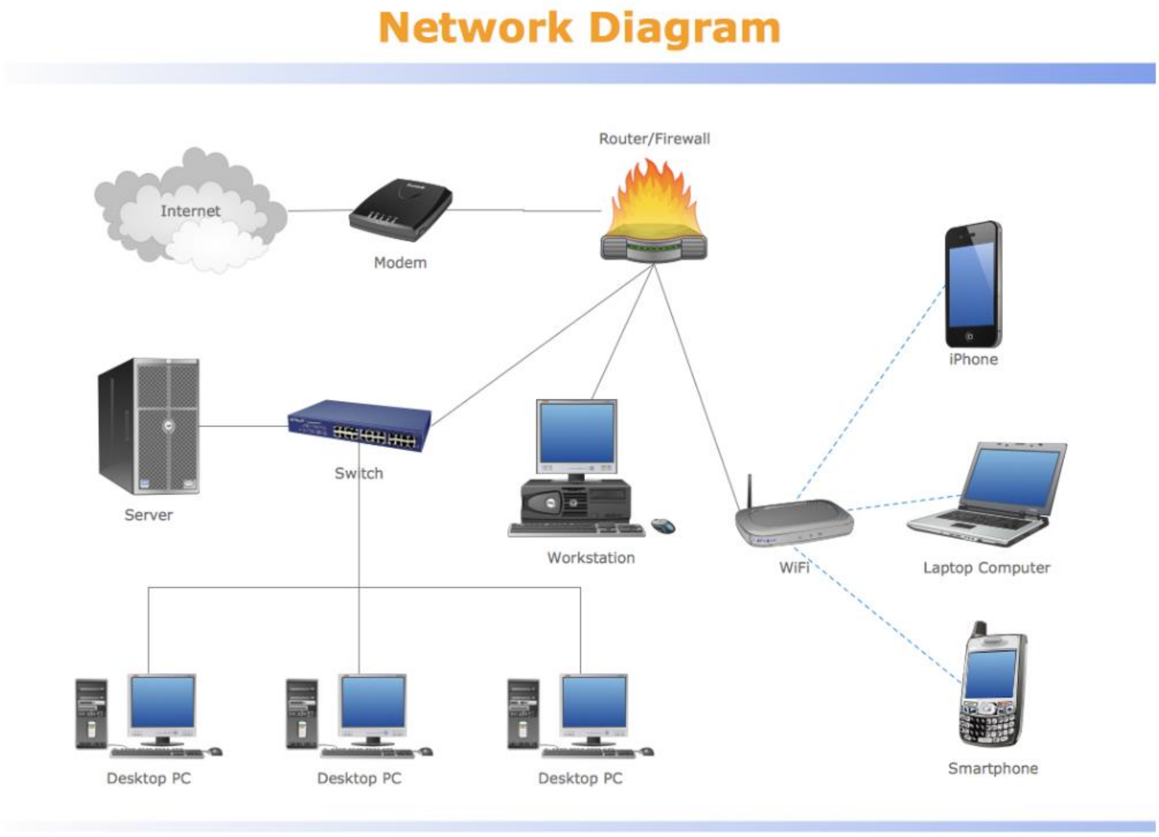
Example: The modem that connects your home network to the internet.

5. Access Point (AP)

Use: Lets wireless devices connect to your network.

How it works: It connects to your router or switch and broadcasts a Wi-Fi signal so you can use your phone, laptop, etc. wirelessly.

Example: The Wi-Fi hotspot in a café that allows customers to connect to the internet.



Network Topologies

1. Star Topology

All devices are connected to a central hub or switch. If the central device fails, the whole network goes down.

Example: Home Wi-Fi network with a router at the center.

2. Bus Topology

All devices share a single central cable (backbone). If the backbone fails, the entire network is affected.

Example: Old Ethernet networks.

3. Ring Topology

Devices are connected in a circular loop. Data travels in one or both directions around the ring.

Example: Token Ring networks (rare nowadays).

4. Mesh Topology

Every device is connected to every other device, providing multiple paths for data. Highly reliable but expensive.

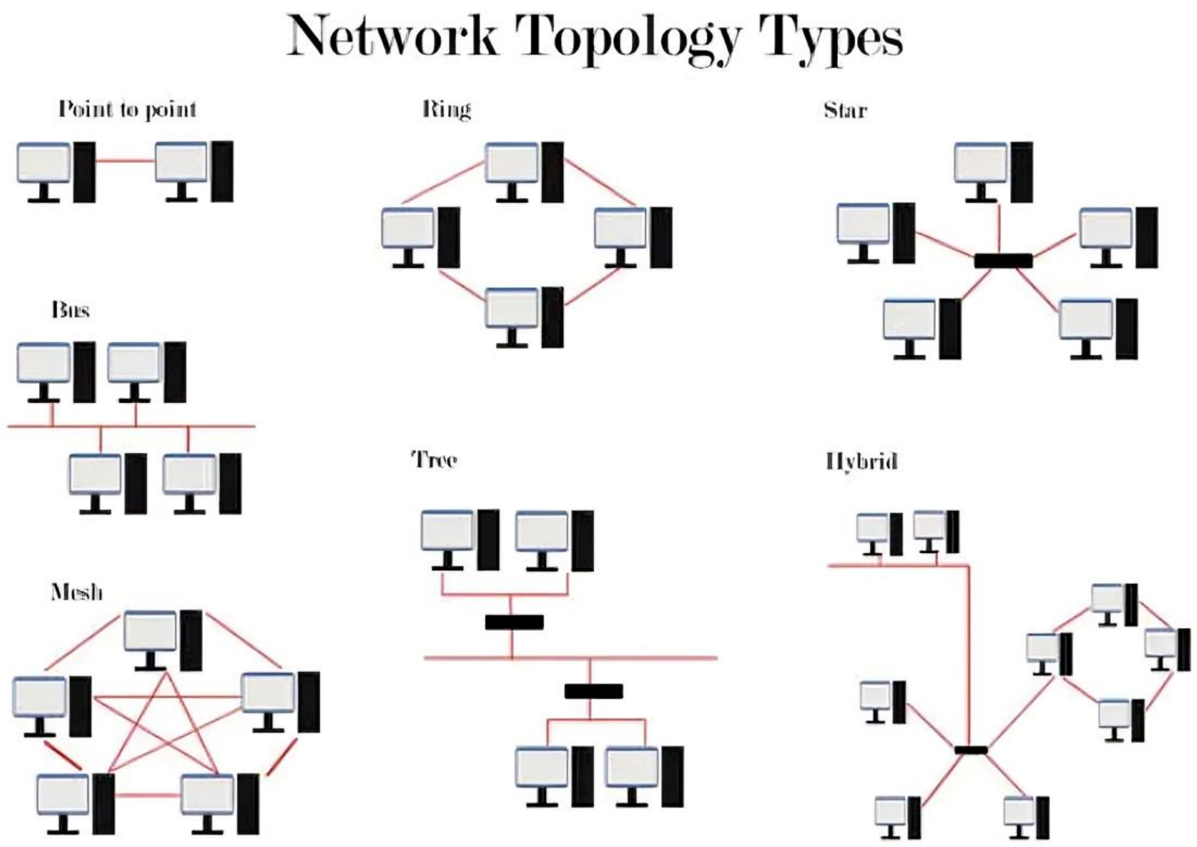
Example: Modern wireless networks in large buildings.

5. Hybrid Topology

Combines two or more topologies (like Star-Bus). Flexible and scalable but complex to manage.

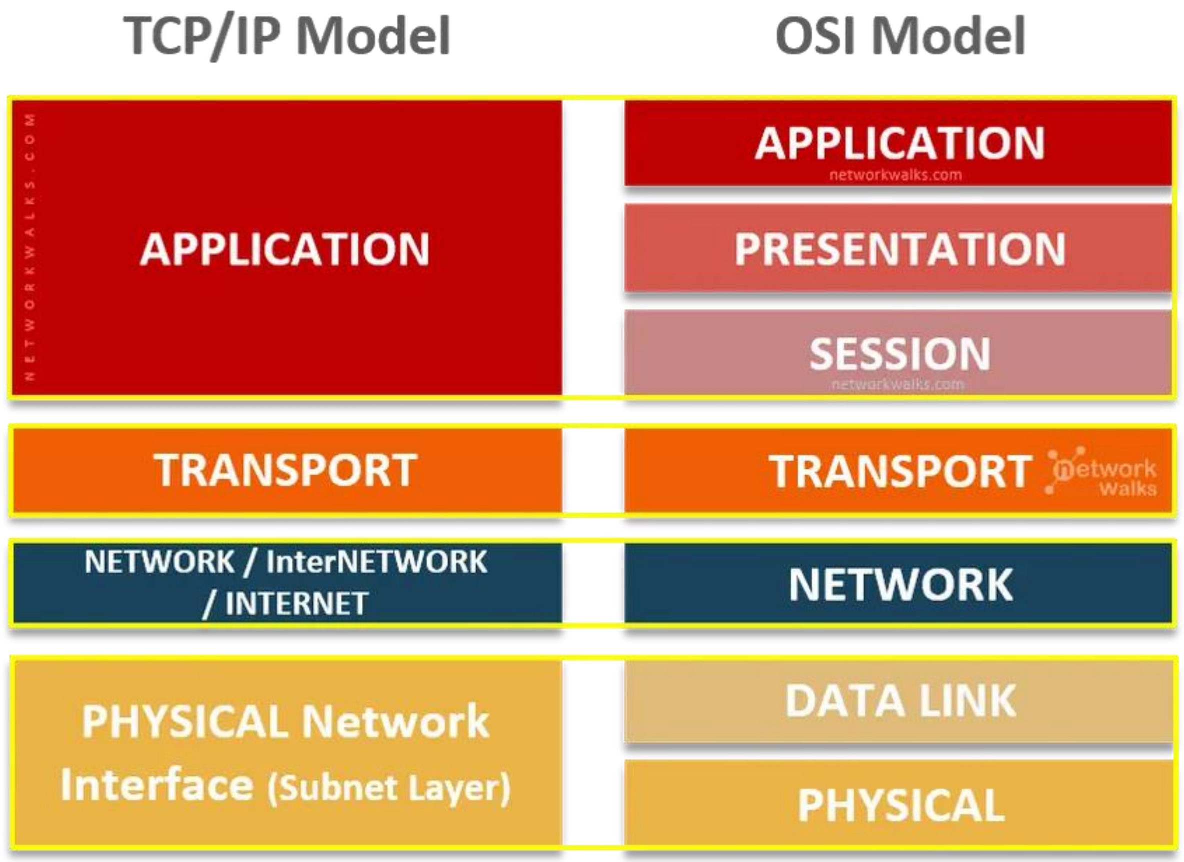
Example: A large corporate network with star and bus segments.

Let me know if you need a diagram or comparison table!



Network Models

Network models are standardized frameworks that describe how data is transmitted over a network. They define different layers, each responsible for specific tasks, to ensure smooth data communication between devices. The two most commonly used models are the OSI Model and the TCP/IP Model.



1. OSI Model (Open Systems Interconnection)

The OSI Model is a conceptual framework that standardizes network functions into **seven layers**. It helps different network devices and systems to communicate regardless of their underlying architecture.

2. TCP/IP Model (Transmission Control Protocol/Internet Protocol)

The TCP/IP model is the foundation of the modern internet and provides a practical way to understand how data is transmitted between devices. It consists of four layers that loosely correspond to the seven layers of the OSI model.

Application Layer (OSI: Application, Presentation, Session)

The Application Layer is where software applications interact with the network. It directly handles tasks like web browsing, file transfers, and sending emails. Protocols used at this layer include HTTP (for websites), FTP (for file transfers), SMTP (for emails), DNS (for domain name resolution), Telnet (for remote access), and SNMP (for network management). Devices such as PCs, smartphones, and other end-user devices operate at this layer.

Transport Layer (OSI: Transport)

The Transport Layer manages the transfer of data between devices, ensuring it reaches its destination correctly. It uses two main protocols:

- TCP (Transmission Control Protocol): Ensures reliable, ordered, and error-checked delivery of data. It is connection-oriented, meaning it establishes a connection before data transfer.
- UDP (User Datagram Protocol): Allows fast data transmission without checking for errors, making it connectionless. Suitable for streaming and real-time applications.

  This layer uses port numbers to identify specific services running on devices, like web servers (port 80 for HTTP) or file transfer services (port 21 for FTP).

Internet Layer (OSI: Network)

The Internet Layer handles logical addressing and routing between networks. It uses IP addresses to determine the best path for data to reach its destination. Key protocols at this layer include:

- IP (Internet Protocol): Handles packet addressing and routing.
- ICMP (Internet Control Message Protocol): Used for error reporting and diagnostics (like ping).

- ARP (Address Resolution Protocol): Maps IP addresses to MAC addresses.
- RIP (Routing Information Protocol): Helps routers exchange information about network topology.
  Devices such as routers primarily operate at this layer, directing data between different networks.

Network Interface Layer (OSI: Data Link + Physical)

The Network Interface Layer controls how data is transmitted physically over a network. It converts data into signals (electrical or light) that travel through cables or wirelessly. Protocols include:

- Ethernet: For wired connections in LANs.
- Wi-Fi (IEEE 802.11): For wireless local area networking.
- ARP: Used here to map IP addresses to MAC addresses.
  Devices such as Network Interface Cards (NICs), hubs, and switches operate at this layer, allowing devices to connect and communicate within a local network.

Common Protocols

1. TCP (Transmission Control Protocol)

TCP is a **connection-oriented protocol** that ensures reliable and ordered data transmission between devices. Before data transfer, it establishes a connection through a process called **"three-way handshake"** (SYN, SYN-ACK, ACK). Once the connection is established, data is sent in **packets**, and TCP makes sure all packets arrive correctly and in the right order. If any packet is lost or corrupted, TCP retransmits it.

Layer (TCP/IP Model): Transport Layer

Common TCP-based protocols:

- **HTTP/HTTPS**: Used for web browsing and secure web communication.
- **FTP**: Used for file transfers between devices.
- **SMTP**: Used for sending emails.

- **SSH**: Securely connects to remote servers.

2. UDP (User Datagram Protocol)

UDP is a **connectionless protocol** that sends data without establishing a connection, making it faster but less reliable than TCP. It does not guarantee data order or integrity, so packets may arrive out of order or not at all. Since it doesn't perform error-checking or retransmission, it is used for applications where speed is more important than accuracy.

Layer (TCP/IP Model): Transport Layer

Common UDP-based protocols:

- **DNS**: Used for domain name resolution.
- **DHCP**: Used to assign IP addresses dynamically.
- **VoIP**: Voice communication over IP networks.

IP (Internet Protocol)

An IP address (Internet Protocol address) is a unique number assigned to every device connected to a network, allowing it to communicate over the internet. It serves as both an identifier and a locator for data transfer between devices.

The Beginning - IPv4:

- The internet was small, and engineers designed the **IPv4** system to assign unique addresses to devices.
- **IPv4 addresses** are made of **32 bits**, written as four numbers separated by dots (e.g., **192.168.1.1**).
- At that time, **4.3 billion addresses** seemed enough for the internet's limited size.

The Problem - Address Shortage:

- As the internet grew, more devices needed unique IP addresses—computers, phones, IoT gadgets, etc.

- IPv4 addresses started running out, like trying to fit an expanding city into a small neighborhood.

The Temporary Solution - Private IP Addresses:

- To extend IPv4's life, engineers introduced **Private IP addresses** for internal networks.
- A **router** would receive a single **public IP** from the **ISP (Internet Service Provider)**.
- The router then generated **private IPs** for connected devices, like **192.168.x.x** or **10.x.x.x**.
- **NAT (Network Address Translation)** allowed multiple devices to share one public IP when accessing the internet.

The Permanent Fix - IPv6:

- Despite the private IP trick, IPv4 was still too limited, so engineers developed **IPv6**.
- IPv6 uses **128 bits**, represented as eight groups of hexadecimal digits (e.g., **2001:0db8:85a3:0000:0000:8a2e:0370:7334**).
- It offers **340 undecillion addresses**, enough to uniquely identify every device for generations.
- IPv6 also improved **security** and **routing efficiency**.

Address Management - RIRs and ISPs:

- To manage this vast address pool, five organizations called **Regional Internet Registries (RIRs)** handle distribution.
- RIRs allocate public IP ranges to **ISPs**, which then assign them to individual users and businesses.
- Private IP addresses are still used locally, while public IPs allow internet connectivity.

Subnetting

Subnetting is the process of dividing a large network into smaller, more manageable sub-networks (subnets). This technique helps organize a network, improve performance, and enhance security.

- An IP address is divided into two parts: the **network part** and the **host part**.
- Subnetting adds another layer by dividing the host part into **subnet ID** and **host ID**.
- This division is controlled by the **subnet mask**, which indicates how many bits are used for the network and subnet parts.

Example:

- IP Address: 192.168.1.0/24
- Subnet Mask: 255.255.255.0
- If subnetted into two subnets, you may get:
    - 192.168.1.0/25 (subnet 1)
    - 192.168.1.128/25 (subnet 2)

References

https://youtube.com/playlist?list=PLIhvC56v63IJVXv0GJcl9vO5Z6znCVb1P&si=A0rUPdgBgYO-YmJk

https://youtu.be/RY32wSQDekE?si=6kWfZXF1-WKWXb6K

https://youtube.com/playlist?list=PLkW9FMxqUvyZaSQNQslneeODER3bJCb2K&si=CARUI9ff8LqJYQP5