Data Communication and Computer Networks- 3050302103

Unit :1 Introduction to Data Communication and Computer Networks

Computer Network – Overview

A computer network is a collection of computing devices that are connected with each other for the purpose of information and resource sharing among a wide variety of users.

A system of interconnected computers and computerized peripherals such as printers is called computer network. This interconnection among computers facilitates information sharing among them. Computers may connect to each other by either wired or wireless media.

What is a Computer Network?

A **computer network** is a system of interconnected computers and other digital devices that can communicate and share resources (like files, internet, printers, etc.) using a communication medium (wired or wireless).

Applications of Computer Networks

Computer networks have become an integral part of modern life, enabling communication, resource sharing, and data access across various domains. Below are the major applications:

1. Business Applications

- **Resource Sharing:** Enables sharing of printers, files, and internet access among employees.
- **Client-Server Architecture:** Centralized databases and applications allow seamless business operations.
- **Communication Tools:** Emails, VoIP, and video conferencing support internal and external communication.
- **Remote Access:** Employees can work from home or different locations using VPNs and remote desktop tools.

2. Home Applications

- **Internet Access:** Allows households to access the internet through Wi-Fi.

- **File and Media Sharing:** Share videos, music, and documents between computers and smart devices.
- **Smart Home Devices:** Home networks enable IoT applications like smart lights, thermostats, and security systems.

3. Mobile and Wireless Applications

- **Mobile Communication:** Cell phones and mobile apps rely heavily on wireless networks.
- **Cloud Computing:** Users can store and retrieve data from cloud services like Google Drive, iCloud, etc.
- **Location-based Services:** Navigation apps like Google Maps depend on wireless network data.

4. Educational Applications

- **E-Learning Platforms:** Online classes, assignments, and exams are conducted over educational networks.
- **Resource Sharing:** Access to digital libraries, academic repositories, and shared software tools.
- **Collaboration Tools:** Students and teachers can collaborate using platforms like Google Classroom, Zoom, and Microsoft Teams.

5. Government and Public Services

- **E-Governance:** Citizens can access government services like tax filing, licenses, and certificates online.
- **Public Safety and Emergency Services:** Police, fire, and medical services use networks for quick response and coordination.
- **Voting Systems:** Some regions use secure networked systems for electronic voting.

6. Healthcare Applications

- **Telemedicine:** Remote diagnosis and treatment through video conferencing and digital reports.
- **Patient Records:** Electronic health records (EHR) are accessed and updated over secure networks.

- **Medical Equipment:** Networked systems allow real-time monitoring of patients.

7. Banking and Financial Services

- **Online Banking:** Fund transfers, bill payments, and account management are done over secure networks.
- **ATM Services:** Operate through connected banking networks.
- **Stock Trading Platforms:** Real-time stock updates and trading are facilitated by high-speed networks.

8. Research and Scientific Applications

- **Data Sharing:** Scientists across the globe collaborate and share massive datasets over networks.
- **Supercomputing Grids:** Distributed computing allows combining processing power from multiple locations.
- **Remote Experimentation:** Labs and instruments can be operated remotely through connected networks.

9. Entertainment

- **Streaming Services:** Platforms like Netflix, YouTube, and Spotify deliver content via the internet.
- **Online Gaming:** Multiplayer games rely on real-time data exchange over networks.
- **Social Media:** Apps like Instagram, WhatsApp, and Facebook run on robust networking infrastructures.

10. Industrial and Manufacturing Applications

- **Automation Systems:** Use networked control systems like SCADA for monitoring and managing equipment.
- **Supply Chain Management:** Networks help track inventory, shipments, and logistics in real-time.
- **Smart Factories (Industry 4.0):** Use of IoT and AI over networks for optimized operations.

Network Types – LAN, MAN, and WAN

1. LAN (Local Area Network)

Definition:

A **Local Area Network (LAN)** is a network that connects computers and devices within a **limited geographical area**, such as a home, office, school, or college campus.

Key Characteristics:

- **Covers:** Small area (up to a few kilometers)
- **Ownership:** Usually owned, controlled, and managed by a single organization or individual
- **Speed:** High data transfer speeds (up to 1 Gbps or more)
- **Reliability:** Very reliable and low latency
- **Cost:** Low setup and maintenance cost

Examples:

- Office or school computer labs
- Home Wi-Fi networks
- College campus networks

Advantages:

- Easy to install and manage
- Low cost
- High-speed data transfer
- Enhanced data security in private setups

Disadvantages:

- Limited to a small area
- Hardware like switches and routers are required

2. MAN (Metropolitan Area Network)

Definition:

A **Metropolitan Area Network (MAN)** is a network that spans a **city or a large campus**, connecting multiple LANs within a specific geographic region.

Key Characteristics:

- **Covers:** Medium area (city or town-wide)
- **Ownership:** May be owned by an individual organization or a service provider
- **Speed:** Moderate to high speeds (10 Mbps to 100 Mbps or more)
- **Connectivity:** Often uses fiber optic cables or wireless microwave links
- **Example:** City-wide cable TV networks, inter-campus university networks

Examples:

- City-wide government network
- University connecting multiple campuses
- Cable TV or broadband service providers

Advantages:

- Covers larger areas than LAN
- Enables centralized data sharing among institutions or branches
- More scalable than LAN

Disadvantages:

- More complex to install and maintain than LAN
- Requires higher costs and skilled management

3. WAN (Wide Area Network)

Definition:

A **Wide Area Network (WAN)** is a network that covers a **large geographical area**, such as a country, continent, or even the entire globe.

Key Characteristics:

- **Covers:** Very large area (multiple cities, countries, continents)
- **Ownership:** Owned and maintained by multiple organizations or service providers
- **Speed:** Lower than LAN/MAN due to long-distance transmission (varies widely)
- **Medium:** Uses public networks like telephone lines, satellite links, or undersea cables

Examples:

- The Internet (largest WAN)
- Global corporate networks (e.g., bank networks)
- International airline reservation systems

Advantages:

- Allows global communication
- Supports multinational business operations
- Centralized data access and control for global offices

Disadvantages:

- High setup and maintenance costs
- Lower security and speed compared to LAN/MAN
- Complex design and troubleshooting

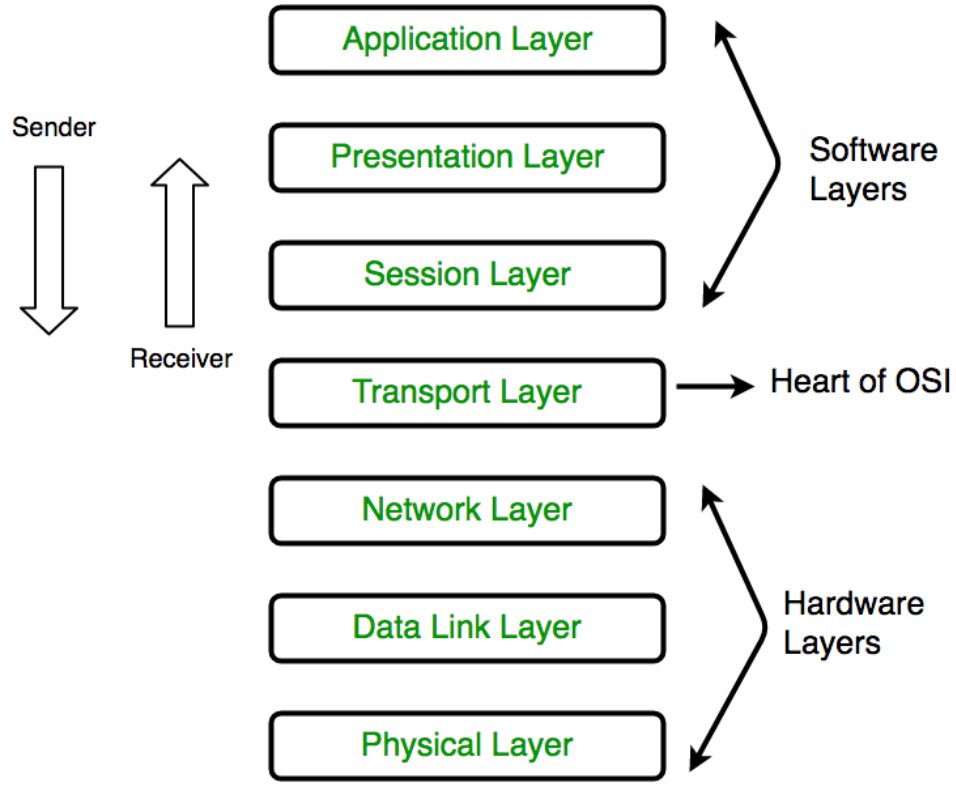
Network Models – OSI Model and TCP/IP Model

What is the OSI Model?

The **OSI (Open Systems Interconnection)** model is a **theoretical framework** developed by the **International Organization for Standardization (ISO)**. It describes how different networking protocols and devices communicate across a network in a **layered architecture**.

- Total **7 Layers**

- Each layer performs a **specific function**
- Promotes **interoperability**, **standardization**, and **modular development**



Physical Layer

The lowest layer of the OSI reference model is the **Physical Layer**. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** Physical Layer is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together. Common physical layer devices are Hub, Repeater, Modem, and Cables.
This layer provides **network services to applications** such as email, file transfer, and web browsing.

- Transmits raw bits over the physical medium
- Deals with the physical connection between devices**.**

Functions:

- Bit-by-bit transmission
- Electrical/optical signals
- Cables, connectors, voltages, pin layout

- Devices: Cables, Hubs, Repeaters
- Media: Fiber, Twisted Pair, Coaxial

Layer 2: Data Link Layer (DLL)

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address. Packet in the Data Link layer is referred to as Frame**.** Switches and Bridges are common Data Link Layer devices.

- Responsible for node-to-node delivery
  Ensures reliable transfer of data over the **physical link** between two devices.
- **Functions:**
  - MAC addressing
  - Framing
  - Error detection (CRC)
  - Flow control
- **Devices:** Switches, Bridges
- **Protocols:** Ethernet, PPP, HDLC

Layer 3: Network Layer

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender and receiver's IP address are

placed in the header by the network layer. Segment in the Network layer is referred to as Packet**.** Network layer is implemented by networking devices such as routers and switches.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender and receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.
- **Handles routing and addressing**
  Determines the **best path** for data to travel between devices in different networks.

  Devices: Routers

  Protocols: IP, ICMP, ARP, OSPF, BGP

Layer 4: Transport Layer

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as **Segments**. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found. Protocols used in Transport Layer are TCP, UDP

End-to-end communication
Ensures **reliable data transmission** with error control and flow control between devices.

- **Functions:**
  - Segmentation and reassembly
  - Error detection and correction
  - Flow control (windowing)

- **Protocols:** TCP (reliable), UDP (unreliable)

Services Provided by Transport Layer

- Connection-Oriented Service
- Connectionless Service

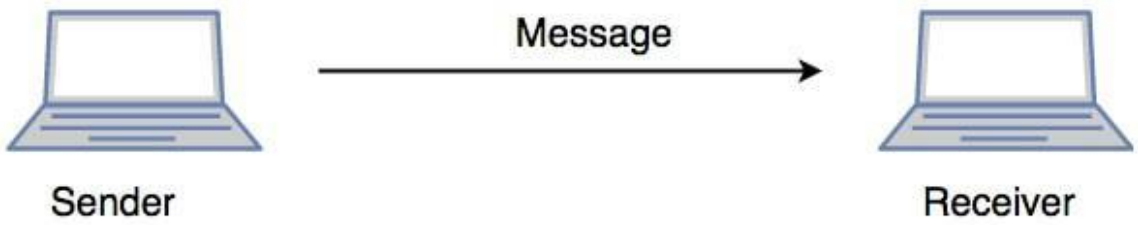
Layer 5: Session Layer

Session Layer in the OSI Model is responsible for the establishment of connections, management of connections, terminations of sessions between two devices. It also provides authentication and security.

Manages sessions and dialogs
Responsible for **establishing, managing, and terminating connections** (sessions) between applications

Functions of the Session Layer

- **Session Establishment, Maintenance, and Termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely, and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full duplex.



Layer 6: Presentation Layer

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network. Protocols used in the Presentation Layer

are TLS/SSL (Transport Layer Security / Secure Sockets Layer).JPEG, MPEG, GIF, are standards or formats used for encoding data, which is part of the presentation layer's role

- **Translator of the network**
  It ensures that data is in a usable format and handles **data encoding, encryption, and compression**.

- **Functions:**
  - Data conversion (EBCDIC ↔ ASCII)
  - Encryption/Decryption (e.g., SSL/TLS)
  - Compression (e.g., ZIP)

Layer 7: Application Layer
At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user. Protocols used in the Application layer are SMTP, FTP, DNS, etc.

Closest to the user
This layer provides **network services to applications** such as email, file transfer, and web browsing.

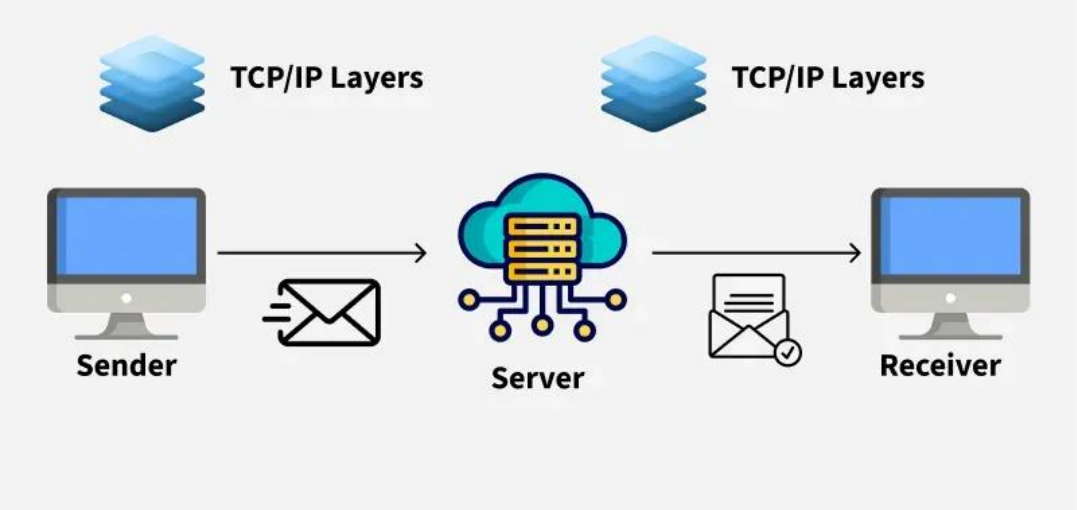
- **Functions:**
  - User interface
  - Network-based services like HTTP, FTP, SMTP
  - File access, emails, remote login
- **Protocols:** HTTP, FTP, SMTP, DNS, Telnet.

TCP/IP Model

What is the TCP/IP Model?

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a real-world, practical network model that forms the foundation of the modern Internet. It defines how data is transmitted and received over interconnected networks.

- Consists of **4 layers**



Application Layer

- Provides services to user applications.
- This layer combines the functions of the OSI Model's **Application, Presentation, and Session Layers**.

The Application Layer is the top layer of the TCP/IP model and the one closest to the user. This is where all the apps you use like web browsers, email clients, or file sharing tools connect to the network. It acts like a bridge between your software (like Chrome, Gmail, or WhatsApp) and the lower layers of the network that actually send and receive data.

2. Transport Layer

The Transport Layer is responsible for making sure that data is sent reliably and in the correct order between devices. It checks that the data you send like a message, file, or video arrives safely and completely. This layer uses two main protocols: TCP and UDP, depending on whether the communication needs to be reliable or faster.

TCP is used when data must be correct and complete, like when loading a web page or downloading a file. It checks for errors, resends missing pieces, and keeps everything in order. On the other hand, UDP (User Datagram Protocol) is faster but doesn't guarantee delivery useful for things like live video or online games where speed matters more than perfect accuracy.
Ensures end-to-end communication

This layer is responsible for **process-to-process delivery** of data across the network.

3. Internet Layer

- **Handles addressing and routing of data packets**

The Internet Layer is used for finding the best path for data to travel across different networks so it can reach the right destination. It works like a traffic controller, helping data packets move from one network to another until they reach the correct device. This layer uses the Internet Protocol (IP) to give every device a unique IP address, which helps identify where data should go.

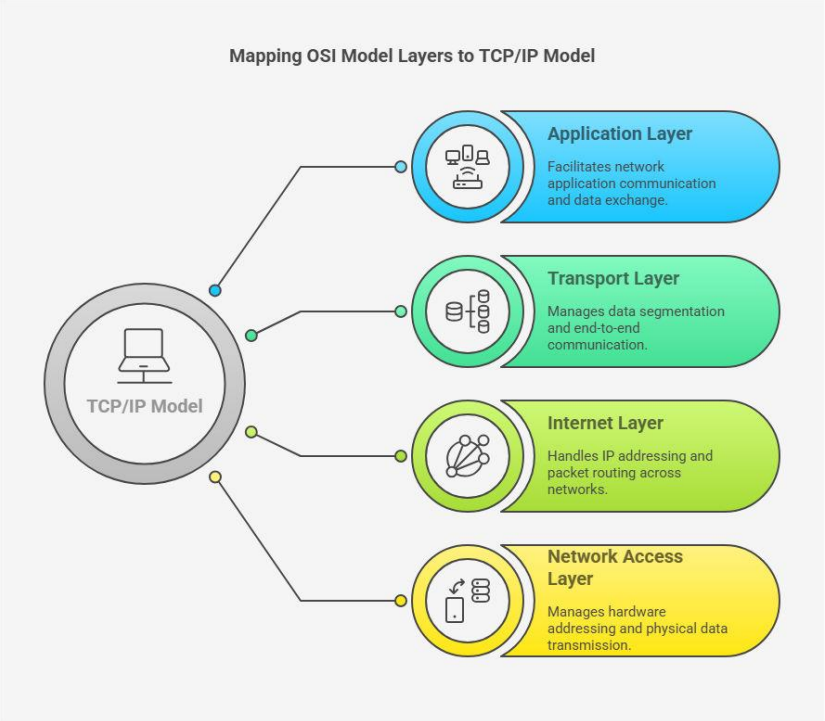
The main job of this layer is routing deciding the best way for data to travel. It also takes care of packet forwarding (moving data from one point to another), fragmentation (breaking large data into smaller parts), and addressing.

4. Network Access Layer

The Network Access Layer is the bottom layer of the TCP/IP model. It deals with the actual physical connection between devices on the same local network like computers connected by cables or communicating through Wi-Fi. This layer makes sure that data can travel over the hardware, such as wires, switches, or wireless signals.

- Responsible for physical transmission of data . This layer combines the OSI's Data Link Layer and Physical Layer.

It also handles important tasks like using MAC addresses to identify devices, creating frames (the format used to send data over the physical link), and checking for basic errors during transmission.



Network Topologies –

What is Network Topology?

Network topology refers to the **arrangement of devices (nodes)** and connections (links) in a computer network. It determines how data flows between devices and how devices interact with each other.

There are **two types** of topology:

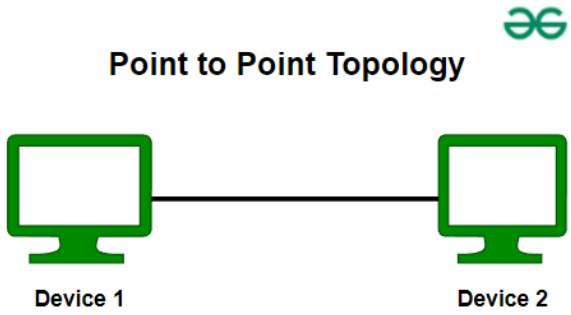
- **Physical topology** – Actual layout of cables and devices.
- **Logical topology** – The way data flows in the network.

Types of Network Topology

- Point to Point Topology
- Mesh Topology
- Star Topology
- Bus Topology
- Ring Topology
- Tree Topology

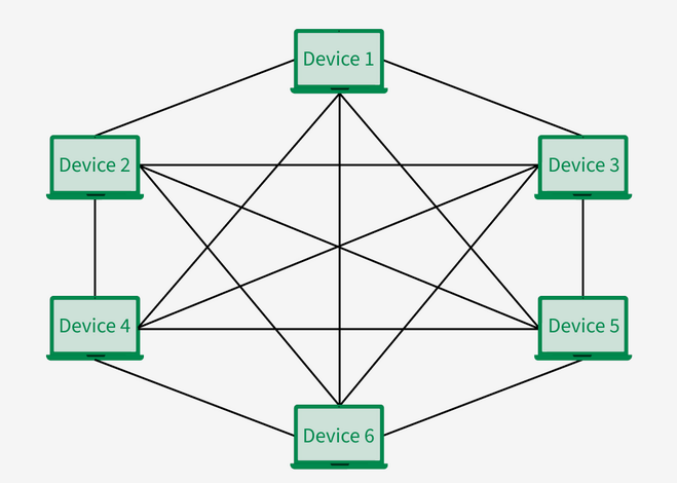
Point to Point Topology

Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Mesh Topology

In a mesh topology, every device is connected to another device via a particular channel. Every device is connected to another via dedicated channels. These channels are known as links. In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Advantages:

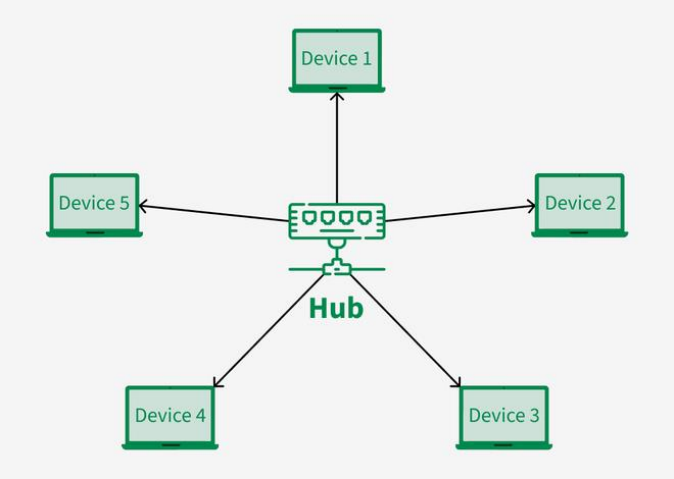
- High fault tolerance and redundancy
- Excellent reliability and speed

Disadvantages:

- Very expensive (lots of cabling and ports)
- Complex to install and manage

Star Topology

In Star Topology, all the devices are connected to a single hub through a cable. This hub is the central node and all other nodes are connected to the central node. The hub can be passive in nature i.e., not an intelligent hub such as broadcasting devices, at the same time the hub can be intelligent known as an active hub. Active hubs have repeaters in them. Coaxial cables or RJ-45 cables are used to connect the computers. In Star Topology, many popular Ethernet LAN protocols are used as CD(Collision Detection), CSMA (Carrier Sense Multiple Access), etc.



Advantages:

- Easy to install and manage
- Failure of one device doesn't affect others
- Easy to add/remove devices

Disadvantages:

- Central hub failure brings down the entire network
- Requires more cables (increased cost)

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Structure:

- All devices are connected to a **single central cable** (called a backbone or bus).
- Data travels in **both directions** along the cable.

Advantages:

- Simple and cost-effective
- Easy to install for small networks

Disadvantages:

- Single point of failure (the bus)
- Difficult to troubleshoot
- Not scalable

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighboring devices. A number of repeaters are used for Ring topology with a large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node

Tree Topology

Network topology is the systematic arrangement of the elements (such as links and nodes) within a communication network. A tree topology, or star-bus topology, is a hybrid network topology in which star networks are interconnected via bus networks. Tree networks are organized hierarchically, allowing each node to have child nodes.

- It merges the features of both star and bus topologies. It includes a node known as the root that connects to one or more star networks called branches. Each branch can further extend into sub-branches, forming a structure resembling that of a tree.

- Tree topology is hierarchical, allowing for easy expansion of the network and better organization. It is commonly used in large networks where scalability and manageability are important.

Advantages:

- Scalable and easy to manage
- Fault isolation is easy

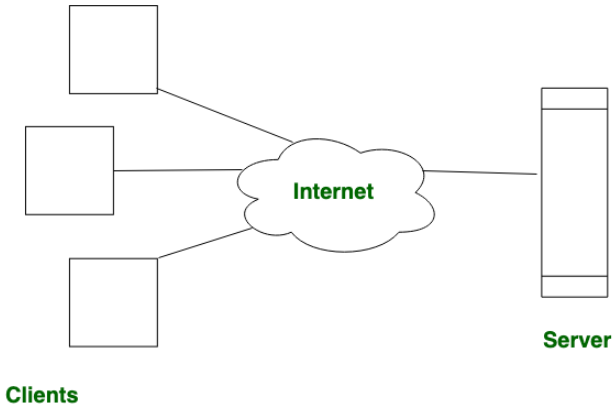
Disadvantages:

- Central node failure affects entire network
- Cabling complexity and cost

Categories of Networks – Peer-to-Peer and Client-Server

What is a Client-Server Network?

This model are broadly used network model. In the Client-Server Network, Clients and servers are differentiated, and Specific servers and clients are present. In Client-Server Network, a Centralized server is used to store the data because its management is centralized. In Client-Server Network, the Server responds to the services which is requested by the Client.



Client-Server Network Model

Peer-to-Peer (P2P) network, **all devices (peers)** are equal and can act as both **clients and servers**. Each computer can share files, printers, or internet directly with others without a centralized server.

Features:

- No central server – all nodes share resources equally.
- Each peer has equal status.
- Best for **small networks** (home or small offices).
- Easy and inexpensive to set up.

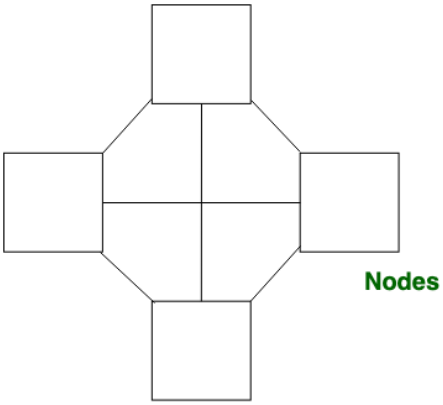
Peer-to-Peer Network?

This model does not differentiate the clients and the servers, In this each and every node is itself client and server. In Peer-to-Peer Network, Each and every node can do both request and respond for the services.

- Peer-to-peer networks are often created by collections of 12 or fewer machines. All of these computers use unique security to keep their data, but they also share data with every other node.

- In peer-to-peer networks, the nodes both consume and produce resources. Therefore, as the number of nodes grows, so does the peer-to-peer network's capability for resource sharing. This is distinct from client-server networks where an increase in nodes causes the server to become overloaded.

- It is challenging to give nodes in peer-to-peer networks proper security because they function as both clients and servers. A denial of service attack may result from this.



Peer-to-Peer Network Model

Client-Server network, one or more central **servers** provide services, and other devices (**clients**) request those services. The server is a powerful machine that stores data and manages access.

Features:

- Dedicated server manages resources and controls access.
- Clients are dependent on the server for services.
- Suitable for medium to large organizations.
- Provides centralized security and control.

Overview of Internet, Intranet, and Extranet

Internet

Definition:

The **Internet** is a **global system of interconnected computer networks** that uses the **TCP/IP protocol suite** to link billions of devices worldwide.

It is a **public network**, accessible to anyone with an internet connection.

Key Features:

- **Global coverage**
- **Publicly accessible**
- Uses **standardized protocols** like TCP/IP, HTTP, FTP, DNS
- Massive resources: websites, emails, social media, cloud storage

Advantages:

- Access to global information
- Communication via email, chat, video conferencing
- E-commerce, e-learning, entertainment
- Real-time updates, social connectivity

Disadvantages:

- Data security and privacy issues
- Cyber threats (viruses, malware, phishing)
- Content may be unreliable or inappropriate

Examples of Use:

- Browsing websites (Google, Wikipedia)
- Online shopping (Amazon, Flipkart)
- Streaming videos (YouTube, Netflix)
- Social media (Facebook, Instagram)

2. Intranet

Definition:

An **Intranet** is a **private network** used within an organization. It uses **internet technologies (like HTTP, TCP/IP)** but is **restricted to internal users**.

Key Features:

- Accessible only by authorized employees within the organization
- Used for internal communication and resource sharing
- Hosted on secure internal servers

Advantages:

- Enhanced communication within the organization
- Increases productivity and information sharing
- Centralized data storage (documents, forms, HR tools)
- Secure compared to public networks

Disadvantages:

- Only accessible within the organization
- Maintenance costs and resource requirements
- Limited access to external users (unless connected via VPN)

Examples of Use:

- Company portals for HR, leave, payroll
- Internal announcements and bulletin boards
- Employee training materials and policy documents

3. Extranet

Definition:

An **Extranet** is an **extension of an Intranet** that allows **controlled access to external users** like business partners, vendors, or clients.

It acts as a **secure bridge** between an organization's intranet and the external world.

Key Features:

- Allows access to selected parts of the intranet
- Typically uses **VPNs**, **authentication**, and **firewalls**
- Facilitates **collaboration** beyond the organization

Advantages:

- Strengthens relationships with partners and suppliers
- Enables efficient supply chain and project management
- Secure information sharing across organizations
- Reduces paperwork and communication delays

Disadvantages:

- Security risks if access control is weak
- Complex to manage and maintain
- Requires robust authentication and encryption

Examples of Use:

- Vendor portal for placing and tracking orders
- Partner collaboration on shared projects or documents
- Client dashboards to view account information or support tickets