Network Basics

Network Definition

A network is a set of technologies- including hardware, software, and media- that can be used to connect computers together, enabling them to communicate, exchange information, and share resources in real time. Networks allow many users to access shared data and programs almost instantly. When data and programs are stored on a network and are shared, individual users can substantially reduce the need for programs on their own computers. Networks open up new ways to communicate, such as e-mail and instant messaging. By allowing users to share expensive hardware resources such as printers, networks reduce the cost of running an organization.

The Advantages of Using a Network

- **Allows Simultaneous Access to Critical Programs and Data.**

Files can be stored on a central location called a "file server" that can be shared and made available to each and every user in an organization. The files can be updated by several users simultaneously by using the network. The organization can store a single copy of a data file on the server that users can access whenever they want. Then, if one user makes a change to the file, other users will see the change when they use the file, and no one needs to figure out who has the latest copy of the data. Software can also be shared through the network. Software is costly for two reasons. First, software can be costly, especially when dozens or hundreds of copies are required. Second, installing and configuring a software on several computers takes a lot of time and effort, and maintaining multiple program installations is an ongoing cost. Without having to install separate software for each user, these issues can be overcome through site licensing and network versions. Under a site license, a business buys a single copy (or a few copies) of an application and then pays the developer for a license to copy the application onto a specified number of computers. In a network version, only one copy of the application is stored on the server. When workers need to use a program, they simply load it from the server into the RAM of their own desktop computers.

- **Allows People to Share Peripheral Devices, Such as Printers and Scanners.**

Organizations can save money by using network-connected peripheral devices like printers, scanners, and copiers. The ability to share peripheral devices (especially expensive ones such as high- volume laser printers, which can cost thousands of dollars) is one of the best reasons for small businesses to set up a network. Although printers are more affordable than they were a few years ago, it is still too expensive to provide every worker with a personal printer. Aside from the cost of purchasing multiple printers, the organization must also pay for printer maintenance and supplies, which ultimately increases the organization's overall cost. When several people can share a printer on a network, printing becomes less expensive and easier to manage. There are two common ways to share a printer. A printer can connect directly to the network or it can be attached to a print server, which is a computer that manages one or more printers.

- **Facilitates Personal Communication with Email and Instant Messaging.**

A computer network facilitates interpersonal communications, allowing users to communicate efficiently and easily via various means like email, instant messaging, and teleconferencing. Instant messaging can now allow users to talk in real time and send files to other people wherever they are in the world. Teleconferencing means connecting two or more participants from different locations electronically to hold discussions and meetings. The three most common types of teleconference are conference calls (voice only), videoconferences (voice and video), and web-based conferences. A conference call is simply a phone call with more than two participants. Video conferencing is a technology that allows users in different locations to hold real-time face-to-face meetings, often at little to no cost. Web conferencing enables the real-time sharing of computer screens, individual applications or web-based content among two or more computers or mobile devices.

- **Makes the Backup Process Easier.**

When one PC's information is corrupted or inaccessible for various reasons, another duplicate of similar information is accessible on another workstation for future usage. In this case data backup is necessary. The network ensures smooth working and further handling without interruption by backing up all the data that is stored on the shared removable media or cloud storage.

Types of Network

A computer network is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.

A computer network can be categorized by their size. The common types of computer networks are;

- Personal Area Network (PAN)
- Home Area Network (HAN)
- Local Area Network (LAN)
- Campus Area Network (CAN)
- Metropolitan Area Network (MAN)
- Wide Area Network (WAN)
- Virtual Private Network (VPN)
- Intranet & Extranet

Personal Area Network (PAN)

PAN (Personal Area Network) is a computer network formed around a person. It generally consists of a computer, mobile, or Personal Digital Assistant (PDA). PAN can be used for establishing communication among these personal devices. A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infrared enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.

Home Area Network (HAN)

A HAN is like a PAN, but even bigger. As the name suggests, a HAN is a very small network that usually covers a single home. This facilitates communication among the digital devices within a home which are connected to the home network. Any device that is connected to this network will be able to share resources, for example the internet, smart appliances, printers, smart meters and even some security systems.

Local Area Network (LAN)

A local area network (LAN) is a data communication system consisting of several devices such as computers and printers. This type of network contains computers that are relatively near each other and are physically connected using cables, infrared links, or wireless media. A LAN can consist of just two or three PCs connected together to share resources, or it can include hundreds of computers of different kinds. Any network that exists within a single building, or even a group of adjacent buildings, is considered a LAN. A LAN is not a system that connects to the public environment (such as the Internet) using phone or data lines. It is often helpful to connect separate LANs together so they can communicate and exchange data. In a large company, for example, two departments located on the same floor of a building may have their own separate LANs, but if the departments need to share data, then they can create a link between the two LANs.

Campus Area Network (CAN)

A Campus Area Network is made up of an interconnection of LANs within a specific geographical area. For example, a university campus can be linked with a variety of campus buildings to connect all the academic departments.

Metropolitan Area Network (MAN)

A metropolitan area network (MAN) is similar to a local area network (LAN) but spans an entire city or campus, or some other municipal or organizational territory. MANs are formed by connecting multiple LANs. Thus, MANs are larger than LANs, but smaller than wide area networks (WAN) that cover dispersed geographical areas, sometimes directly connecting users around the world. MANs are typically extremely efficient and can provide fast communication via high-speed carriers, such as fiber optic cables. Television cable is an example of a MAN. It is also used in communication between the banks in a city.

Wide Area Network (WAN)

A Wide Area Network is a network that extends over a large geographical area such as states or countries. A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links. The internet is one of the biggest WAN in the world. A Wide Area Network is widely used in the field of Business, government, and education.

Virtual Private Network (VPN)

A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public internet connection. VPNs mask your internet protocol (IP) address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections to provide greater privacy than even a secured Wi-Fi hotspot. VPNs are primarily used for remote access to a private network. For example, employees at a branch office could use a VPN to connect to the main office's internal network. Alternatively, a remote worker, who may be working from home, could need to connect to their company's internet or restricted applications.

Intranet & Extranet

An intranet functions as a company's private communication network. It's a private website for employees with company news, information, documents, and business process tools that are critical for completing work. Whereas an extranet is a private network too. It allows business partners, suppliers, and other authorized parties to communicate. The extranet is accessible to designated people from outside the company. It can be shared by more than one organization, such as a business that allows its vendors to access the company extranet for product and billing purposes.

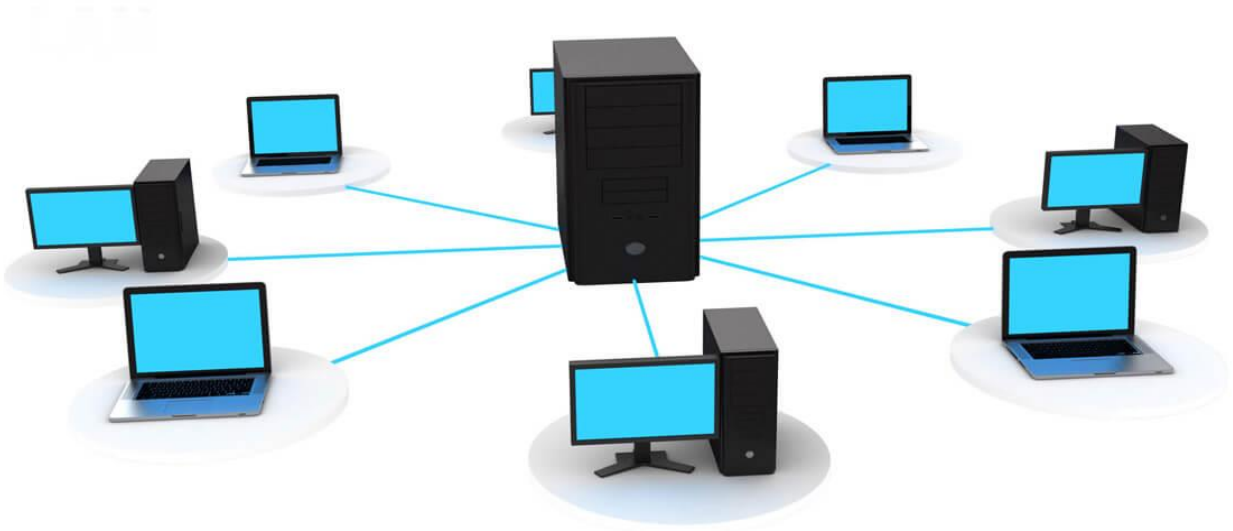
How Network is Structured

Based on network design, a computer network can be divided into the following two types:

1. Server-Based Network
2. Peer-to-Peer Network

1. Server-Based Network

A Server-Based network can also be termed as a Client-Server network. In a client server network, there are clients and servers. A client can be a device or a program. It helps the end users to access the web. Some examples of clients are desktop, laptops, smartphones, web browsers, etc. A server is a device or a program that responds to the clients with the services. It provides files, databases, web pages, shared resources according to its type. In this network, a client requests services from the server. The server listens to the client requests and responds to them by providing the required service. There is various kind of servers depending upon their use, they can be a web server (which servers HTTP requests), Database servers (which runs DBMS), File server (which provides files to clients), Mail server, print server, Game server, Application server, and so on.



Figure; Sever-Based Network

Following are the advantages of using a server-based network:

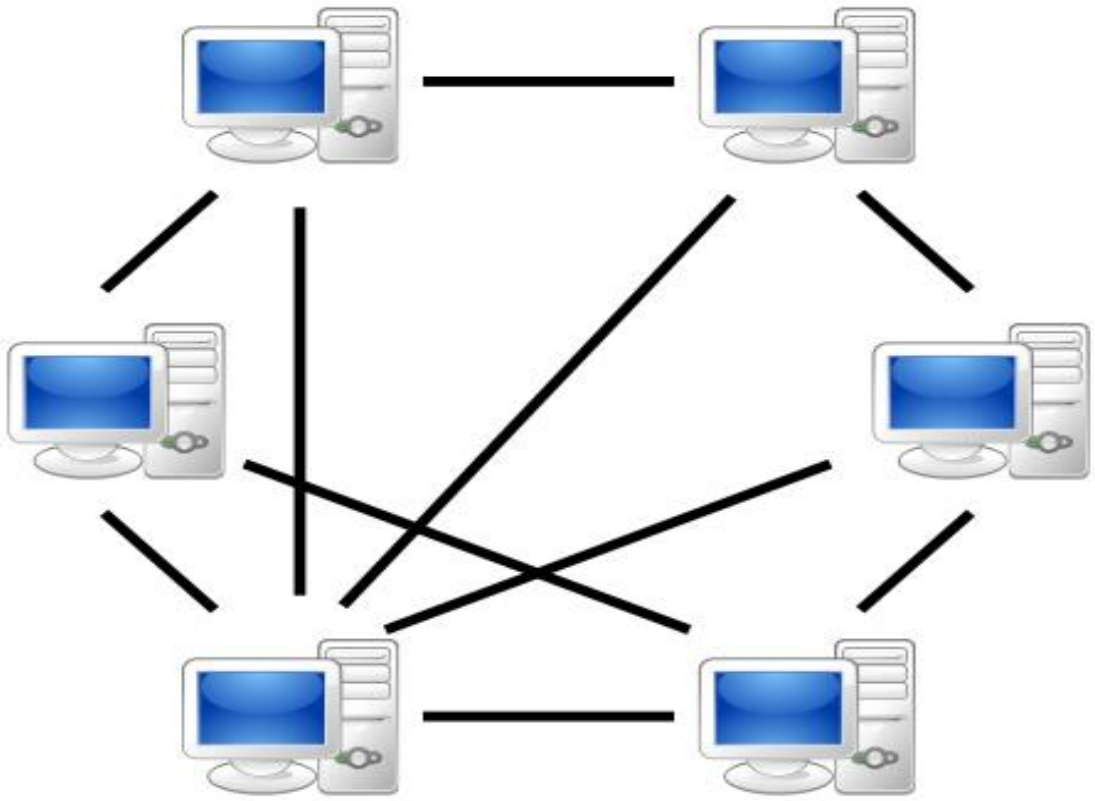
- It facilitates a Centralized storage system.
- Centralization makes administration easy.
- Data can be easily backed in such networks.
- Server-based networks are scalable networks, meaning they are easily expandable.
- Data sharing speed is high.
- Servers can serve multiple clients at a time.

Following are the disadvantages of using a server-based network:

- Dependency is more on a centralized server.
- If the server's data is corrupted, all nodes will be affected.
- A network administrator is required.
- The cost of the server and network software is very high.

2. Peer-to-Peer Network

The Peer-to-Peer network is also called P2P or computer-to-computer network. In a peer to peer network, there is no specific client or a server. A device can send and receive data directly with each other. Each node can either be a client or a server. It can request or provide services accordingly. A node is also called a peer. In networking, a node is either a connection point, a redistribution point, or a communication endpoint. Nodes are devices or data points on a large network, devices such a PC, phone, or printer are considers nodes. In peer to peer network, a node joins the network and start providing services and request for services from other nodes. There are two methods to identify which node provides which service. A node registers the service it provides into a centralized lookup service. When any node requires obtaining a service, it checks the centralized lookup to find which node provides which facilities. Then, the service providing node and service requesting node communicate with each other. In the other method, a node that requires specific services can send a broadcast message to all other nodes requesting a service. Then, the node that has the required service responds to the requested node by providing the service.



Figure; Peer-to-Peer Network

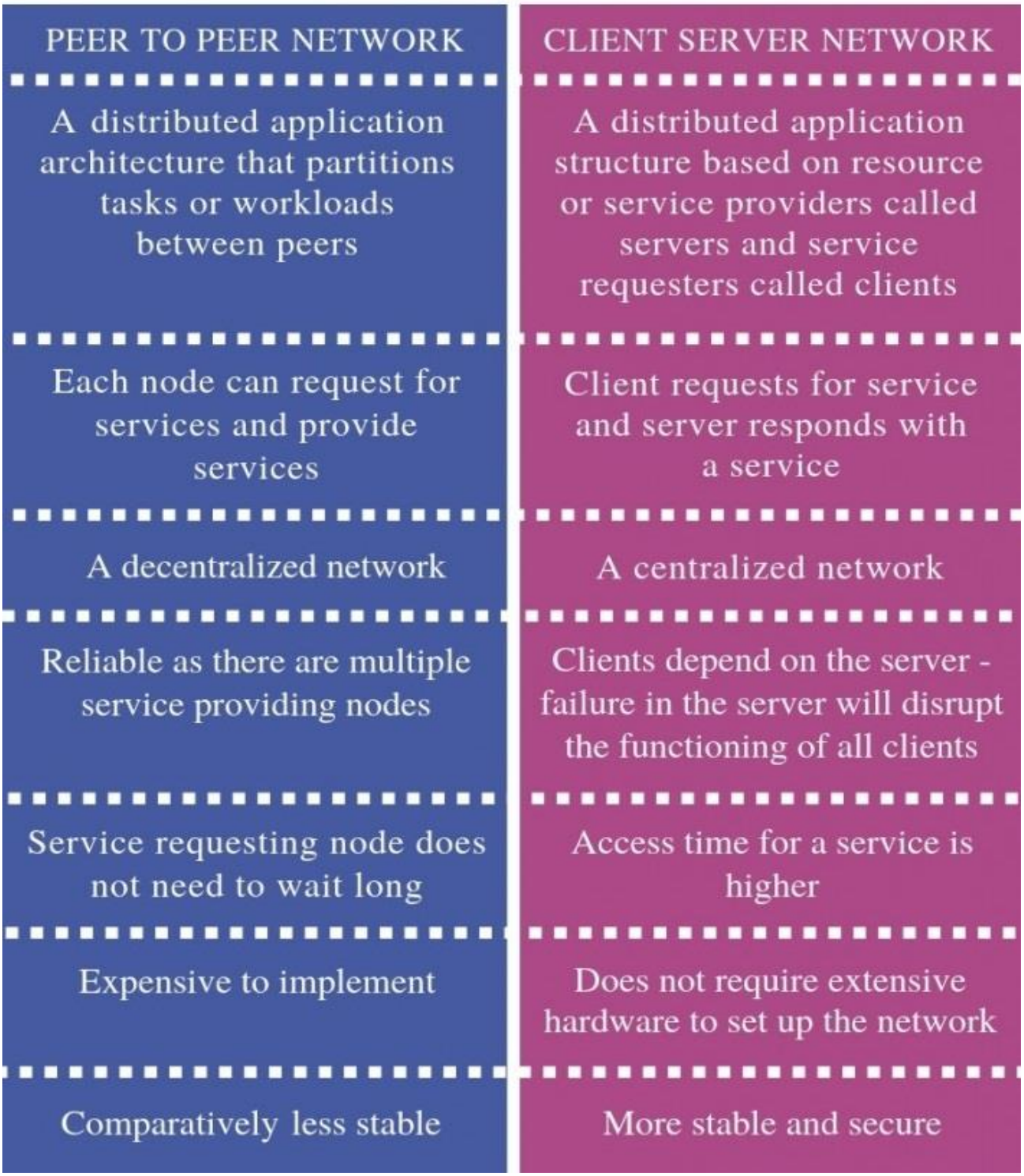
Following are the advantages of using a peer-to-peer network:

- Easy to implement and manage.
- Nodes or workstations are independent of one another. Also, no access permissions are needed.
- The network is reliable in nature. If a peer fails, it will not affect the working of others.
- There is no need for any professional software in such kind of networks.
- The cost of implementation of such networks is very less.

Following are the disadvantages of using a peer-to-peer network:

- Storage is decentralized, and also not so efficiently managed.
- No data backup options are available in peer-to-peer networks.
- These kinds of networks are not so secure.

Difference between Peer-To-Peer and Server Based Network



Network Topology

Topology defines the structure of the network of how all the components are interconnected to each other. It is the logical layout of the cables and devices that connect the nodes of the network. Network designers consider several factors when deciding which topology or combination of topologies to use: the type of computers and cabling (if any) in place, the distance between computers, the speed at which data must travel around the network, and the cost of setting up the network. Data moves though the network in a structure called packets. Packets are pieces of a message broken down into small units by the sending PC and reassembled by the receiving PC. A network's topology and related technologies are important for two reasons. First, a correctly designed network, using the most appropriate topology for the organization's needs, will move data packers as efficiently as possible. Second, the network's topology plays a role in preventing collisions, which is what happens when multiple nodes try to transmit data at the same time. Their packets can collide and destroy each other.

Types of Network Topology

The various network topologies are:

- Bus Topology
- Star Topology
- Tree Topology
- Ring Topology
- Mesh Topology
- Hybrid Topology

Bus Topology

The bus topology is designed in such a way that all the network device are connected through a single cable known as a backbone cable. Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable. The configuration of a bus topology is quite simpler as compared to other topologies. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Bus Topology:

- It is the easiest network topology for connecting peripherals or computers in a linear fashion.
- It works very efficient well when there is a small network.
- It is easy to connect or remove devices in this network without affecting any other device.
- Very cost-effective as compared to other network topology
- It is easy to understand topology.
- Easy to expand by joining the two cables together.

Disadvantages of Bus Topology:

- Bus topology is not great for large networks.
- Identification of problem becomes difficult if whole network goes down.
- Troubleshooting of individual device issues is very hard.
- Additional devices slow network down.
- Need of terminators are required at both ends of main cable.
- If a main cable is damaged, whole network fails or splits into two.
- Packet loss is high.
- This network topology is very slow as compared to other topologies.

Star Topology

A star may be a topology in which all nodes are individually connected to a central connection point, sort of a hub or a switch. A star takes more cable than e.g. a bus, but the benefit is that if a cable fails, just one node is going to be brought down. Each device within the network is connected to a central device called hub. If one device wants to send data to another device, it's to first send the info to hub then the hub transmits that data to the designated device.

Advantages of Star Topology

- It is very reliable – if one cable or device fails then all the others will still work
- It is high-performing as no data collisions can occur
- Robust in nature
- Easy fault detection because the link are often easily identified.
- No disruptions to the network when connecting or removing devices.
- Each device requires just one port i.e. to attach to the hub.

Disadvantages of Star Topology

- Requires more cable than a linear bus.
- If the connecting network device (network switch) fails, nodes attached are disabled and can't participate in network communication.
- More expensive than linear bus topology due to the value of the connecting devices (network switches)
- If hub goes down everything goes down, none of the devices can work without hub.
- Hub requires more resources and regular maintenance because it's the central system of star.
- Extra hardware is required (hubs or switches) which adds to cost

Tree Topology

In computer networks, a tree topology is also known as a star bus topology. It incorporates elements of both a bus topology and a star topology. The pattern of connection resembles a tree in which all branches spring from one root.

Advantages of Tree Topology:

- This topology provides a hierarchical as well as central data arrangement of the nodes.
- This is very flexible and also has better scalability.
- The other nodes in a network are not affected, if one of their nodes get damaged or not working.
- Nodes can be added by simply adding a hub
- Tree topology provides easy maintenance and easy fault identification can be done.

Disadvantages of Tree Topology:

- This network is very difficult to configure as compared to the other network topologies.
- Due to the presence of large number of nodes, the network performance of tree topology becomes a bit slowly.
- Requires large number of cables compared to star and ring topology.
- As the data needs to travel from the central cable this creates dense network traffic.
- The backbone appears as the failure point of the entire segment of the network.
- If the bulk of nodes are added in this network, then the maintenance will become complicated.

Ring Topology

Ring topology is like a bus topology, but with connected ends. The node that receives the message from the previous computer will retransmit to the next node. The data flows in one direction, i.e., it is unidirectional. The data flows in a single loop continuously known as an endless loop. It has no terminated ends, i.e., each node is connected to other node and having no termination point. The data in a ring topology flow in a clockwise direction.

Advantages of Ring Topology:

- In this data flows in one direction which reduces the chance of packet collisions.
- In this topology additional workstations can be added after without impacting performance of the network.
- Equal access to the resources.
- Speed to transfer the data is very high in this type of topology.
- Easy to manage.
- Ring network is extremely orderly organized.

Disadvantages of Ring Topology:

- It is Expensive.
- Difficult to troubleshoot the ring.
- In order for all the computer to communicate with each other, all computer must be turned on.
- Total dependence in on one cable.
- They were not scalable.

Mesh Topology

- Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
- There are multiple paths from one computer to another computer.
- It does not contain the switch, hub or any central computer which acts as a central point of communication.
- The Internet is an example of the mesh topology.

- Mesh topology can be formed by using the formula: **Number of cables = (n*(n-1))/2;** (Where n is the number of nodes that represents the network)

Advantages of Mesh Topology:

- Failure during a single device won't break the network.
- Fault identification is straightforward.
- This topology provides multiple paths to succeed in the destination and tons of redundancy.
- It provides high privacy and security.
- Data transmission is more consistent because failure doesn't disrupt its processes.
- Adding new devices won't disrupt data transmissions.
- This topology has robust features to beat any situation.

Disadvantages of Mesh Topology:

- It's costly as compared to the opposite network topologies
- Installation is extremely difficult in the mesh.
- Power requirement is higher as all the nodes will need to remain active all the time and share the load.
- Complex process.
- Maintenance needs are challenging with a mesh.

Hybrid Topology

- The combination of various different topologies is known as Hybrid topology.
- A Hybrid topology is a connection between different links and nodes to transfer the data.
- When two or more different topologies are combined together is termed as Hybrid topology and if similar topologies are connected with each other will not result in Hybrid topology. For example, if there exist a ring topology in one branch of ABC bank and bus topology in another branch of ABC bank, connecting these two topologies will result in Hybrid topology.

Advantages of Hybrid Topology:

- This type of topology combines the benefits of different types of topologies in one topology.
- Can be modified as per requirement.
- It is extremely flexible.
- It is very reliable.
- It is easily scalable
- Error detecting and trouble shooting is easy.
- It is used for create large network.

Disadvantages of Hybrid Topology:

- It is a type of expensive network.
- Design of a hybrid network is very complex.
- Requires a lot of cables in installation process.
- Installation is a difficult process.

Network Linking Devices

Repeater

A repeater is a network device that retransmits a received signal with more power and to an extended geographical or topological network boundary than the original signal could. A repeater is implemented in computer networks to expand the coverage area of the network, re-propagate a weak or broken signal, and/or service remote nodes. Repeaters amplify the received or input signal to a higher frequency domain so that it is reusable, scalable, and available.

Hub

A hub is a type of networking device that connects devices on a computer network together. The hub is used as a central connective device in the star topology. Computers are connected to each other through hubs. After receiving the signal delivered to the hub, it broadcasts it to all computers linked to it.

Switch

A network switch is a type of networking device that connects devices on a computer network together. The work of the switch and hub is almost the same. However, after receiving the signal sent to the hub, it sends the signal to all the computers at the same time. That is, it broadcasts the signal, but after receiving the signal sent to the switch, it only sends it to the target computer. This is why switches are called "intelligent devices."

Router

The router can be compared to a postman. The router must keep track of all network segment updates, just as the postman must identify all possible routes for delivering the recipient's paper. The router delivers data packets from the source computer to the destination computer. The router uses the shortest distance route to deliver the data packets to the destination. Routers are more expensive than other networking devices like hubs, bridges and switches.

Bridge

A bridge is a network device that connects multiple LANs (local area networks) together to form a larger LAN. The process of aggregating networks is called network bridging. A bridge connects the different components so that they appear as parts of a single network. The main function of this is to examine the incoming traffic and examine whether to filter it or forward it.

Network Protocols

A network protocol is an established set of rules that determine how data is transmitted between different devices in the same network. Essentially, it allows connected devices to communicate with each other, regardless of any differences in their internal processes, structure or design. Network protocols are the reason you can easily communicate with people all over the world, and thus play a critical role in modern digital communications. The common protocols are;

- OSI Model
- TCP/IP Model
- WWW

OSI Model

The OSI Model (Open Systems Interconnection Model) was published in 1984 by the International Organization for Standardization (ISO). It is a conceptual framework used to describe the functions of a networking system. The OSI model characterizes computing functions into a universal set of

rules and requirements in order to support interoperability between different products and software. In the OSI reference model, the communications between a computing systems are split into seven different abstraction layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.

1. Physical Layer

The physical layer is responsible for the physical cable or wireless connection between network nodes. It defines the connector, the electrical cable or wireless technology connecting the devices, and is responsible for transmission of the raw data, which is simply a series of 0s and 1s, while taking care of bit rate control.

2. Data Link Layer

The data link layer establishes and terminates a connection between two physically-connected nodes on a network. It breaks up packets into frames and sends them from source to destination. This layer is composed of two parts—Logical Link Control (LLC), which identifies network protocols, performs error checking and synchronizes frames, and Media Access Control (MAC) which uses MAC addresses to connect devices and define permissions to transmit and receive data.

3. Network Layer

The network layer has two main functions. One is breaking up segments into network packets, and reassembling the packets on the receiving end. The other is routing packets by discovering the best path across a physical network. The network layer uses network addresses (typically Internet Protocol addresses) to route packets to a destination node.

4. Transport Layer

The transport layer takes data transferred in the session layer and breaks it into “segments” on the transmitting end. It is responsible for reassembling the segments on the receiving end, turning it back into data that can be used by the session layer. The transport layer carries out flow control, sending data at a rate that matches the connection speed of the receiving device, and error control, checking if data was received incorrectly and if not, requesting it again.

5. Session Layer

The session layer creates communication channels, called sessions, between devices. It is responsible for opening sessions, ensuring they remain open and functional while data is being transferred, and closing them when communication ends. The session layer can also set checkpoints during a data transfer—if the session is interrupted, devices can resume data transfer from the last checkpoint.

6. Presentation Layer

The presentation layer prepares data for the application layer. It defines how two devices should encode, encrypt, and compress data so it is received correctly on the other end. The presentation layer takes any data transmitted by the application layer and prepares it for transmission over the session layer.

7. Application Layer

The application layer is used by end-user software such as web browsers and email clients. It provides protocols that allow software to send and receive information and present meaningful data to users. A few examples of application layer protocols are the Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Simple Mail Transfer Protocol (SMTP), and Domain Name System (DNS).

TCP/IP Model

TCP/IP, in full Transmission Control Protocol/Internet Protocol**,** standard Internet communications protocols that allow digital computers to communicate over long distances. The Internet is a packet-switched network, in which information is broken down into small packets, sent individually over many different routes at the same time, and then reassembled at the receiving end. TCP is the component that collects and reassembles the packets of data, while IP is responsible for making sure the packets are sent to the right destination. TCP/IP was developed in the 1970s and adopted as the protocol standard for ARPANET (the predecessor to the Internet) in 1983.

The four layers of the TCP/IP model are as follows:

1. **Network Interface Layer:**

This layer defines how data should be sent, handles the physical act of sending and receiving data, and is responsible for transmitting data between applications or devices on a network. This includes defining how data should be signaled by hardware and other transmission devices on a network, such as a computer's device driver, an Ethernet cable, a network interface card (NIC), or a wireless network. It is also referred to as the link layer, network access layer, network interface layer, or physical layer and is the combination of the physical and data link layers of the Open Systems Interconnection (OSI) model, which standardizes communications functions on computing and telecommunications systems.

2. **Internet Layer:**

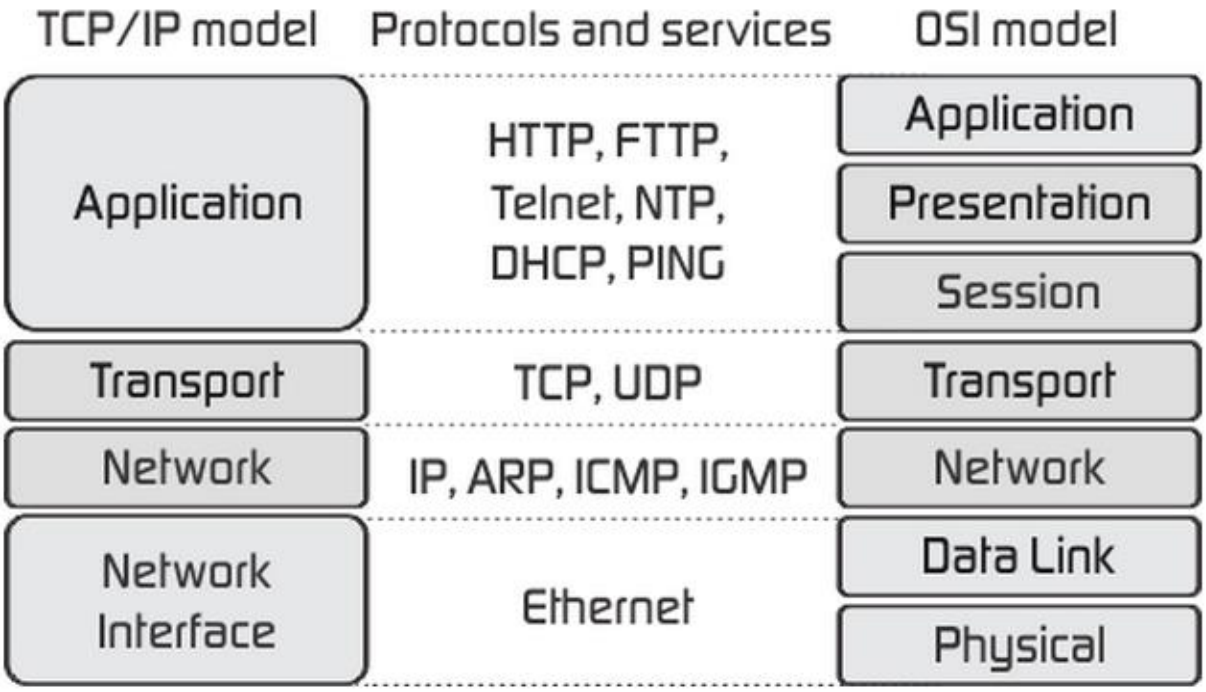
The internet layer is responsible for sending packets from a network and controlling their movement across a network to ensure they reach their destination. It provides the functions and procedures for transferring data sequences between applications and devices across networks.

3. **Transport Layer:**

The transport layer is responsible for providing a solid and reliable data connection between the original application or device and its intended destination. This is the level where data is divided into packets and numbered to create a sequence. The transport layer then determines how much data must be sent, where it should be sent to, and at what rate. It ensures that data packets are sent without errors and in sequence and obtains the acknowledgment that the destination device has received the data packets.

4. **Application Layer:**

The application layer refers to programs that need TCP/IP to help them communicate with each other. This is the level that users typically interact with, such as email systems and messaging platforms. It combines the session, presentation, and application layers of the OSI model.



Figure; OSI & TCP/IP Model

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable

TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.
Transport layer in TCP/IP does not provide assurance delivery of packets.	In OSI model, transport layer provides assurance delivery of packets.
TCP/IP model network layer only provides connection less services.	Connection less and connection oriented both services are provided by network layer in OSI model.
Protocols cannot be replaced easily in TCP/IP model.	While in OSI model, Protocols are better covered and is easy to replace with the change in technology.

World Wide Web (**WWW**)

The World Wide Web (WWW), commonly known as the Web, is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs, such as https://example.com/), which may be interlinked by hyperlinks, and are accessible over the Internet. The resources of the Web are transferred via the Hypertext Transfer Protocol (HTTP), may be accessed by users by a software application called a web browser, and are published by a software application called a web server. English scientist Tim Berners-Lee invented the World Wide Web in 1989.