Computer Network

Unit-1 Introduction to Computer Network and Network Model

1.1 What is Computer Network?
1.2 Application of Computer Networks
1.3 Transmission Mode, Network Structure
1.4 Network Topologies
1.5 ISO OSI Reference Models, TCP / IP Reference Model & their Comparison.

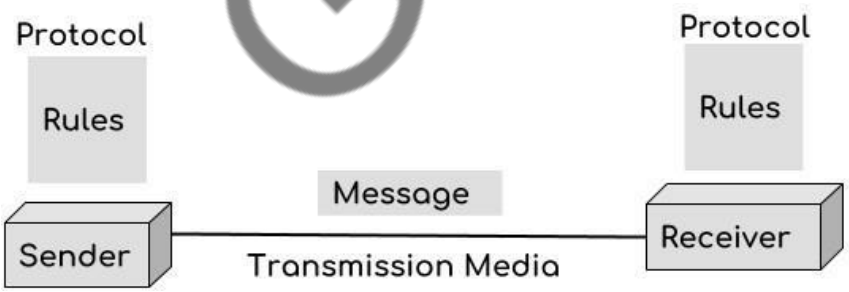
1.1 What is Computer Network?

A computer network is a collection of two or more computer systems that are linked together for transmitting and sharing information. A network connection can be established using either cable or wireless media.

A computer network is a group computing of devices (nodes) such as computers, printers, scanners, Fax machines etc. connected with each other through a transmission medium such as wires, cables etc. to send and receive data stored in other devices over the network.

A computer network is a system that connects two or more computing devices for transmitting and sharing information. Computing devices include everything from a mobile phone to a server. These devices are connected using physical wires such as fiber optics, but they can also be wireless.

There are **five basic components** of a computer network: Sender, Receiver, Transmission media, Message, Protocol.



Sender: The sender is the device that sends the data message to other device connected to the network. It can be a computer, workstation, telephone handset, video camera, and so on.

Receiver: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.

Transmission media: It is the physical path by which a message travels from sender to receiver. In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

GMP

Message: The message is the data or information to be communicated from one device to another device over a computer network. Popular forms of information include text, numbers, pictures, audio, and video.

Protocol: A protocol is a set of rules that govern data communications in both sender and receiver. Without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol. For example, http and https are the two protocols used by web browsers to get and post the data to internet; similarly SMTP protocol is used by email services connected to the internet.

Types of Computer Networks

Computer networks can be classified based on several criteria, such as the transmission medium, the network size, the topology, and organizational intent.

Based on a geographical scale, the different types of networks are:

1. **Nanoscale networks**: These networks enable communication between minuscule sensors and actuators.
2. **Personal area network (PAN)**: PAN refers to a network used by just one person to connect multiple devices, such as laptops to scanners, etc.
3. **Local area network (LAN)**: The local area network connects devices within a limited geographical area, such as schools, hospitals, or office buildings.
4. **Storage area network (SAN)**: SAN is a dedicated network that facilitates block-level data storage. This is used in storage devices such as disk arrays and tape libraries.
5. **Campus area network (CAN)**: Campus area networks are a collection of interconnected LANs. They are used by larger entities such as universities and governments.
6. **Metropolitan area network (MAN)**: MAN is a large computer network that spans across a city.
7. **Wide area network (WAN)**: Wide area networks cover larger areas such as large cities, states, and even countries.
8. **Enterprise private network (EPN):** An enterprise private network is a single network that a large organization uses to connect its multiple office locations.
9. **Virtual private network (VPN)**: VPN is an overlay private network stretched on top of a public network.
10. **Cloud network**: Technically, a cloud network is a WAN whose infrastructure is delivered via cloud services.

Based on organizational intent, networks can be classified as:

1. **Intranet**: Intranet is a set of networks that is maintained and controlled by a single entity. It is generally the most secure type of network, with access to authorized users alone. An intranet usually exists behind the router in a local area network.
2. **Internet**: The internet (or the internetwork) is a collection of multiple networks connected by routers and layered by networking software. This is a global system that connects governments, researchers, corporates, the public, and individual computer networks.
3. **Extranet**: An extranet is similar to the intranet but with connections to particular external networks. It is generally used to share resources with partners, customers, or remote employees.
4. **Darknet**: The Darknet is an overlay network that runs on the internet and can only be accessed by specialized software. It uses unique, customized communication protocols.

GMP

1.2 Application of Computer Networks

1. **Resource Sharing:**

Resource sharing is an application of a computer network. Resource sharing means you can share one Hardware and Software among multiple users. Hardware includes printers, Disks, Fax Machines, etc. Computing devices. And Software includes Atom, Oracle VM Virtual Box, Postman, Android Studio, etc.

2. **Information Sharing:**

Using a Computer network, we can share Information over the network, and it provides Search capabilities such as WWW. Over the network, single information can be shared among the many users over the internet.

3. **Communication:**

Communication includes email, calls, message broadcast, electronic funds transfer system etc.

4. **Entertainment Industry:**

In Entertainment industry also uses computer networks widely. Some of the Entertainment industries are Video on demand, Multiperson real-time simulation games, movie/TV programs, etc.

5. **Access to Remote Databases:**

Computer networks allow us to access the Remote Database of the various applications by the end- users. Some applications are Reservation for Hotels, Airplane Booking, Home Banking, Automated Newspaper, Automated Library etc.

6. **Home applications:**

There are many common uses of the computer network are as home applications. For example, you can consider user-to-user communication, access to remote instruction, electronic commerce and entertainment. Another way is managing bank accounts, transferring money to some other banks, paying bills electronically. A computer network arranges a robust connection mechanism between users.

7. **Business applications:**

The result of business application here is resource sharing. And the purpose of resource sharing is that without moving to the physical location of the resource, all the data, plans and tools can be shared to any network user. Most of the companies are doing business electronically with other companies and with other clients worldwide with the help of a computer network.

8. **Mobile users:**

The rapidly growing sectors in computer applications are mobile devices like notebook computers and PDAs (personal digital assistants). Here mobile users/device means portable device. The computer network is widely used in new-age technology like smartwatches, wearable devices, tablets, online transactions, purchasing or selling products online, etc.

9. **Social media:**

Social media is also a great example of a computer network application. It helps people to share and receive any information related to political, ethical and social issues.

GMP

Uses of Computer Network:

- It allows you to share resources such as printers, scanners, etc.
- You can share expensive software and database among network users.
- It facilitates communications from one computer to another computer.
- It allows the exchange of data and information among users through a network.

Features of computer network:

Performance: Performance of a computer network is measured in terms of response time. The response time of sending and receiving data from one node (computer in a computer network are often referred as node) to another should be minimal.

Data Sharing: One of the reason, why we use a computer network is to share the data between different systems connected with each other through a transmission media.

Backup: A computer network must have a central server that keeps the backup of all the data that is to be shared over a network so that in case of a failure it should be able to recover the data faster.

Software and hardware compatibility: A computer network must not limit all the computers in a computer network to use same software and hardware; instead it should allow the better compatibility between the different software and hardware configuration.

Reliability: There should not be any failure in the network or if it occurs the recovery from a failure should be fast.

Security: A computer network should be secure so that the data transmitting over a network should be safe from unauthorized access. Also, the sent data should be received as it is at the receiving node, which means there should not be any loss of data during transmission.

Scalability: A computer network should be scalable which means it should always allow adding new computers (or nodes) to the already existing computer network. For example, a company runs 100 computers over a computer network for their 100 employees, let's say they hire another 100 employees and want to add new 100 computers to the already existing LAN then in that case the local area computer network should allow this.

1.3 Transmission Mode, Network Structure

Transmission mode:

Transmission modes in computer networks are used to transfer data between the connected devices. In a network, devices can communicate with each other through transmission modes. Transmission modes are also called communication modes.

Transmission modes are categorized based on the direction of data flow and help optimise how devices communicate.

GMP

Importance of Transmission Modes

A transmission mode helps in:

- Efficiently managing data flow
- Optimizing network performance
- Ensuring compatible communication across devices
- Selecting the correct transmission mode based on the use case

Types of Transmission Modes

There are three types of transmission modes in computer networks as follows

- Simplex Communication Mode
- Half-duplex Communication Mode
- Full-duplex Communication Mode

Simplex Communication Mode

In simplex communication mode, the information is communicated in only one direction. There is only one transmitter and one receiver, hence the system is unidirectional.

The following are examples of simplex communication mode.

- A connection between a machine and a keyboard contains a simplex duplex transmission.
- A television advertisement is an example of simplex duplex transmission.
- A loudspeaker system is also a simplex transmission. A broadcaster communicates into a microphone, and his speech is transmitted by an amplifier and then to all the talkers.
- Radio Systems.

These devices can only transmit the data and cannot receive it.

The following diagram shows the simplex communication mode between two connected devices A and B.
As you can see in the following diagram, A is working as a sender and B as a receiver. Hence, the direction of data is from A to B.

Simplex Mode

Half-duplex Communication Mode

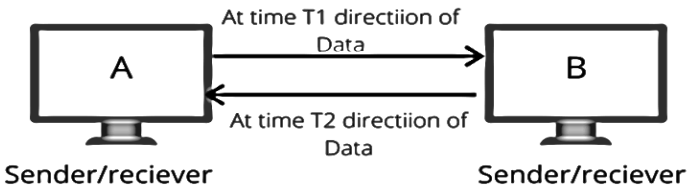
In half-duplex mode, the data flow is bidirectional, but not at the same time. It means both connected devices can transmit and receive data, but not simultaneously. At a time, the device can work either as a transmitter or receiver.

GMP

The examples are Transceiver and Walky talky set.

The following diagram shows a half-duplex mode between A And B. At a time T1, A works as a transmitter and B as a receiver. At time T2, A works as receiver and B as a transmitter.

Hence at time T1 data flows from A to B and at time T2 data flow from B to A.



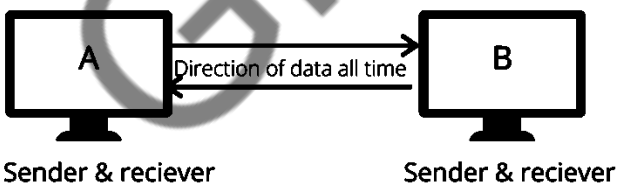
Half-duplex mode

Full duplex Communication Mode

In full-duplex mode, the data flow is bidirectional. It means both connected devices can transmit and receive data simultaneously. The devices can send or receive data at the same time.

An example of a full-duplex mode is the telephone system. When two persons interact through phone using a phone line, both can speak and listen together.

The following diagram shows full-duplex communication between A and B. A and B both work as sender or receiver. And data flow is also from both directions.



Full-duplex mode

Difference Between Simplex, Half duplex and Full duplex Communication

Parameters	Simplex	Half Duplex	Full Duplex
The direction of communication	Simplex mode is a uni-directional communication.	Half Duplex mode is a two-way directional communication but one at a time.	Full Duplex mode is a two-way directional communication simultaneously.

GMP

Parameters	Simplex	Half Duplex	Full Duplex
Sender and Receiver	In simplex mode, Sender can send the data but that sender can't receive the data.	In Half Duplex mode, Sender can send the data and also can receive the data but one at a time.	In Full Duplex mode, Sender can send the data and also can receive the data simultaneously.
Channel usage	Usage of one channel for the transmission of data.	Usage of one channel for the transmission of data.	Usage of two channels for the transmission of data.
Performance	The simplex mode provides less performance than half duplex and full duplex.	The Half Duplex mode provides less performance than full duplex.	Full Duplex provides better performance than simplex and half duplex mode.
Bandwidth Utilization	Simplex utilizes the maximum of a single bandwidth.	The Half-Duplex involves lesser utilization of single bandwidth at the time of transmission.	The Full-Duplex doubles the utilization of transmission bandwidth.
Suitable for	It is suitable for those transmissions when there is requirement of full bandwidth for delivering data.	It is suitable for those transmissions when there is requirement of sending data in both directions, but not at the same time.	It is suitable for those transmissions when there is requirement of sending and receiving data simultaneously in both directions.
Examples	Example of simplex mode are: Keyboard and monitor.	Example of half duplex mode is: Walkie-Talkies.	Example of full duplex mode is: Telephone.

GMP

Network Structure

A network structure is the logical arrangement of nodes and links in a computer network, defining how devices communicate and interact with each other. It establishes the topology, protocols, and rules for data transmission within the network.

A network structure is a logical and physical arrangement of nodes and links that make up a network. It defines how data is transmitted, shared, and processed within the network. The structure can vary greatly depending on the size, complexity, and purpose of the network.

A network structure typically consists of the following elements:

- **Nodes:** Devices that connect to the network and communicate with each other. These can include computers, servers, routers, switches, and other Networking equipment.
- **Links:** Physical or wireless connections that establish communication pathways between nodes. These can include cables, fiber optics, Wi-Fi, and cellular networks.
- **Topology:** The geometric arrangement of nodes and links that defines the overall shape of the network. Common topologies include bus, star, ring, and mesh.
- **Protocols:** Rules and standards that govern how data is transmitted, formatted, and processed within the network. These protocols ensure compatibility and interoperability between different devices and applications.

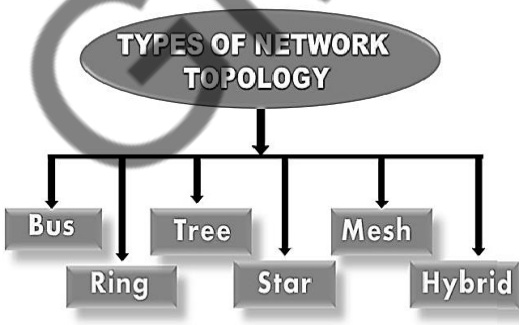
The network structure determines the performance, reliability, and scalability of the network. It influences factors such as data throughput, latency, fault tolerance, and network security.

1.4 Network Topologies

Network topology is the way devices are connected in a network. It defines how these components are connected and how data transfer between the networks.

The major categories of Network Topology are Physical Network topology and Logical Network Topology. Physical Network Topology refers to the actual structure of the physical medium for the transmission of data. Logical network Topology refers to the transmission of data between devices present in the network irrespective of the way devices are connected. The structure of the network is important for the proper functioning of the network. one must choose the most suitable topology as per their requirement.

Types of Network Topology



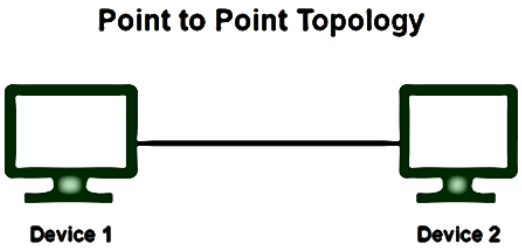
The various types of Network Topology are given below.

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

CMP

Point to Point Topology

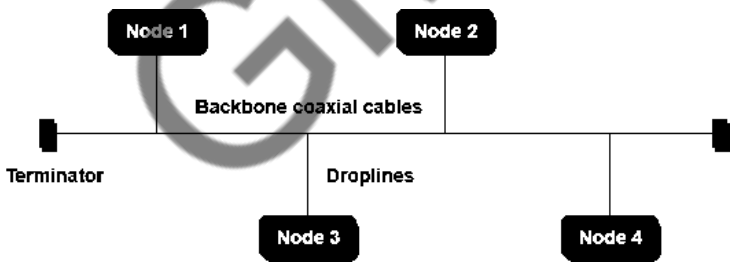
Point-to-point topology is a type of topology that works on the functionality of the sender and receiver. It is the simplest communication between two nodes, in which one is the sender and the other one is the receiver. Point-to-Point provides high bandwidth.



Point to Point Topology

Bus Topology

Bus Topology is a network type in which every computer and network device is connected to a single cable known as a backbone cable. It is bi-directional. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes. Each network device (node) is either connected to the backbone cable by drop cable or directly connected to the backbone cable. When a node wants to send a message over the network, it puts a message over the network. All the stations available in the network will receive the message whether it has been addressed or not. In Bus Topology, various MAC (Media Access Control) protocols are followed by LAN Ethernet connections like TDMA, Pure Aloha, CDMA, Slotted Aloha, etc.



Bus Topology

Advantages of Bus Topology

- If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, known as backbone cable, and N drop lines are required.
- Coaxial or twisted pair cables are mainly used in bus-based networks that support up to 10 Mbps.
- The cost of the cable is less compared to other topologies, but it is used to build small networks.
- Bus topology is familiar technology as installation and troubleshooting techniques are well known.
- CSMA is the most common method for this type of topology.

GMP

Disadvantages of Bus Topology

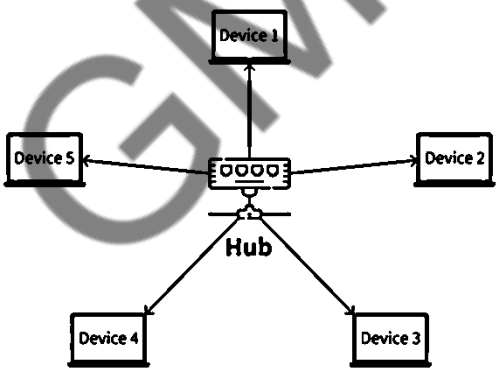
- A bus topology is quite simpler, but still, it requires a lot of cabling.
- If the common cable fails, then the whole system will crash down.
- If the network traffic is heavy, it increases collisions in the network. To avoid this, various protocols are used in the MAC layer known as Pure Aloha, Slotted Aloha, CSMA/CD, etc.
- Adding new devices to the network would slow down networks.
- Security is very low.

A common example of bus topology is the Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. This topology is also used in cable television networks.

Star Topology

Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer. This hub is the central node and all other nodes are connected to the central node. The central computer is known as a server and the peripheral devices are known as clients. 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.

GMP



Star Topology

Advantages of Star Topology

- If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
- Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
- It is Robust. If one link fails only that link will affect and not other than that.
- Easy to fault identification and fault isolation.
- Star topology is cost-effective as it uses inexpensive coaxial cable.

Disadvantages of Star Topology

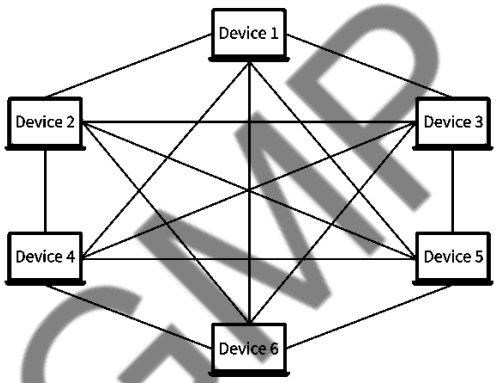
- If the concentrator (hub) on which the whole topology relies fails, the whole system will crash down.
- The cost of installation is high.
- Performance is based on the single concentrator i.e. hub.

A common example of star topology is a **local area network (LAN)** in an office where all computers are connected to a central hub. This topology is also used in wireless networks where all devices are connected to a wireless access point.

Mesh Topology

In a mesh topology, every device has a dedicated point-to-point link to every other device. The term dedicated means that the link carries traffic only between the two devices it connects.

In Mesh Topology, the protocols used are AHCP (Ad Hoc Configuration Protocols), DHCP (Dynamic Host Configuration Protocol), etc.



Mesh Topology

- Suppose, the N numbers of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).
- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is N C 2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

Disadvantages of Mesh Topology

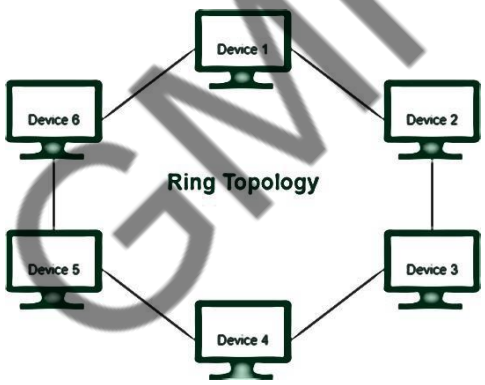
- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

Ring Topology

In a Ring Topology, it forms a ring connecting devices with exactly two neighbouring devices. Each device is linked to only its immediate neighbors (either physically or logically). 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. Hence to prevent data loss repeaters are used in the network.

The data flows in one direction, i.e. it is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology. In-Ring Topology, the Token Ring Passing protocol is used by the workstations to transmit the data.



Ring Topology

The most common access method of ring topology is token passing.

- **Token passing:** It is a network access method in which a token is passed from one node to another node.
- **Token:** It is a frame that circulates around the network.

Operations of Ring Topology

- One station is known as a **monitor** station which takes all the responsibility for performing the operations.
- To transmit the data, the station has to hold the token. After the transmission is done, the token is to be released for other stations to use.
- When no station is transmitting the data, then the token will circulate in the ring.

GMP

- There are two types of token release techniques: **Early token release** releases the token just after transmitting the data and **Delayed token release** releases the token after the acknowledgment is received from the receiver.

Advantages of Ring Topology

- The data transmission is high-speed.
- The possibility of collision is minimum in this type of topology.
- Cheap to install and expand.
- It is less costly than a star topology.

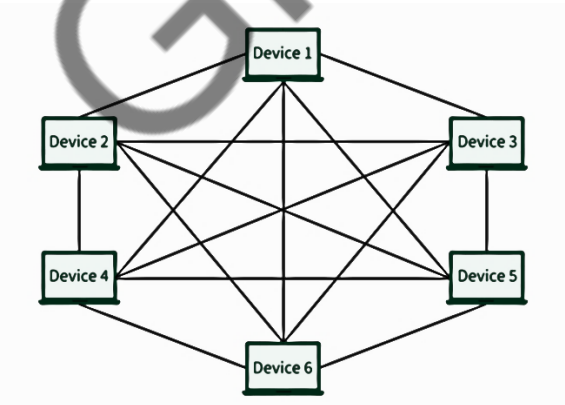
Disadvantages of Ring Topology

- The failure of a single node in the network can cause the entire network to fail.
- Troubleshooting is difficult in this topology.
- The addition of stations in between or the removal of stations can disturb the whole topology.
- Less secure.

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.

GMP



Mesh Topology

- Suppose, the N number of devices are connected with each other in a mesh topology, the total number of ports that are required by each device is N-1. In Figure 1, there are 5 devices connected to each other, hence the total number of ports required by each device is 4. The total number of ports required = N * (N-1).

- Suppose, N number of devices are connected with each other in a mesh topology, then the total number of dedicated links required to connect them is N C 2 i.e. N(N-1)/2. In Figure 1, there are 5 devices connected to each other, hence the total number of links required is 5*4/2 = 10.

Advantages of Mesh Topology

- Communication is very fast between the nodes.
- Mesh Topology is robust.
- The fault is diagnosed easily. Data is reliable because data is transferred among the devices through dedicated channels or links.
- Provides security and privacy.

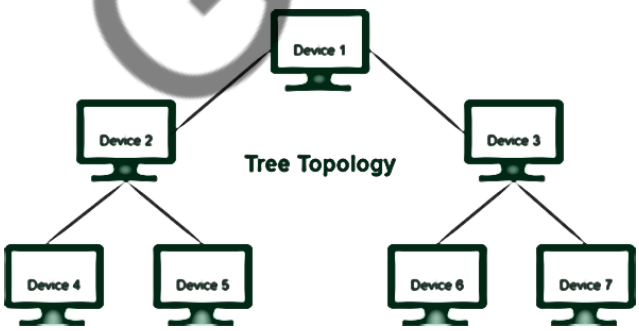
Disadvantages of Mesh Topology

- Installation and configuration are difficult.
- The cost of cables is high as bulk wiring is required, hence suitable for less number of devices.
- The cost of maintenance is high.

A common example of mesh topology is the internet backbone, where various internet service providers are connected to each other via dedicated channels. This topology is also used in military communication systems and aircraft navigation systems.

Tree Topology

Tree topology is the variation of the Star topology. This topology has a hierarchical flow of data. In Tree Topology, protocols like DHCP and **SAC (Standard Automatic Configuration)** are used.



Tree Topology

In tree topology, the various secondary hubs are connected to the central hub which contains the repeater. This data flow from top to bottom means from the central hub to the secondary and then to the devices or from bottom to top i.e. devices to the secondary hub and then to the central hub. It is a multi-point connection and a non-robust topology because if the backbone fails the topology crashes.

Advantages of Tree Topology

- It allows more devices to be attached to a single central hub thus it decreases the distance that is travelled by the signal to come to the devices.
- It allows the network to get isolated and also prioritize from different computers.

GMP

- We can add **new devices to the existing network.**
- **Error detection** and **error correction** are very easy in a tree topology.

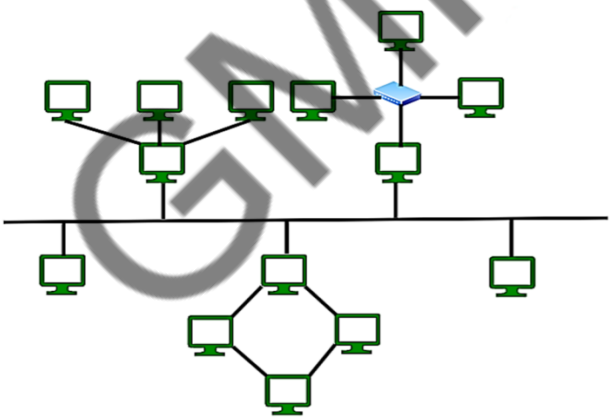
Disadvantages of Tree Topology

- If the central hub gets fails the entire system fails.
- The cost is high because of the cabling.
- If new devices are added, it becomes difficult to reconfigure.

A common example of a tree topology is the hierarchy in a large organization. At the top of the tree is the CEO, who is connected to the different departments or divisions (child nodes) of the company. Each department has its own hierarchy, with managers overseeing different teams (grandchild nodes). The team members (leaf nodes) are at the bottom of the hierarchy, connected to their respective managers and departments.

Hybrid Topology

Hybrid Topology is the combination of all the various types of topologies we have studied above. Hybrid Topology is used when the nodes are free to take any form. It means these can be individuals such as Ring or Star topology or can be a combination of various types of topologies seen above. Each individual topology uses the protocol that has been discussed earlier.



Hybrid Topology

The above figure shows the structure of the Hybrid topology. As seen it contains a combination of all different types of networks.

Advantages of Hybrid Topology

- This topology is **very flexible**.
- The size of the network can be easily expanded by **adding new devices.**

Disadvantages of Hybrid Topology

- It is challenging **to design the architecture** of the Hybrid Network.
- **Hubs** used in this topology are **very expensive.**

- The infrastructure cost is very high as a hybrid network **requires a lot of cabling and network devices**.

A common example of a hybrid topology is a university campus network. The network may have a backbone of a star topology, with each building connected to the backbone through a switch or router. Within each building, there may be a bus or ring topology connecting the different rooms and offices. The wireless access points also create a mesh topology for wireless devices. This hybrid topology allows for efficient communication between different buildings while providing flexibility and redundancy within each building.

1.5 ISO OSI Reference Models, TCP / IP Reference Model & their Comparison.

ISO OSI Reference Models

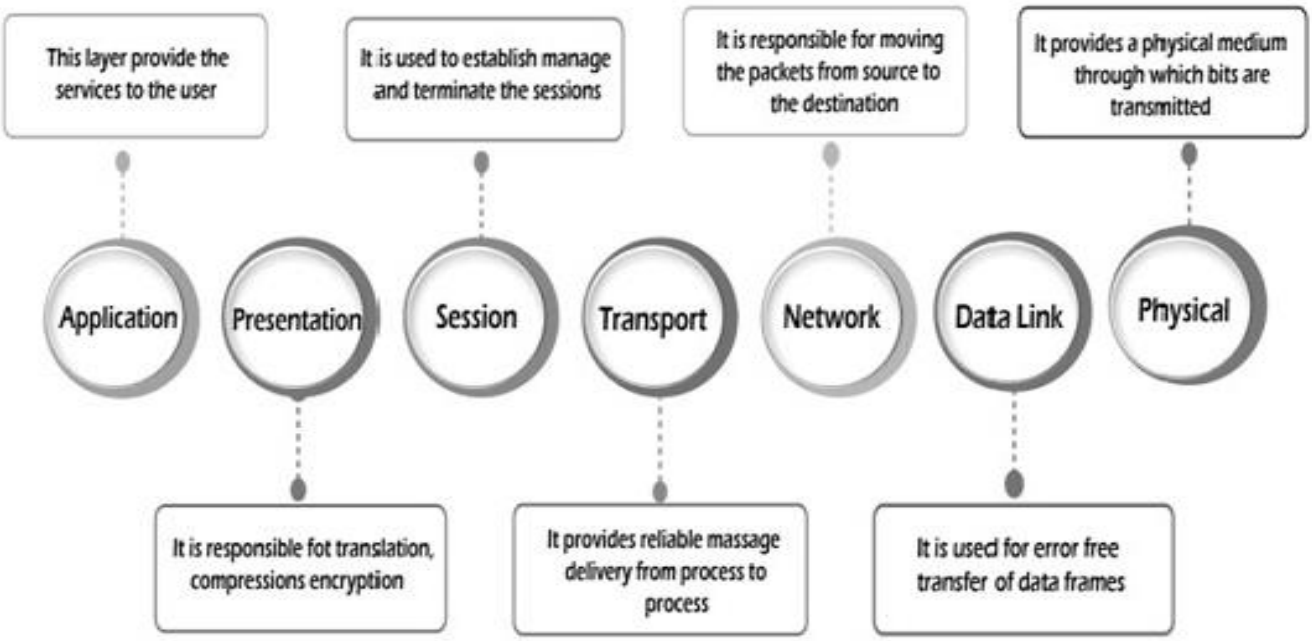
- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

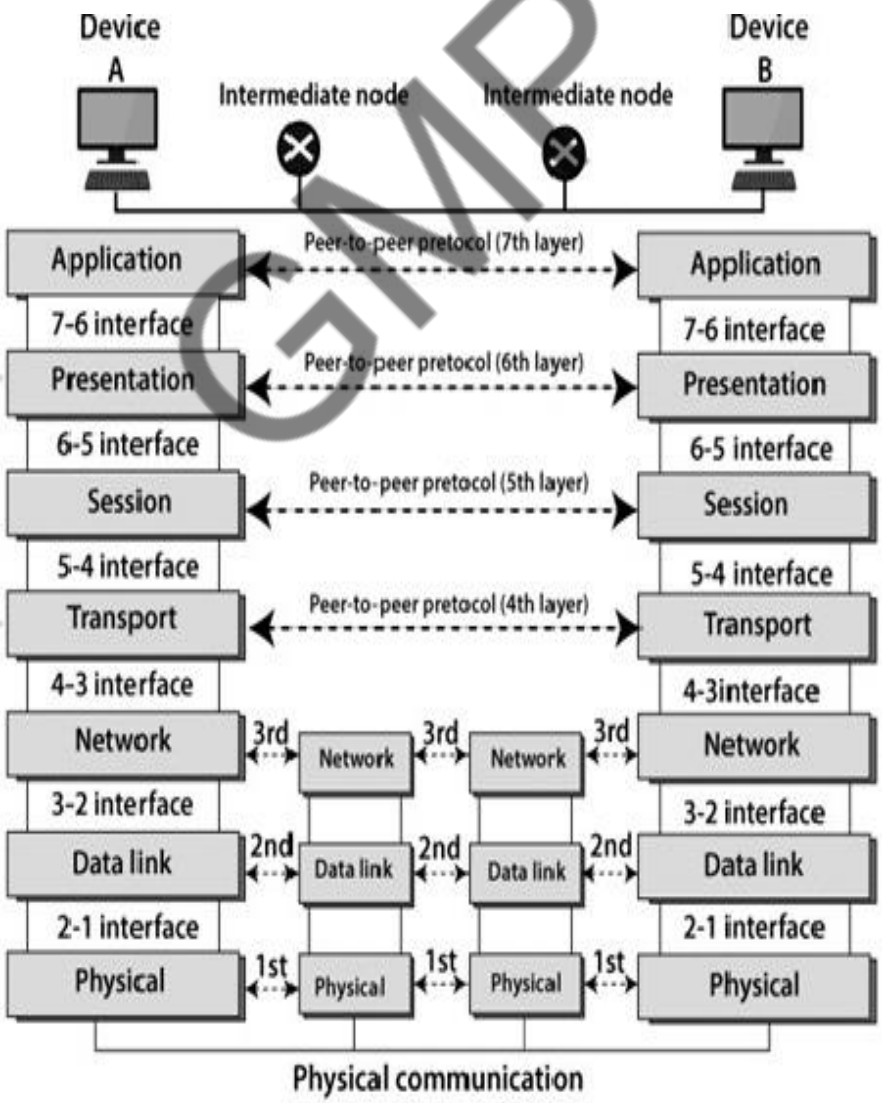
GMP

7 Layers of OSI Model:

There are the seven OSI layers. Each layer has different functions. Lists of seven layers are given below:

1. Physical Layer
2. Data-Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer


This layer provide the services to the user
It is used to establish manage and terminate the sessions
It is responsible for moving the packets from source to the destination
It provides a physical medium through which bits are transmitted
Application
Presentation
Session
Transport
Network
Data Link
Physical
It is responsible fot translation, compressions encryption
It provides reliable massage delivery from process to process
It is used for error free transfer of data frames


Device A
Intermediate node
Intermediate node
Device B
Application
Peer-to-peer pretocol (7th layer)
Application
7-6 interface
Presentation
Peer-to-peer pretocol (6th layer)
Presentation
6-5 interface
Session
Peer-to-peer pretocol (5th layer)
Session
5-4 interface
Transport
Peer-to-peer pretocol (4th layer)
Transport
4-3 interface
4-3interface
Network
3rd
Network
Network
Network
3-2 interface
Data link
2nd
Data link
Data link
Data link
2-1 interface
Physical
1st
Physical
Physical
Physical
Physical communication

GMP

1) Physical layer:

- ✓ The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- ✓ It is the lowest layer of the OSI model.
- ✓ It establishes, maintains and deactivates the physical connections.
- ✓ It determines the type of the signal used for transmitting the information connection.
- ✓ It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

Line Configuration: It defines the way how two or more devices can be connected physically.

Data Transmission: It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

Topology: It defines the way how network devices are arranged.

2) Data-Link Layer:

- ✓ This layer is responsible for the error-free transfer of data frames.
- ✓ It defines the format of the data on the network.
- ✓ It provides a reliable and efficient communication between two or more devices.
- ✓ It is mainly responsible for the unique identification of each device resides on a local network.
- ✓ It contains two sub-layers:
- ✓ **Logical Link Control Layer:**
  - o It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
  - o It identifies the address of the network layer protocol from the header.
  - o It also provides flow control.
- o **Media Access Control Layer:**
  - o A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - o It is used for transferring the packets over the network.

TCP / IP Reference Model

The TCP/IP Reference Model:

TCP/IP means Transmission Control Protocol and Internet Protocol It was developed by Department of Defense's (DoD) ARPA, later DARPA-Defense Advanced Research Projects Agency in the 1960s as a part of a research project of network interconnection to connect remote machines.

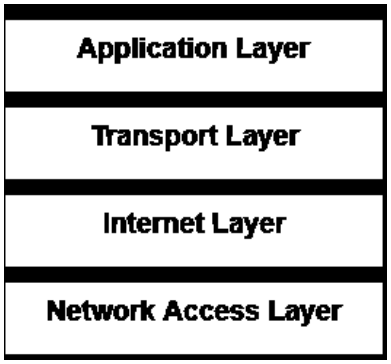
TCP/IP Reference Model is a four-layered suite of communication protocols. It is named after the two main protocols that are used in the model, namely, **TCP and IP**.

The TCP/IP model was developed prior to the OSI model.

The TCP/IP model is not exactly similar to the OSI model.

GMP

Diagram Representation of TCP/IP Model



The four layers in the TCP/IP protocol suite are −

1. **Network Access Layer/ Host-to- Network Layer** −It is the lowest layer deals with the physical transmission of data between devices and the local network. TCP/IP does not specifically define any protocol here but supports all the standard protocols. It includes protocols like Ethernet, Wi-Fi, and Bluetooth, which handle the physical connection, data framing, and media access control.

2. **Internet Layer** −It defines the protocols for logical transmission of data over the network. The Internet Layer is responsible for routing packets of data from one device to another across a network. It does this by assigning each device a unique IP address, which is used to identify the device and determine the route that packets should take to reach it.
   The main protocol in this layer is Internet Protocol (IP) and it is supported by the protocols ICMP, IGMP, RARP, and ARP.

   IP: IP stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions- IPv4 and IPv6. IPv4 is the one that most websites are using currently. But IPv6 is growing as the number of IPv4 addresses is limited in number when compared to the number of users.
   ICMP: ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
   ARP: ARP stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.

Following are the responsibilities of this protocol:

- **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
- **Host-to-host communication:** It determines the path through which the data is to be transmitted.
- **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely; it encapsulates the data into message known as IP datagram.
- **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is

GMP

greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.

- **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

3. **Transport Layer** − It is responsible for error-free end-to-end delivery of data. The TCP/IP transport layer protocols exchange data receipt acknowledgments and retransmit missing packets to ensure that packets arrive in order and without error. The transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).
   Transmission Control Protocol (TCP) provides reliable, connection-oriented communication with features like sequencing, error detection, and flow control.
   User Datagram Protocol (UDP) offers connectionless, unreliable communication suitable for real-time applications.

Functions of Transport layer-

- It decides if data transmission should be on parallel path or single path.
- Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.
- The applications can read and write to the transport layer.
- Transport layer adds header information to the data.
- Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
- Transport layer also arrange the packets to be sent, in sequence.

4. **Application Layer** − This is the topmost layer and defines the interface of host programs with the transport layer services. The Application Layer includes protocols and services that enable specific application functionalities.
   This layer includes all high-level protocols like Telnet, DNS, HTTP, FTP, SMTP, etc.
   HTTP is used for web browsing, **FTP** for file transfer, **SMTP** for email, **DNS** for domain name resolution, and **DHCP** for dynamic IP address assignment.

Features of Application Layer-

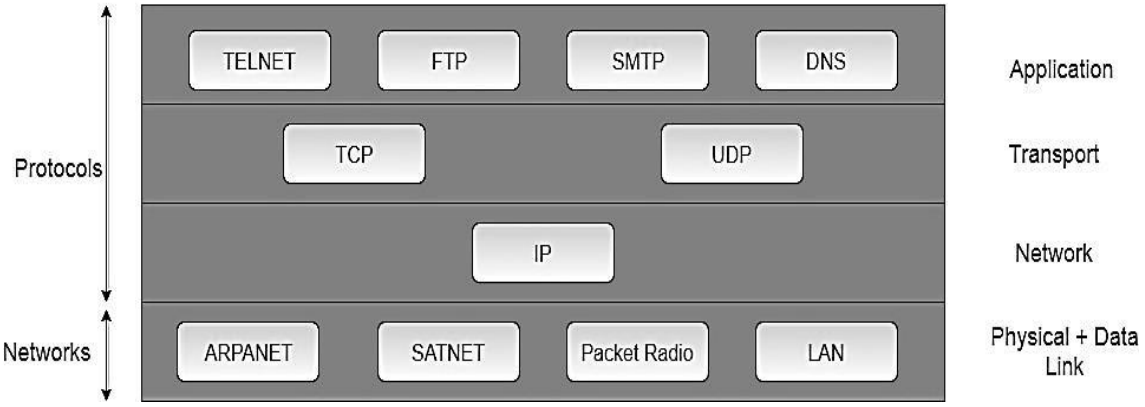
- The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.
- TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
- FTP (File Transfer Protocol) is a protocol, that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
- SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
- DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected

GMP

over a network.

- It allows peer entities to carry conversation.
- It defines two end-to-end protocols: TCP and UDP

Protocols and networks in the TCP/IP model:



The features of the TCP/IP reference model:

- Support for a flexible architecture.
- Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.
- The overall idea was to allow one application on one computer to talk to (send data packets) another application running on different computer.

GMP

Difference between TCP/IP and OSI Model

TCP/IP	OSI
TCP refers to Transmission Control Protocol.	OSI refers to Open Systems Interconnection.
TCP/IP uses both the session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP follows connectionless a horizontal approach.	OSI follows a vertical approach.
The Transport layer in TCP/IP does not provide assurance delivery of packets.	In the OSI model, the transport layer provides assurance delivery of packets.
Protocols cannot be replaced easily in TCP/IP model.	While in the OSI model, Protocols are better covered and are easy to replace with the technology change.

TCP/IP	OSI
TCP/IP model network layer only provides connectionless (IP) services. The transport layer (TCP) provides connections.	Connectionless and connection-oriented services are provided by the network layer in the OSI model.

GMP