**Computer Network**

* A computer network is a collection of computers or devices connected to share resources.
* Any device which can share or receive the data is called a Node.
* Through which the information or data propagate is known as channels, It can be guided or unguided.
* Computer Networking is the practice of connecting computers together to enable communication and data exchange between them.
* In general, Computer Network is a collection of two or more computers. It helps users to communicate more easily.

## **Working of Computer Network :**

* Basics building blocks of a Computer network are Nodes and Links.
* A Network Node can be illustrated as Equipment for Data Communication like a Modem, Router, etc., or Equipment of a Data Terminal like connecting two computers or more.
* Link in Computer Networks can be defined as wires or cables or free space of wireless networks.
* The working of Computer Networks can be simply defined as rules or protocols which help in sending and receiving data via the links which allow Computer networks to communicate.
* Each device has an IP Address, that helps in identifying a device.

## **Basic Terminologies of Computer Networks:**

**Network:**

A network is a collection of computers and devices that are connected together to enable communication and data exchange.

**Nodes:**

Nodes are devices that are connected to a network. These can include computers, Servers, Printers, [Routers,](https://www.geeksforgeeks.org/introduction-of-a-router/) [Switches](https://www.geeksforgeeks.org/types-of-switches-in-computer-network/), and other devices.

**Protocol:**

A protocol is a set of rules and standards that govern how data is transmitted over a network. Examples of protocols include [TCP/IP](https://www.geeksforgeeks.org/tcp-ip-model/), [HTTP](https://www.geeksforgeeks.org/http-full-form/), and [FTP](https://www.geeksforgeeks.org/file-transfer-protocol-ftp-in-application-layer/).

**Topology:**

Network topology refers to the physical and logical arrangement of nodes on a network. The common network topologies include bus, star, ring, mesh, and tree.

**Service Provider Networks:**

These types of Networks give permission to take Network Capacity and Functionality on lease from the Provider. Service Provider Networks include Wireless Communications, Data Carriers, etc.

**IP Address**:

An IP address is a unique numerical identifier that is assigned to every device on a network. IP addresses are used to identify devices and enable communication between them.

**DNS:**

The [Domain Name System (DNS)](https://www.geeksforgeeks.org/domain-name-system-dns-in-application-layer/) is a protocol that is used to translate human-readable domain names (such as www.google.com) into IP addresses that computers can understand.

**Firewall:**

A [firewall](https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/) is a security device that is used to monitor and control incoming and outgoing network traffic. Firewalls are used to protect networks from unauthorized access and other security threats.

## **Types of Enterprise** Networks

**LAN:**

A [Local Area Network (LAN)](https://www.geeksforgeeks.org/types-of-area-networks-lan-man-and-wan/)is a network that covers a small area, such as an office or a home. LANs are typically used to connect computers and other devices within a building or a campus.

**WAN:**

A [Wide Area Network (WAN)](https://www.geeksforgeeks.org/wan-full-form/) is a network that covers a large geographic area, such as a city, country, or even the entire world. WANs are used to connect LANs together and are typically used for long-distance communication.

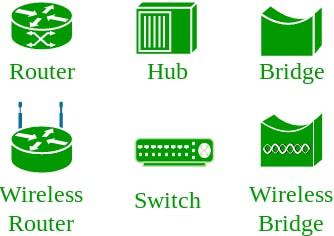
**Cloud Networks:**

[Cloud Networks](https://www.geeksforgeeks.org/cloud-networking/) can be visualized with a Wide Area Network (WAN) as they can be hosted on public or private cloud service providers and cloud networks are available if there is a demand. Cloud Networks consist of Virtual Routers, Firewalls, etc.

Networking is a vast and complex field, and there are many more concepts and technologies involved in building and maintaining networks.

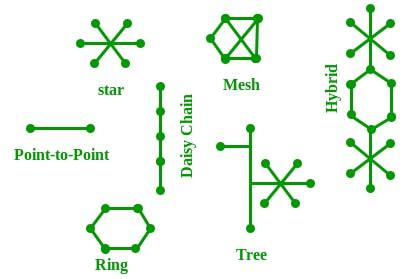
## **Network Devices**

* An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media.
* Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as [Network devices](https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/) and include things such as routers, switches, hubs, and bridges.



## **Network Topology**

The [Network Topology](https://www.geeksforgeeks.org/types-of-network-topology/) is the layout arrangement of the different devices in a network. Common examples include Bus, Star, Mesh, Ring, and Daisy chain.



### **OSI Model** ([Open Systems Interconnection](https://www.geeksforgeeks.org/layers-of-osi-model/))

* It is a reference model that specifies standards for communications protocols and also the functionalities of each layer.
* The OSI has been developed by the International Organization For Standardization and it is 7 layer architecture.
* Each layer of OSI has different functions and each layer has to follow different protocols.
* The 7 layers are as follows:
* [Physical Layer](https://www.geeksforgeeks.org/physical-layer-in-osi-model/) [Data link Layer](https://www.geeksforgeeks.org/data-link-layer/)
* [Network Layer](https://www.geeksforgeeks.org/network-layer-services-packetizing-routing-and-forwarding/) [Transport Layer](https://www.geeksforgeeks.org/transport-layer-responsibilities/)
* [Session Layer](https://www.geeksforgeeks.org/session-layer-in-osi-model/) [Presentation Layer](https://www.geeksforgeeks.org/presentation-layer-in-osi-model/)
* [Application Layer](https://www.geeksforgeeks.org/application-layer-in-osi-model/)

### **Protocol**

A protocol is a set of rules or algorithms which define the way how two entities can communicate across the network and there exists a different protocol defined at each layer of the OSI model.

A few such protocols are TCP, IP, UDP, ARP, DHCP, FTP, and so on.

**ARP(Address Resolution Protocol):**

* It is used to convert an IP address to its corresponding physical address(i.e., MAC Address).
* ARP is used by the Data Link Layer to identify the MAC address of the Receiver’s machine.

**RARP(Reverse Address Resolution Protocol):**

* As the name suggests, it provides the IP address of the device given a physical address as input.
* But RARP has become obsolete since the time DHCP has come into the picture.

**Network**:

A collection of interconnected devices, such as computers, printers, and servers, that can communicate with each other.

**Node:**

Any device connected to a network, such as a computer, printer, or router.

**Protocol:**

A set of rules and standards that define how devices on a network communicate with each other.

**IP Address:**

A unique numerical identifier assigned to each device on a network, used to identify and communicate with other devices.

**Router:**

A networking device that connects multiple networks together and forwards data packets between them.

**Switch:**

A networking device that connects devices on a network and forwards data packets between them.

**Firewall:**

A security device or software that monitors and controls incoming and outgoing network traffic, based on a set of predefined security rules.

**DNS (Domain Name System):**

A system that translates domain names (such as www.example.com) into IP addresses, allowing devices to locate and connect to websites and other network resources.

**LAN (Local Area Network):**

A network that connects devices within a limited geographical area, such as a home, office, or building.

**WAN (Wide Area Network):**

A network that connects devices over a large geographical area, such as multiple offices in different cities or countries.

**DHCP (Dynamic Host Configuration Protocol):**

A protocol that automatically assigns IP addresses and network configuration settings to devices on a network.

**TCP/IP (Transmission Control Protocol/Internet Protocol):**

A set of protocols used to communicate over the internet and other networks.

These are just a few basic networking terms, but understanding them is essential to building a strong foundation in computer networking.

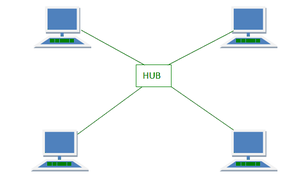
* **LANs (Local Area Networks)**
* **MANs (Metropolitan Area Networks)**
* **WANs (Wide Area Networks)**
* A host can act as a ***Client*** when he is requesting information.
* A host can act as a ***Server*** when he provides information.
* A host can also request and provide information, which is called ***Peer***.

# Physical Components of Computer Network

* It is a system that connects multiple independent computers in such a way that they can share information and resources.
* Some of the Physical Components of the Computer Network are mentioned below:

1. HUB Router Switch
2. **HUB:**

* It is a basically multi-port repeater.
* It connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
* Hubs cannot filter data, so data packets are sent to all connected devices.
* In other words, the collision domain of all hosts connected through Hub remains one.



1. **Router:**

* It is a device like a switch that routes data packets based on their IP addresses.
* It is mainly a Network Layer device.
* Routers normally connect LANs and WANs and have a dynamically updating routing table based on which they make decisions on routing the data packets.
* The router divides the broadcast domains of hosts connected through it.



1. **Switch:**

* It is a multiport bridge with a buffer and a design that can boost its efficiency(a large number of ports imply less traffic) and performance.
* It is a data link layer device.
* The switch can perform error checking before forwarding data, which makes it very efficient as it does not forward packets that have errors and forward good packets selectively to the correct port only.

**Media:**

* Also known as Link which is going to carry data from one side to another side.
* This link can be Wired Medium (Guided Medium) and Wireless Medium (Unguided Medium).
* It is of two types:

1. [Wired Media](https://www.geeksforgeeks.org/wired-communication-media/) [Wireless Media](https://www.geeksforgeeks.org/different-types-of-wireless-communication-media/)

**Ethernet:**

* Ethernet is the most widely used LAN technology, which is defined under IEEE standards 802.3.
* There are two types of Ethernet:

1. Ethernet **straight-through** cable (used for two different devices).
2. Ethernet **crossover cable** (used for two same devices).

# Network Topology

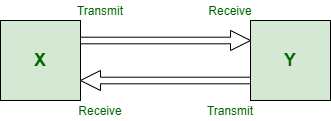
* In Computer Network ,there are various ways through which different components are connected to one another.
* **Network Topology** is the way that defines the structure, and how these components are connected to each other.
* The arrangement of a network that comprises nodes and connecting lines via sender and receiver is referred to as **Network Topology**.

The various network topologies are:

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

### **Point to Point Topology**

* It 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.



# Domain (Collision and Broadcast)

* The most common network devices used are routers and switches. But we still hear people talking about hubs, repeaters, and bridges.
* Do you ever wonder why these former devices are preferred over the latter ones? One reason could be: ‘because they are more efficient and powerful’.

**Collision Domain –**

* It is a scenario in which when a device sends out a message to the network, all other devices which are included in its collision domain have to pay attention to it, no matter if it was destined for them or not.
* This causes a problem because, in a situation where two devices send out their messages simultaneously, a collision will occur leading them to wait and re-transmit their respective messages, one at a time.
* Remember, It happens only in the case of a half-duplex mode.

#### **Advantages:**

**High Network Performance:**

* It helps to improve network performance by reducing collisions on the network, which can improve data transmission and reduce packet loss.

**Efficient Use of Network Resources:**

* It enables efficient use of network resources, such as bandwidth, by reducing the number of collisions and avoiding wastage of network resources.

**Better Network Security:**

* It can help to improve network security by reducing the risk of unauthorized access and network attacks, which can occur due to network congestion.

#### **Disadvantages**:

**Limited Scalability:**

* It may not be scalable in larger networks, as the number of devices connected to the network increases, which can lead to network congestion and performance degradation.

**Complex Network Management:**

* It can be complex to manage, requiring the use of protocols such as Carrier Sense Multiple Access with Collision Detection (CSMA/CD), which can be difficult to configure and maintain.

**Broadcast Domain –**

* It is a scenario in which when a device sends out a broadcast message, all the devices present in its broadcast domain have to pay attention to it.
* This creates a lot of congestion in the network, commonly called LAN congestion, which affects the bandwidth of the users present in that network.

#### **Advantages:**

**Efficient Network Communication:**

* It enables efficient network communication by allowing multiple devices to receive the same message simultaneously.

**Simplified Network Management:**

* It can simplify network management by allowing administrators to manage network devices and policies more easily.

**Improved Collaboration:**

* It can improve collaboration by enabling real-time communication and collaboration among network users.

#### **Disadvantages:**

**Increased Network Congestion:**

* It can lead to increased network congestion, particularly in larger networks, which can impact network performance and lead to packet loss.

**Reduced Network Security:**

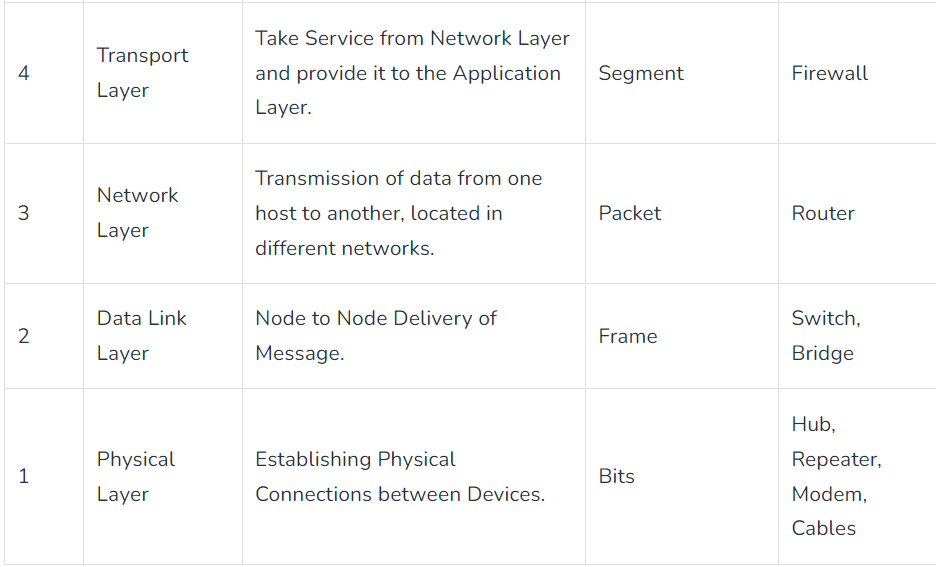
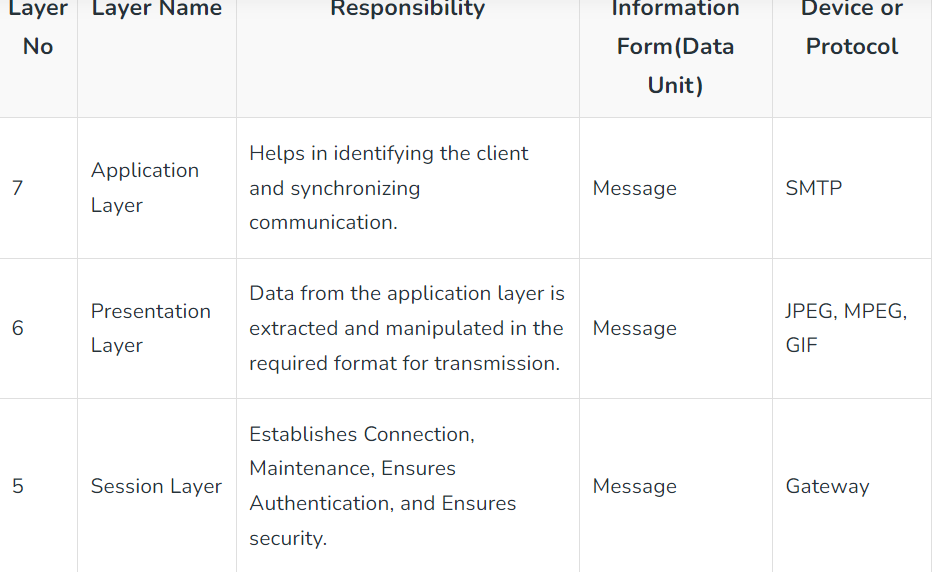
* It can reduce network security by increasing the risk of unauthorized access and network attacks, particularly in environments with a large number of devices.

The more the number of domains(collision and broadcast), the more efficient is the network providing better bandwidth to all its users.

**OSI model** acts as a reference model and is not implemented on the Internet because of its late invention.

The current model being used is the TCP/IP model.

Note:



## **Modes of Transmission Medium**

1. **Simplex mode:**

* In this mode, out of two devices, only one device can transmit the data, and the other device can only receive the data.

Example: Input from keyboards, monitors, TV broadcasting, Radio broadcasting, etc.

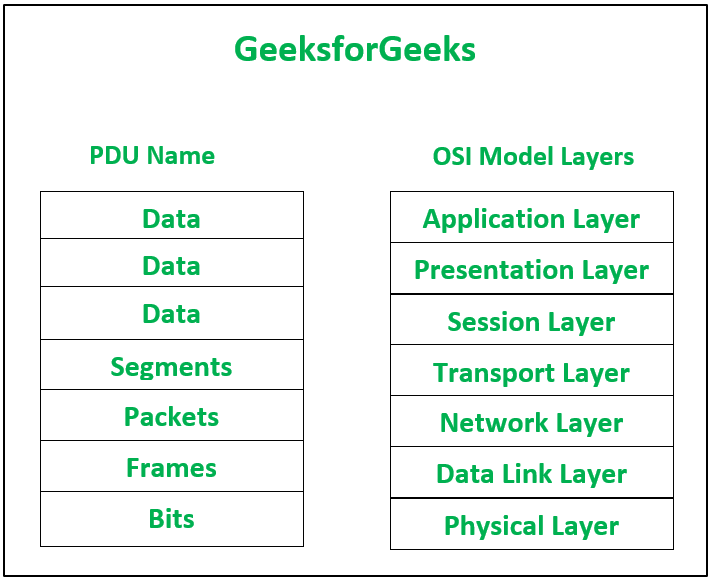
1. **Half Duplex mode:**

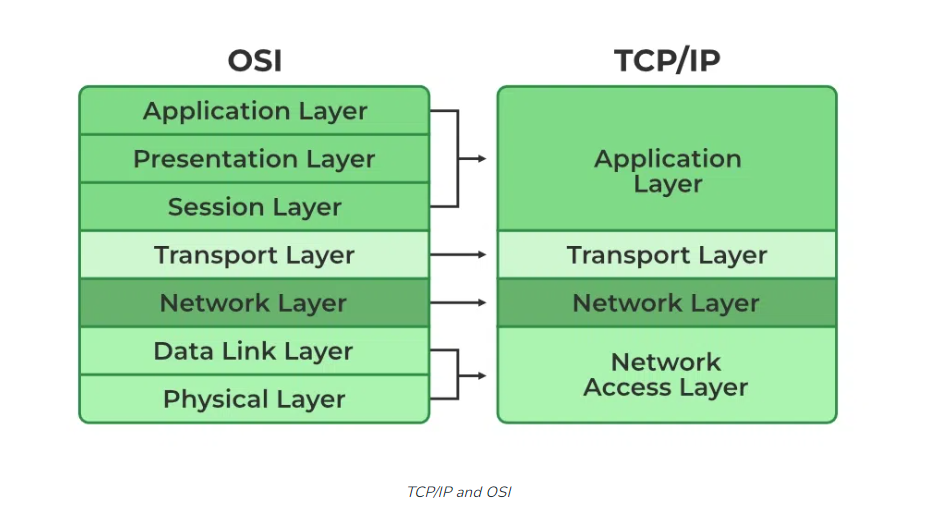
* In this mode, out of two devices, both devices can send and receive the data but only one at a time not simultaneously.

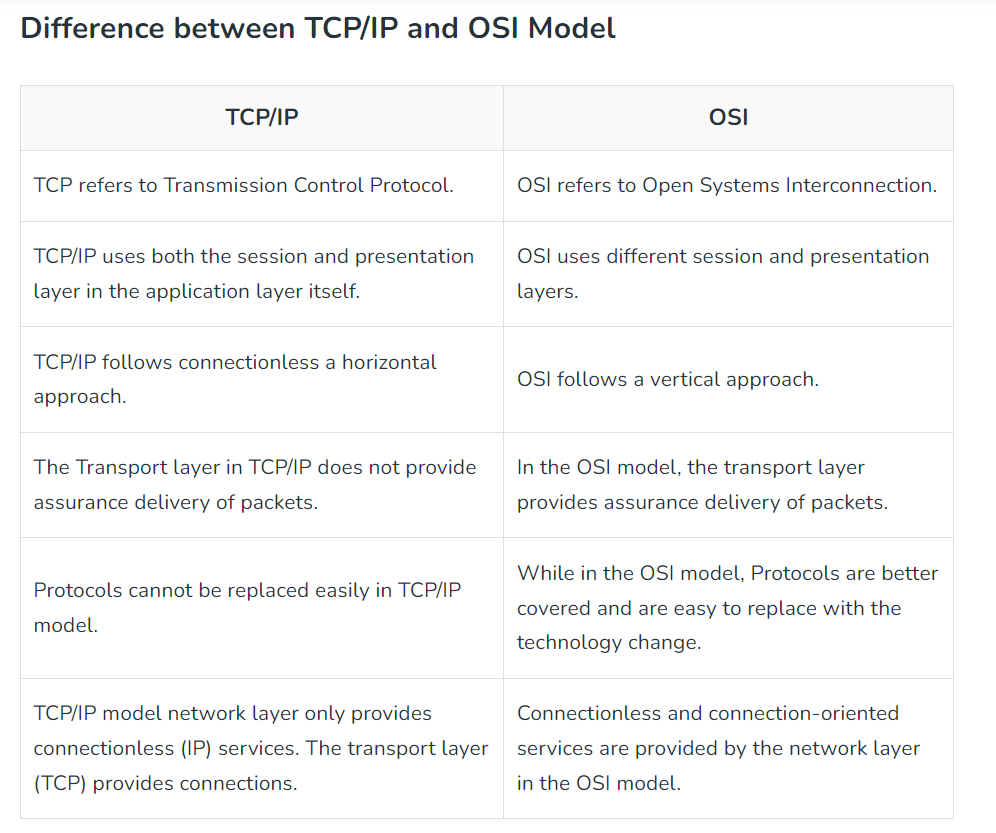
Examples- Walkie-Talkie, Railway Track, etc.

1. **Full-Duplex mode:**

* In this mode, both devices can send and receive the data simultaneously. Examples- Telephone Systems, Chatting applications, etc.







# Difference Between OSI Model and TCP/IP Model

* Data communication is a process or act in which we can send or receive data. For data communication two models are available:
* OSI Model TCP/IP Model

## **OSI Model**

* OSI stands for Open Systems Interconnection.
* It has 7 layers named Physical layer, Data Link layer, Network layer, Transport layer, Session layer, Presentation layer, and Application layer.
* Each layer performs its task independently.
* It was developed in 1984 by the International Organization for Standardization (ISO).

**Advantages**

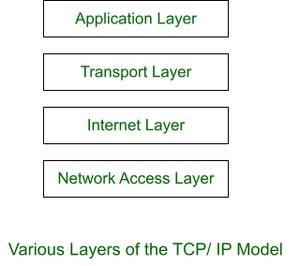
* Both services (connection-oriented and connectionless) are supported.
* It is quite flexible.
* All the layers work independently.

**Disadvantages**

* Setting up a model is a challenging task.
* Sometimes, it becomes difficult to fit a new protocol into this model.
* It is only used as a reference model.

## **TCP/IP Model**

* TCP/IP stands for Transmission Control Protocol/Internet Protocol.
* It has 4 layers named as Physical layer, Network layer, Transport layer, and Application layer.
* It also can be used as a communications protocol in a private computer network.
* It was designed by Vint Cerf and Bob Kahn in the 1970s.



**Advantages**

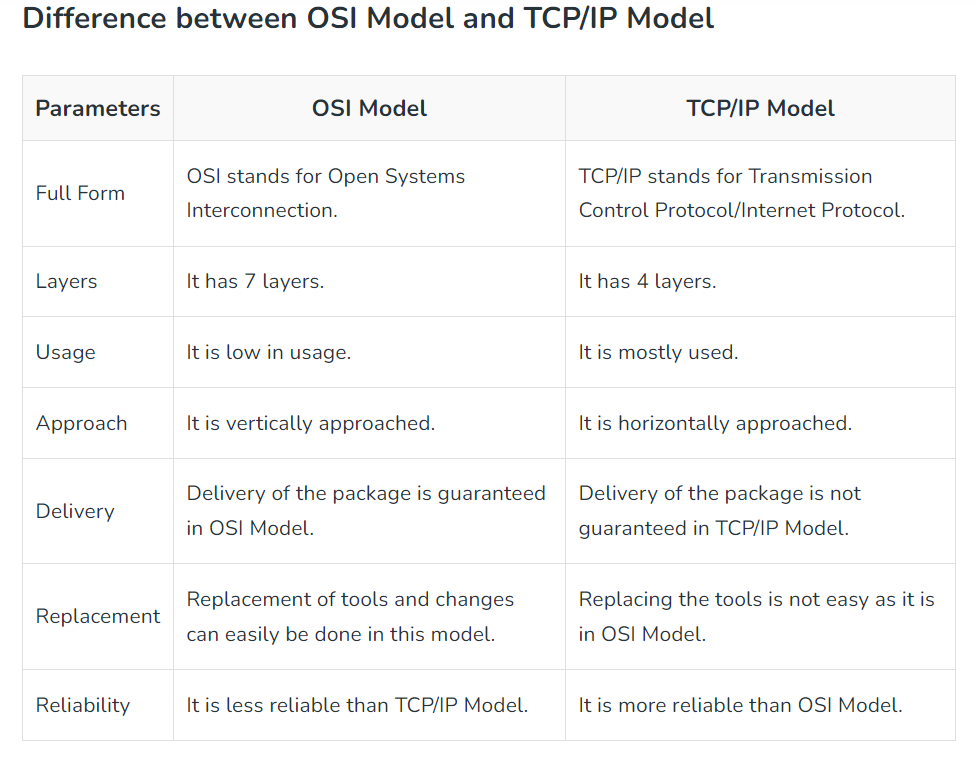
* Many Routing protocols are supported.
* It is highly scalable and uses a client-server architecture.
* It is lightweight.

**Disadvantages**

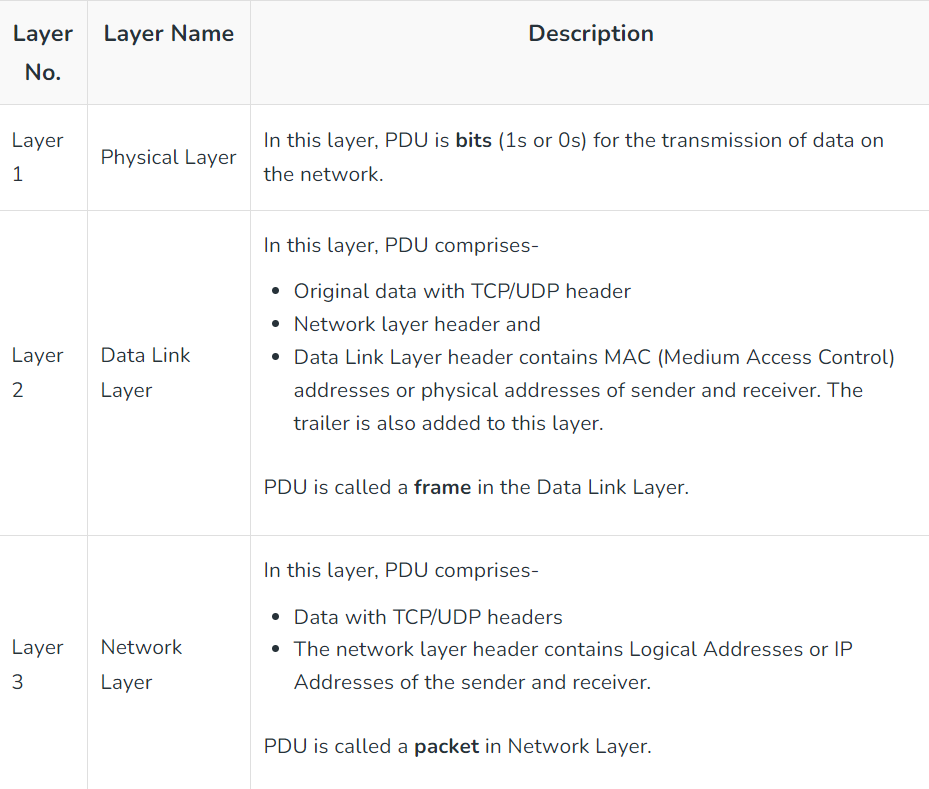
* Little difficult to set up.
* Delivery of packets is not guaranteed by the transport layer.
* Vulnerable to a synchronization attack.

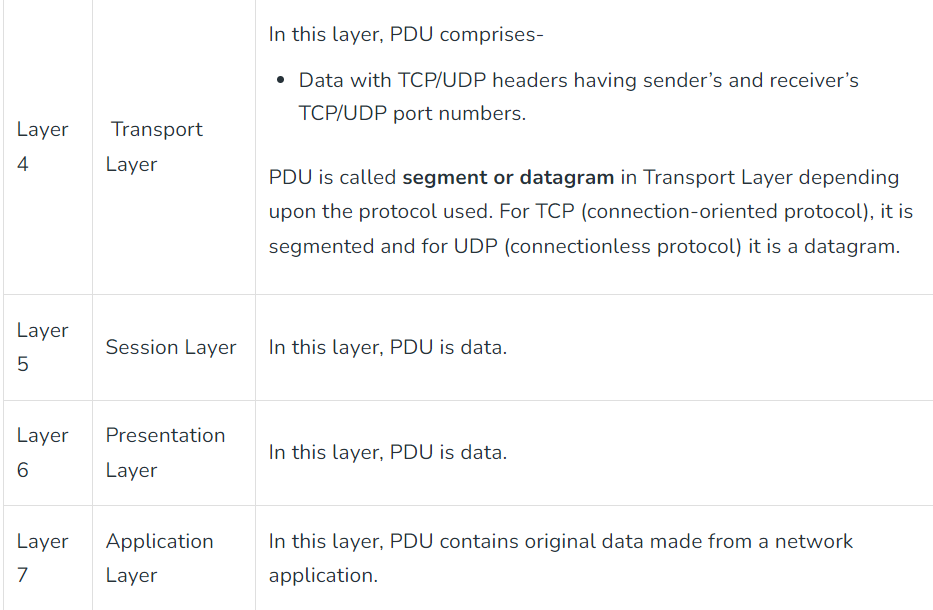
## **Similarities**

* OSI and TCP/IP both are logical models.
* They both describe how information is transmitted between two devices across a network.
* Both models define a set of layers.
* Each layer performs a specific set of functions to enable the transmission of data.
* Both use the concept of encapsulation, in which data is packaged into a series of headers and trailers that contain information about the data being transmitted and how it should be handled by the network.



### Protocol Data Unit (PDU)





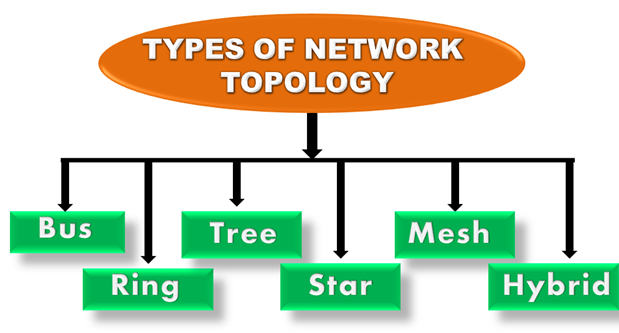
# What is Network Topology?

Topology defines the structure of the network of how all the components are interconnected to each other.

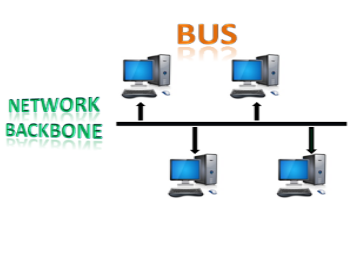
There are two types of topology: physical and logical topology.

## **Types of Network Topology**

* Physical topology is the geometric representation of all the nodes in a network.
* There are six types of network topology which are Bus Topology, Ring Topology, Tree Topology, Star Topology, Mesh Topology, and Hybrid Topology.



## **1) Bus Topology**



* It is designed in such a way that all the stations 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.
* 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.
* The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
* The configuration of a bus topology is quite simpler as compared to other topologies.
* The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
* The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).

### **Advantages:**

* **Low-cost cable:** In bus topology, nodes are directly connected to the cable without passing through a hub. Therefore, the initial cost of installation is low.
* **Moderate data speeds:** Coaxial or twisted pair cables are mainly used in bus-based networks that support upto 10 Mbps.
* **Familiar technology:** Bus topology is a familiar technology as the installation and troubleshooting techniques are well known, and hardware components are easily available.
* **Limited failure:** A failure in one node will not have any effect on other nodes.

### **Disadvantages:**

* **Extensive cabling:** A bus topology is quite simpler, but still it requires a lot of cabling.
* **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
* **Signal interference:** If two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Attenuation:** Attenuation is a loss of signal leads to communication issues. Repeaters are used to regenerate the signal.

## **2) 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.
* The most common access method of the ring topology is **token passing**.
  + **Token passing:** It is a network access method in which token is passed from one node to another node.
  + **Token:** It is a frame that circulates around the network.

### **Working of Token passing:**

* A token moves around the network, and it is passed from computer to computer until it reaches the destination.
* The sender modifies the token by putting the address along with the data.
* The data is passed from one device to another device until the destination address matches. Once the token received by the destination device, then it sends the acknowledgment to the sender.
* In a ring topology, a token is used as a carrier.

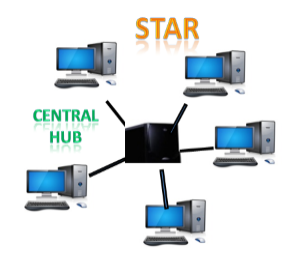
### **Advantages:**

* **Network Management:** Faulty devices can be removed from the network without bringing the network down.
* **Product availability:** Many hardware and software tools for network operation and monitoring are available.
* **Cost:** Twisted pair cabling is inexpensive and easily available. Therefore, the installation cost is very low.
* **Reliable:** It is a more reliable network because the communication system is not dependent on the single host computer.

### **Disadvantages:**

* **Difficult troubleshooting:** It requires specialized test equipment to determine the cable faults. If any fault occurs in the cable, then it would disrupt the communication for all the nodes.
* **Failure:** The breakdown in one station leads to the failure of the overall network.
* **Reconfiguration difficult:** Adding new devices to the network would slow down the network.
* **Delay:** Communication delay is directly proportional to the number of nodes. Adding new devices increases the communication delay.

## **3) Star Topology**



* It is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* The central computer is known as a **server**, and the peripheral devices attached to the server are known as **clients**.
* Coaxial cable or RJ-45 cables are used to connect the computers.
* Hubs or Switches are mainly used as connection devices in a **physical star topology**.
* Star topology is the most popular topology in network implementation.

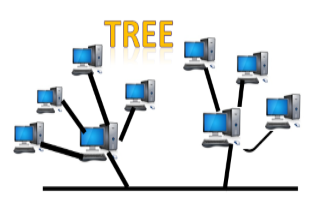
### **Advantages:**

* **Efficient troubleshooting:** Troubleshooting is quite efficient in a star topology as compared to bus topology. In a bus topology, the manager has to inspect the kilometers of cable. In a star topology, all the stations are connected to the centralized network. Therefore, the network administrator has to go to the single station to troubleshoot the problem.
* **Network control:** Complex network control features can be easily implemented in the star topology. Any changes made in the star topology are automatically accommodated.
* **Limited failure:** As each station is connected to the central hub with its own cable, therefore failure in one cable will not affect the entire network.
* **Familiar technology:** Star topology is a familiar technology as its tools are cost-effective.
* **Easily expandable:** It is easily expandable as new stations can be added to the open ports on the hub.
* **Cost effective:** Star topology networks are cost-effective as it uses inexpensive coaxial cable.
* **High data speeds:** It supports a bandwidth of approx 100Mbps. Ethernet 100BaseT is one of the most popular Star topology networks.

### **Disadvantages:**

* **A Central point of failure:** If the central hub or switch goes down, then all the connected nodes will not be able to communicate with each other.
* **Cable:** Sometimes cable routing becomes difficult when a significant amount of routing is required.

## **4) Tree topology**



* It combines the characteristics of bus topology and star topology.
* It is a type of structure in which all the computers are connected with each other in hierarchical fashion.
* The top-most node in tree topology is known as a root node, and all other nodes are the descendants of the root node.
* There is only one path exists between two nodes for the data transmission. Thus, it forms a parent-child hierarchy.

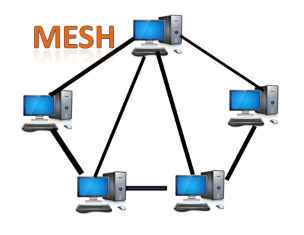
### **Advantages:**

* **Support for broadband transmission:** Tree topology is mainly used to provide broadband transmission, i.e., signals are sent over long distances without being attenuated.
* **Easily expandable:** We can add the new device to the existing network. Therefore, we can say that tree topology is easily expandable.
* **Easily manageable:** In tree topology, the whole network is divided into segments known as star networks which can be easily managed and maintained.
* **Error detection:** Error detection and error correction are very easy in a tree topology.
* **Limited failure:** The breakdown in one station does not affect the entire network.
* **Point-to-point wiring:** It has point-to-point wiring for individual segments.

### **Disadvantages:**

* **Difficult troubleshooting:** If any fault occurs in the node, then it becomes difficult to troubleshoot the problem.
* **High cost:** Devices required for broadband transmission are very costly.
* **Failure:** A tree topology mainly relies on main bus cable and failure in main bus cable will damage the overall network.
* **Reconfiguration difficult:** If new devices are added, then it becomes difficult to reconfigure.

## **5) Mesh topology**

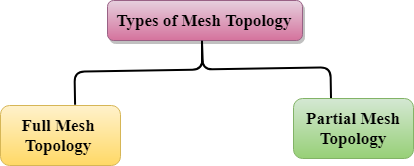


* It is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point of communication.
* The Internet is an example of the mesh topology.
* It is mainly used for WAN implementations where communication failures are a critical concern.
* Mesh topology is mainly used for wireless networks.
* 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.

**Mesh topology is divided into two categories:**

* Fully connected mesh topology
* Partially connected mesh topology



* **Full Mesh Topology:** In a full mesh topology, each computer is connected to all the computers available in the network.
* **Partial Mesh Topology:** In a partial mesh topology, not all but certain computers are connected to those computers with which they communicate frequently.

### **Advantages:**

**Reliable:** The mesh topology networks are very reliable as if any link breakdown will not affect the communication between connected computers.

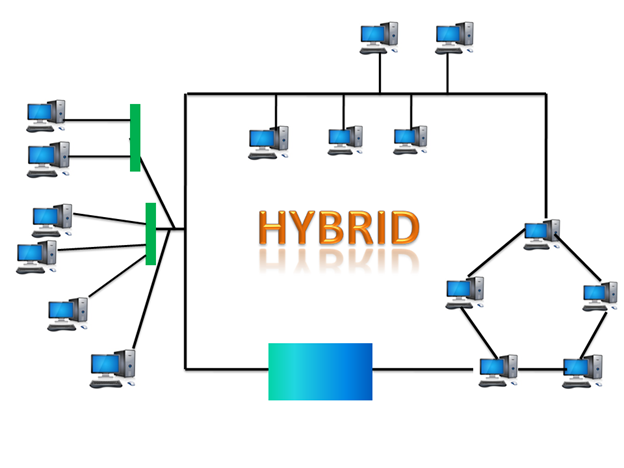
**Fast Communication:** Communication is very fast between the nodes.

**Easier Reconfiguration:** Adding new devices would not disrupt the communication between other devices.

### **Disadvantages:**

* **Cost:** A mesh topology contains a large number of connected devices such as a router and more transmission media than other topologies.
* **Management:** Mesh topology networks are very large and very difficult to maintain and manage. If the network is not monitored carefully, then the communication link failure goes undetected.
* **Efficiency:** In this topology, redundant connections are high that reduces the efficiency of the network.

## **6) 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.
* 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 ICICI bank and bus topology in another branch of ICICI bank, connecting these two topologies will result in Hybrid topology.

### **Advantages:**

* **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
* **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
* **Flexible:** This topology is very flexible as it can be designed according to the requirements of the organization.
* **Effective:** Hybrid topology is very effective as it can be designed in such a way that the strength of the network is maximized and weakness of the network is minimized.

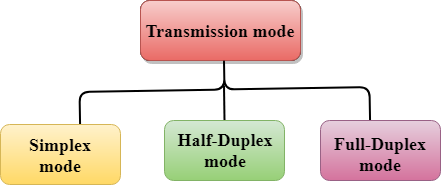
### **Disadvantages:**

* **Complex design:** The major drawback of the Hybrid topology is the design of the Hybrid network. It is very difficult to design the architecture of the Hybrid network.
* **Costly Hub:** The Hubs used in the Hybrid topology are very expensive as these hubs are different from usual Hubs used in other topologies.
* **Costly infrastructure:** The infrastructure cost is very high as a hybrid network requires a lot of cabling, network devices, etc.

# Transmission modes

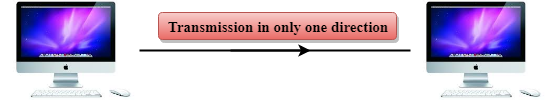
* The way in which data is transmitted from one device to another device is known as **transmission mode**.
* It is also known as the communication mode.
* Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission mode is also known as a directional mode.
* The transmission mode is defined in the physical layer.

The Transmission mode is divided into three categories:



* Simplex mode Half-duplex mode
* Full-duplex mode

## **Simplex mode**



* In Simplex mode, the communication is unidirectional, i.e., the data flow in one direction.
* A device can only send the data but cannot receive it or it can receive the data but cannot send the data.
* This transmission mode is not very popular as mainly communications require the two-way exchange of data.
* The simplex mode is used in the business field as in sales that do not require any corresponding reply.
* The radio station is a simplex channel as it transmits the signal to the listeners but never allows them to transmit back.
* Keyboard and Monitor are the examples of the simplex mode as a keyboard can only accept the data from the user and monitor can only be used to display the data on the screen.
* The main advantage of the simplex mode is that the full capacity of the communication channel can be utilized during transmission.

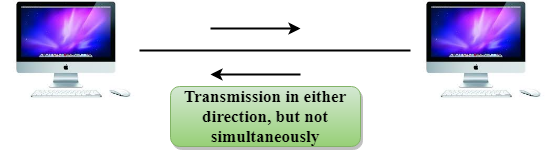
### **Advantages:**

* In simplex mode, the station can utilize the entire bandwidth of the communication channel, so that more data can be transmitted at a time.

### **Disadvantages:**

* Communication is unidirectional, so it has no inter-communication between devices.

## **Half-Duplex mode**



* In a Half-duplex channel, direction can be reversed, i.e., the station can transmit and receive the data as well.
* Messages flow in both the directions, but not at the same time.
* The entire bandwidth of the communication channel is utilized in one direction at a time.
* In half-duplex mode, it is possible to perform the error detection, and if any error occurs, then the receiver requests the sender to retransmit the data.
* A **Walkie-talkie** is an example of the Half-duplex mode.
* In Walkie-talkie, one party speaks, and another party listens. After a pause, the other speaks and first party listens.
* Speaking simultaneously will create the distorted sound which cannot be understood.

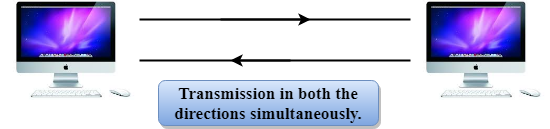
### **Advantages:**

* In half-duplex mode, both the devices can send and receive the data and also can utilize the entire bandwidth of the communication channel during the transmission of data.

### **Disadvantages:**

* In half-duplex mode, when one device is sending the data, then another has to wait, this causes the delay in sending the data at the right time.

## **Full-duplex mode**



* In Full duplex mode, the communication is bi-directional, i.e., the data flow in both the directions.
* Both the stations can send and receive the message simultaneously.
* Full-duplex mode has two simplex channels.
* One channel has traffic moving in one direction, and another channel has traffic flowing in the opposite direction.
* The Full-duplex mode is the fastest mode of communication between devices.
* The most common example of the full-duplex mode is a telephone network.
* When two people are communicating with each other by a telephone line, both can talk and listen at the same time.

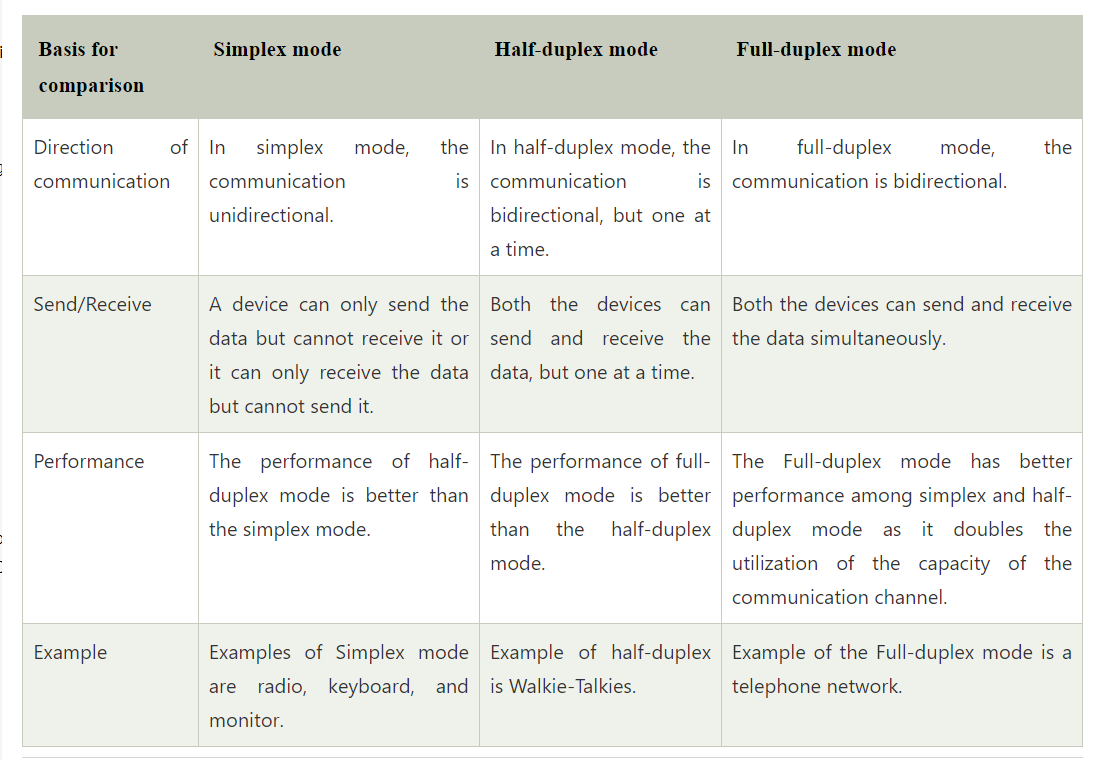
### **Advantages:**

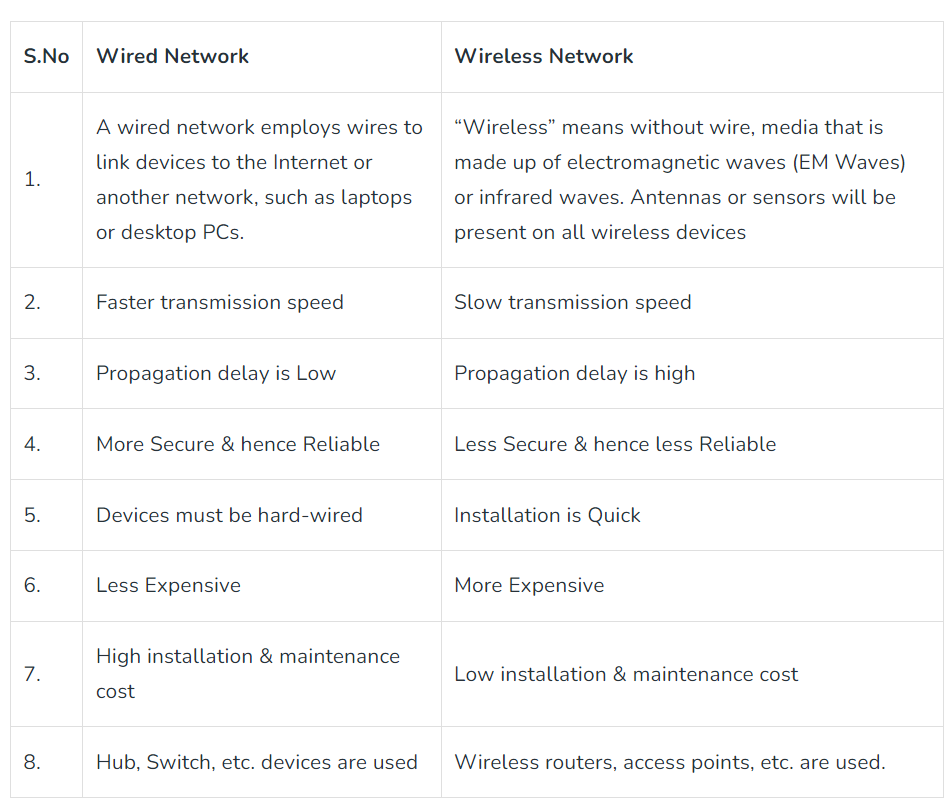
* Both the stations can send and receive the data at the same time.

### **Disadvantages:**

* If there is no dedicated path exists between the devices, then the capacity of the communication channel is divided into two parts.

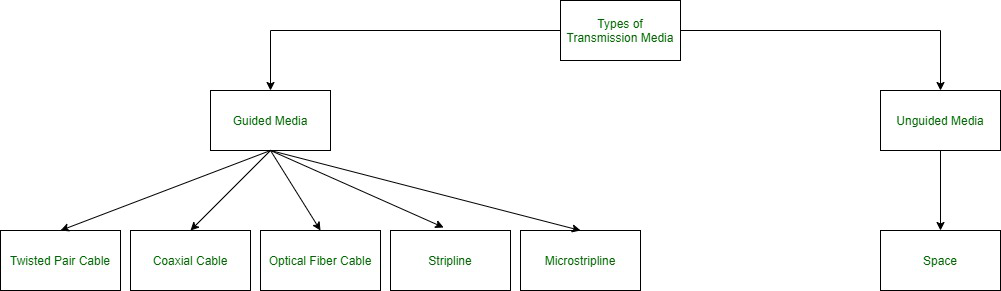
**Differences b/w Simplex, Half-duplex and Full-duplex mode**





# Transmission Media

* In data communication terminology, a transmission medium is a physical path between the transmitter and the receiver i.e. it is the channel through which data is sent from one place to another.
* Transmission Media is broadly classified into the following types:



**Guided Media:**

* It is also referred to as Wired or Bounded transmission media.
* Signals being transmitted are directed and confined in a narrow pathway by using physical links.

Features:

* High Speed
* Secure
* Used for comparatively shorter distances

Major types of Guided Media:

1. **Twisted Pair Cable –**   
   It consists of 2 separately insulated conductor wires wound about each other. Generally, several such pairs are bundled together in a protective sheath. They are the most widely used Transmission Media.

Types:

**Unshielded Twisted Pair (UTP):**

* UTP consists of two insulated copper wires twisted around one another.
* This type of cable has the ability to block interference and does not depend on a physical shield for this purpose.
* It is used for telephonic applications.



**Advantages:**

Least expensive Easy to install High-speed capacity

**Disadvantages:**

⇢ Susceptible to external interference

⇢ Lower capacity and performance in comparison to STP

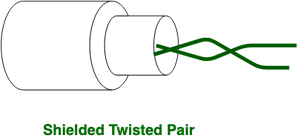
⇢ Short distance transmission due to attenuation

**Applications:**

Used in telephone connections and LAN networks.

**Shielded Twisted Pair (STP):**

* This type of cable consists of a special jacket (a copper braid covering or a foil shield) to block external interference.
* It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.



**Advantages:**

* Better performance at a higher data rate in comparison to UTP
* Eliminates crosstalk Comparatively faster

**Disadvantages:**

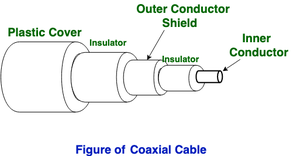
* Comparatively difficult to install and manufacture
* More expensive Bulky

**Applications:**

* It is most frequently used in extremely cold climates, where the additional layer of outer covering makes it perfect for withstanding such temperatures or for shielding the interior components.

1. **Coaxial Cable –**

* It has an outer plastic covering containing an insulation layer made of PVC or Teflon and 2 parallel conductors each having a separate insulated protection cover.
* The coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth). Broadband mode(cable bandwidth is split into separate ranges).
* Cable TVs and analog television networks widely use Coaxial cables.



**Advantages:**

* High Bandwidth Better noise Immunity
* Easy to install and expand Inexpensive

**Disadvantages:**

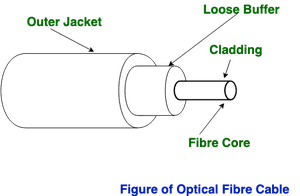
* Single cable failure can disrupt the entire network

**Applications:**

* Radio frequency signals are sent over coaxial wire.
* It can be used for cable television signal distribution, digital audio (S/PDIF), computer network connections (like Ethernet), and feedlines that connect radio transmitters and receivers to their antennas.

1. **Optical Fiber Cable –**

* It uses the concept of refraction of light through a core made up of glass or plastic.
* The core is surrounded by a less dense glass or plastic covering called the cladding.
* It is used for the transmission of large volumes of data.
* The cable can be unidirectional or bidirectional.
* The WDM (Wavelength Division Multiplexer) supports two modes, namely unidirectional and bidirectional mode.



**Advantages:**

* Increased capacity and bandwidth Lightweight
* Less signal attenuation
* Immunity to electromagnetic interference
* Resistance to corrosive materials

**Disadvantages:**

* Difficult to install and maintain
* High cost Fragile

**Applications:**

* Medical Purpose: Used in several types of medical instruments.
* Defence Purpose: Used in transmission of data in aerospace.
* For Communication: This is largely used in formation of internet cables.
* Industrial Purpose: Used for lighting purposes and safety measures in designing the interior and exterior of automobiles.

**Unguided Media:**

* It is also referred to as Wireless or Unbounded transmission media.
* No physical medium is required for the transmission of electromagnetic signals.

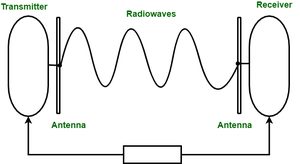
**Features:**

* The signal is broadcasted through air
* Less Secure Used for larger distances

Types unguided media:

1. **Radio waves –**

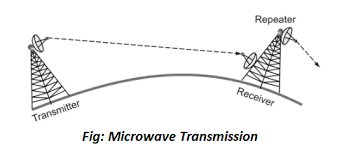
* These are easy to generate and can penetrate through buildings.
* The sending and receiving antennas need not be aligned.
* Frequency Range:3KHz – 1GHz.
* AM and FM radios and cordless phones use Radio waves for transmission.



Further Categorized as (i) Terrestrial and (ii) Satellite.

1. **Microwaves:**

* It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other.
* The distance covered by the signal is directly proportional to the height of the antenna.
* Frequency Range:1GHz – 300GHz.
* These are majorly used for mobile phone communication and television distribution.



1. **Infrared:**

* Infrared waves are used for very short distance communication.
* They cannot penetrate through obstacles.
* This prevents interference between systems.
* Frequency Range:300GHz – 400THz.
* It is used in TV remotes, wireless mouse, keyboard, printer ,Telivision , wifi etc.

# Computer Network Components

Depending on the type of network that we need to install, some network components can also be removed. For example, the wireless network does not require a cable.

## **Hub**

* It is a hardware device that divides the network connection among multiple devices.
* When computer requests for some information from a network, it first sends the request to the Hub through cable.
* Hub will broadcast this request to the entire network.
* All the devices will check whether the request belongs to them or not.
* If not, the request will be dropped.

The process used by the Hub consumes more bandwidth and limits the amount of communication. Nowadays, the use of hub is obsolete, and it is replaced by more advanced computer network components such as Switches, Routers.

## **Switch**

* It is a hardware device that connects multiple devices on a computer network.
* It contains more advanced features than Hub.
* It contains the updated table that decides where the data is transmitted or not.
* It delivers the message to the correct destination based on the physical address present in the incoming message.
* It does not broadcast the message to the entire network like the Hub.
* It determines the device to whom the message is to be transmitted.
* It provides a direct connection between the source and destination.
* It increases the speed of the network.

## **Router**

* It is a hardware device which is used to connect a LAN with an internet connection.
* It is used to receive, analyze and forward the incoming packets to another network.
* It works in a **Layer 3 (Network layer)** of the OSI Reference model.
* It forwards the packet based on the information available in the routing table.
* It determines the best path from the available paths for the transmission of the packet.

### **Advantages Of Router:**

# Multiple Access Protocols in Computer Network

The Data Link Layer is responsible for transmission of data between two nodes. Its main functions are-

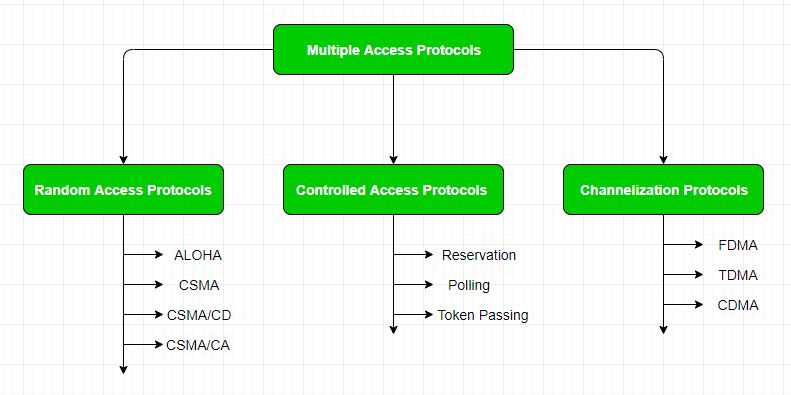
* Data Link Control
* Multiple Access Control



**Data Link control –**   
The data link control is responsible for reliable transmission of message over transmission channel by using techniques like framing, error control and flow control. For Data link control refer to – [Stop and Wait ARQ](https://www.geeksforgeeks.org/stop-and-wait-arq/)

**Multiple Access Control –**   
If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created( data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as – 



**1. Random Access Protocol:** In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium’s state( idle or busy). It has two features:

1. There is no fixed time for sending data
2. There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

**(a) ALOHA –** It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

* **Pure Aloha:**   
  When a station sends data it waits for an acknowledgement. If the acknowledgement doesn’t come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

Vulnerable Time = 2\* Frame transmission time

Throughput = G exp{-2\*G}

Maximum throughput = 0.184 for G=0.5

* **Slotted Aloha:**   
  It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

Vulnerable Time = Frame transmission time

Throughput = G exp{-\*G}

Maximum throughput = 0.368 for G=1

For more information on ALOHA refer – [LAN Technologies](https://www.geeksforgeeks.org/local-area-network-lan-technologies/)

**(b) CSMA –** Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.

CSMA access modes-

* **1-persistent:**The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
* **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
* **P-persistent:**The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
* **O-persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

**(c) CSMA/CD –**Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected.

# Efficiency

**Carrier sense multiple access with collision detection (CSMA/CD) –** The CSMA method does not tell us what to do in case there is a collision. Carrier sense multiple access with collision detection (CSMA/CD) adds to the CSMA algorithm to deal with the collision. In CSMA/CD, the size of a frame must be large enough so that collision can be detected by the sender while sending the frame. So, the frame transmission delay must be at least *two times* the maximum propagation delay. Assume some station transmitted data packet and successfully get to the destination but it is just the *Best Case*, so we have to take the *Worst Case* scenario in which there will be contention slots. Contention slots are those slots that are not able to transmit their journey due to the collision. Suppose station A transmitted data but collide and the worst-case time wasted is **2Tp** and then some station B found out a way to transmit the data so it took (As shown in Figure)

Tp ( propagation delay) + Tt(transmission time)

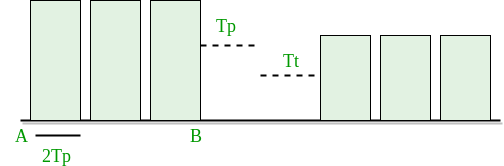
Now we don’t know how many contention slots, so we consider the worst-case to be of **n** contention slots.

Efficiency = Tt / ( C\*2\*Tp + Tt + Tp)

Tt - transmission time

Tp - propagation time

C - number of collision



In CSMA/CD, for success, only 1 station should transmit while others shouldn’t. Let p be the probability to transmit data successfully.

P(success) = nC1 \* p \* (1-p)n-1 (by using Binomial distribution)

For max P(success), differentiate with respect to p and equate to zero (to get maxima and minima).

We get P(max) = 1/e

Number of times we need to try before getting 1st success

1/P(MAX) = 1/(1/e) = e

Here number of times we need to try (C) = e. Put a = Tt/Tp and divide by T in Efficiency = Tt / (C\* 2 \* Tp + Tt + Tp) We get,

Efficiency = 1/(e\*2a + 1 + a)

a = Tp/Tt

e = 2.72

Now

**Efficiency** = 1/( 1 + 6.44a)

**Further Analysis of Efficiency :**

Efficiency = 1/ (1 + 6.44a)

= 1/ {1 + 6.44(Tp/Tt)}

= 1/ {1 + 6.44((distance/speed)/(packet length/Bandwidth))}

= 1/ {1+ 6.44 ((distance \* bandwidth)/ (speed\*packet length))}

From this derivation, we can conclude many relations :

* If distance increases, the efficiency of CSMA decreases.
* CSMA is not suitable for long-distance networks like WAN but works optimally for LAN.
* If the length of the packet is bigger, the efficiency of CSMA also increases; but the maximum limit for length is 1500 Bytes.
* Transmission Time >= 2\*Propagation Time

**(d) CSMA/CA –**Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA avoids collision by:

1. **Interframe space –** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
2. **Contention Window –** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
3. **Acknowledgement –** The sender re-transmits the data if acknowledgement is not received before time-out.

**2. Controlled Access:**   
In this, the data is sent by that station which is approved by all other stations. For further details refer – [Controlled Access Protocols](https://www.geeksforgeeks.org/computer-network-controlled-access-protocols/)

**3. Channelization:**   
In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

* **Frequency Division Multiple Access (FDMA) –**The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
* **Time Division Multiple Access (TDMA) –**In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.   
  For more details refer – [Circuit Switching](https://www.geeksforgeeks.org/computer-network-circuit-switching/)
* **Code Division Multiple Access (CDMA) –**One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.

### Features of multiple access protocols:

**Contention-based access:** Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.

**Carrier Sense Multiple Access (CSMA):** CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.

**Collision Detection (CD):**CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred and take appropriate action, such as backing off and retrying the transmission.

**Collision Avoidance (CA):** CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.

**Token passing:**Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel. Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.

**Bandwidth utilization:** Multiple access protocols can affect the overall bandwidth utilization of a network. For example, contention-based protocols may result in lower bandwidth utilization due to collisions, while token passing protocols may result in higher bandwidth utilization due to the controlled access to the communication channel.