**UNIT : I**

**Computer Network**

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

## ****Applications 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, a 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.

Computer Network Types

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



* LAN(Local Area Network)
* PAN(Personal Area Network)
* MAN(Metropolitan Area Network)
* WAN(Wide Area Network)

LAN(Local Area Network)

* Local Area Network is a group of computers connected to each other in a small area such as building, office.
* LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
* It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
* The data is transferred at an extremely faster rate in Local Area Network.
* Local Area Network provides higher security.



PAN(Personal Area Network)

* Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
* Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
* **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
* Personal Area Network covers an area of **30 feet**.
* Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.



**There are two types of Personal Area Network:**



* Wired Personal Area Network
* Wireless Personal Area Network

**Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WiFi, Bluetooth. It is a low range network.

**Personal Area Network:** Wired Personal Area Network is created by using the USB.

MAN(Metropolitan Area Network)

* A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
* Government agencies use MAN to connect to the citizens and private industries.
* In MAN, various LANs are connected to each other through a telephone exchange line.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than Local Area Network(LAN).



Uses Of Metropolitan Area Network:

* MAN is used in communication between the banks in a city.
* It can be used in an Airline Reservation.
* It can be used in a college within a city.
* It can also be used for communication in the military.

WAN(Wide Area Network)

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



Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

* **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
* **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.
* **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
* **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
* **Global business:** We can do the business over the internet globally.

**Disadvantages of Wide Area Network:**

The following are the disadvantages of the Wide Area Network:

* **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
* **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
* **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
* **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

**Transmission Media**

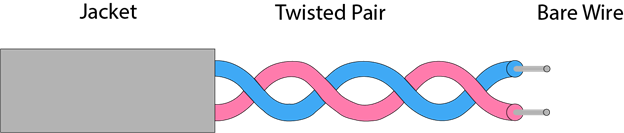
The transmission media is nothing but the physical media over which **communication takes place in computer networks.**

## Twisted pair:

Twisted pair is a physical media made up of a pair of cables twisted with each other. A twisted pair cable is cheap as compared to other transmission media. Installation of the twisted pair cable is easy, and it is a lightweight cable. The frequency range for twisted pair cable is from 0 to 3.5KHz.

A twisted pair consists of two insulated copper wires arranged in a regular spiral pattern.

The degree of reduction in noise interference is determined by the number of turns per foot. Increasing the number of turns per foot decreases noise interference.



**Types of Twisted pair:**

Unshielded Twisted Pair

### Shielded Twisted Pair

### Unshielded Twisted Pair:

An unshielded twisted pair is widely used in telecommunication. Following are the categories of the unshielded twisted pair cable:

* **Category 1:** Category 1 is used for telephone lines that have low-speed data.
* **Category 2:** It can support upto 4Mbps.
* **Category 3:** It can support upto 16Mbps.
* **Category 4:** It can support upto 20Mbps. Therefore, it can be used for long-distance communication.
* **Category 5:** It can support upto 200Mbps.

**Advantages Of Unshielded Twisted Pair:**

* It is cheap.
* Installation of the unshielded twisted pair is easy.
* It can be used for high-speed LAN.

**Disadvantage:**

* This cable can only be used for shorter distances because of attenuation.

### Shielded Twisted Pair

A shielded twisted pair is a cable that contains the mesh surrounding the wire that allows the higher transmission rate.

**Characteristics Of Shielded Twisted Pair:**

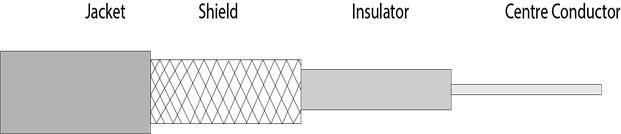
* The cost of the shielded twisted pair cable is not very high and not very low.
* An installation of STP is easy.
* It has higher capacity as compared to unshielded twisted pair cable.
* It has a higher attenuation.
* It is shielded that provides the higher data transmission rate.

**Disadvantages**

* It is more expensive as compared to UTP and coaxial cable.
* It has a higher attenuation rate.

## Coaxial Cable

* Coaxial cable is very commonly used transmission media, for example, TV wire is usually a coaxial cable.
* The name of the cable is coaxial as it contains two conductors parallel to each other.
* It has a higher frequency as compared to Twisted pair cable.
* The inner conductor of the coaxial cable is made up of copper, and the outer conductor is made up of copper mesh. The middle core is made up of non-conductive cover that separates the inner conductor from the outer conductor.
* The middle core is responsible for the data transferring whereas the copper mesh prevents from the **EMI**(Electromagnetic interference).



**Coaxial cable is of two types:**

1. **Baseband transmission:** It is defined as the process of transmitting a single signal at high speed.
2. **Broadband transmission:** It is defined as the process of transmitting multiple signals simultaneously.

**Advantages Of Coaxial cable:**

* The data can be transmitted at high speed.
* It has better shielding as compared to twisted pair cable.
* It provides higher bandwidth.

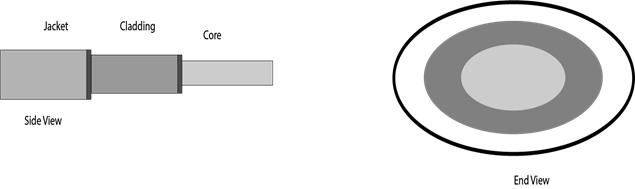
**Disadvantages Of Coaxial cable:**

* It is more expensive as compared to twisted pair cable.
* If any fault occurs in the cable causes the failure in the entire network.

## Fibre Optic

* Fibre optic cable is a cable that uses electrical signals for communication.
* Fibre optic is a cable that holds the optical fibres coated in plastic that are used to send the data by pulses of light.
* The plastic coating protects the optical fibres from heat, cold, electromagnetic interference from other types of wiring.
* Fibre optics provide faster data transmission than copper wires.

**Diagrammatic representation of fibre optic cable:**



**Basic elements of Fibre optic cable:**

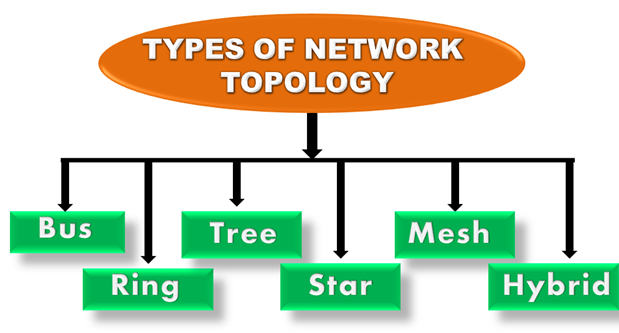
* **Core:** The optical fibre consists of a narrow strand of glass or plastic known as a core. A core is a light transmission area of the fibre. The more the area of the core, the more light will be transmitted into the fibre.
* **Cladding:** The concentric layer of glass is known as cladding. The main functionality of the cladding is to provide the lower refractive index at the core interface as to cause the reflection within the core so that the light waves are transmitted through the fibre.
* **Jacket:** The protective coating consisting of plastic is known as a jacket. The main purpose of a jacket is to preserve the fibre strength, absorb shock and extra fibre protection.

**Following are the advantages of fibre optic cable over copper:**

* **Greater Bandwidth:** The fibre optic cable provides more bandwidth as compared copper. Therefore, the fibre optic carries more data as compared to copper cable.
* **Faster speed:** Fibre optic cable carries the data in the form of light. This allows the fibre optic cable to carry the signals at a higher speed.
* **Longer distances:** The fibre optic cable carries the data at a longer distance as compared to copper cable.
* **Better reliability:** The fibre optic cable is more reliable than the copper cable as it is immune to any temperature changes while it can cause obstruct in the connectivity of copper cable.
* **Thinner and Sturdier:** Fibre optic cable is thinner and lighter in weight so it can withstand more pull pressure than copper cable.

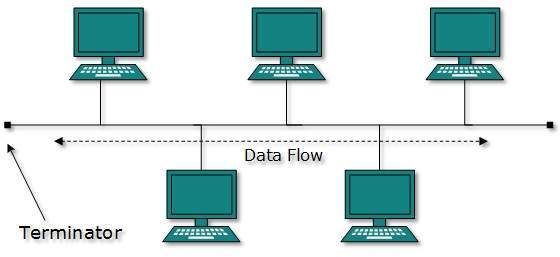
# What is Topology?

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



## Bus Topology

In case of Bus topology, all devices share single communication line or cable.Bus topology may have problem while multiple hosts sending data at the same time. Therefore, Bus topology either uses CSMA/CD technology or recognizes one host as Bus Master to solve the issue. It is one of the simple forms of networking where a failure of a device does not affect the other devices. But failure of the shared communication line can make all other devices stop functioning.



Both ends of the shared channel have line terminator. The data is sent in only one direction and as soon as it reaches the extreme end, the terminator removes the data from the line.

**Advantages of this topology:**

* If N devices are connected to each other in a bus topology, then the number of cables required to connect them is 1, which is 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.

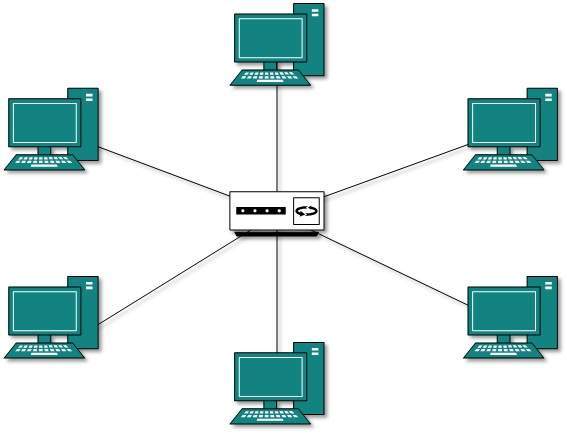
**Disadvcantages of this topology:**

* 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 network would slow down networks.
* Security is very low.

## Star Topology

All hosts in Star topology are connected to a central device, known as hub device, using a point-to-point connection. That is, there exists a point to point connection between hosts and hub. The hub device can be any of the following:

* Layer-1 device such as hub or repeater
* Layer-2 device such as switch or bridge
* Layer-3 device such as router or gateway



As in Bus topology, hub acts as single point of failure. If hub fails, connectivity of all hosts to all other hosts fails. Every communication between hosts, takes place through only the hub.Star topology is not expensive as to connect one more host, only one cable is required and configuration is simple.

**Advantages of this topology:**

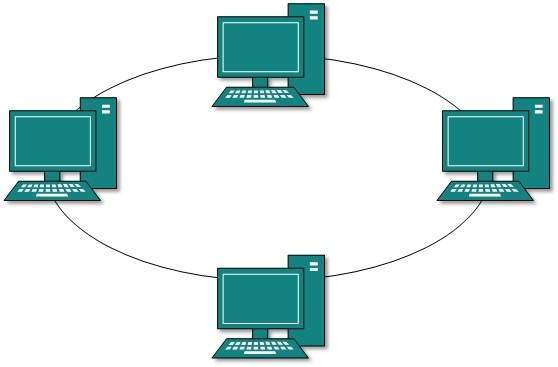
* If N devices are connected to each other in a star topology, then the number of cables required to connect them is N. So, it is easy to set up.
* Each device requires only 1 port i.e. to connect to the hub, therefore the total number of ports required is N.
* It is Robust. If one link fails only that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

**Disadvcantages of this 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

## Ring Topology

In ring topology, each host machine connects to exactly two other machines, creating a circular network structure. When one host tries to communicate or send message to a host which is not adjacent to it, the data travels through all intermediate hosts. To connect one more host in the existing structure, the administrator may need only one more extra cable.



Failure of any host results in failure of the whole ring.Thus, every connection in the ring is a point of failure. There are methods which employ one more backup ring.

**Advantages of this topology:**

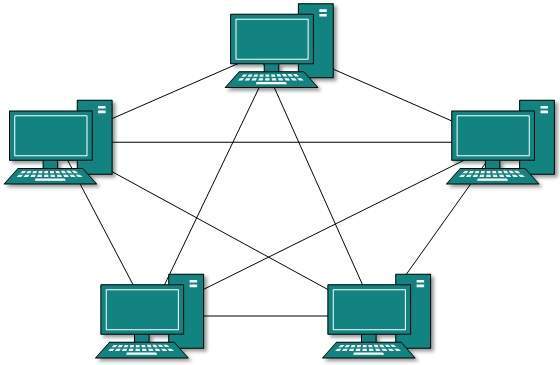
* The data transmission is high-speed.
* The possibility of collision is minimum in this type of topology.
* Cheap to install and expand. It is less costly than a star topology.

**Disadvcantages of this 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 removal of stations can disturb the whole topology.
* Less secure.

## Mesh Topology

In this type of topology, a host is connected to one or multiple hosts.This topology has hosts in point-to-point connection with every other host or may also have hosts which are in point-to-point connection to few hosts only.



Hosts in Mesh topology also work as relay for other hosts which do not have direct point-to-point links. Mesh technology comes into two types:

* **Full Mesh**: All hosts have a point-to-point connection to every other host in the network. Thus for every new host n(n-1)/2 connections are required. It provides the most reliable network structure among all network topologies.
* **Partially Mesh**: Not all hosts have point-to-point connection to every other host. Hosts connect to each other in some arbitrarily fashion. This topology exists where we need to provide reliability to some hosts out of all.

**Advantages of this topology:**

* Communication is very fast between at the nodes.
* It 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.

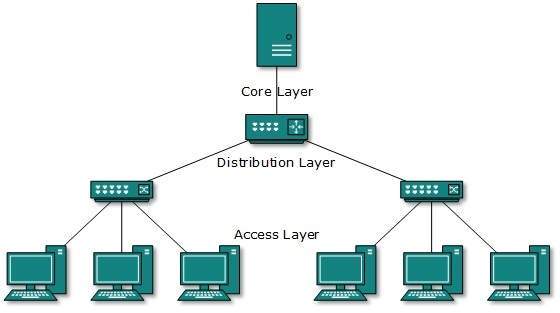
**Disadvcantages of this topology:**

* 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.

## Tree Topology

Also known as Hierarchical Topology, this is the most common form of network topology in use presently.This topology imitates as extended Star topology and inherits properties of bus topology.

This topology divides the network in to multiple levels/layers of network. Mainly in LANs, a network is bifurcated into three types of network devices. The lowermost is access-layer where computers are attached. The middle layer is known as distribution layer, which works as mediator between upper layer and lower layer. The highest layer is known as core layer, and is central point of the network, i.e. root of the tree from which all nodes fork.



All neighboring hosts have point-to-point connection between them.Similar to the Bus topology, if the root goes down, then the entire network suffers even.though it is not the single point of failure. Every connection serves as point of failure, failing of which divides the network into unreachable segment.

**Advantages of this topology :**

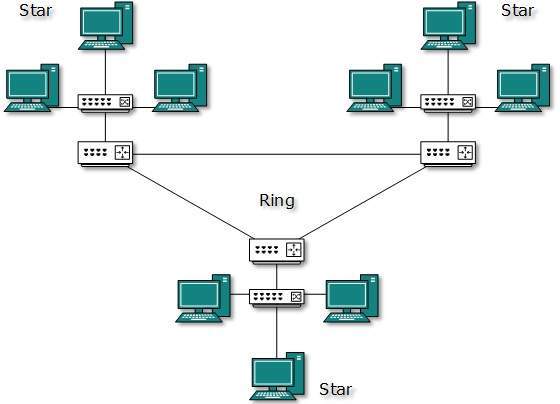
* It allows more devices to be attached to a single central hub thus it decreases the distance that is traveled by the signal to come to the devices.
* It allows the network to get isolated and also prioritize from different computers.
* We can add **new device to existing network.**
* The **Error detection** and **error correction** is very easy in tree topology.

**Disadvcantages of this topology :**

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

## Hybrid Topology

A network structure whose design contains more than one topology is said to be hybrid topology. Hybrid topology inherits merits and demerits of all the incorporating topologies.



The above picture represents an arbitrarily hybrid topology. The combining topologies may contain attributes of Star, Ring, Bus, and Daisy-chain topologies. Most WANs are connected by means of Dual-Ring topology and networks connected to them are mostly Star topology networks. Internet is the best example of largest Hybrid topology.

**Advantages of this topology :**

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

**Disadvcantages of this topology :**

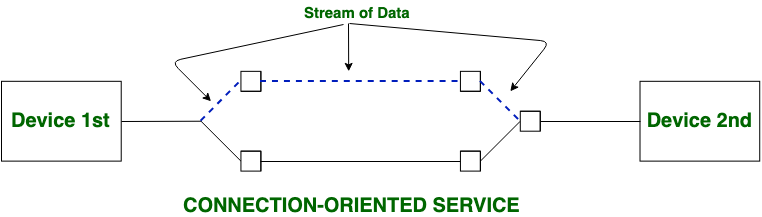
* It is very **difficult to design the architectur**e of the Hybrid Network.
* **Hubs**used in this topology are**very expensive.**
* The infrastructure cost is very high as hybrid network **requires a lot of cabling, network devices**.

# Connection-oriented and Connection-less Services

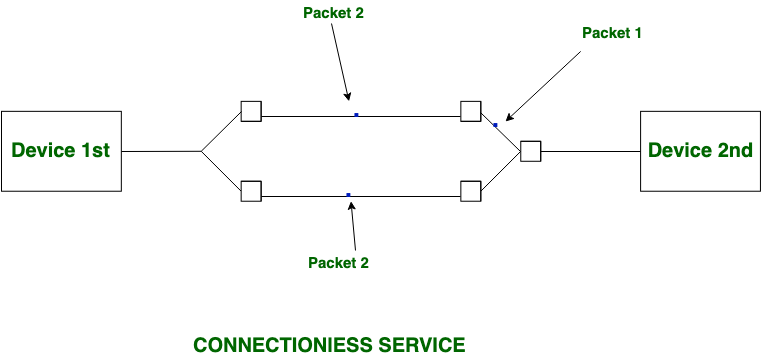
Both [Connection-oriented service and Connection-less service](https://practice.geeksforgeeks.org/problems/what-is-connection-oriented-and-connection-less-transmission-in-transport-layer) are used for the connection establishment between two or more than two devices. These types of services are offered by the network layer.

**Connection-oriented service**

**Connection-oriented service** is related to the telephone system. It includes connection establishment and connection termination. In a connection-oriented service, the Handshake method is used to establish the connection between sender and receiver.

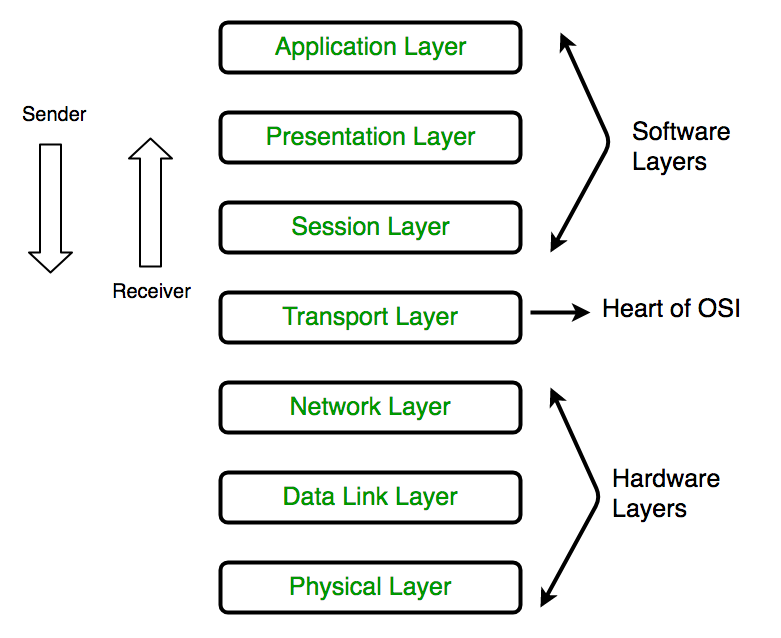
**Connection-less service**

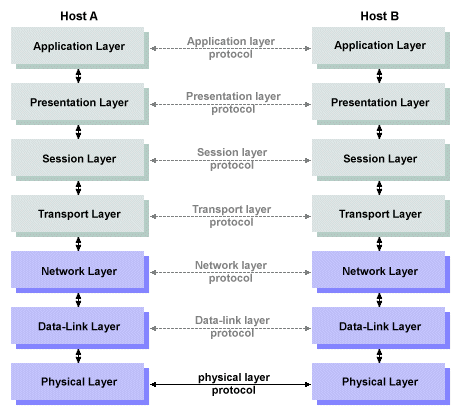
**Connection-less service** is related to the postal system. It does not include any connection establishment and connection termination. Connection-less Service does not give a guarantee of reliability. In this, Packets do not follow the same path to reach their destination.   


# UNIT : II

# OSI Model

OSI stands for **Open Systems Interconnection**. It has been developed by ISO – ‘**International Organization for Standardization**‘, in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.





### **1. Physical Layer (Layer 1) :**

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of**bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

### **2. Data Link Layer (DLL) (Layer 2) :**

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

### **3. Network Layer (Layer 3) :**

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

### **4. Transport Layer (Layer 4) :**

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

### **5. Session Layer (Layer 5) :**

This layer is responsible for the establishment of connection, maintenance of sessions, authentication, and also ensures security. The layer allows the two processes to establish, use and terminate a connection. The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

### **6. Presentation Layer (Layer 6):**

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

* **Translation:** For example, ASCII to EBCDIC.
* **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
* **Compression:** Reduces the number of bits that need to be transmitted on the network.

### **7. Application Layer (Layer 7) :**

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

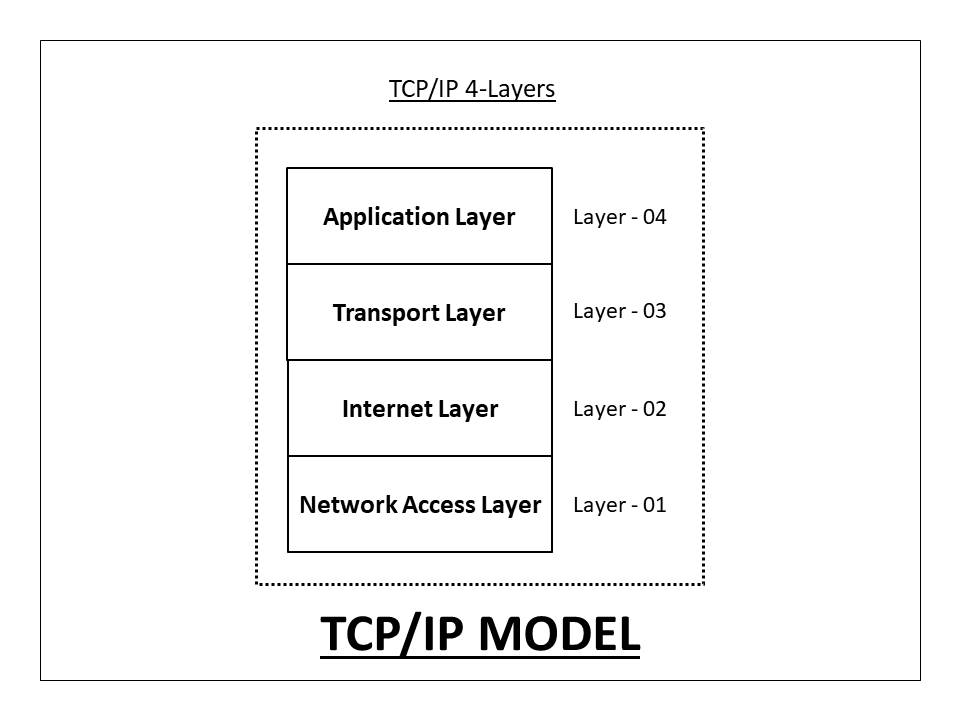
Example: Application – Browsers, Skype Messenger, etc.

# TCP/IP Model

The **OSI Model** we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The **TCP/IP model** is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

**The layers are:**

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer



### 1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.  
We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

### 2. Internet Layer –

This layer parallels the functions of OSI’s Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. **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 of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.
2. **ICMP –** stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
3. **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.

### 3. Host-to-Host Layer –

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. **Transmission Control Protocol (TCP) –** It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
2. **User Datagram Protocol (UDP) –** On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

### 4. Application Layer –

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at [Protocols in Application Layer](https://www.geeksforgeeks.org/protocols-application-layer/) for some information about these protocols.

Protocols other than those present in the linked article are :

* + 1. **HTTP and HTTPS –** HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.
    2. **SSH –** SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.
    3. **NTP –** NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

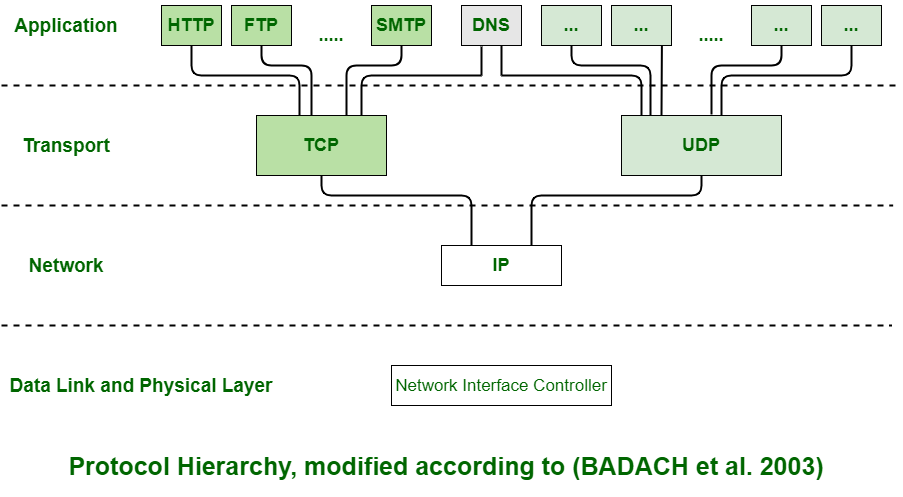
**Protocol Hierarchies**

A **protocol** is simply defined as a set of rules and regulations for data communication. Rules are basically defined for each and every step and process at time of communication among two or more computers. Networks are needed to follow these protocols to transmit data successfully. All protocols might be implemented using hardware, software, or combination of both of them.

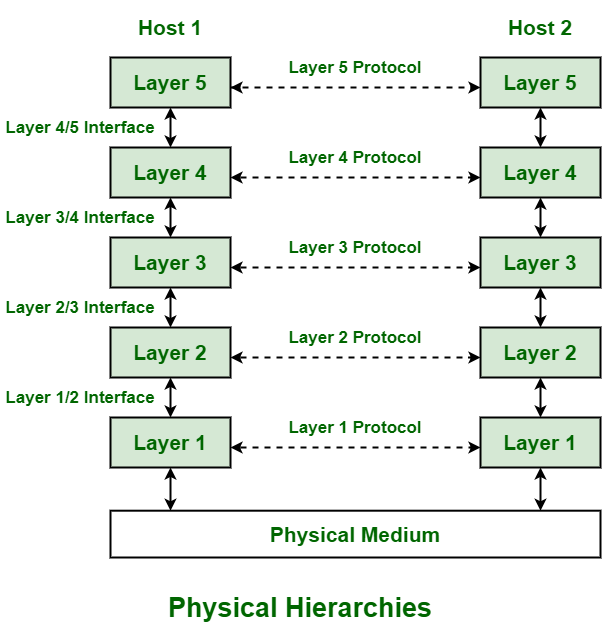
The three aspects of a protocol are −

* **Syntax** − It defines the format of data that is to be sent or received.
* **Semantics** − It defines the meaning of each section of bits that are transferred.
* **Timings** − It defines the time at which data is transferred as well as the speed at which it is transferred.

**Protocol Hierarchies :**  
Generally, Computer networks are comprised of or contain a large number of pieces of hardware and software. To just simplify network design, various networks are organized and arranged as a stack of layers of hardware and software, one on top of another. The number, name, content, and function of each layer might vary and can be different from one network to another. The main purpose of each of layers is just to offer and provide services to higher layers that are present. Each and every layer has some particular task or function. In programming, this concept is very common. The networks are organized and arranged as different layers or levels simply to reduce and minimize complexity of design of network software.



**Example :**  
Below is diagram representing a five-layer network. The diagram shows communication between Host 1 and Host 2. The data stream is passed through a number of layers from one host to other. Virtual communication is represented using dotted lines between peer layers. Physical communication is represented using solid arrows between adjacent layers. Through physical medium, actual communication occurs. The layers at same level are commonly known as peers. The peer basically has a set of communication protocols. An interface is present between each of layers that are used to explain services provided by lower layer to higher layer.



**Advantages :**

* The layers generally reduce complexity of communication between networks
* It increases network lifetime.
* It also uses energy efficiently.
* It does not require overall knowledge and understanding of network.

# Design Issues for the Layers

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows −

## Reliability

Network channels and components may be unreliable, resulting in loss of bits while data transfer. So, an important design issue is to make sure that the information transferred is not distorted.

## Scalability

Networks are continuously evolving. The sizes are continually increasing leading to congestion. Also, when new technologies are applied to the added components, it may lead to incompatibility issues. Hence, the design should be done so that the networks are scalable and can accommodate such additions and alterations.

## Addressing

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

## Error Control

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

## Flow Control

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

## Resource Allocation

Computer networks provide services in the form of network resources to the end users. The main design issue is to allocate and deallocate resources to processes. The allocation/deallocation should occur so that minimal interference among the hosts occurs and there is optimal usage of the resources.

## Statistical Multiplexing

It is not feasible to allocate a dedicated path for each message while it is being transferred from the source to the destination. So, the data channel needs to be multiplexed, so as to allocate a fraction of the bandwidth or time to each host.

## Routing

There may be multiple paths from the source to the destination. Routing involves choosing an optimal path among all possible paths, in terms of cost and time. There are several routing algorithms that are used in network systems.

## Security

A major factor of data communication is to defend it against threats like eavesdropping and surreptitious alteration of messages. So, there should be adequate mechanisms to prevent unauthorized access to data through authentication and cryptography.

# Service Primitives

**Service** generally includes set of various primitives. A primitive simply means Operations.

A Service is specified by set of primitives that are available and given to user or other various entities to access the service. All these primitives simply tell the service to perform some action or to report on action that is taken by peer entity. Each of the protocol that communicates in layered architecture also communicates in peer-to-peer manner with some of its remote protocol entity.

Primitives are called calling functions between the layers that are used to manage communication among the adjacent protocol layers i.e., among the same communication node. The set of primitives that are available generally depends upon the nature of the service that is being provided.

**Classification of Service Primitives :**

|  |  |
| --- | --- |
|  |  |
| **Request** | It represent entity that wants or request service to perform some action or do some work (requesting for connection to remote computer). |
| **Indication** | It represent entity that is to be informed about event (receiver just have received request of connection). |
| **Response** | It represents entity that is responding to event (receiver is simply sending the permission or allowing to connect). |
| **Confirm** | It represent entity that acknowledges the response to earlier request that has come back (sender just acknowledge the permission to get connected to the remote host). |

**Primitives of Connection-Oriented Service :**

|  |  |
| --- | --- |
|  |  |
| **Listen :** | When server is ready to accept request of incoming connection, it simply put this primitive into action. Listen primitive simply waiting for incoming connection request. |
| **Connect :** | This primitive is used to connect the server simply by creating or establishing connection with waiting peer. |
| **Accept :** | This primitive simply accepts incoming connection form peer. |
| **Receive :** | These primitive afterwards block the server. Receive primitive simply waits for incoming message. |
| **Send :** | This primitive is put into action by the client to transmit its request that is followed by putting receive primitive into action to get the reply. Send primitive simply sends or transfer the message to the peer. |
| **Disconnect:** | This primitive is simply used to terminate or end the connection after which no one will be able to send any of the message. |

**Primitives of Connectionless Service :**

|  |  |
| --- | --- |
| Primitive | Meaning |
| **Unitdata :** | Unitdata primitive is simply required to send packet of data or information. |
| **Facility, Report :** | This primitive is required for getting details about the performance and working of the network such as delivery statistics or report. |

**UNIT : III**

**Protocol Stack Design Issues of the layers :**

1. **Addressing :**

At a particular time, innumerable messages are being transferred between large numbers of computers. So, a naming or addressing system should exist so that each layer can identify the sender and receivers of each message.

1. **Error Control :**

Unreliable channels introduce a number of errors in the data streams that are communicated. So, the layers need to agree upon common error detection and error correction methods so as to protect data packets while they are transferred.

1. **Flow Control :**

If the rate at which data is produced by the sender is higher than the rate at which data is received by the receiver, there are chances of overflowing the receiver. So, a proper flow control mechanism needs to be implemented.

1. **Multiplexing** :  
   Gathering data from multiple application processes of the sender, enveloping that data with a header, and sending them as a whole to the intended receiver is called multiplexing.
2. **Demultiplexing** :  
   Delivering received segments at the receiver side to the correct app layer processes is called demultiplexing.

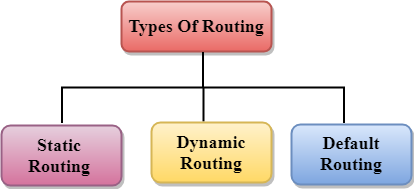
# Routing

* A Router is a process of selecting path along which the data can be transferred from source to the destination. Routing is performed by a special device known as a router.
* A Router works at the network layer in the OSI model and internet layer in TCP/IP model
* A router is a networking device that forwards the packet based on the information available in the packet header and forwarding table.
* The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.
* The routing protocols use the metric to determine the best path for the packet delivery. The metric is the standard of measurement such as hop count, bandwidth, delay, current load on the path, etc. used by the routing algorithm to determine the optimal path to the destination.
* The routing algorithm initializes and maintains the routing table for the process of path determination.

## Types of Routing

Routing can be classified into three categories:

* Static Routing
* Default Routing
* Dynamic Routing



## Static Routing

* Static Routing is also known as Nonadaptive Routing.
* It is a technique in which the administrator manually adds the routes in a routing table.
* A Router can send the packets for the destination along the route defined by the administrator.
* In this technique, routing decisions are not made based on the condition or topology of the networks

### Advantages Of Static Routing

Following are the advantages of Static Routing:

* **No Overhead:** It has ho overhead on the CPU usage of the router. Therefore, the cheaper router can be used to obtain static routing.
* **Bandwidth:** It has not bandwidth usage between the routers.
* **Security:** It provides security as the system administrator is allowed only to have control over the routing to a particular network.

### Disadvantages of Static Routing:

Following are the disadvantages of Static Routing:

* For a large network, it becomes a very difficult task to add each route manually to the routing table.
* The system administrator should have a good knowledge of a topology as he has to add each route manually.

## Default Routing:

* Default Routing is a technique in which a router is configured to send all the packets to the same hop device, and it doesn't matter whether it belongs to a particular network or not. A Packet is transmitted to the device for which it is configured in default routing.
* Default Routing is used when networks deal with the single exit point.
* It is also useful when the bulk of transmission networks have to transmit the data to the same hp device.
* When a specific route is mentioned in the routing table, the router will choose the specific route rather than the default route. The default route is chosen only when a specific route is not mentioned in the routing table.

## Dynamic Routing :

* It is also known as Adaptive Routing.
* It is a technique in which a router adds a new route in the routing table for each packet in response to the changes in the condition or topology of the network.
* Dynamic protocols are used to discover the new routes to reach the destination.
* In Dynamic Routing, RIP and OSPF are the protocols used to discover the new routes.
* If any route goes down, then the automatic adjustment will be made to reach the destination.

**The Dynamic protocol should have the following features:**

* All the routers must have the same dynamic routing protocol in order to exchange the routes.
* If the router discovers any change in the condition or topology, then router broadcast this information to all other routers.

### Advantages of Dynamic Routing:

* It is easier to configure.
* It is more effective in selecting the best route in response to the changes in the condition or topology.

### Disadvantages of Dynamic Routing:

* It is more expensive in terms of CPU and bandwidth usage.
* It is less secure as compared to default and static routing.

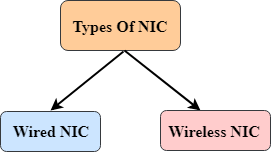
**Network Devices**

**Network Devices:** Network devices, also known as networking hardware, are physical devices that allow hardware on a computer network to communicate and interact with one another. For example Repeater, Hub, Bridge, Switch, Routers, Gateway, Brouter, and NIC, etc.

## NIC :

* NIC stands for network interface card.
* NIC is a hardware component used to connect a computer with another computer onto a network
* It can support a transfer rate of 10,100 to 1000 Mb/s.
* The MAC address or physical address is encoded on the network card chip which is assigned by the IEEE to identify a network card uniquely. The MAC address is stored in the PROM (Programmable read-only memory).

### There are two types of NIC:



Wired NIC

Wireless NIC

**Wired NIC:** The Wired NIC is present inside the motherboard. Cables and connectors are used with wired NIC to transfer data.

**Wireless NIC:** The wireless NIC contains the antenna to obtain the connection over the wireless network. For example, laptop computer contains the wireless NIC.

1. **Repeater**

A repeater operates at the physical layer. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that they do not amplify the signal. When the signal becomes weak, they copy it bit by bit and regenerate it at its star topology connectors connecting if original strength. It is a 2-port device.

1. **HUB** –

A hub is a basically multi-port repeater. A hub 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](https://en.wikipedia.org/wiki/Collision_domain) of all hosts connected through Hub remains one.  Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

**Types of HUB**

* **Active Hub:-**These are the hubs that have their power supply and can clean, boost, and relay the signal along with the network. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
* **Passive Hub:-**These are the hubs that collect wiring from nodes and power supply from the active hub. These hubs relay signals onto the network without cleaning and boosting them and can’t be used to extend the distance between nodes.
* **Intelligent Hub:-** It works like an active hub and includes remote management capabilities. They also provide flexible data rates to network devices. It also enables an administrator to monitor the traffic passing through the hub and to configure each port in the hub.

1. **Bridge** –

A bridge operates at the data link layer. A bridge is a repeater, with add on the functionality of filtering content by reading the MAC addresses of the source and destination. It is also used for interconnecting two LANs working on the same protocol. It has a single input and single output port, thus making it a 2 port device.

**Types of Bridges**

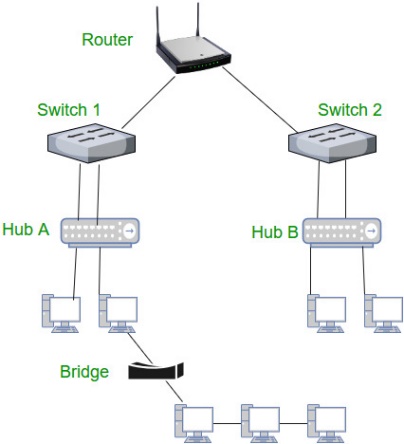
* **Transparent Bridges:-**These are the bridge in which the stations are completely unaware of the bridge’s existence i.e. whether or not a bridge is added or deleted from the network, reconfiguration of the stations is unnecessary. These bridges make use of two processes i.e. bridge forwarding and bridge learning.
* **Source Routing Bridges:-**In these bridges, routing operation is performed by the source station and the frame specifies which route to follow. The host can discover the frame by sending a special frame called the discovery frame, which spreads through the entire network using all possible paths to the destination.

1. **Switch** –

A switch 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. A switch 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.  In other words, the switch divides the collision domain of hosts, but the [broadcast domain](https://en.wikipedia.org/wiki/Broadcast_domain) remains the same.   
  

**5. Routers** –

A router is a device like a switch that routes data packets based on their IP addresses. The router 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. **Gateway** –

A gateway, as the name suggests, is a passage to connect two networks that may work upon different networking models. They work as messenger agents that take data from one system, interpret it, and transfer it to another system. Gateways are also called protocol converters and can operate at any network layer. Gateways are generally more complex than switches or routers. A gateway is also called a protocol converter.