**UNIT – I**

**09-03-2022**

**Define Network.**

A network is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

“Computer network’’ to mean a collection of autonomous computers interconnected by a single technology. Two computers are said to be interconnected if they are able to exchange information.

**Components of the Network**

A data communications system has five components.

1. Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.

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

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

4. Transmission medium. The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves

5. Protocol. A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

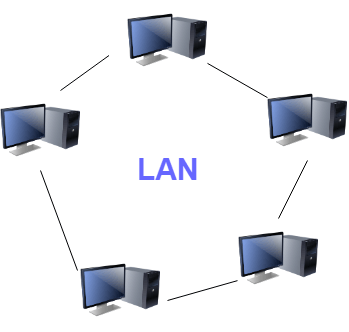
**1.1 Evolution of Computer Networks**

**1.2 Types of Computer Networks**

Some of the most popular computer network types are:

**What is a LAN (Local Area Network)?**

A **Local Area Network** (LAN) is a group of computer and peripheral devices which are connected in a limited area such as school, laboratory, home, and office building. It is a widely useful network for sharing resources like files, printers, games, and other application. The simplest type of LAN network is to connect computers and a printer in someone’s home or office. In general, LAN will be used as one type of transmission medium. It is a network which consists of less than 5000 interconnected devices across several buildings.



Local Area Network (LAN)

**Characteristics of LAN**

Here are the important characteristics of a LAN network:

* It is a private network, so an outside regulatory body never controls it.
* LAN operates at a relatively higher speed compared to other WAN systems.
* There are various kinds of media access control methods like token ring and ethernet.

**Advantages of LAN**

Here are the pros/benefits of LAN:

* Computer resources like hard-disks, DVD-ROM, and printers can share local area networks. This significantly reduces the cost of hardware purchases.
* You can use the same software over the network instead of purchasing the licensed software for each client in the network.
* Data of all network users can be stored on a single hard disk of the server computer.
* You can easily transfer data and messages over networked computers.
* It will be easy to manage data at only one place, which makes data more secure.
* Local Area Network offers the facility to share a single internet connection among all the LAN users.

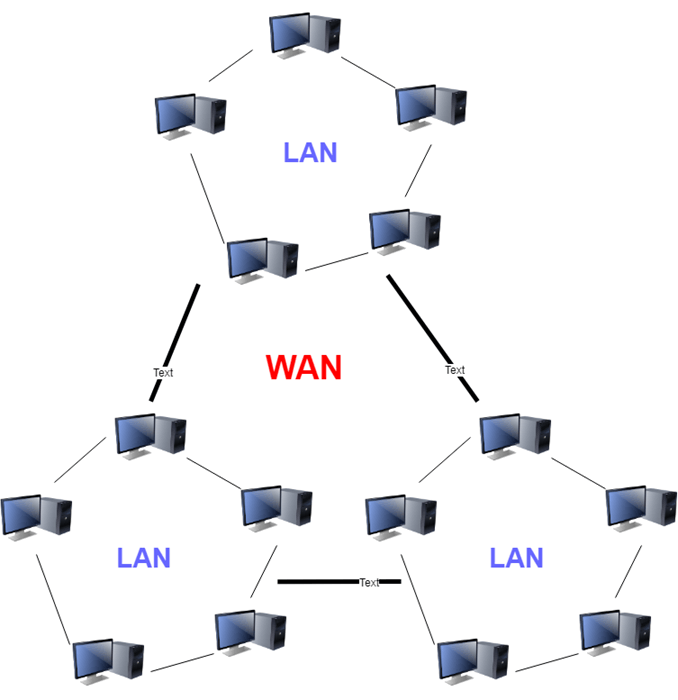
**Disadvantages of LAN**

Here are the cons/drawbacks of LAN:

* LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
* The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
* Unauthorized users can access critical data of an organization in case LAN admin is not able to secure centralized data repository.
* Local Area Network requires a constant LAN administration as there are issues related to software setup and hardware failures

**What is WAN (Wide Area Network)?**

**WAN** (Wide Area Network) is another important computer network that which is spread across a large geographical area. WAN network system could be a connection of a LAN which connects with other LAN’s using telephone lines and radio waves. It is mostly limited to an enterprise or an organization.



Wide Area Network (WAN)

**Characteristics of WAN**

Below are the characteristics of WAN:

* The software files will be shared among all the users; therefore, all can access to the latest files.
* Any organization can form its global integrated network using WAN.

**Advantages of WAN**

Here are the benefits/pros of WAN:

* WAN helps you to cover a larger geographical area. Therefore business offices situated at longer distances can easily communicate.
* Contains devices like mobile phones, laptop, tablet, computers, gaming consoles, etc.
* WLAN connections work using radio transmitters and receivers built into client devices.

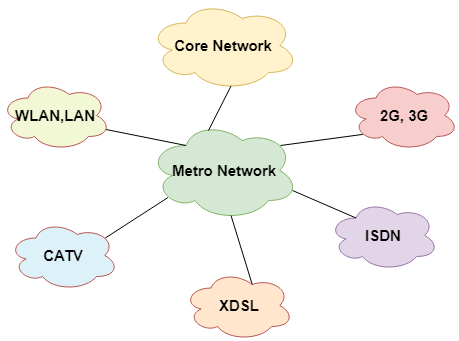
**Disadvantages of WAN**

Here are the drawbacks/cons of WAN network:

* The initial setup cost of investment is very high.
* It is difficult to maintain the WAN network. You need skilled technicians and network administrators.
* There are more errors and issues because of the wide coverage and the use of different technologies.
* It requires more time to resolve issues because of the involvement of multiple wired and wireless technologies.
* Offers lower security compared to other types of network in computer.

**What is MAN (Metropolitan Area Network)?**

A **Metropolitan Area Network** or MAN is consisting of a computer network across an entire city, college campus, or a small region. This type of network is large than a LAN, which is mostly limited to a single building or site. Depending upon the type of configuration, this type of network allows you to cover an area from several miles to tens of miles.



Metropolitan Area Network (MAN)

**Characteristics of MAN**

Here are important characteristics of the MAN network:

* It mostly covers towns and cities in a maximum 50 km range
* Mostly used medium is optical fibers, cables
* Data rates adequate for distributed computing applications.

**Advantages of MAN**

Here are the pros/benefits of MAN network:

* It offers fast communication using high-speed carriers, like [fiber optic cables](https://www.guru99.com/ethernet-cables-types.html).
* It provides excellent support for an extensive size network and greater access to WANs.
* The dual bus in MAN network provides support to transmit data in both directions concurrently.
* A MAN network mostly includes some areas of a city or an entire city.

**Disadvantages of MAN**

Here are drawbacks/cons of using the MAN network:

* You need more cable to establish MAN connection from one place to another.
* In MAN network it is tough to make the system secure from hackers

**What is PAN (Personal Area Network)?**

**PAN** (Personal Area Network) is a computer network formed around a person. It generally consists of a computer, mobile, or personal digital assistant. PAN can be used for establishing communication among these personal devices for connecting to a digital network and the internet.

**Characteristics of PAN**

Below are the main characteristics of PAN:

* It is mostly personal devices network equipped within a limited area.
* Allows you to handle the interconnection of IT devices at the surrounding of a single user.
* PAN includes mobile devices, tablet, and laptop.
* It can be wirelessly connected to the internet called WPAN.
* Appliances use for PAN: cordless mice, keyboards, and Bluetooth systems.

**Advantages of PAN**

Here are the important pros/benefits of PAN network:

* PAN networks are relatively secure and safe
* It offers only short-range solution up to ten meters
* Strictly restricted to a small area

**Disadvantages of PAN**

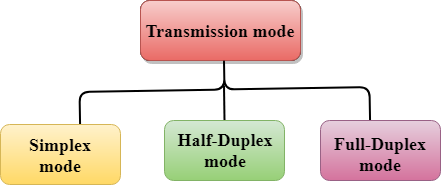
Here are the cons/drawbacks of using PAN network:

* It may establish a bad connection to other networks at the same radio bands.
* Distance limits.

**1.3 Data Transmission Modes**

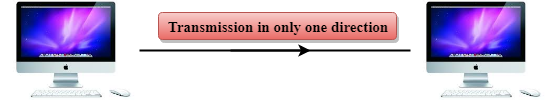
* The way in which data is transmitted from one device to another device is known as **transmission mode**.
* The transmission mode is also known as the communication mode.
* Each communication channel has a direction associated with it, and transmission media provide the direction. Therefore, the transmission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

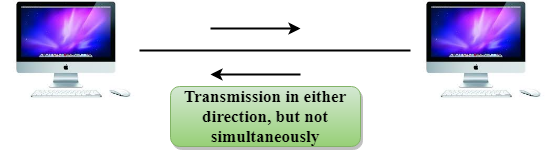
**Advantage of Simplex mode:**

* It utilizes the full capacity of the communication channel during data transmission.
* It has the least or no data traffic issues as data flows only in one direction.

**Disadvantage of Simplex mode:**

* It is unidirectional in nature having no inter-communication between devices.
* There is no mechanism for information to be transmitted back to the sender(No mechanism for acknowledgement).

**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.

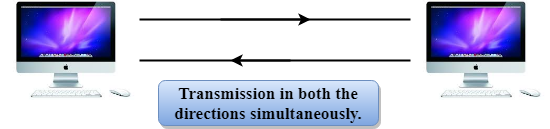
**Advantage of Half-duplex mode:**

* It facilitates the optimum use of the communication channel.
* It provides two-way communication.

**Disadvantage of Half-Duplex mode:**

* The two-way communication cannot be established simultaneously at the same time.
* Delay in transmission may occur as only one way communication can be possible at a 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.

**Advantage of Full-duplex mode:**

* The two-way communication can be carried out simultaneously in both directions.
* It is the fastest mode of communication between devices.

**Disadvantage of Full-duplex mode:**

* The capacity of the communication channel is divided into two parts. Also, no dedicated path exists for data transfer.
* It has improper channel bandwidth utilization as there exist two separate paths for two communicating devices.

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

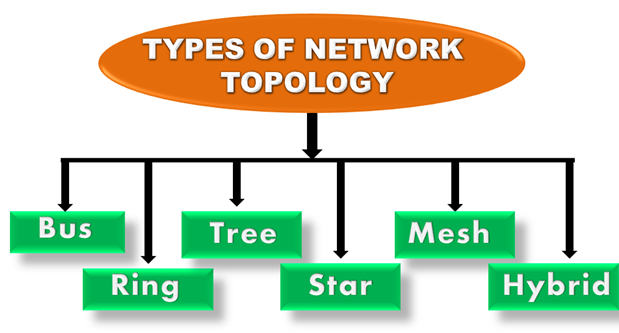
|  |  |  |  |
| --- | --- | --- | --- |
| **Basis for comparison** | **Simplex mode** | **Half-duplex mode** | **Full-duplex mode** |
| Direction of communication | In simplex mode, the communication is unidirectional. | In half-duplex mode, the communication is bidirectional, but one at a time. | In full-duplex mode, the communication is bidirectional. |
| Send/Receive | A device can only send the data but cannot receive it or it can only receive the data but cannot send it. | Both the devices can send and receive the data, but one at a time. | Both the devices can send and receive the data simultaneously. |
| Performance | The performance of half-duplex mode is better than the simplex mode. | The performance of full-duplex mode is better than the half-duplex mode. | The Full-duplex mode has better performance among simplex and half-duplex mode as it doubles the utilization of the capacity of the communication channel. |
| Example | Examples of Simplex mode are radio, keyboard, and monitor. | Example of half-duplex is Walkie-Talkies. | Example of the Full-duplex mode is a telephone network. |

**1.4 Network topologies**

**What is Topology?**

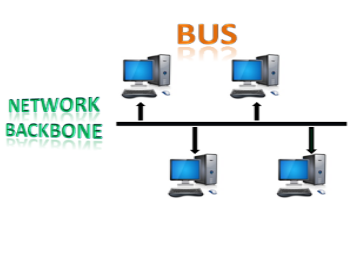
Topology defines the structure of the network of how all the components are interconnected to each other. There are two types of topology: physical and logical topology.

Physical topology is the geometric representation of all the nodes in a network.



A logical topology is a concept in networking that defines the architecture of the communication mechanism for all nodes in a network. Using network equipment such as routers and switches, the logical topology of a network can be dynamically maintained and reconfigured.

**Bus Topology**



* The bus topology 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).

**CSMA:** It is a media access control used to control the data flow so that data integrity is maintained, i.e., the packets do not get lost. There are two alternative ways of handling the problems that occur when two nodes send the messages simultaneously.

* **CSMA CD:** CSMA CD (**Collision detection**) is an access method used to detect the collision. Once the collision is detected, the sender will stop transmitting the data. Therefore, it works on "**recovery after the collision**".
* **CSMA CA:** **CSMA CA (Collision Avoidance)** is an access method used to avoid the collision by checking whether the transmission media is busy or not. If busy, then the sender waits until the media becomes idle. This technique effectively reduces the possibility of the collision. It does not work on "recovery after the collision".

**Advantages of Bus topology:**

* **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 of Bus topology:**

* **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.

**16-03-2022**

**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.

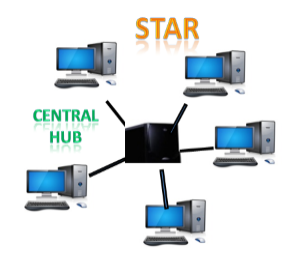
**Advantages of Ring topology:**

* **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 of Ring topology:**

* **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.

**Star Topology**



* Star topology is an arrangement of the network in which every node is connected to the central hub, switch or a central computer.
* 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.

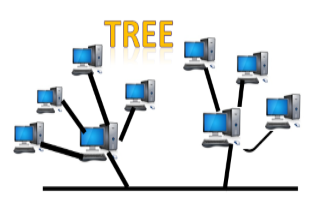
**Advantages of Star topology**

* **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 of Star topology**

* **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.

**Tree topology**



* Tree topology combines the characteristics of bus topology and star topology.
* A tree topology 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.

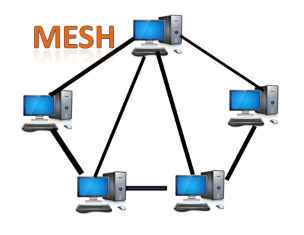
**Advantages of Tree topology**

* **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 of Tree topology**

* **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.

**Mesh topology**

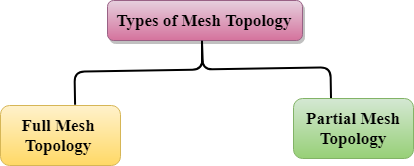


* Mesh technology is an arrangement of the network in which computers are interconnected with each other through various redundant connections.
* There are multiple paths from one computer to another computer.
* It does not contain the switch, hub or any central computer which acts as a central point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

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

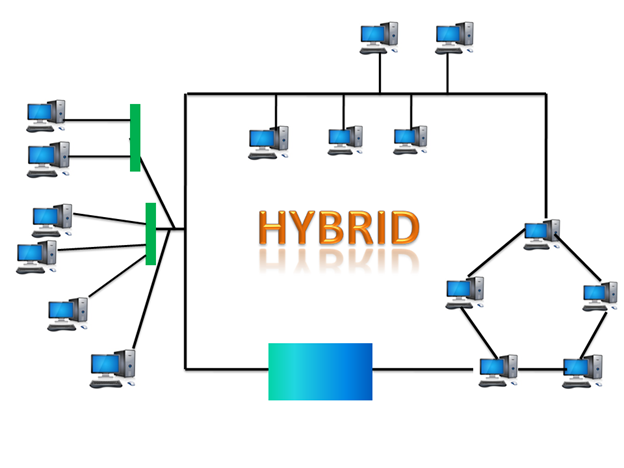
**Fast Communication:** Communication is very fast between the nodes.

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

**Disadvantages of Mesh topology**

* **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.

**Hybrid Topology**



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

**Advantages of Hybrid Topology**

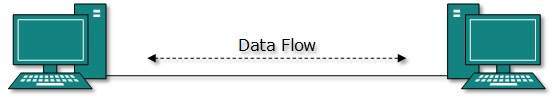
* **Reliable:** If a fault occurs in any part of the network will not affect the functioning of the rest of the network.
* **Scalable:** Size of the network can be easily expanded by adding new devices without affecting the functionality of the existing network.
* **Flexible:** This topology is very 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 of Hybrid topology**

* **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.

**Point-to-Point**

Point-to-point networks contains exactly two hosts such as computer, switches or routers, servers connected back to back using a single piece of cable. Often, the receiving end of one host is connected to sending end of the other and vice-versa.



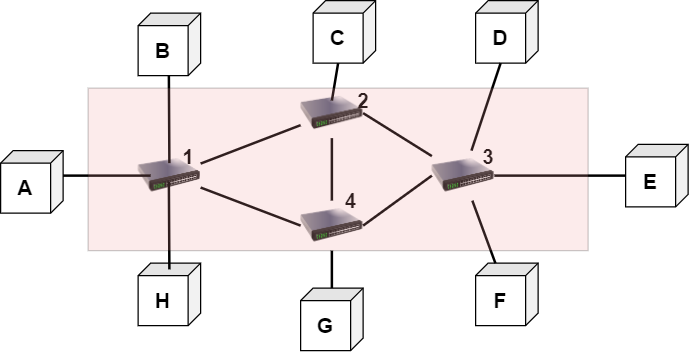
If the hosts are connected point-to-point logically, then may have multiple intermediate devices. But the end hosts are unaware of underlying network and see each other as if they are connected directly.

**1.5 Circuit Switching and Packet Switching**

**Switched Networks**

A switched network basically consists of a series of**interlinked nodes.** These interlinked nodes are known as **switches.**

* Thus in a switched network, connectivity is usually provided by making the **use of switches**.
* Switches are those devices that are capable of creating temporary connections between two or more devices that are linked to them.
* In this network, some switches are connected to the end system (like computer systems or telephones) while other switches are used for routing.
* The network device switch is mainly a layer-2 device of the OSI model.
* Packet forwarding is done by the switch on the basis of the MAC address.
* Thus the Switch mainly transfers the data only to the device that has been addressed (means having proper mac address). Because verification of destination address is done by the switch in order to route the packet appropriately.



**Figure: Switched Network**

In the above figure; A, B, C, D, E, F, G, H are **end systems** or we can say communicating devices. And there are 4 switches labeled as 1,2,3,4. Also, you can see that each switch is connected to multiple links.

The concept of switching is needed for the effective utilization of the bandwidth. Also whenever two or more devices communicate with each other then there are many chances for the occurrence of the collision of data packets in the network; switching is the best solution for this problem.

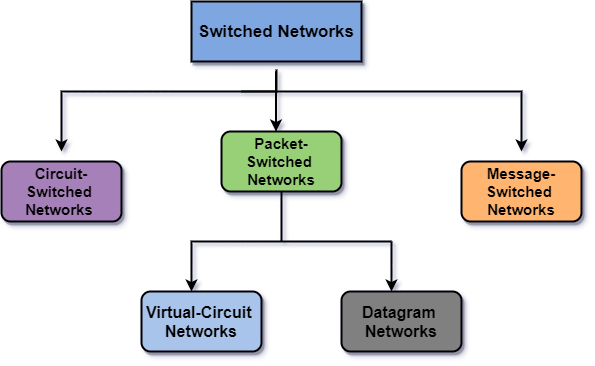
**Methods of Switching**

In order to decide the best route for data transmission, a switching technique is used. The switching techniques mainly connect the systems in such a way to make one-to-one communication easier.

Given below are three methods used for switching or we can say there are three switching techniques:

* Circuit Switching
* Packet Switching
* Message Switching

On the basis of the above-given techniques, switched networks are broadly classified as follows:



**Advantages of Switched Networks**

Given below are some benefits of switched networks:

* As switches help in creating collision domain for each connection in the networks. Thus there are fewer chances of frame collision.
* There is an increase in the performance of networks by using switches.
* There is an increase in the available bandwidth on the network by using switches.
* The workload on the individual PC gets reduced by using switches in the network.
* There is a direct connection of the switch with the workstation.

**Disadvantages of Switched Networks**

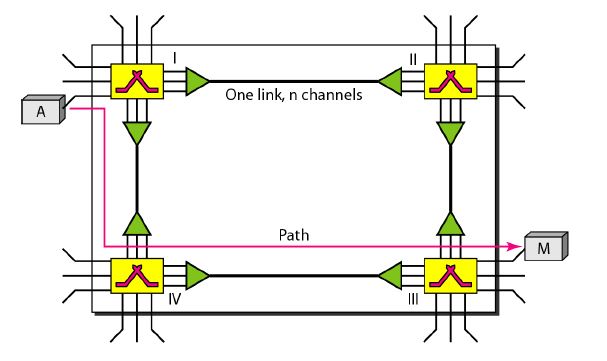
There are some drawbacks of using switches:

* As we are using switches in the switched network, so the network becomes expensive because switches are expensive.
* It is difficult to trace the connectivity issues in the network through a switch.
* There are chances for the occurrence of trouble in broadcast traffic.
* In order to handle multicast packets, proper design and configuration are needed.

**Circuit-Switched Networks**

A network consists of a set of switches that are connected by the physical links commonly known as Circuit-Switched Network.

* Whenever one device communicates with another device then a dedicated communication path is established between them over the network.
* There is only a dedicated channel on each link used by each connection. Also, each link can be easily divided into **n channels** by using the **TDM**(Time Division Multiplexing)or**FDM**( Frequency Divison Multiplexing)technique.
* The**Circuit Switching technique** is mainly used in the**public telephone network** for **voice communication** as well as for **data communication**.
* Data communication is less efficient than voice communication.
* The Circuit switching technique mainly takes place at the physical layer.
* In Circuit-switched networks, the data transfer mode mainly involves a dedicated end-to-end connection. Until the end of the communication, this dedicated path is maintained. After the communication is over the link is released.



**The figure shows a trivial circuit-switched Network**

Phases in Circuit Switching

In order to transfer data using Circuit switching there is a need to establish a circuit (these circuits can either be permanent or temporary) so that data transfer can take place smoothly. Given below are three phases that are used in Circuit Switching for actual communication:

* Setup Phase
* Data Transfer Phase
* Teardown Phase

1. Setup Phase

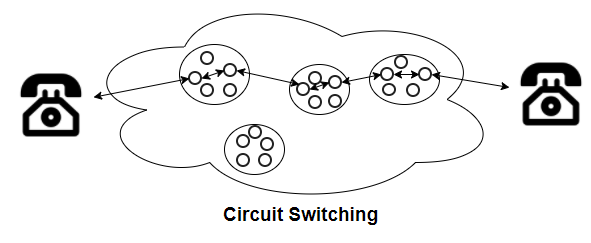
There is an establishment of the circuit that simply means a dedicated link is established between the sender and the receiver with the help of several switching centers or nodes.

2. Data Transfer Phase

After the establishment of the circuit, the connection is established which means that data transfer can take place between sender and receiver.

3. Teardown Phase

On the completion of communication between the sender and receiver the circuit disconnects. In order to disconnect a signal is sent either by the sender or receiver



One of the best examples of Circuit switching is a **telephone**. Suppose there are two persons Person A and Person B; they both want to communicate with each other and located at a distance far from each other.

**Advantages of Circuit Switching**

Given below are some of the benefits of Circuit Switching:

**1. Offers Dedicated Transmission**

As there is a dedicated link between the sender and the receiver. Thus Circuit-Switched network provides a guarantee of dedicated transmission.

**2. No Delay in Transmission**

There is a dedicated path between sender and receiver thus there are no chances for the delay.

3. The Circuit switching technique is best for long transmission because it facilitates a dedicated link between sender and receiver.

**Disadvantages of Circuit Switching**

There are some drawbacks of Circuit Switching and these are as follows:

* One of the main disadvantages of Circuit switching is that as there is a dedicated path between sender and receiver; thus this path is received for these two particular devices and cannot be used by any other device.
* There is a need for more bandwidth as a dedicated path requires more bandwidth.
* Utilization of resources is not done properly as resources are allocated to a connection for the entire duration and thus became unavailable for all other connections.
* It becomes inefficient in the case if the connection is established between sender and receiver but there is no data transfer between them.
* Sometimes it takes a long time to establish the connection between sender and receiver.
* As there is a dedicated path between sender and receiver; thus, this technique is expensive.

**Message-Switched Networks**

The Message-Switching Technique was mainly developed to act as an **alternative to circuit switching**, this was **before packet switching was introduced**. Basically, the message is a smaller unit.

* In the Message-Switching technique, the communication between end users is done by sending and receiving the message, and this message includes the **entire data to be shared.**
* In Message-Switching there is no dedicated path between the sender and receiver like circuit switching.
* The sender and receiver are connected by way of several intermediate nodes which helps and ensures proper data transfer between them.
* Message-Switched data networks are also known as **hop-by-hop** systems.

**Characteristics of Message Switching**

Given below are two characteristics of Message switching:

* **Store and Forward** As we have already told you that the sender and the receiver are not directly connected to each other. Thus intermediate nodes between sender and receiver are, mainly responsible for transferring the message to the next node in the path. Thus in order to transfer the message, intermediate nodes must have the storage capacity because any message will only be delivered if the next node and the link between them are available to connect otherwise this message will be stored indefinitely. A store-and-forward switch thus forwards a message only if sufficient resources are available and the next node is ready to accept the data. The process continues till the data is delivered to the destination computer. Hence, it is called store-&-forward property. The store-and-forward property was earlier used in telegraph message switching centers.
* **Message delivery:** In the Message Switching the entire information is compiled into a single message and then that message is transmitted from source to destination. To successfully reach its destination each message must contain the routing information in its header section.

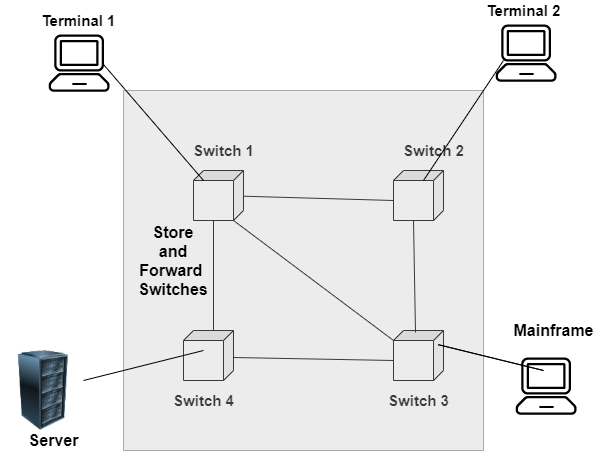


Figure: Message Switching and Message-switched Network

**Advantages of Message Switching**

* In this Switching, data channels are shared among network devices.
* There is Management of traffic in an efficient way by assigning priorities to the messages.
* There is an improvement in efficiency as a single channel can now be used for transferring many messages.
* There is a reduction in network traffic congestion because in this technique we are using store and forward property and also any switching node can store the messages till the availability of the network.
* With the use of Message Switching, messages of unlimited size can be sent.
* It requires less bandwidth while broadcasting the messages; thus it consumes less bandwidth than circuit switching.
* In Message switching, if the next node or link is not available then the current node stores the message

**Disadvantages of Message Switching**

There are some drawbacks of using Message Switching and these are as follows:

* For the whole network, message switching requires a large capacity.
* This technique cannot be used for real-time applications because the storing of messages causes delay.
* The message-switched networks are very slow in nature because the processing takes place in each and every node and thus it may result in poor performance.

**Packet Switching in Computer Networks**

Packet Switching is a technique of switching in which the message is usually divided into smaller pieces that are known as packets.

* Every packet contains a header that contains the knowledge of the destination. With the help of this knowledge/information, these packets find the route.
* A unique number is given to each packet in order to identify them at the receiving end.
* One of the biggest examples of the Packet-switched network is the Internet.
* The header of the Packet mainly comprises of two things: header and payload.
  + where the header mainly contains the routing information.
  + and the payload contains the data that is to be transferred.
* This switching is also based on the store and forward method.
* In the Packet Switched network, there is no resource reservation, and resources are allocated on demand.
* As we know that each packet contains the information of source and destination in their headers. Thus all packets can independently travel in the network.
* Packets related to the same file might take different paths and it mainly depends upon the availability of the path. These packets will be then re-assembled at the destination. It is the responsibility of the receiver node to re-arrange the received packet in order to get the original data.
* The message of acknowledgment will be sent by the receiver if packets reach the receiver in the correct order.
* In case of a missing packet or corrupted packet, the message will be sent by the receiver to the sender to resend the message.

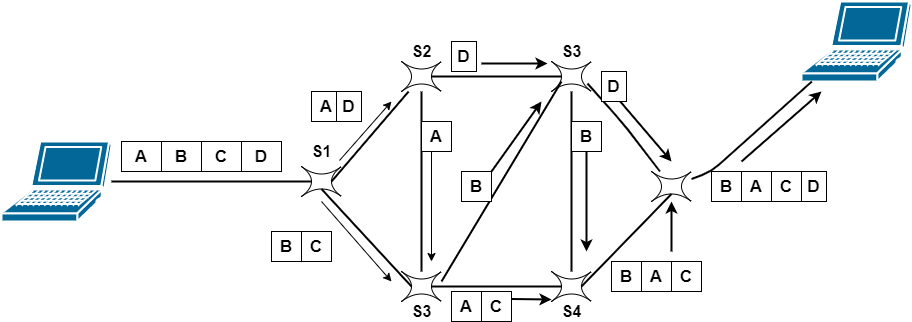


Figure: Packet Switching

Two different approaches used for Packet switching are as follows:

* Datagram Packet Switching
* Virtual Circuit Switching

**23-03-2022**

Let us discuss these two approaches one by one:

**Datagram Packet Switching**

In Datagram Switching, the packet is commonly known as a**datagram**. Datagram Packet switching is also known as Connectionless Packet Switching. In this technique, each packet routed individually by network devices on the basis of the destination address that is contained within each packet.

* Each packet is basically treated independently of all others.
* Datagram packet switching is done at the network layer.
* This is Connectionless packet switching because the packet switch does not keep the information about the connection state.
* In the Datagram packet switching the path is not fixed.
* Routing decisions are taken by the intermediate nodes in order to forward the packets.
* Thus all datagrams that belong to the same message may travel through different paths in order to reach their destination.
* On the receiving node, all the packets are reassembled to get the message in the original form.
* Due to lack of resources packets may also be lost or dropped.
* In most of the protocols, it is the responsibility of the upper-layer protocol to reorder the datagrams or to ask for the lost datagrams before passing them on to the application.

**Virtual Circuit Switching**

Virtual Circuit Switching is also known as Connection-Oriented Switching. This switching contains the characteristics of circuit switching as well as datagram packet switching. In this type of packet switching the data-packets are first assembled and then sequentially numbered. Now they are ready to travel across a predefined route, sequentially. The information about the address is not required here, because all the data packets are sent in sequence.

* In addition to the data transfer phase, there are setup and teardown phases.
* The resource allocation is done during the setup phase like it is done in the circuit-switched network or it can be done on demand like in datagram networks.
* The data is in the form of packets like the datagram network and also each packet carries the destination address in the header.
* Like the circuit-switched network, all packets in the Virtual network follows the same path that is established during the connection.
* This switching is normally implemented in the data link layer.

**Advantages of Packet Switching**

Given below are some benefits of the Packet Switching:

* More efficient utilization of bandwidth.
* Latency in the transmission is minimum in packet switching.
* This technique is cheaper to implement and thus it is cost-effective.
* The same channel can be used by many users simultaneously.
* As there are improved protocols, thus packet switching is used by many applications like Skype, WhatsApp, etc.
* The fault tolerance in this technique is more in case of any link down because packets may follow different paths.
* This technique is more reliable than other techniques because it can easily detect missing packets.

**Disadvantages of Packet Switching**

Some of the drawbacks of Packet Switching are as follows:

* This technique cannot be used by those applications that cannot afford more delays like applications of high-quality voice calls.
* Protocols used in this technique are complex and thus their implementation cost is high.
* In the case of an overloaded network, the packet may get lost or there might occur delay which causes the loss of critical information.
* On the receiver's side sorting of the packets sent by the sender is required.

# Difference between Circuit Switching and Packet Switching

|  |  |
| --- | --- |
| **Circuit Switching** | **Packet Switching** |
| In circuit switching there are 3 phases:  i) Connection Establishment.  ii) Data Transfer.  iii) Connection Released. | In Packet switching directly data transfer takes place. |
| In circuit switching, each data unit know the entire path address which is provided by the source. | In Packet switching, each data unit just know the final destination address intermediate path is decided by the routers. |
| In Circuit switching, data is processed at source system only | In Packet switching, data is processed at all intermediate node including source system. |
| Delay between data units in circuit switching is uniform. | Delay between data units in packet switching is not uniform. |
| Resource reservation is the feature of circuit switching because path is fixed for data transmission. | There is no resource reservation because bandwidth is shared among users. |
| Circuit switching is more reliable. | Packet switching is less reliable. |
| Wastage of resources are more in Circuit Switching | Less wastage of resources as compared to Circuit Switching |
| It is not a store and forward technique. | It is a store and forward technique. |
| Transmission of the data is done by the source. | Transmission of the data is done not only by the source, but also by the intermediate routers. |
| Congestion can occur during the connection establishment phase, because there might be a case where a request is being made for a channel but the channel is already occupied. | Congestion can occur during data transfer phase, large number of packets comes in no time. |
| Circuit switching is not convenient for handling bilateral traffic. | Packet switching is suitable for handling bilateral traffic. |
| In Circuit switching, charge depend on time and distance, not on traffic in the network. | In Packet switching, charge is based on the number of bytes and connection time. |
| Recording of packet is never possible in circuit switching. | Recording of packet is possible in packet switching. |
| In Circuit Switching there is a physical path between the source and the destination | In Packet Switching there is no physical path between the source and the destination |
| Circuit Switching does not support store and forward transmission | Packet Switching supports store and forward transmission |

**1.6 Protocols and standards**

**Protocols**

In Computer Networks, basically, communication occurs between entities in different systems. An entity is anything that is capable of sending or receiving information. Any two entities cannot simply send bitstreams to each other and expect to be understood.

The entities must need to agree on a protocol in order of occurrence of the communication.

A Protocol is a set of rules that mainly govern data communications. The protocol mainly defines what is communicated, how it is communicated, and when it is communicated.

**Levels of a Protocol**

There are mainly three levels of a protocol, they are as follows:

1. **Hardware Level:**In this level, the protocol enables the hardware devices to connect and communicate with each other for various purposes.
2. **Software Level:**In the software level, the protocol enables different software to connect and communicate with each other to work collaboratively.
3. **Application Level:**In this level, the protocol enables the application programs to connect and communicate with each other for various purposes.

**Key Elements of protocols​**

The key elements of the protocol determine what to be communicated, how it is communicated, and when it is communicated.

There are mainly three key elements of a protocol, they are as follows:

1. **Syntax**
2. **Semantics**
3. **Timing**

Let's learn these elements in detail.

***Syntax​***

Syntax refers to the structure or format of data and signal levels. It indicates how to read the data in the form of bits or fields. It also decides the order in which the data is presented to the receiver.

**Example:** A protocol might expect that the size of a data packet will be 16 bits. In which, the first 4 bits are the sender’s address, the next 4 bits are the receiver’s address, the next 4 bits are the check-sum bits, and the last 4 bits will contain the message. So, every communication that is following that protocol should send 16-bit data.

***Semantics​***

Semantics refers to the interpretation or meaning of each section of bits or fields. It specifies which field defines what action. It defines how a particular section of bits or pattern can be interpreted, and what action needs to be taken. It includes control information for coordination and error handling.

**Example:** It interprets whether the bits of address identify the route to be taken or the final destination of the message or something else.

***Timing​***

Timing refers to two characteristics:

1. when the data should be sent?
2. what will be the speed of sending and receiving the data?

It performs speed matching, sequencing and flow control of the data items.

**Example:** A sender can send the data at a speed of 100 Mbps, but the receiver can consume it only at a speed of 20 Mbps, then there may be data losses or the packets might get dropped. So, proper synchronization must be there between a sender and a receiver.

**Characteristics of Protocols**

Refer PPT

**Functions of protocols**

Following are the main functionalities of a protocol:

* **Data Sequencing:**It mainly refers to dive data into packets i.e. it divided the whole data into some packets.
* **Data Flow​:**It mainly deals with sending data to the correct destination i.e. the flow of the data is correct or not.
* **Data Routing​:**It refers to select the best path for data transmission between a sender and a receiver because there can be many routes from sender to receiver and you should select the best possible route.
* **Encapsulation​:**It refers to the process of taking one protocol and transferring it to some other another protocol.
* **Segmentation & Reassembly​:**It deals with segmenting the data message i.e. diving the data into packets when data flows from the upper protocol layer to lower, and reassembly is vice-versa of segmentation i.e. all the segmented packets are recollected in the correct order at the receiver side.
* **Connection Control​:** It ensures connection oriented data transfer for lengthy data items.
* **Multiplexing​:** ​ It allows combining multiple transmission unit signals or channels of higher-level protocols in one transmission unit of a lower-level protocol. Multiplexing can be upward or downward.
* **Ordered Delivery​:** ​ Protocol facilitates ordered delivery of data, by providing a unique sequence number to each data packet. It is the function of the sender to maintain ordered delivery. By doing so, the receiver will receive the data in the same order as sent by the sender.
* **Transmission Services​: ​** It mainly deals with priority, Quality of Service (QoS), and security of data packets.
* **Addressing​:** ​ It mainly deals with addressing levels, addressing scope, communication identifiers, and addressing modes.
* **Flow Control​:** ​ It facilitates to limit the flow of data. It is the function of the receiver's end to maintain flow control of data.
* **Error Control​:** It deals with error detection (using the checksum bits) and its control. If any error is detected during the transmission of the data, a request for retransmission of data is sent to the sender by the receiver, and the corrupt data packet is discarded.

**Standard Organizations**

Data communication standards fall into two categories: *de facto*( meaning "by fact" or "by convention") and *de jure*(meaning "by law" and "by regulation").

* **De facto.**Standards that have not been approved by an organized body but have been adopted as standards through widespread use are **de facto standards.**De facto standards are often established originally by manufacturers that seek to define the functionality of a new product or technology.
* **De jure. De jure standards**are those that have been legislated by an oficially recognized body.

Standards are mainly developed through the cooperation of Standard creation committees, government regulatory agencies, and forums.

Some Standard Creation committees are :

* International Organization of Standardization(ISO)
* American National Standards Institute(ANSI)
* Electronic Industries Association(EIA)
* Institute of Electrical and Electronics Engineers(IEEE)

**Forums**  
Telecommunications technology development is moving faster than the ability of standards committee to ratify standards. Standards committees are procedural bodies and by nature slow moving. to accommodate the need from working models and agreements  and to facilitate the standardization process, many special-interest groups have developed *forums*made up of representatives from interested corporations. The forums work with universities and users to test, evaluate and standardize new technologies.  By concentrating their efforts on a particular technology, the forums are able to speed acceptance and use of those technologies in the telecommunications community. The forums present their conclusions to the standards bodies. Some important forums for the telecommunications industry include the following:

* **Frame Relay Forum.**The Frame Relay Forum was formed by digital equipment Corporation, Northern Telecom, Cisco, and StrataCom to promote the acceptance and implementation of frame relay. Today, it has around 40 members representing North America, Europe, and the Pacific Rim. Issues under Review include flow control. Encapsulation, translation, and multicasting. The forum's results are submitted to the ISO.
* **ATM Forum.**[**http://www.atmforum.com/**](http://www.atmforum.com/)The ATM Forum provides acceptance and use of Asynchronous Transfer Mode (ATM) technology. The ATM Forum is made up of Customer Premises Equipment (e.g., PBX systems) vendors and Central Office (e.g., telephone exchange) providers. It is concerned with the standardization of service to ensure interoperability.

**Regulatory Agencies**

All communications technology is subject to regulation by government agencies such as Federal Communication Commission in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications.

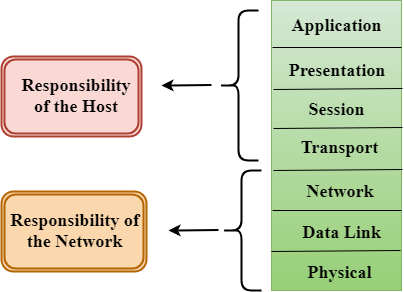
* **Federal Communications Commission (FCC).**[**http://www.fcc.gov/**](http://www.fcc.gov/)The Federal Communications Commission (FCC) has authority over interstate and international commerce as it relates to communications.

**1.7 Layers in the OSI model**

**OSI Model**

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

**Characteristics of OSI Model:**

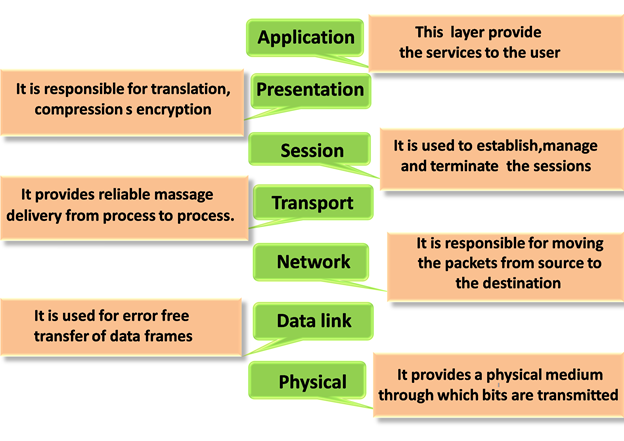


* The OSI model is divided into two layers: upper layers and lower layers.
* The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software. The application layer is closest to the end user. Both the end user and the application layer interact with the software applications. An upper layer refers to the layer just above another layer.
* The lower layer of the OSI model deals with the data transport issues. The data link layer and the physical layer are implemented in hardware and software. The physical layer is the lowest layer of the OSI model and is closest to the physical medium. The physical layer is mainly responsible for placing the information on the physical medium.

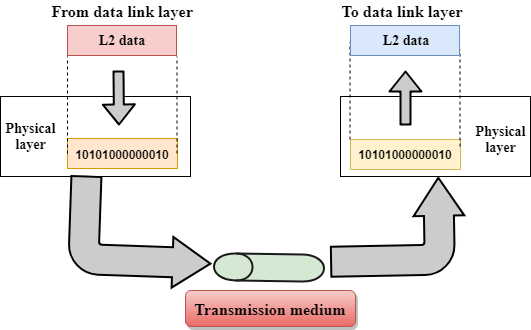
**Functions of the OSI Layers**

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

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



**Physical layer**

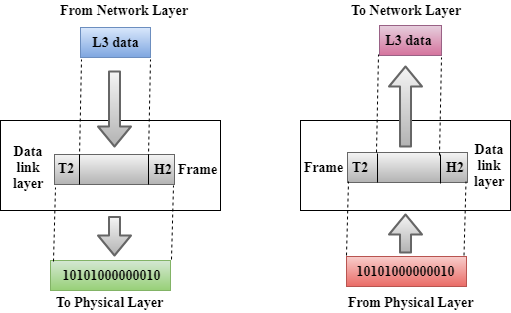


* The main functionality of the physical layer is to transmit the individual bits from one node to another node.
* It is the lowest layer of the OSI model.
* It establishes, maintains and deactivates the physical connection.
* It specifies the mechanical, electrical and procedural network interface specifications.

**Functions of a Physical layer:**

* **Line Configuration:** It defines the way how two or more devices can be connected physically.
* [**Data Transmission**](https://www.javatpoint.com/computer-network-transmission-modes)**:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
* [**Topology**](https://www.javatpoint.com/computer-network-topologies)**:** It defines the way how network devices are arranged.
* **Signals:** It determines the type of the signal used for transmitting the information.

**Data-Link Layer**



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

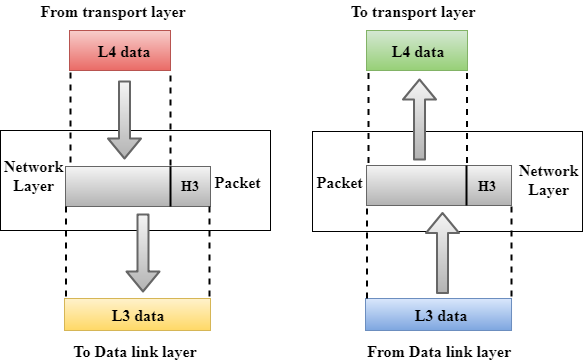
**Functions of the Data-link layer**

* **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.

OSI Model

* **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.
* **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.
* **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occurr, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
* **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

**Network Layer**

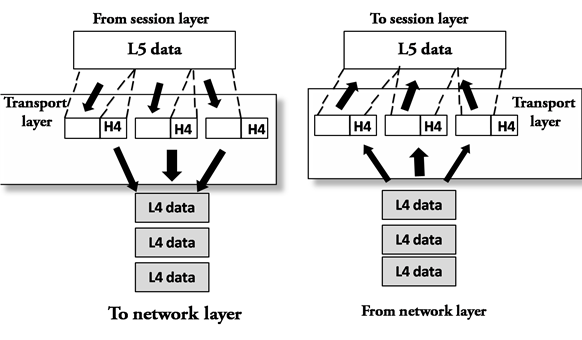


* It is a layer 3 that manages device addressing, tracks the location of devices on the network.
* It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
* The Data link layer is responsible for routing and forwarding the packets.
* Routers are the layer 3 devices, they are specified in this layer and used to provide the routing services within an internetwork.
* The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

**Functions of Network Layer:**

* **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
* [**Addressing**](https://www.javatpoint.com/network-addressing)**:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.
* [**Routing**](https://www.javatpoint.com/computer-network-routing)**:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
* **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).

**Transport Layer**



* The Transport layer is a Layer 4 ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
* The main responsibility of the transport layer is to transfer the data completely.
* It receives the data from the upper layer and converts them into smaller units known as segments.
* This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

**30-03-2022**

**The two protocols used in this layer are:**

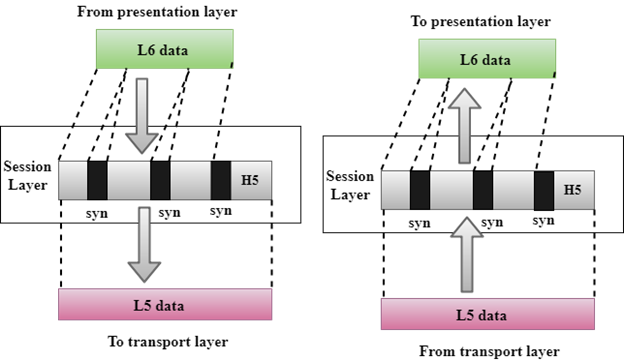
* **Transmission Control Protocol**
  + It is a standard protocol that allows the systems to communicate over the internet.
  + It establishes and maintains a connection between hosts.
  + When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments. Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.
* **User Datagram Protocol**
  + User Datagram Protocol is a transport layer protocol.
  + It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

**Functions of Transport Layer:**

* **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process. The transport layer adds the header that contains the address known as a service-point address or port address. The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.
* **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments, and each segment is assigned with a sequence number that uniquely identifies each segment. When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.
* **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service. A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination. A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets. In connection-oriented service, all the packets travel in the single route.
* **Flow control:** The transport layer also responsible for flow control but it is performed end-to-end rather than across a single link.
* **Error control:** The transport layer is also responsible for Error control. Error control is performed end-to-end rather than across the single link. The sender transport layer ensures that message reach at the destination without any error.

**Session Layer**

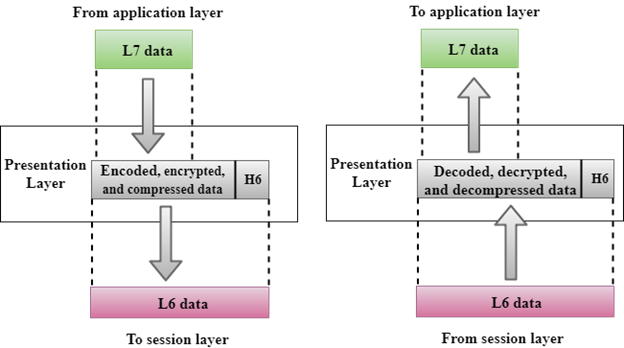
* It is a layer 5 in the OSI model.
* The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.



**Functions of Session layer:**

* **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
* **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

**Presentation Layer**

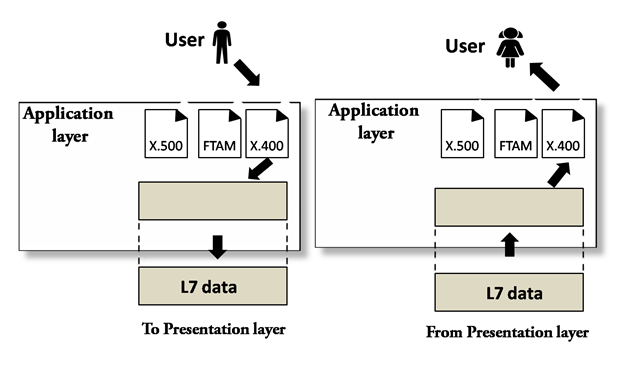


* A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
* It acts as a data translator for a network.
* This layer is a part of the operating system that converts the data from one presentation format to another format.
* The Presentation layer is also known as the syntax layer.

**Functions of Presentation layer:**

* **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on. Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods. It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.
* **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
* **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.

**Application Layer**



* An application layer serves as a window for users and application processes to access network service.
* It handles issues such as network transparency, resource allocation, etc.
* An application layer is not an application, but it performs the application layer functions.
* This layer provides the network services to the end-users.

**Functions of Application layer:**

* **File transfer, access, and management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
* **Mail services:** An application layer provides the facility for email forwarding and storage.
* **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.

| **Layer** | **Name** | **Function** | **Protocols** |
| --- | --- | --- | --- |
| Layer 7 | Application | To allow access to network resources. | SMTP, HTTP, FTP, POP3, SNMP |
| Layer 6 | Presentation | To translate, encrypt and compress data. | MPEG, ASCH, SSL, TLS |
| Layer 5 | Session | To establish, manage, and terminate the session | NetBIOS, SAP |
| Layer 4 | Transport | The transport layer builds on the network layer to provide data transport from a process on a source machine to a process on a destination machine. | TCP, UDP |
| Layer 3 | Network | To provide internetworking. To move packets from source to destination | IPV5, IPV6, ICMP, IPSEC, ARP, MPLS. |
| Layer 2 | Data Link | To organize bits into frames. To provide hop-to-hop delivery | RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc. |
| Layer 1 | Physical | To transmit bits over a medium. To provide mechanical and electrical specifications | RS232, 100BaseTX, ISDN, 11. |

**1.8 TCP/IP model**

* The TCP/IP model was developed prior to the OSI model.
* The TCP/IP model is not exactly similar to the OSI model.
* The TCP/IP model consists of five layers: the application layer, transport layer, network layer, data link layer and physical layer.
* The first four layers provide physical standards, network interface, internetworking, and transport functions that correspond to the first four layers of the OSI model and these four layers are represented in TCP/IP model by a single layer called the application layer.
* TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

Here, hierarchical means that each upper-layer protocol is supported by two or more lower-level protocols.

**Functions of TCP/IP layers:**



**Network Access Layer**

* A network layer is the lowest layer of the TCP/IP model.
* A network layer is the combination of the Physical layer and Data Link layer defined in the OSI reference model.
* It defines how the data should be sent physically through the network.
* This layer is mainly responsible for the transmission of the data between two devices on the same network.
* The functions carried out by this layer are encapsulating the IP datagram into frames transmitted by the network and mapping of IP addresses into physical addresses.
* The protocols used by this layer are ethernet, token ring, FDDI, X.25, frame relay.

**Internet Layer**

* An internet layer is the second layer of the TCP/IP model.
* An internet layer is also known as the network layer.
* The main responsibility of the internet layer is to send the packets from any network, and they arrive at the destination irrespective of the route they take.

Following are the protocols used in this layer are:

**IP Protocol:** IP protocol is used in this layer, and it is the most significant part of the entire TCP/IP suite.

Following are the responsibilities of this protocol:

* **IP Addressing:** This protocol implements logical host addresses known as IP addresses. The IP addresses are used by the internet and higher layers to identify the device and to provide internetwork routing.
* **Host-to-host communication:** It determines the path through which the data is to be transmitted.
* **Data Encapsulation and Formatting:** An IP protocol accepts the data from the transport layer protocol. An IP protocol ensures that the data is sent and received securely, it encapsulates the data into message known as IP datagram.
* **Fragmentation and Reassembly:** The limit imposed on the size of the IP datagram by data link layer protocol is known as Maximum Transmission unit (MTU). If the size of IP datagram is greater than the MTU unit, then the IP protocol splits the datagram into smaller units so that they can travel over the local network. Fragmentation can be done by the sender or intermediate router. At the receiver side, all the fragments are reassembled to form an original message.
* **Routing:** When IP datagram is sent over the same local network such as LAN, MAN, WAN, it is known as direct delivery. When source and destination are on the distant network, then the IP datagram is sent indirectly. This can be accomplished by routing the IP datagram through various devices such as routers.

**ARP Protocol**

* ARP stands for **Address Resolution Protocol**.
* ARP is a network layer protocol which is used to find the physical address from the IP address.
* **The two terms are mainly associated with the ARP Protocol:**
  + **ARP request:** When a sender wants to know the physical address of the device, it broadcasts the ARP request to the network.
  + **ARP reply:** Every device attached to the network will accept the ARP request and process the request, but only recipient recognize the IP address and sends back its physical address in the form of ARP reply. The recipient adds the physical address both to its cache memory and to the datagram header

**ICMP Protocol**

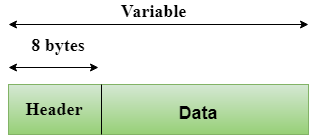
* **ICMP** stands for Internet Control Message Protocol.
* It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
* A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because of some unusual conditions such as disabled links, a device is on fire or network congestion, then the ICMP protocol is used to inform the sender that the datagram is undeliverable.
* An ICMP protocol mainly uses two terms:
  + **ICMP Test:** ICMP Test is used to test whether the destination is reachable or not.
  + **ICMP Reply:** ICMP Reply is used to check whether the destination device is responding or not.
* The core responsibility of the ICMP protocol is to report the problems, not correct them. The responsibility of the correction lies with the sender.
* ICMP can send the messages only to the source, but not to the intermediate routers because the IP datagram carries the addresses of the source and destination but not of the router that it is passed to.

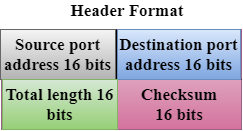
**Transport Layer**

The transport layer is responsible for the reliability, flow control, and correction of data which is being sent over the network.

The two protocols used in the transport layer are **User Datagram protocol and Transmission control protocol**.

* **User Datagram Protocol (UDP)**
  + It provides connectionless service and end-to-end delivery of transmission.
  + It is an unreliable protocol as it discovers the errors but not specify the error.
  + User Datagram Protocol discovers the error, and ICMP protocol reports the error to the sender that user datagram has been damaged.
  + **UDP consists of the following fields:**  
    **Source port address:** The source port address is the address of the application program that has created the message.  
    **Destination port address:** The destination port address is the address of the application program that receives the message.  
    **Total length:** It defines the total number of bytes of the user datagram in bytes.  
    **Checksum:** The checksum is a 16-bit field used in error detection.
  + UDP does not specify which packet is lost. UDP contains only checksum; it does not contain any ID of a data segment.





* **Transmission Control Protocol (TCP)**
  + It provides a full transport layer services to applications.
  + It creates a virtual circuit between the sender and receiver, and it is active for the duration of the transmission.
  + TCP is a reliable protocol as it detects the error and retransmits the damaged frames. Therefore, it ensures all the segments must be received and acknowledged before the transmission is considered to be completed and a virtual circuit is discarded.
  + At the sending end, TCP divides the whole message into smaller units known as segment, and each segment contains a sequence number which is required for reordering the frames to form an original message.
  + At the receiving end, TCP collects all the segments and reorders them based on sequence numbers.

**Application Layer**

* An application layer is the topmost layer in the TCP/IP model.
* It is responsible for handling high-level protocols, issues of representation.
* This layer allows the user to interact with the application.
* When one application layer protocol wants to communicate with another application layer, it forwards its data to the transport layer.
* There is an ambiguity occurs in the application layer. Every application cannot be placed inside the application layer except those who interact with the communication system. For example: text editor cannot be considered in application layer while web browser using **HTTP** protocol to interact with the network where **HTTP** protocol is an application layer protocol.

Following are the main protocols used in the application layer:

* **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the World Wide Web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there are rapid jumps from one document to another.
* **SNMP:** SNMP stands for Simple Network Management Protocol. It is a framework used for managing the devices on the internet by using the TCP/IP protocol suite.
* **SMTP:** SMTP stands for Simple mail transfer protocol. The TCP/IP protocol that supports the e-mail is known as a Simple mail transfer protocol. This protocol is used to send the data to another e-mail address.
* **DNS:** DNS stands for Domain Name System. An IP address is used to identify the connection of a host to the internet uniquely. But, people prefer to use the names instead of addresses. Therefore, the system that maps the name to the address is known as Domain Name System.
* **TELNET:** It is an abbreviation for Terminal Network. It establishes the connection between the local computer and remote computer in such a way that the local terminal appears to be a terminal at the remote system.
* **FTP:** FTP stands for File Transfer Protocol. FTP is a standard internet protocol used for transmitting the files from one computer to another computer.

Some important differences between the OSI & TCP/IP model:

| **OSI Model** | **TCP/IP model** |
| --- | --- |
| OSI model provides a clear distinction between interfaces, services, and protocols. | TCP/IP doesn’t offer any clear distinguishing points between services, interfaces, and protocols. |
| OSI uses the network layer to define routing standards and protocols. | TCP/IP uses only the Internet layer. |
| OSI model use two separate layers physical and data link to define the functionality of the bottom layers | TCP/IP uses only one layer (link). |
| OSI model, the transport layer is only connection-oriented. | A layer of the TCP/IP model is both connection-oriented and connectionless. |
| In OSI model, data link layer and physical are separate layers. | In TCP data link layer and physical layer are combined as a single host-to-network layer. |
| The minimum size of the OSI header is 5 bytes. | Minimum header size is 20 bytes. |

**1.9 Link layer protocols**

Data Link protocols are classified into three categories, as given below −

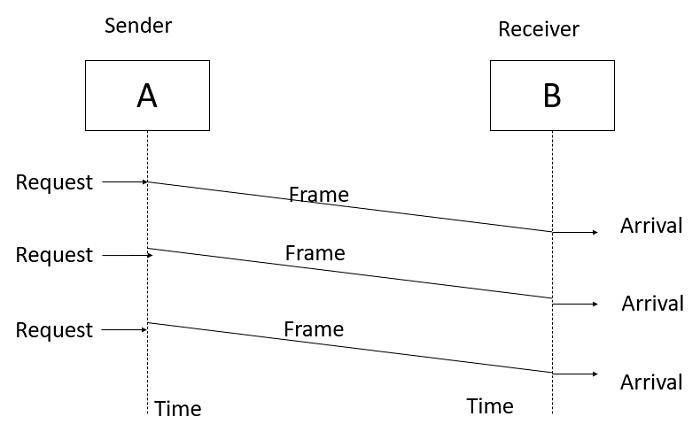
* Protocol 1 − Unrestricted simplex protocol
* Protocol 2 − Simplex stop and wait protocol
* Protocol 3 − Simplex protocol for noisy channels.

Let us discuss each protocol one by one.

**Unrestricted Simplex Protocol**

Data transmitting is carried out in one direction only. The transmission (Tx) and receiving (Rx) are always ready and the processing time can be ignored. In this protocol, infinite buffer space is available, and no errors are occurring that is no damage frames and no lost frames.

The Unrestricted Simplex Protocol is diagrammatically represented as follows −



**Simplex Stop and Wait protocol**

In this protocol we assume that data is transmitted in one direction only. No error occurs; the receiver can only process the received information at finite rate. These assumptions imply that the transmitter cannot send frames at rate faster than the receiver can process them.

The main problem here is how to prevent the sender from flooding the receiver. The general solution for this problem is to have the receiver send some sort of feedback to sender, the process is as follows −

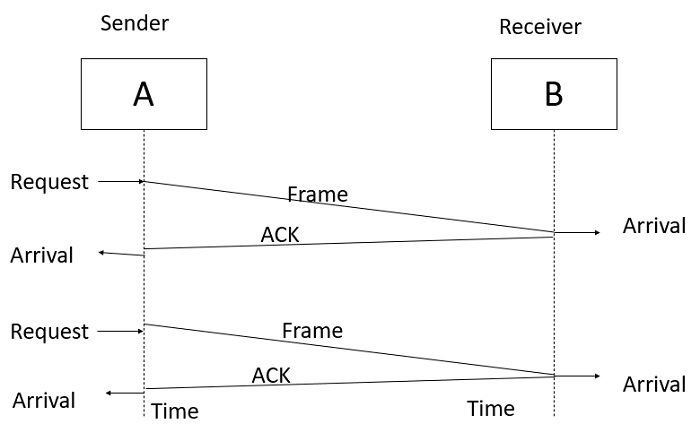
**Step1** − The receiver send the acknowledgement frame back to the sender telling the sender that the last received frame has been processed and passed to the host.

**Step 2** − Permission to send the next frame is granted.

**Step 3** − The sender after sending the sent frame has to wait for an acknowledge frame from the receiver before sending another frame.

This protocol is called Simplex Stop and wait protocol, the sender sends one frame and waits for feedback from the receiver. When the ACK arrives, the sender sends the next frame.

The Simplex Stop and Wait Protocol is diagrammatically represented as follows −

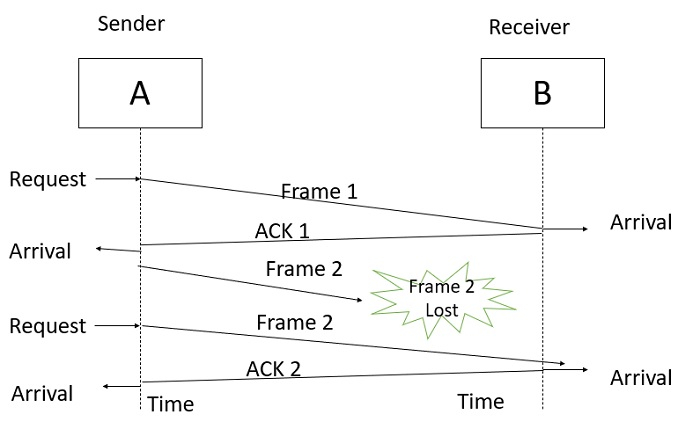


**Simplex Protocol for Noisy Channel**

Data transfer is only in one direction, consider separate sender and receiver, finite processing capacity and speed at the receiver, since it is a noisy channel, errors in data frames or acknowledgement frames are expected. Every frame has a unique sequence number.

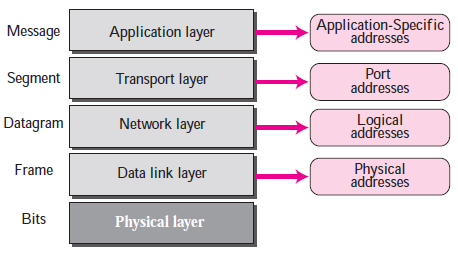
After a frame has been transmitted, the timer is started for a finite time. Before the timer expires, if the acknowledgement is not received , the frame gets retransmitted, when the acknowledgement gets corrupted or sent data frames gets damaged, how long the sender should wait to transmit the next frame is infinite.

The Simplex Protocol for Noisy Channel is diagrammatically represented as follows −



**Discuss the different types of addresses used in the TCP/IP protocol.**

Four levels of addresses are used in the TCP/IP protocol: **physical address, logical address, port address, and application-specific address** as shown in Figure.



**Physical Addresses**

* The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN.
* The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address.
* Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network.
* Example: Most local area networks use a 48-bit (6-byte) physical address written as 12 hexadecimal digits; every byte (2 hexadecimal digits) is separated by a colon, as shown below: A 6-byte (12 hexadecimal digits) physical address **07:01:02:01:2C:4B**

Unicast, Multicast, and Broadcast Physical Addresses

Physical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (to be received by all systems in the network). Some networks support all three addresses.

A source address is always a unicast address—the frame comes from only one station. The destination address, however, can be unicast, multicast, or broadcast.

The least significant bit of the first byte defines the type of address.

Q: Define the type of the following destination addresses:

1. 4A:30:10:21:10:1A

2. 47:20:1B:2E:08:EE

3. FF:FF:FF:FF:FF:FF

**Logical Addresses**

* Logical addresses are used by networking software to allow packets to be independent of the physical connection of the network, that is, to work with different network topologies and types of media.
* A logical address in the Internet is currently a 32-bit address that can uniquely define a host connected to the Internet. An internet address in IPv4 in decimal numbers **132.24.75.9**
* No two publicly addressed and visible hosts on the Internet can have the same IP address.
* The physical addresses will change from hop to hop, but the logical addresses remain the same.
* The logical addresses can be either unicast (one single recipient), multicast (a group of recipients), or broadcast (all systems in the network). There are limitations on broadcast addresses.

**Port Addresses**

* There are many application running on the computer. Each application run with a port no.(logically) on the computer.
* A port number is part of the addressing information used to identify the senders and receivers of messages.
* Port numbers are most commonly used with TCP/IP connections.
* These port numbers allow different applications on the same computer to share network resources simultaneously.
* The physical addresses change from hop to hop, but the logical and port addresses usually remain the same.
* Example: a port address is a 16-bit address represented by one decimal number **753**

**Application-Specific Addresses**

* Some applications have user-friendly addresses that are designed for that specific application.
* Examples include the e-mail address (for example, forouzan@fhda.edu) and the Universal Resource Locator (URL) (for example, www.mhhe.com). The first defines the recipient of an e-mail; the second is used to find a document on the World Wide Web.