**Data Communication**

When we communicate, we are sharing information. This sharing can be local or remote, between individuals, local communication usually occurs face to face, while remote communication takes place over distance. The term ***telecommunication,*** which includes telephony, telegraphy, and television, means communication at a distance *(tele* is Greek for “far”).

The word *data* refers to information presented in whatever form is agreed upon by the parties creating and using the data. Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable. For data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs). The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness, and jitter.

1. . **Delivery.** The system must deliver data to the correct destination. Data must be

received by the intended device or user and only by that device or user.

* 1. **Accuracy.** The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
  2. **Timeliness.** The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called *real-time* transmission.
  3. **Jitter.** Jitter refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 30 ms. If some of the packets arrive with 30-ms delay and others with 40-ms delay, an uneven quality in the video is the result.

Components

A data communications system has five components (see Figure 1.1).

* 1. *Five components of data communication*



Protocol p ¢



Message

Medium

Rule 1:

Rule 2:

Rule n:

Rule 1 i Rule 2•

Rule ai

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

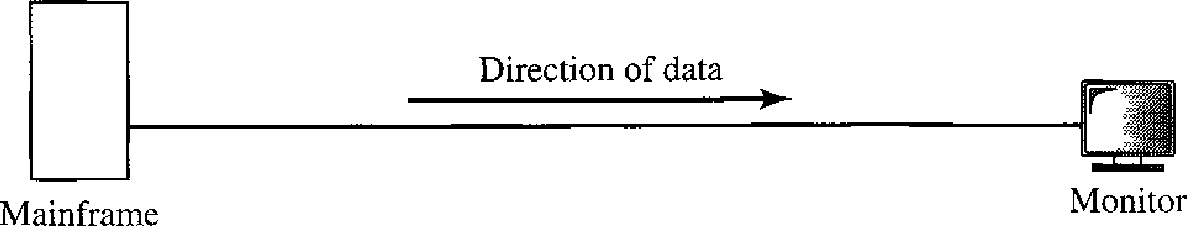
1. Sender. The sender is the device that sends the data message. It can be a com- puter, workstation, telephone handset, video camera, and so on.
2. Receiver. The receiver is the device that receives the message. It can be a com- puter, workstation, telephone handset, television, and so on.
3. Transmission 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.

Data Flow

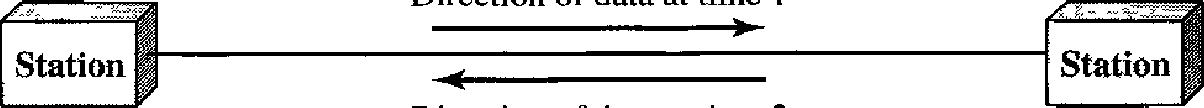
Communication between two devices can be simplex, half-duplex, or full-duplex as

shown in Figure 1.2.

Figure 1.2 *Data flow (simplex, half-duplex, and full-duplex)*



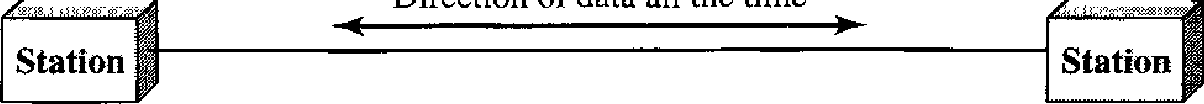
* 1. Simplex



Direction of data at time 1

Direction of data at time 2

* 1. Half-duplex



Direction of data all the time

Station

* 1. Full-duplex

***Simplex***

In simplex mode, the communication is unidirectional, as on a one-way street. Only one of the two devices on a link can transmit; the other can only receive (see Figure 1.2a).

Keyboards and traditional monitors are examples of simplex devices. The key- board can only introduce input; the monitor can only accept output. The simplex mode can use the entire capacity of the channel to send data in one direction.

***Half-Duplex***

In half-duplex mode, each station can both transmit and receive, but not at the same time. .

When one device is sending, the other can only receive, and vice versa (see Figure 1.2b).

Walkie-tallies and CB (citizens band) radios are both half-duplex systems.

The half-duplex mode is used in cases where there is no need for communication in both directions at the same time; the entire capacity of the channel can be utilized for each direction.

***Full-Duplex***

In **full-duplex mede** (also callcd **duplex),** both stations can transmit and receive simul- taneously (see Figure 1.2c).

The full-duplex mode is like a two-way street with traffic flowing in both direc- tions at the same time. In full-duplex mode, signals going in one direction share the capacity of the link with signals going in the other direction. This sharing can occur in two ways: Either the link must contain two physically separate t-ransmission paths, one for sending and the other for receiving; or the capacity of the channel is divided between signals traveling in both directions.

One common example of full-duplex communication is the telephone network. When two people are communicating by a telephone line, both can talk and listen at the same time.

The full-duplex mode is used when communication in both directions is required all the time. The capacity of the channel, however, must be divided between the two directions.

**The Internet**

The Internet ([contraction](https://en.wikipedia.org/wiki/Contraction_(grammar)) of interconnected network) is the global system of interconnected [computer networks](https://en.wikipedia.org/wiki/Computer_network) that use the [Internet protocol suite](https://en.wikipedia.org/wiki/Internet_protocol_suite) (TCP/IP) to link devices worldwide. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. The Internet carries a vast range of information resources and services, such as the inter-linked [hypertext](https://en.wikipedia.org/wiki/Hypertext) documents and [applications](https://en.wikipedia.org/wiki/Web_application) of the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web) (WWW), [electronic mail](https://en.wikipedia.org/wiki/Email), [telephony](https://en.wikipedia.org/wiki/Voice_over_IP), and [file sharing](https://en.wikipedia.org/wiki/File_sharing).

**NETWORKS**

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.

**Distributed Processing**

Most networks use **distributed processing,** in which a task is divided among multiple computers. Instead of one single large machine being responsible for all aspects of process, separate computers (usually a personal computer or workstation) handle a subset.

**Network Criteria**

A network must be able to meet a certain number of criteria. The most important of these are performance, reliability, and security.

***Performance***

**Performance** can be measured in many ways, including transit time and response time. Transit time is the amount of time required for a message to travel from one device to

***Reliability***

In addition to accuracy of delivery, network **reliability** is measured by the frequency of failure, the time it takes a link to recover from a failure, and the network’s robustness in a catastrophe.

***Security***

Network **security** issues include protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.

Computer networks come in many forms: Home networks, business networks, and the Internet are three common examples. Devices may use any of several different methods to connect to these (and other kinds of) networks. Three basic types of network connections exist:

**Point-to-point** connections allow one device to directly communicate with exactly one other device. For example, two phones may pair with each other to exchange contact information or pictures.

**Broadcast/multicast**connections allow a device to send one message out to the network and have copies of that message delivered to multiple recipients

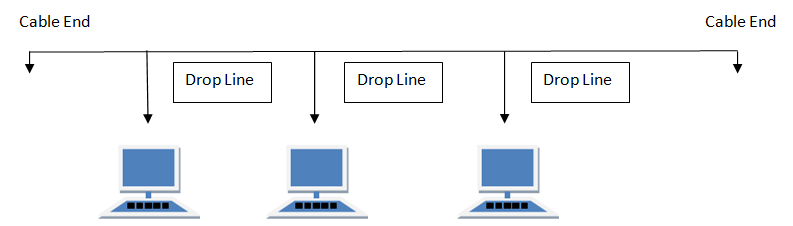
**Multipoint**connections allow one device to directly connect and deliver messages to multiple devices in parallel.

Network Topology

**Network Topology is the schematic description of a network arrangement**, connecting various nodes(sender and receiver) through lines of connection.

## **BUS Topology**

Bus topology is a network type in which every computer and network device is connected to single cable. When it has exactly two endpoints, then it is called **Linear Bus topology**.



#### Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable

#### Advantages of Bus Topology

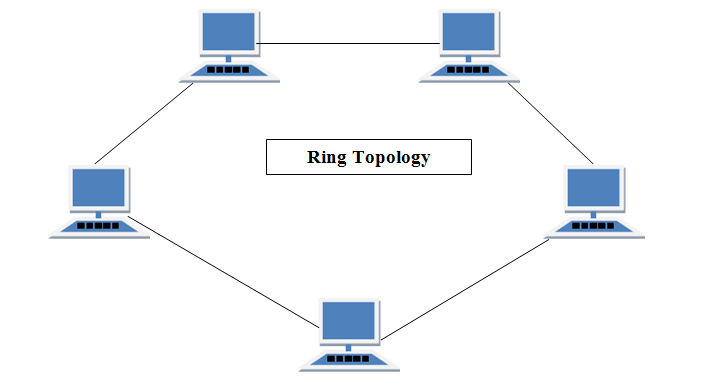
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

#### Disadvantages of Bus Topology

1. Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

## **RING Topology**

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.



#### Features of Ring Topology

1. A number of repeaters are used for Ring topology with large number of nodes, because if someone wants to send some data to the last node in the ring topology with 100 nodes, then the data will have to pass through 99 nodes to reach the 100th node. Hence to prevent data loss repeaters are used in the network.
2. The transmission is unidirectional, but it can be made bidirectional by having 2 connections between each Network Node, it is called Dual Ring Topology.
3. In Dual Ring Topology, two ring networks are formed, and data flow is in opposite direction in them. Also, if one ring fails, the second ring can act as a backup, to keep the network up.
4. Data is transferred in a sequential manner that is bit by bit. Data transmitted, has to pass through each node of the network, till the destination node.

#### Advantages of Ring Topology

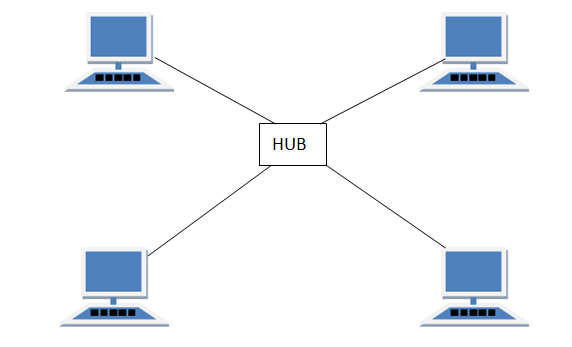
1. Transmitting network is not affected by high traffic or by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand

#### Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

## **STAR Topology**

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.



#### Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre or coaxial cable.

#### Advantages of Star Topology

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed, rest of the nodes can work smoothly.

#### Disadvantages of Star Topology

1. Cost of installation is high.
2. Expensive to use.
3. If the hub fails then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity

## **MESH Topology**

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. Mesh has n(n-1)/2 physical channels to link n devices.

There are two techniques to transmit data over the Mesh topology, they are :

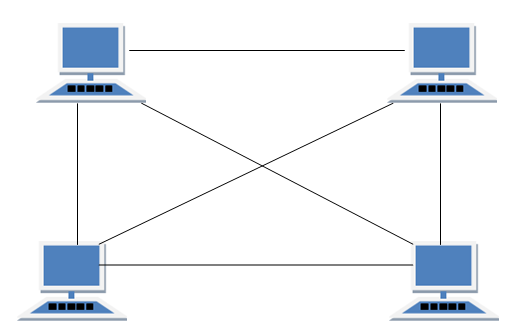
1. Routing
2. Flooding

### MESH Topology: Routing

In routing, the nodes have a routing logic, as per the network requirements. Like routing logic to direct the data to reach the destination using the shortest distance. Or, routing logic which has information about the broken links, and it avoids those node etc. We can even have routing logic, to re-configure the failed nodes.

### MESH Topology: Flooding

In flooding, the same data is transmitted to all the network nodes, hence no routing logic is required. The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.



#### Types of Mesh Topology

1. **Partial Mesh Topology :**In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.
2. **Full Mesh Topology :**Each and every nodes or devices are connected to each other.

#### Features of Mesh Topology

1. Fully connected.
2. Robust.
3. Not flexible.

#### Advantages of Mesh Topology

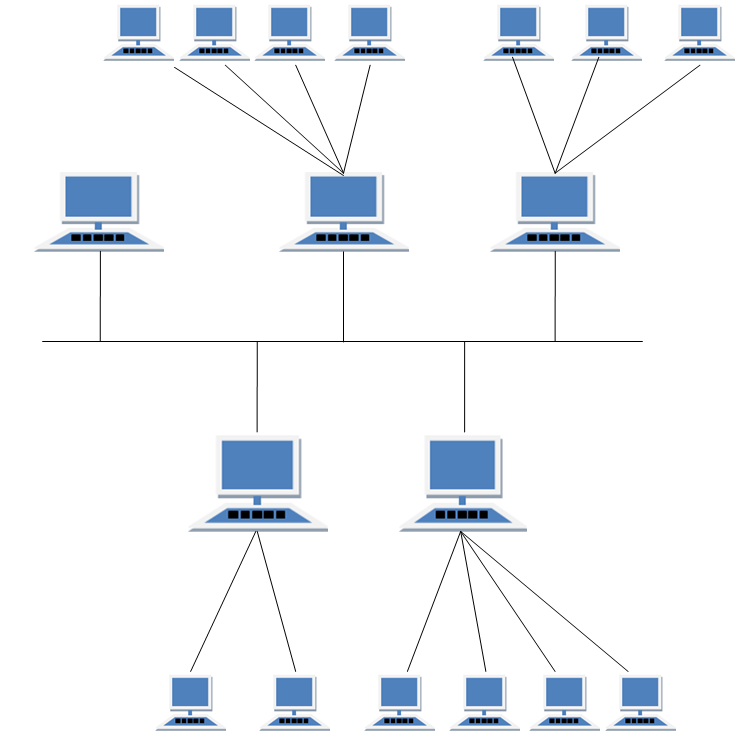
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

#### Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

## **HYBRID Topology**

It is two different types of topologies which is a mixture of two or more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).



#### Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included

#### Advantages of Hybrid Topology

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

#### Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

**PROTOCOLS AND STANDARDS**

**Protocols**

In computer networks, communication occurs between entities in different systems. An entity is anything capable of sending or receiving information. However, two entities can- not simply send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing.

O **Syntax.** The term *syntax* refers to the structure or format of the data, meaning the order in which they are presented. For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

**Semantics.** The word ***semantics*** refers to the meaning of each section of bits. How is a particular pattern to be interpreted, and what action is to be taken based on that interpretation? For example, does an address identify the route to be taken or the final destination of the message?

**Timing.** The term ***timing*** refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

Standards

**Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and in guaranteeing national and international interoperability of data and telecommunications technology and processes.**

Standards provide guidelines to manufacturers, vendors, government agencies, and other service providers to ensure the kind of interconnectivity necessary in today’s marketplace and in international communications. Data communication standards fall into two **categories: de facto (meaning “by fact” or “by convention”) and de jure (meaning “by law” or “by regulation”).**

**O 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 who seek to define the functionality of a new product or technology.

**O De jure.** Those standards that have been legislated by an officially recognized body are de jure standards.

**Standards Organizations**

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

**Standard Creation Committees**

While many organizations are dedicated to the establishment of standards, data tele- communications in North America rely primarily on those published by the following:

1. **International Organization for Standardization (ISO)**. The ISO is a multinational body whose membership is drawn mainly from the standards creation committees of various governments throughout the world. The ISO is active in developing cooperation in the realms of scientific, technological, and economic activity.
2. **International Telecommunication Union**Telecommunication Standards Sector (ITU-T). By the early 1970s, a number of countries were defining national standards for telecommunications, but there was still little international compatibility. The United Nations responded by forming, as part of its International Telecommunication Union (ITU), a committee, the Consultative Committee for International Telegraphy and Telephony (CCITT). This committee was devoted to the research and establishment of standards for telecommunications in general and for phone and data systems in particular. On March 1, 1993, the name of this committee was changed to the International Telecommunication Union— Telecommunication Standards Sector (ITU-T).
3. **American National Standards Institute (ANSI).** Despite its name, the American National Standards Institute is a completely private, nonprofit corporation not affili- ated with the U.S. federal government. However, all ANSI activities are undertaken with the welfare of the United States and its citizens occupying primary importance.
4. **Institute of Electrical and Electronics Engineers (IEEE).** The Institute of Electrical and Electronics Engineers is the largest professional engineering society in the world. International in scope, it aims to advance theory, creativity, and product quality in the fields of electrical engineering, electronics, and radio as well as in all related branches of engineering. As one of its goals, the IEEE oversees the develop- ment and adoption of international standards for computing and communications.
5. **Electronic Industries Association (EIA).** Aligned with ANSI, the Electronic Industries Association is a non profit organization devoted to the promotion of electronics manufacturing concerns. Its activities include public awareness education and lobbying efforts in addition to standards development. In the field of information technology, the EIA has made significant contributions by defining physical connec- tion interfaces and electronic signaling specifications for data communication.

**Forums**

**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.

**Regulatory Agencies**

All communications technology is subject to regulation by government agencies such as the Federal Communications Commission (FCC) in the United States. The purpose of these agencies is to protect the public interest by regulating radio, television, and wire/cable communications. The FCC has authority over interstate and international commerce as it relates to communications.

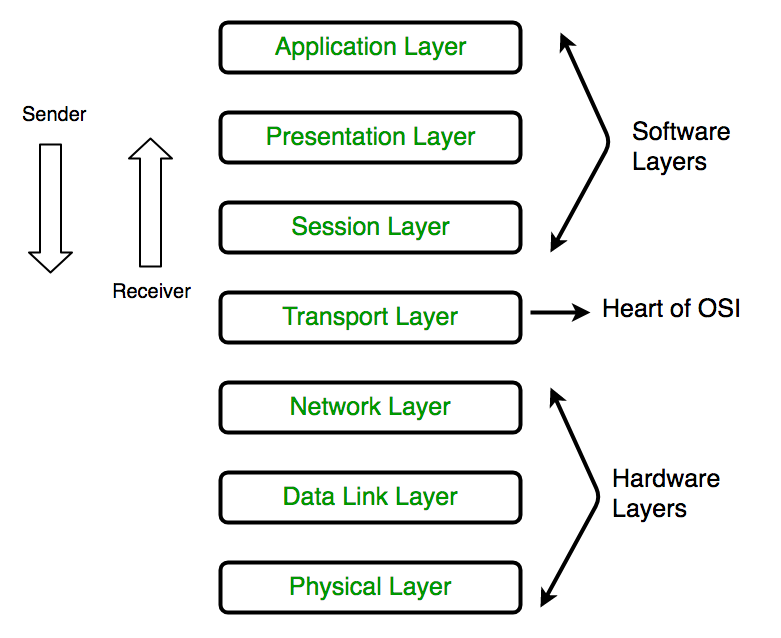
**Internet Standards**

An Internet standard is a thoroughly tested specification that is useful to and adhered to by those who work with the Internet. It is a formalized regulation that must be followed. There is a strict procedure by which a specification attains Internet standard status. A specification begins as an Internet draft. An Internet draft is a working document (a work in progress) with no official status and a 6-month lifetime. Upon recommendation from the Internet authorities, a draft may be published as a Request for Comment (RFC). Each RFC is edited, assigned a number, and made available to all interested parties. RFCs go through maturity levels and are categorized according to their requirement level.

**Network Models**

* 1. **Open Systems Interconnection(OSI Model)**

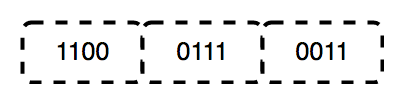
OSI stands for **Open Systems Interconnection**. It has been developed by ISO – ‘**International Organization of Standardization**‘, in the year 1974. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from 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 the actual physical connection between the devices.
* 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.



**The functions of the physical layer are :**

1. **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.
2. **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
3. **Physical topologies:** Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topology.
4. **Transmission mode:** Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

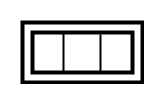
### 2. Data Link Layer (DLL) (Layer 2) :

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.  
  Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.  
  
The functions of the data Link layer are :

1. **Framing:**Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.
3. **Error control:** Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
4. **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.
5. **Access control:**When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

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

Network layer works for the transmission of data from one host to the other located in different networks.

* It 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 address are placed in the header by network layer.

The functions of the Network layer are :

1. **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.
2. **Logical Addressing:**In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver’s IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

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

Transport layer provides services to application layer and takes services from 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. Transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

**• At sender’s side:**  
Transport layer receives the formatted data from the upper layers, performs **Segmentation** and also implements **Flow & Error control** to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.  
  
**• At receiver’s side:**  
Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. **Segmentation and Reassembly:** This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.
2. **Service Point Addressing:** In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

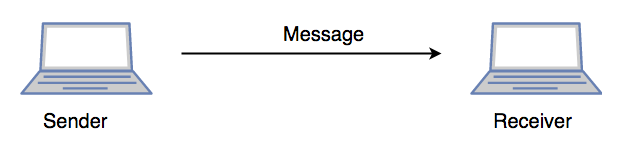
The services provided by transport layer :

1. **Connection Oriented Service:** It is a three-phase process which include  
   – Connection Establishment  
   – Data Transfer  
   – Termination / disconnection  
   In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.
2. **Connection less service:** It is a one phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection oriented Service is more reliable than connection less Service.

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

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.  
The functions of the session layer are :

1. **Session establishment, maintenance and termination:** The layer allows the two processes to establish, use and terminate a connection.
2. **Synchronization :** This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
3. **Dialog Controller :** The session layer determines which device will communicate first and the amount of data that will be sent.

application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0’s and 1’s) so that it can be transmitted.  


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

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.  
The functions of the presentation layer are :

1. **Translation :** For example, ASCII to EBCDIC.
2. **Encryption/ Decryption :** Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
3. **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 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.  
Ex: Application – Browsers, Skype Messenger etc.  
\*\*Application Layer is also called as Desktop Layer. **The functions of the Application layer are :

1. Network Virtual Terminal
2. FTAM-File transfer access and management
3. Mail Services
4. Directory Services

OSI model acts as a reference model and is not implemented in Internet because of its late invention. Current model being used is the TCP/IP model.

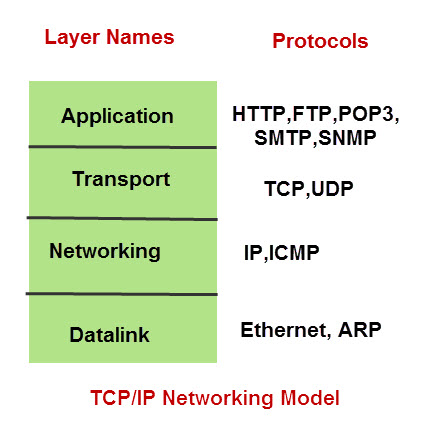
* 1. **The TCP/IP protocol suite**

The TCP/IP protocol suite ( Internet Protocol Suite) is a collection of protocols that collectively provides the data transport services used on the Internet. They provide a robust and efficient mechanism for moving data between machines across computer networks.

The suite is split into five layers

#### TCP/IP Five Layer Model

* **Application Layer** - interfaces between application processes and transport layer services on host computer.
* **Transport Layer** - determines how to use the network layer to provide a virtual point-to-point connection between source and destination.
* **Network/Internet Layer** - layer by which data packets are routed from source to destination.
* **Data Link Layer** - provides data transfer control across the physical layer
* **Physical Layer** - the actual physical medium used for the transfer (e.g. cables, Infra red and microwave)



**ARP (Address Resolution Protocol)** – used to associate an IP address with a MAC address.

IP (Internet Protocol) – used to deliver packets from the source host to the destination host based on the IP addresses.

**ICMP (Internet Control Message Protocol)** – used to detects and reports network error conditions. Used in ping.

**TCP (Transmission Control Protocol)** – a connection-oriented protocol that enables reliable data transfer between two computers.

**UDP (User Datagram Protocol)** – a connectionless protocol for data transfer. Since a session is not created before the data transfer, there is no guarantee of data delivery.

**FTP (File Transfer Protocol)** – used for file transfers from one host to another.

Telnet (Telecommunications Network) – used to connect and issue commands on a remote computer.

**DNS (Domain Name System)** – used for host names to the IP address resolution.

HTTP (Hypertext Transfer Protocol) – used to transfer files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web.

**ADDRESSING**

Four levels of addresses are used in an internet employing the TCP/IP protocols:

Physical address, logical address, port address, and application-specific address.

Physical Addresses: The physical address, also known as the link address, is the address of a node as defined by its LAN or WAN. It is included in the frame used by the data link layer. It is the lowest-level address. The size and format of these addresses vary depending on the network. For example, Ethernet uses a 6-byte (48-bit) physical address that is imprinted on the network interface card (NIC).

Logical Addresses: Logical addresses are necessary for universal communications that are independent of underlying physical networks. Physical addresses are not adequate in an internetwork environment where different networks can have different address formats. A universal addressing system is needed in which each host can be identified uniquely, regardless of the underlying physical network. The logical addresses are designed for this purpose. A logical address in the Internet is currently a 32- bit address that can uniquely define a host connected to the Internet. No two publicly addressed and visible hosts on the Internet can have the same IP address.

Port Addresses The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host. However, arrival at the destination host is not the final objective of data communications on the Internet. Computers are devices that can run multiple processes at the same time. The end objective of Internet communication is a process communicating with another process. For example, computer A can communicate with computer C by using TELNET. At the same time, computer A communicates with computer B by using the File Transfer Protocol (FTP). For these processes to receive data simultaneously, we need a method to label the different processes. In other words, they need addresses. In the TCP/IP architecture, the label assigned to a process is called a port address. A port address in TCP/IP is 16 bits in length.

Application-Specific Addresses Some applications have user-friendly addresses that are designed for that specific application. Examples include the e-mail address (for example, co\_sci@yahoo.com) 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. These addresses, however, get changed to the corresponding port and logical addresses by the sending computer.