UNIT 1 (PART 1)

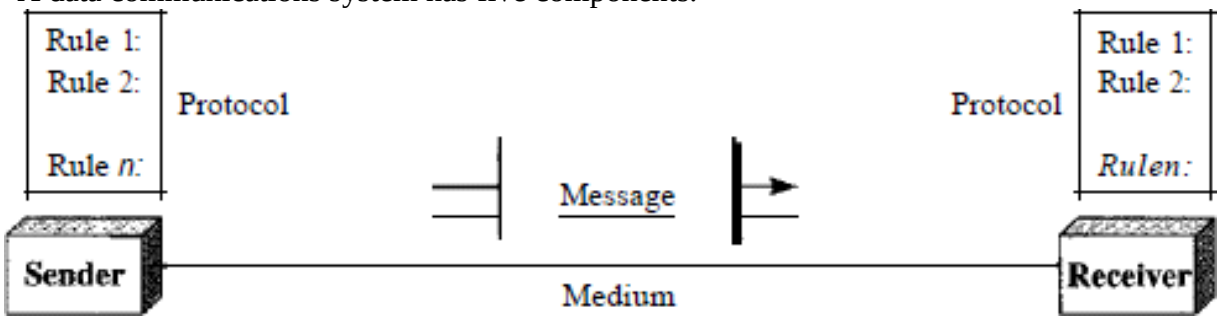
1. DATA COMMUNICATIONS : Components, Data Representation, Data Flow

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.

Components:

A data communications system has five components.



- Message. The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
- Sender. The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
- Receiver. The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
- Transmission 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
- 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.

Data Representation:

Information today comes in different forms such as text, numbers, images, audio, and video.

Text:

In data communications, text is represented as a bit pattern, a sequence of bits (Os or Is). Different sets of bit patterns have been designed to represent text symbols. Each set is called a code, and the process of representing symbols is called coding. Today, the prevalent coding system is called Unicode, which uses 32 bits to represent a symbol or character used in any language in the world. The American Standard Code for Information Interchange (ASCII), developed some decades ago in the United States, now constitutes the first 127 characters in Unicode and is also referred to as Basic Latin.

Numbers:

Numbers are also represented by bit patterns. However, a code such as ASCII is not used to represent numbers; the number is directly converted to a binary number to simplify mathematical operations. Appendix B discusses several different numbering systems.

Images:

Images are also represented by bit patterns. In its simplest form, an image is composed of a matrix of pixels (picture elements), where each pixel is a small dot

Audio:

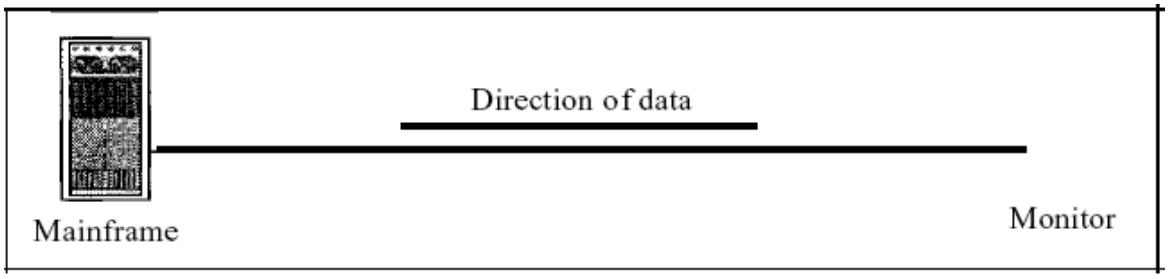
Audio refers to the recording or broadcasting of sound or music. Audio is by nature different from text, numbers, or images. It is continuous, not discrete

Video:

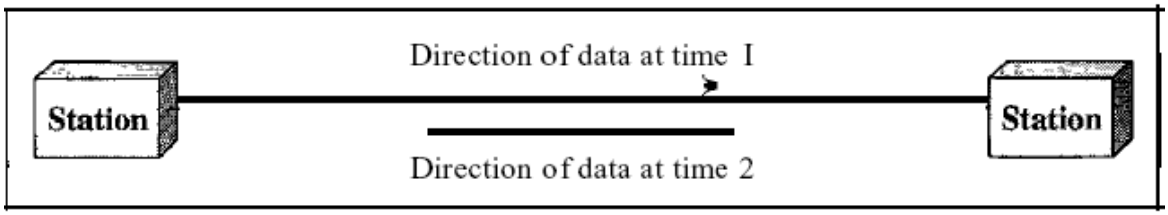
Video refers to the recording or broadcasting of a picture or movie. Video can either be produced as a continuous entity (e.g., by a TV camera), or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion. Again we can change video to a digital or an analog signal.

Data Flow

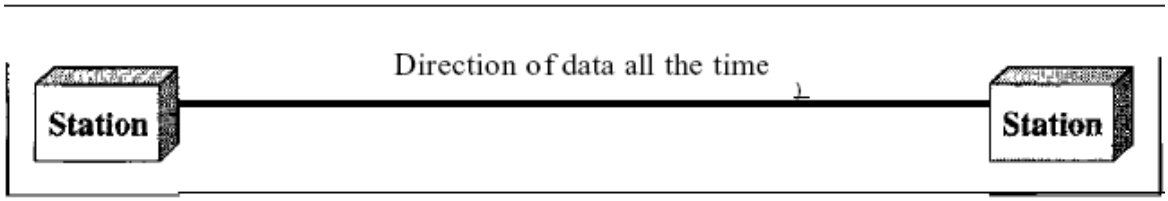
Communication between two devices can be simplex, half-duplex, or full-duplex as shown in Figure



a. Simplex



b. Half-duplex



c. 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 a). Keyboards and traditional monitors are examples of simplex devices. The keyboard 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 The half-duplex mode is like a one-lane road with traffic allowed in both directions.

When cars are traveling in one direction, cars going the other way must wait. In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time. Walkie-talkies 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 both stations can transmit and receive simultaneously 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.

2. NETWORKS: Network Criteria, Physical Structures

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 a 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 another. Response time is the elapsed time between an inquiry and a response. The performance of a network depends on a number of factors, including the number of users, the type of transmission medium, the capabilities of the connected hardware, and the efficiency of the software. Performance is often evaluated by two networking metrics:

throughput and delay. We often need more throughput and less delay. However, these two criteria are often contradictory. If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

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.

Physical Structures:

Type of Connection

A network is two or more devices connected through links. A link is a communications pathway that transfers data from one device to another. For visualization purposes, it is simplest to imagine any link as a line drawn between two points. For communication to occur, two devices must be connected in some way to the same link at the same time. There are two possible types of connections: point-to-point and multipoint.

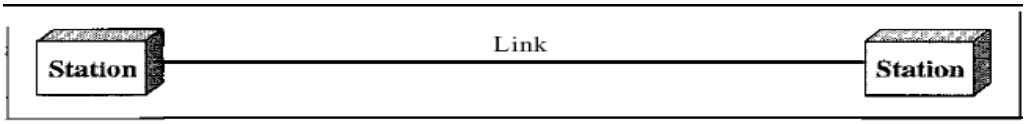
1.Point-to-Point:

A point-to-point connection provides a dedicated link between two devices. The entire capacity of the link is reserved for transmission between those two devices. Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible. When you change television channels by infrared remote control, you are establishing a point-to-point connection between the remote control and the television's control system.

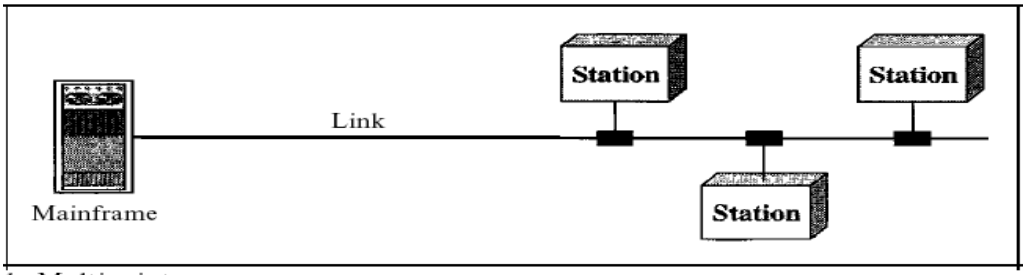
2.Multipoint:

A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link

simultaneously, it is a *spatially shared* connection. If users must take turns, it is a *timeshared* connection.



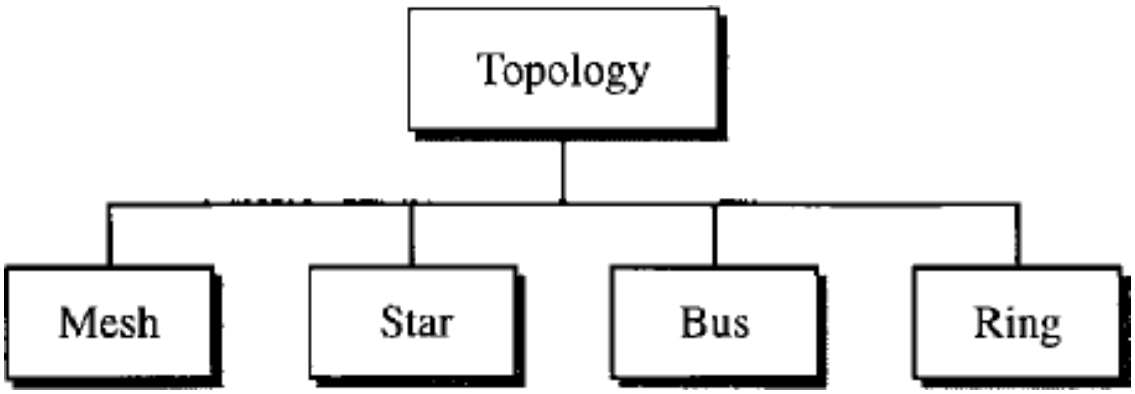
a. Point-to-point



b. Multipoint

- ***Physical Topology***

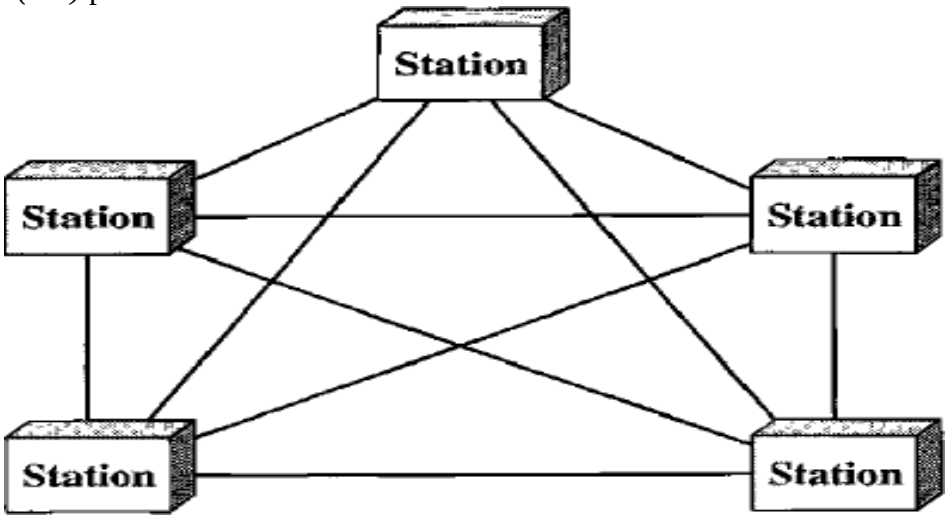
The term *physical topology* refers to the way in which a network is laid out physically. One or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another. There are four basic topologies possible: mesh, star, bus, and ring



Mesh: In a mesh topology, every device has a dedicated point-to-point link to every other device. The term *dedicated* means that the link carries traffic only between the two devices it connects. To find the number of physical links in a fully connected mesh network with *n* nodes, we first consider that each node must be connected to every other node. Node 1 must be connected to *n* - I nodes, node 2 must be connected to *n* – 1 nodes, and finally node *n* must be connected to *n* - 1 nodes. We need *n(n* - 1) physical links. However, if each physical link allows communication in both directions (duplex mode),

we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need $n(n-1)/2$ duplex-mode links.

To accommodate that many links, every device on the network must have $n - 1$ input/output *(VO)* ports to be connected to the other $n - 1$ stations.



Advantages:

- The use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
- A mesh topology is robust. If one link becomes unusable, it does not incapacitate the entire system. Third, there is the advantage of privacy or security. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages. Finally, point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages:

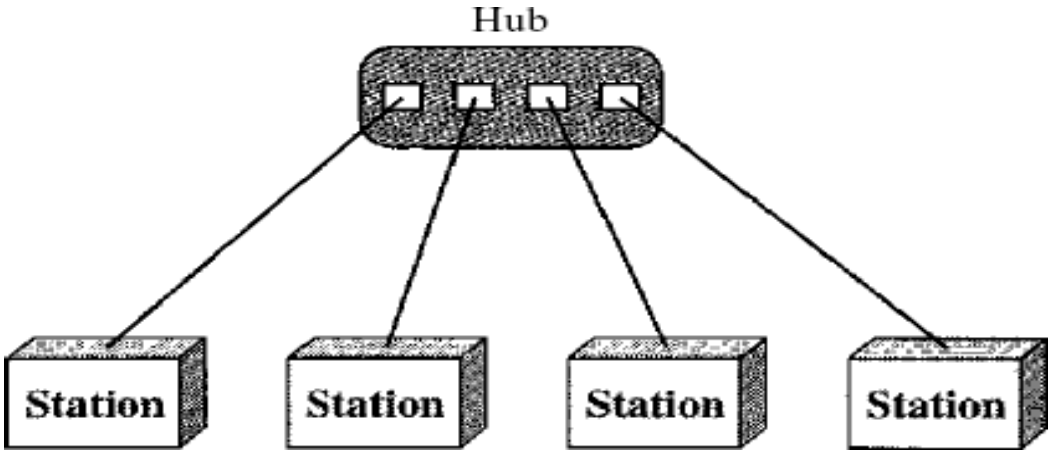
- Disadvantage of a mesh are related to the amount of cabling because every device must be connected to every other device, installation and reconnection are difficult.
- Second, the sheer bulk of the wiring can be greater than the available space (in walls, ceilings, or floors) can accommodate. Finally, the hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

Star Topology:

In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another. Unlike a mesh topology, a star topology does not allow direct traffic between devices. The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device .

A star topology is less expensive than a mesh topology. In a star, each device needs only one link and one I/O port to connect it to any number of others. This factor also makes it easy to install and reconfigure.

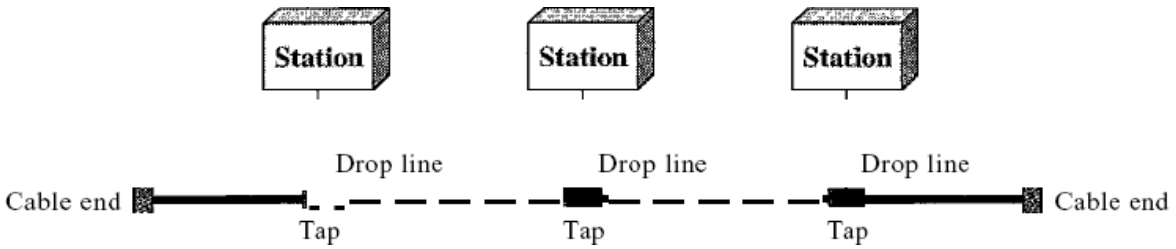
Other advantages include robustness. If one link fails, only that link is affected. All other links remain active. This factor also lends itself to easy fault identification and fault isolation. As long as the hub is working, it can be used to monitor link problems and bypass defective links.



One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub. If the hub goes down, the whole system is dead. Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies (such as ring or bus).

Bus Topology:

The preceding examples all describe point-to-point connections. A **bus topology,** on the other hand, is multipoint. One long cable acts as a **backbone** to link all the devices in a network



Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and the main cable. A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core. As a signal travels along the backbone, some of its energy is transformed into heat. Therefore, it becomes weaker and weaker as it travels farther and farther. For this reason there is a limit on the number of taps a bus can support and on the distance between those taps.

Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths. In this way, a bus uses less cabling than mesh or star topologies. In a star, for example, four network devices in the same room require four lengths of cable reaching all the way to the hub. In a bus, this redundancy is eliminated. Only the backbone cable stretches through the entire facility. Each drop line has to reach only as far as the nearest point on the backbone.

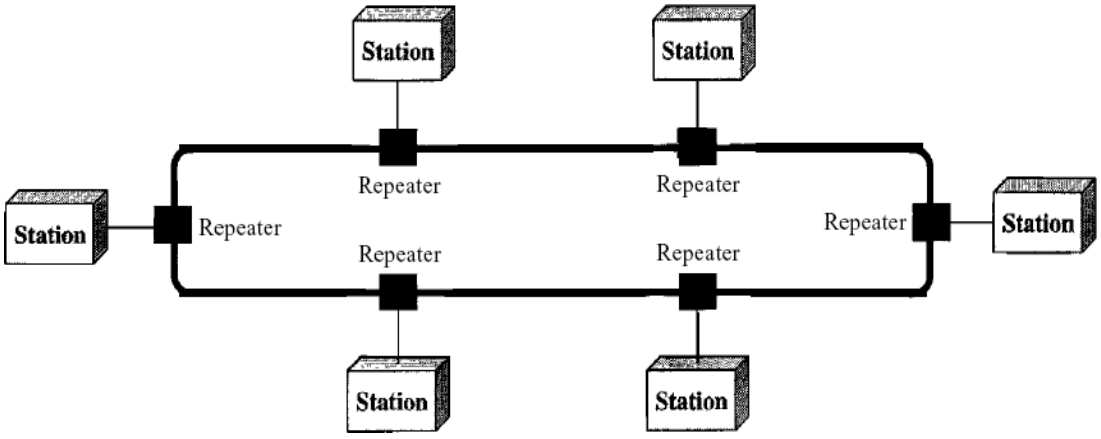
Disadvantages include difficult reconnection and fault isolation. A bus is usually designed to be optimally efficient at installation. It can therefore be difficult to add new devices. Signal reflection at the taps can cause degradation in quality. This degradation can be controlled by limiting the number and spacing of devices connected to a given length of cable. Adding new devices may therefore require modification or replacement of the backbone.

In addition, a fault or break in the bus cable stops all transmission, even between devices on the same side of the problem. The damaged area reflects signals back in the direction of origin, creating noise in both directions.

Bus topology was the one of the first topologies used in the design of early local area networks. Ethernet LANs can use a bus topology, but they are less popular.

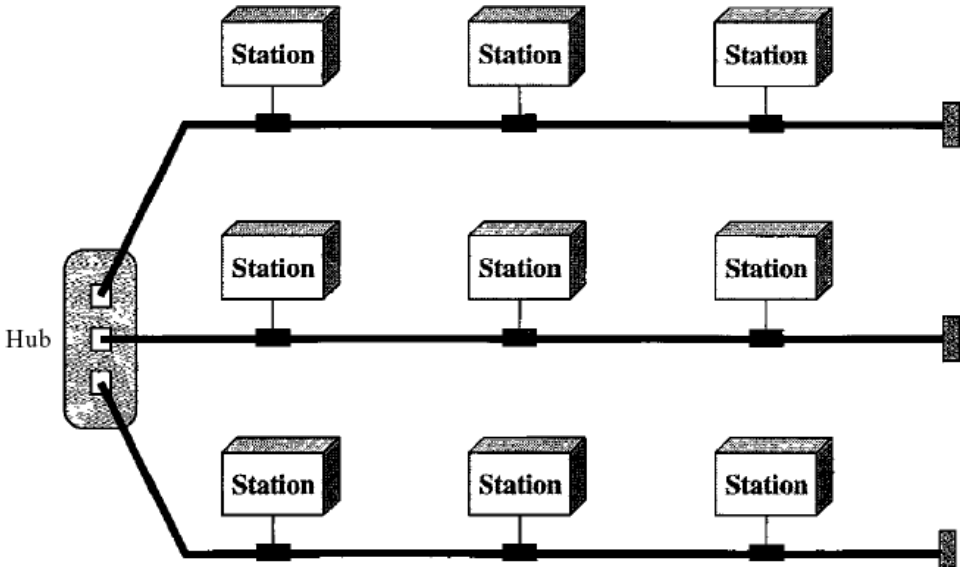
Ring Topology In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring

incorporates a repeater. When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along



A ring is relatively easy to install and reconfigure. Each device is linked to only its immediate neighbors (either physically or logically). To add or delete a device requires changing only two connections. The only constraints are media and traffic considerations (maximum ring length and number of devices). In addition, fault isolation is simplified. Generally in a ring, a signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm. The alarm alerts the network operator to the problem and its location.

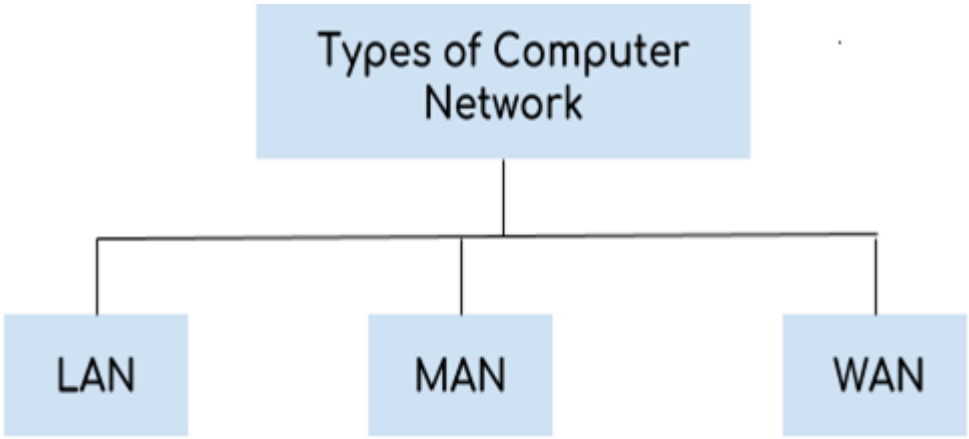
However, unidirectional traffic can be a disadvantage. In a simple ring, a break in the ring (such as a disabled station) can disable the entire network. This weakness can be solved by using a dual ring or a switch capable of closing off the break. Ring topology was prevalent when IBM introduced its local-area network Token Ring. Today, the need for higher-speed LANs has made this topology less popular. Hybrid Topology A network can be hybrid. For example, we can have a main star topology with each branch connecting several stations in a bus topology as shown in Figure



3. NETWORK TYPES: Local Area Network, Wide Area Network,

NETWORK TYPES / **Categories of Networks**

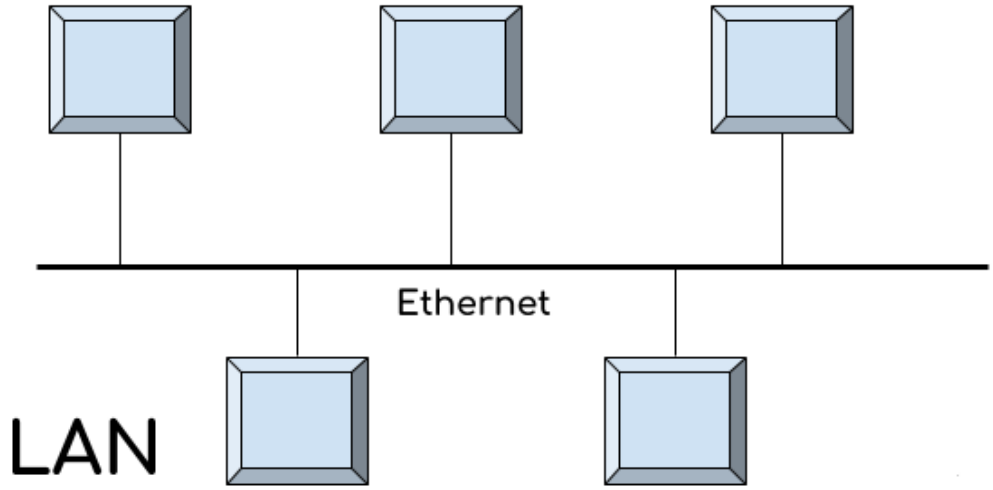
Types of Computer Network



There are mainly three types of computer networks based on their size:
1. Local Area Network (LAN)

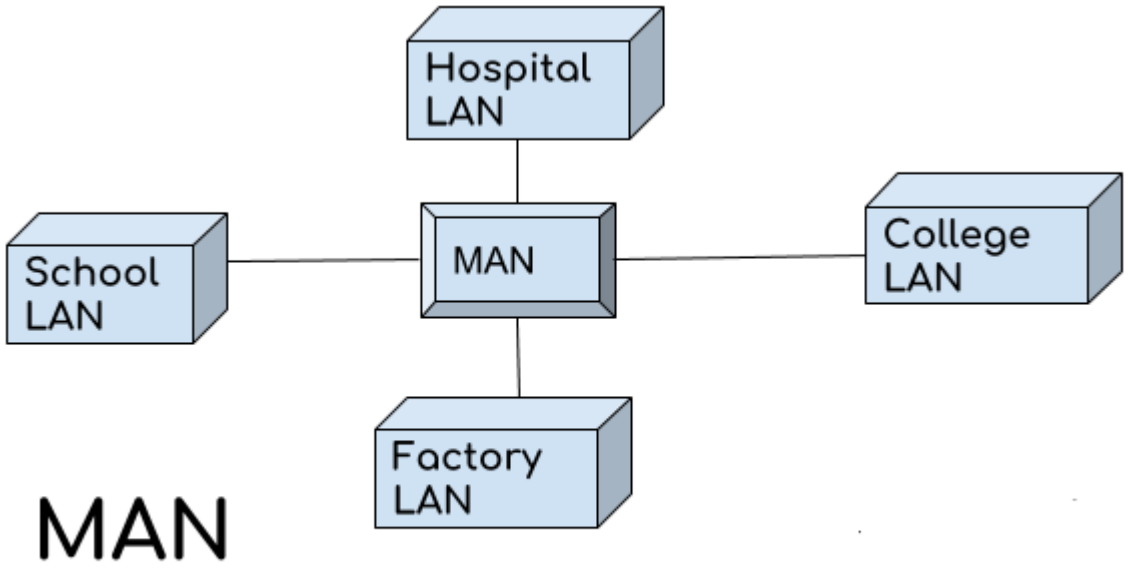
2. Metropolitan Area Network (MAN)
3. Wide area network (WAN)

1. Local Area Network (LAN)



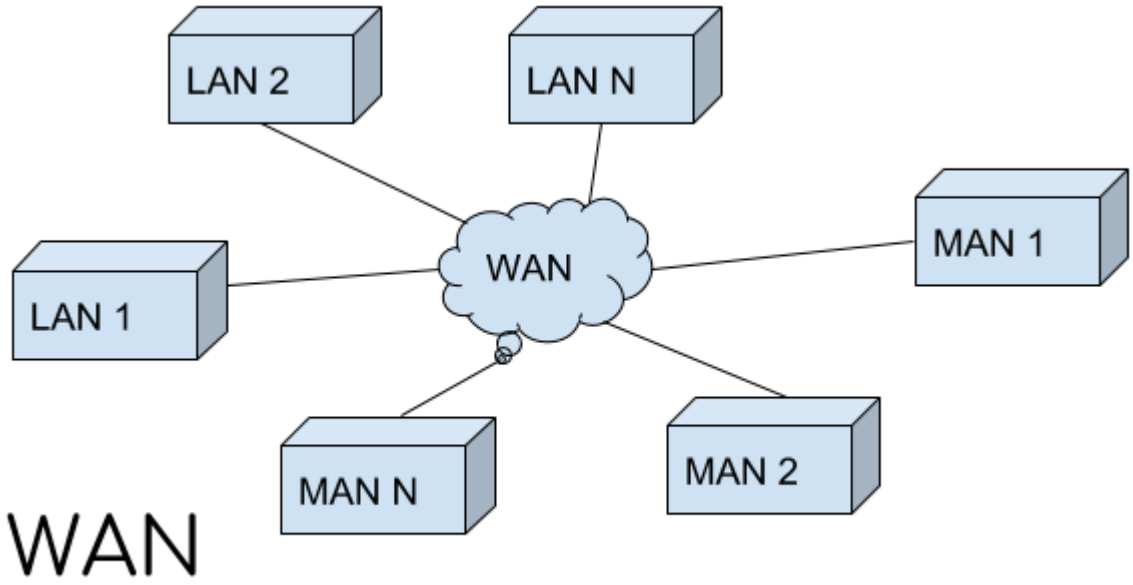
1. Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc.
2. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside.
3. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps.
4. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

2. Metropolitan Area Network (MAN)



MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.

3. Wide area network (WAN)



Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole

world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Advantages of WAN:

- Centralized infrastructure: One of the main advantage of WAN is the that we do not need to maintain the backup and store data on local system as everything is stored online on a data centre, from where we can access the data through WAN.
- Privacy: We can setup the WAN in such a way that it encrypts the data that we share online that way the data is secure and minimises the risk of unauthorized access.
- Increased Bandwidth: With the WAN we get to choose the bandwidth based on the need, a large organization can have larger bandwidth that can carry large amount of data faster and efficiently.
- Area: A WAN can cover a large area or even a whole world though internet connection thus we can connect with the person in another country through WAN which is not possible is other type of computer networks.

Disadvantages of WAN:

- Antivirus: Since our systems are connected with the large amount of systems, there is possibility that we may unknowingly download the virus that can affect our system and become threat to our privacy and may lead to data loss.

- Expensive: Cost of installation is very high.

- Issue resolution: Issue resolution takes time as the WAN covers large area, it is really difficult to pin point the exact location where the issues raised and causing the problem.

Difference between LAN, MAN, and WAN

The following table highlights all the key differences between LAN, MAN, and WAN −

Basis of Comparison	LAN	MAN	WAN
Full Form	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
Definition	It is the type of networking system in which systems are very	It is a type of networking system in which two or more	This networking system has many connections, and

	near to each other. This system is generally in a single office, building or home.	LANs are communicated. It is located in a vast geographical area.	these are associated with various companies or organizations at an equivalent time.
Ownership of Network	LAN is under the complete control of the owner, i.e., Private.	The ownership of the network can be private or public.	The ownership of the network can be private or public.
Speed	Data transmission speed is high.	Data transmission speed is average.	Data transmission speed is low.
Maintenance and Design	It can be easy to design and maintain.	It is tough to maintain.	It is tough to maintain.
Operational Speed	Its operational speed usually is 10,100 and 1000 Mbps.	Its operational speed usually is 1.5 Mbps, and it may be very at the wireless network.	Its operation is speed usually is 100 Mbps.
Fault Tolerance	There is higher fault tolerance in LAN.	There is smaller fault tolerance.	There is smaller fault tolerance.
Communication Allotment	LAN allows a small number of computers to establish a communication.	MAN allows simultaneous communication of a large number of computers.	WAN allows a very large number of computers to interact simultaneously with each other
Congestion	In LANs, the network congestion is very low due to less number of computers	In MANs, the network congestion is high.	In WANs, the network is very high.
Propagation Delay	In LANs, the propagation delay is very less.	In MANs, the propagation delay is moderate.	In WANs, the propagation delay is very high.
Examples	Computer networks of schools, homes, offices, hospitals, etc. are the common examples of LANs.	Computer networks that spread over a small city, or town are the examples of MANs.	Computer networks that cover an entire city, or globe like internet are the examples WANs.

Q) What are the advantages of a multipoint connection over a point-to-point one? What are some of the factors that determine whether a communication system is a LAN or WAN?

Ans) The advantages of a multipoint connection over a point-to-point connection are **ease of installation, low cost, reliability**. A point to point connection is used for connecting 2 devices, whereas in a multipoint connection more than 2 devices share the communication link.

Geographical area spanned by a network determines whether it is a LAN or a WAN. A LAN, or Local Area Network, spans a relatively smaller area, whereas a WAN, or Wide Area Network, covers a much larger area. Also, WANs have a higher propagation delay than LANs because of the large distance to be covered

NOTE : Write about LAN and WAN DEPENDING UPON Marks.

4. PROTOCOL LAYERING: Scenarios, Principles of Protocol Layering, Logical Connections

What is Protocol Layering?

A **protocol** is a set of rules and standards that primarily outline a language that devices will use to communicate. There are an excellent range of protocols in use extensively in networking, and that they are usually implemented in numerous layers.

It provides a communication service where the process is used to exchange the messages. When the communication is simple, we can use only one simple protocol.

When the communication is complex, we must divide the task between different layers, so, we need to follow a protocol at each layer, this technique we used to call protocol layering. This layering allows us to separate the services from the implementation.

Each layer needs to receive a set of services from the lower layer and to give the services to the upper layer. The modification done in any one layer will not affect the other layers.

Basic Elements of Layered Architecture

The basic elements of the layered architecture are as follows −

- Service − Set of actions or services provided from one layer to the higher layer.
- Protocol − It defines a set of rules where a layer uses to exchange the information with its peer entity. It is concerned about both the contents and order of the messages used.
- Interface − It is a way through that the message is transferred from one layer to another layer.

Reasons

The reasons for using layered protocols are explained below −

- Layering of protocols provides well-defined interfaces between the layers, so that a change in one layer does not affect an adjacent layer.
- The protocols of a network are extremely complicated and designing them in layers makes their implementation more feasible.

Advantages

The advantages of layered protocols are as follows −

- Assists in protocol style, as a result of protocols that operate at a particular layer have outlined information that they work and a defined interface to the layers on top of and below.
- Foster's competition because products from completely different vendors will work along.
- Prevents technology or capability changes in one layer from touching different layers above and below.
- Provides a typical language to explain networking functions and capabilities.

Disadvantages

The disadvantages of layered protocols are as follows −

- The main disadvantages of layered systems consist primarily of overhead each in computation and in message headers caused by the abstraction barriers between layers. Because a message typically should pass through several (10 or more) protocol layers the overhead of those boundaries is commonly more than the computation being done.
- The upper-level layers cannot see what is within the lower layers, implying that an application cannot correct where in an exceedingly connection a problem is or precisely what the matter is.
- The higher-level layers cannot control all aspects of the lower layers, so that they cannot modify the transfer system if helpful (like controlling windowing, header compression, CRC/parity checking, et cetera), nor specify routing, and should rely on the lower protocols operating, and cannot specify alternatives when there are issues.

Logical Connections

- A logical network is a portion of a physical network that connects two or more logical network interfaces or devices. A logical network interface or device is the software entity that is known by an operating system.

  What is a logical network example?

- "When designing a network, the "logical" part refers to the IP addressing scheme used within the network. For example, **192.168. 0.0/24** could be the logical network used for our design.

5. TCP/IP PROTOCOL SUITE : Layered Architecture, Layers in the TCP/IP Protocol Suite, Description of Each Layer, Encapsulation and Decapsulation, Addressing, Multiplexing and Demultiplexing

Layered Architecture :

Computer Network Models

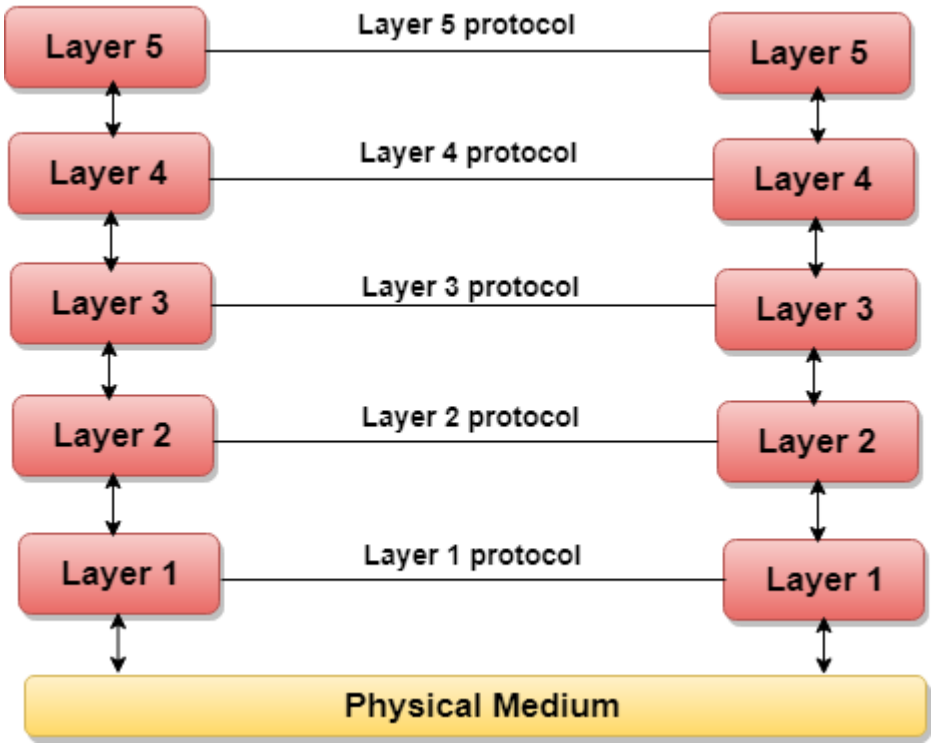
A communication subsystem is a complex piece of Hardware and software. Early attempts for implementing the software for such subsystems were based on a single, complex, unstructured program with many interacting components. The resultant software was very difficult to test and modify. To overcome such problem, the ISO has developed a layered approach. In a layered approach, networking concept is divided into several layers, and each layer is assigned a particular task. Therefore, we can say that networking tasks depend upon the layers.

Layered Architecture

- The main aim of the layered architecture is to divide the design into small pieces.
- Each lower layer adds its services to the higher layer to provide a full set of services to manage communications and run the applications.
- It provides modularity and clear interfaces, i.e., provides interaction between subsystems.
- It ensures the independence between layers by providing the services from lower to higher layer without defining how the services are implemented. Therefore, any modification in a layer will not affect the other layers.

- The number of layers, functions, contents of each layer will vary from network to network. However, the purpose of each layer is to provide the service from lower to a higher layer and hiding the details from the layers of how the services are implemented.
- The basic elements of layered architecture are services, protocols, and interfaces.
    - **Service:** It is a set of actions that a layer provides to the higher layer.
    - **Protocol:** It defines a set of rules that a layer uses to exchange the information with peer entity. These rules mainly concern about both the contents and order of the messages used.
    - **Interface:** It is a way through which the message is transferred from one layer to another layer.
- In a layer n architecture, layer n on one machine will have a communication with the layer n on another machine and the rules used in a conversation are known as a layer-n protocol.

Let's take an example of the five-layered architecture.



- In case of layered architecture, no data is transferred from layer n of one machine to layer n of another machine. Instead, each layer passes the data to the layer immediately just below it, until the lowest layer is reached.

- Below layer 1 is the physical medium through which the actual communication takes place.
- In a layered architecture, unmanageable tasks are divided into several small and manageable tasks.
- The data is passed from the upper layer to lower layer through an interface. A Layered architecture provides a clean-cut interface so that minimum information is shared among different layers. It also ensures that the implementation of one layer can be easily replaced by another implementation.
- A set of layers and protocols is known as network architecture.

Why do we require Layered architecture?

- **Divide-and-conquer approach:** Divide-and-conquer approach makes a design process in such a way that the unmanageable tasks are divided into small and manageable tasks. In short, we can say that this approach reduces the complexity of the design.
- **Modularity:** Layered architecture is more modular. Modularity provides the independence of layers, which is easier to understand and implement.
- **Easy to modify:** It ensures the independence of layers so that implementation in one layer can be changed without affecting other layers.
- **Easy to test:** Each layer of the layered architecture can be analyzed and tested individually.

Layers in the TCP/IP Protocol Suite

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.

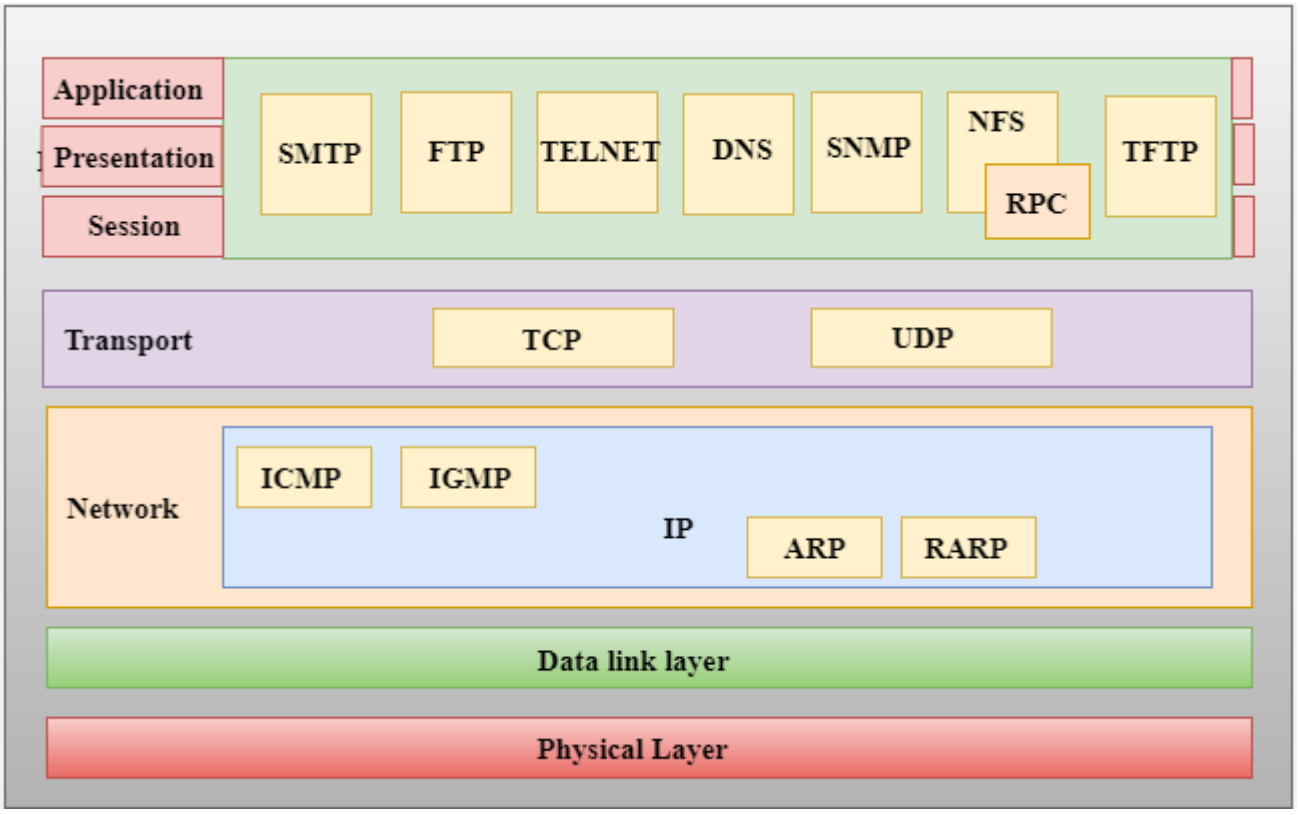
- TCP/IP is a hierarchical protocol made up of interactive modules, and each of them provides specific functionality.

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

Functions of TCP/IP layers:

The layers are:

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



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

- **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

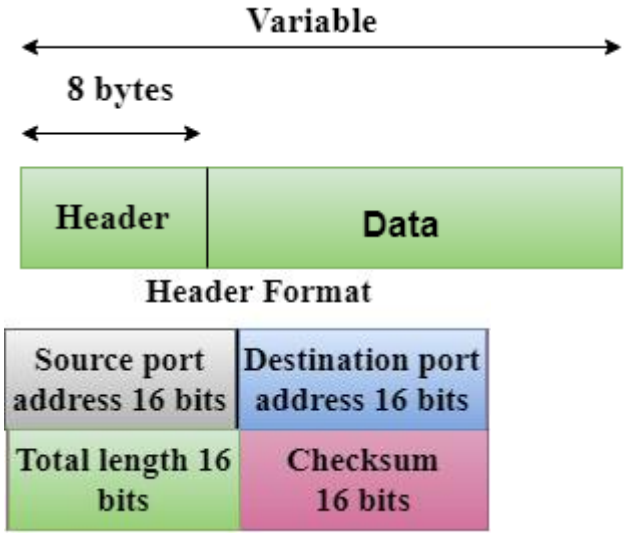
- **ICMP** stands for Internet Control Message Protocol.
- It is a mechanism used by the hosts or routers to send notifications regarding datagram problems back to the sender.
- A datagram travels from router-to-router until it reaches its destination. If a router is unable to route the data because 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:

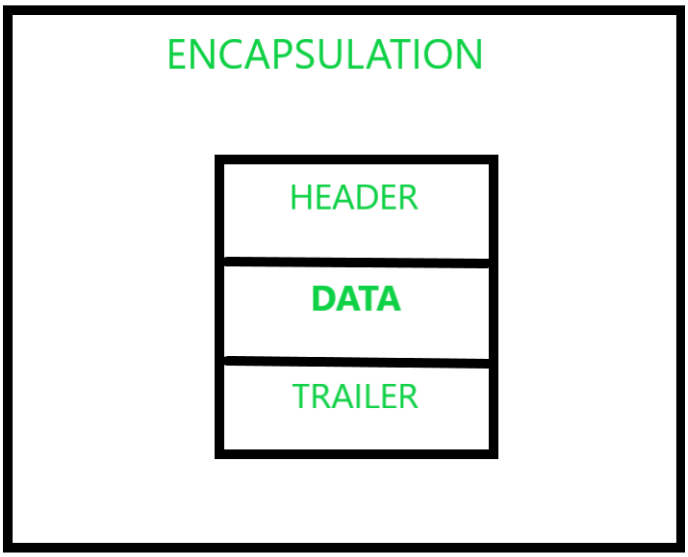
- **HTTP:** HTTP stands for Hypertext transfer protocol. This protocol allows us to access the data over the world wide web. It transfers the data in the form of plain text, audio, video. It is known as a Hypertext transfer protocol as it has the efficiency to use in a hypertext environment where there 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.

Encapsulation and Decapsulation in computer network :

Encapsulation:

Encapsulation refers to attaching new information in the Application Layer data as it is passed onto next layers in the TCP/IP model. This additional information basically divided into two parts, Header and Trailer. These are elements attached in order to make the transmission more smoother, on each layer a PDU (Protocol Data Unit) is generated. The concept of Encapsulations can be summarized in the screenshot attached ahead.



Decapsulation :

Decapsulation refers to the removal of all these additional information and extraction of originally existing data, and this process continues till the last layer i.e. the Application Layer. This process removes, fragments of distinct information in each layer as it approaches that layer. Here is the pictorial representation of the whole process.

Multiplexing and Demultiplexing

Multiplexing

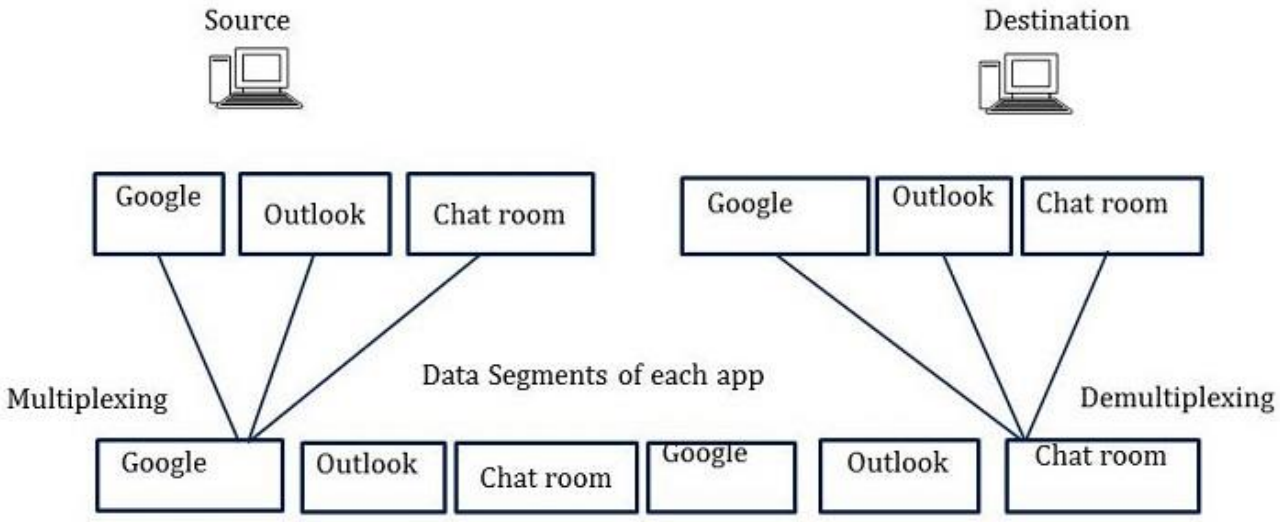
Multiplexing is the process of collecting the data from multiple application processes of the sender, enveloping that data with headers and sending them as a whole to the intended receiver.

- In Multiplexing at the Transport Layer, the data is collected from various application processes. These segments contain the source port number, destination port number, header files, and data.
- These segments are passed to the Network Layer which adds the source and destination IP address to get the datagram.

Demultiplexing

Delivering the received segments at the receiver side to the correct app layer processes is called demultiplexing.

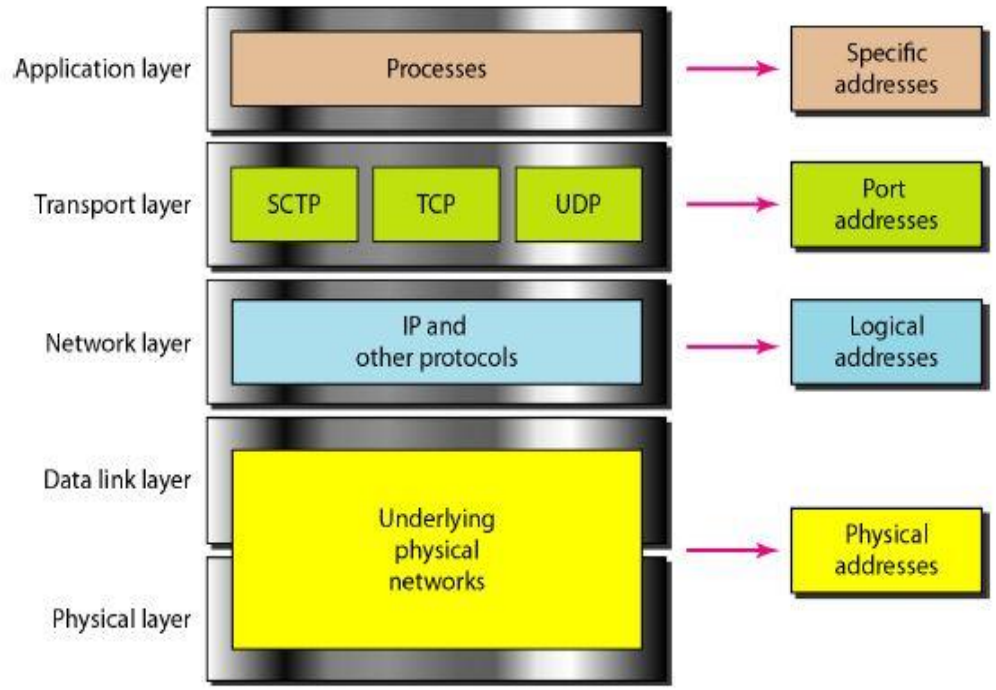
- The destination host receives the IP datagrams; each datagram has a source IP address and a destination IP address.
- Each datagram carries 1 transport layer segment.
- Each segment has the source and destination port number.
- The destination host uses the IP addresses and port numbers to direct the segment to the appropriate socket.



ADDRESSING

- Addresses used in the TCP/IP Protocol :
- Four levels of addresses are used in the TCP/IP protocol:
    1. **Physical address**
    2. **Logical address**
    3. **Port address**
    4. **Application-specific address**

Figure *Relationship of layers and addresses in TCP/IP*



- In networking, physical address refers to **a computer's MAC address**, which is a unique identifier associated with a network adapter that is used for identifying a computer in a network.
- An **IP address** is also known as a logical address and it can change over time as well as from one network to another.
- A port number is a **way to identify a specific process to which an internet or other network message is** to be forwarded when it arrives at a server.
- Application-specific addresses are **used to identify particular applications**. For example, the author@beingintelligent.com is the address of email, www.beingintelligent.com is the address of a website.

So, these are the four type of addresses used to communicate in the network using TCP/IP protocols.

6. THE OSI MODEL: OSI versus TCP/IP, Lack of OSI Model's Success

OSI Model

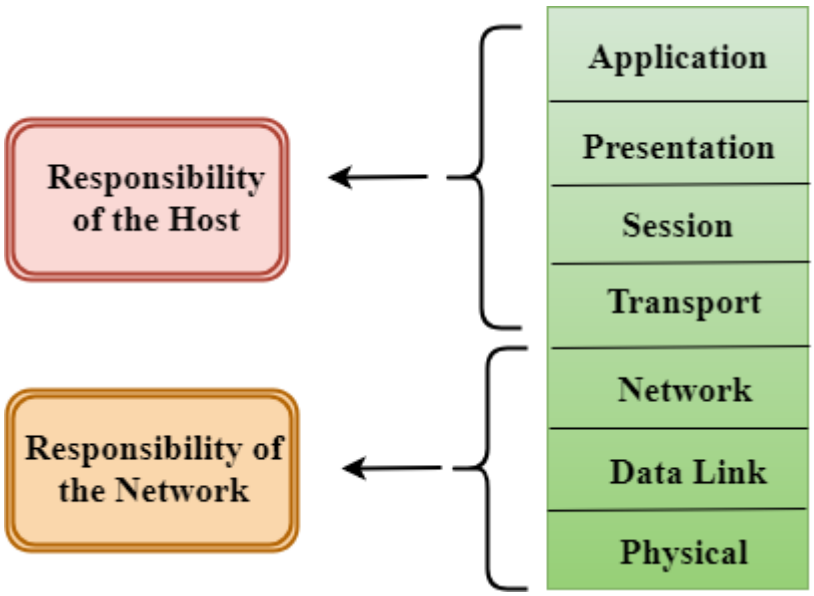
- OSI stands for **Open System Interconnection** is a reference model that describes how information from a software

  application in one computer

  moves through a physical medium to the software application in another computer.

- OSI consists of seven layers, and each layer performs a particular network function.
- OSI model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered as an architectural model for the inter-computer communications.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

Characteristics of OSI Model:



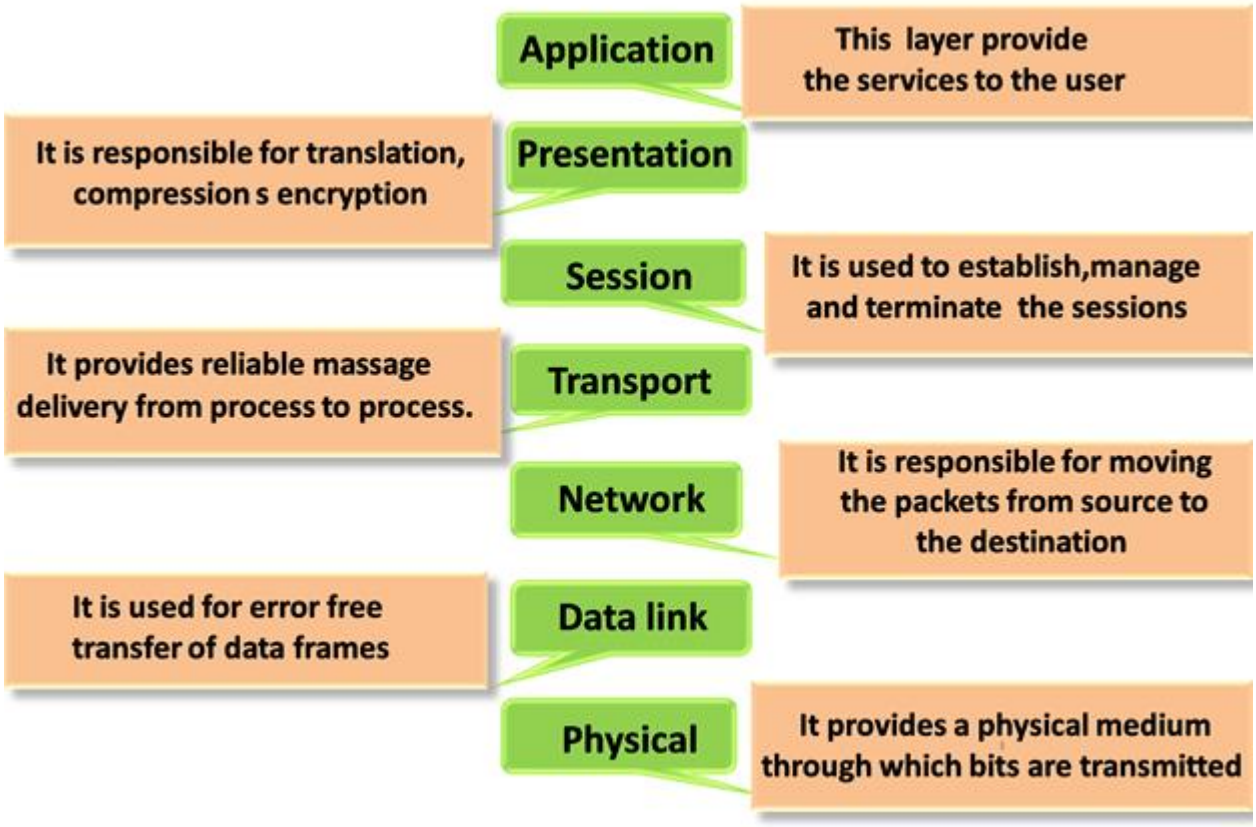
- The OSI model is divided into two layers: upper layers and lower layers.

- 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.

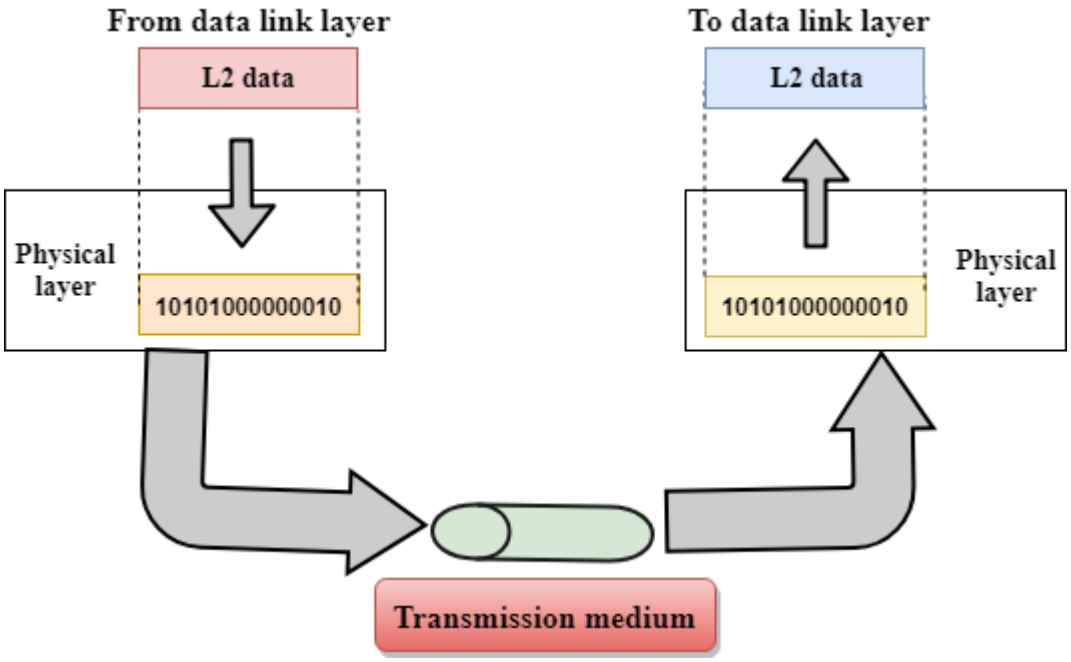
7 Layers of OSI Model

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



1) Physical layer



- The main functionality of the physical layer is to transmit the individual bits from one node to another node.
- It is the lowest layer of the OSI model.

- It establishes, maintains and deactivates the physical connection.
- It specifies the mechanical, electrical and procedural network interface specifications.

Functions of a Physical layer:

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

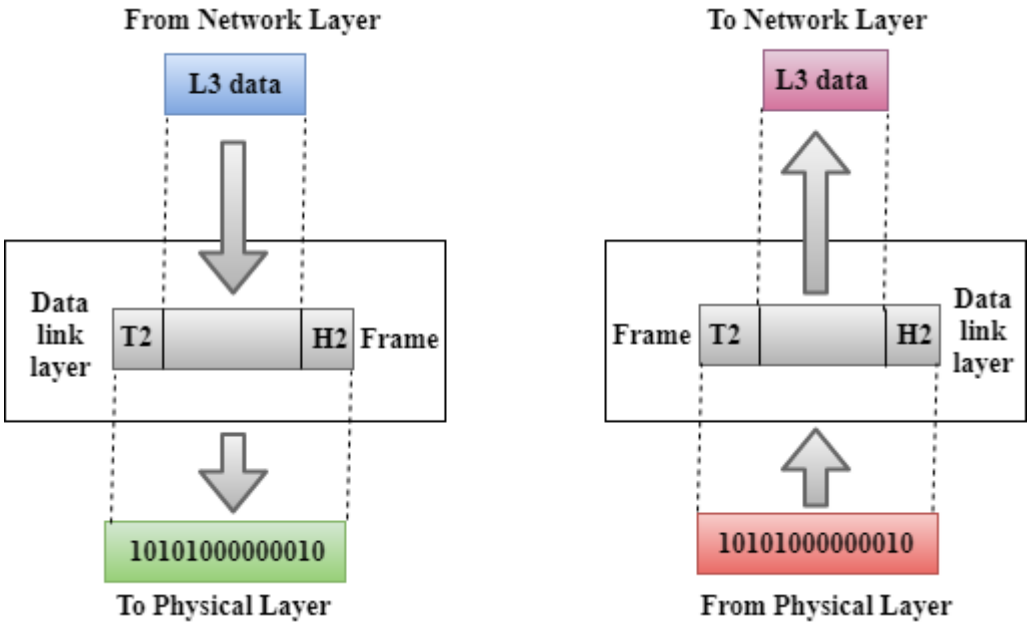
  : It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.

- **Topology**

  : It defines the way how network devices are arranged.

- **Signals:** It determines the type of the signal used for transmitting the information.

2) Data-Link Layer



- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.

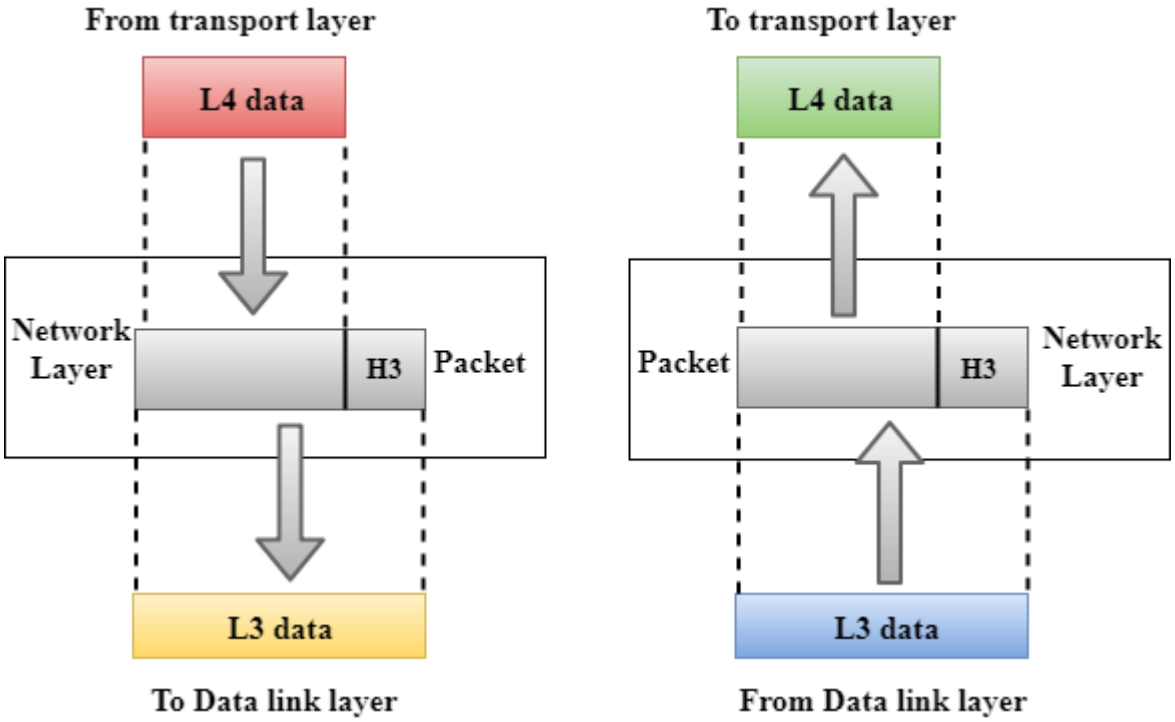
- It contains two sub-layers:
    - **Logical Link Control Layer**
        - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
        - It identifies the address of the network layer protocol from the header.
        - It also provides flow control.
    - **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.

- **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.

3) 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**

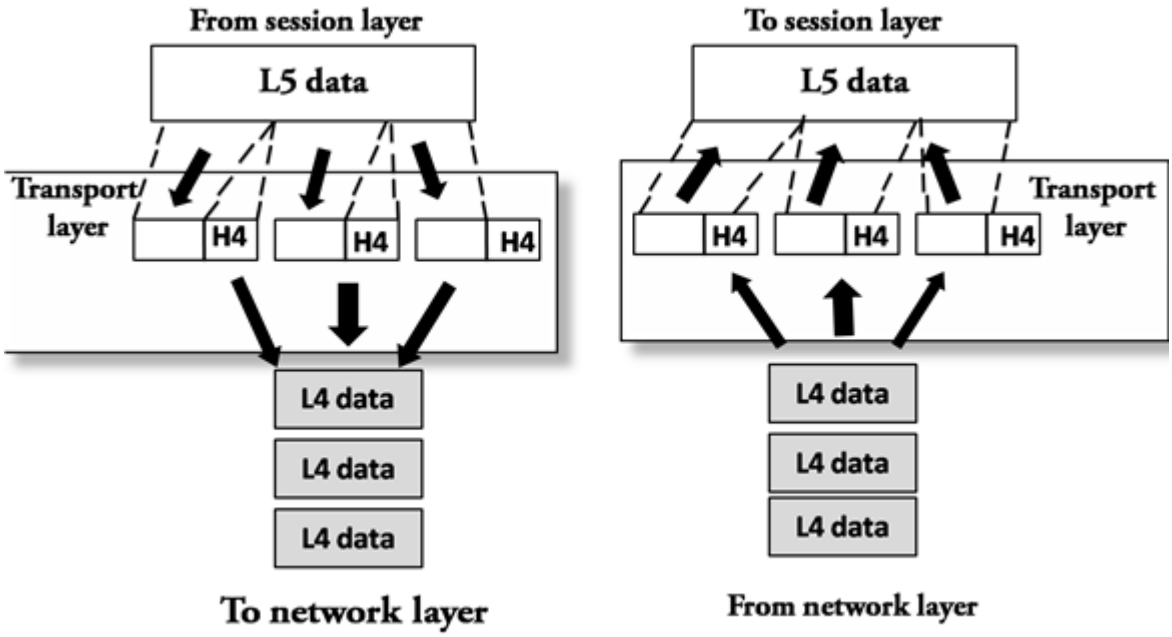
  : A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

- **Routing**

  : 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).

4) 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.

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.

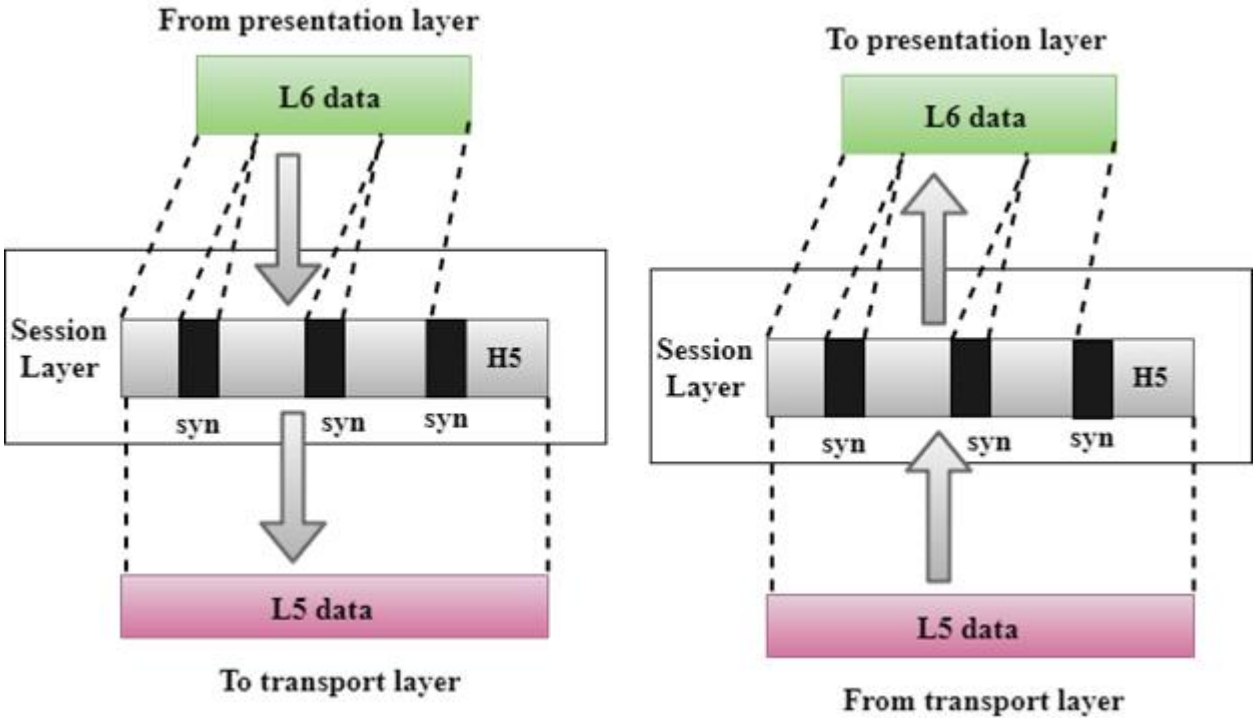
- **User Datagram Protocol**
  - User Datagram Protocol is a transport layer protocol.
  - It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

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.

5) Session Layer

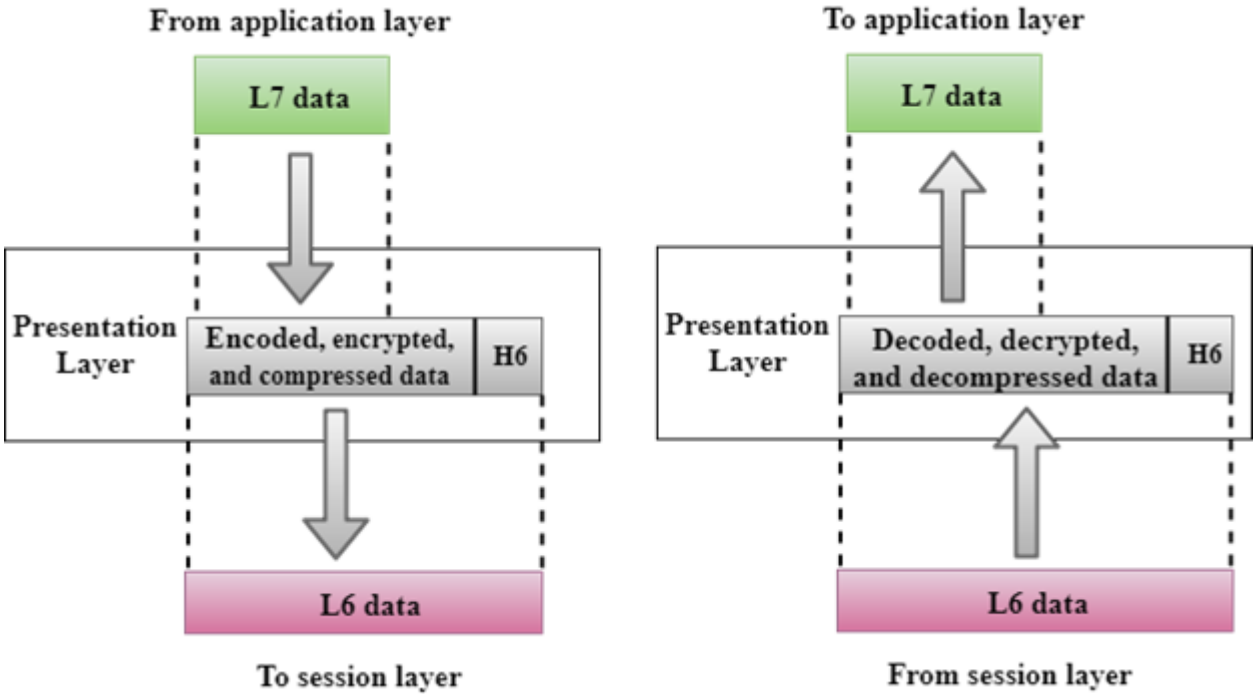


- It is a layer 3 in the OSI model.
- The Session layer is used to establish, maintain and synchronizes the interaction between communicating devices.

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.

6) Presentation Layer



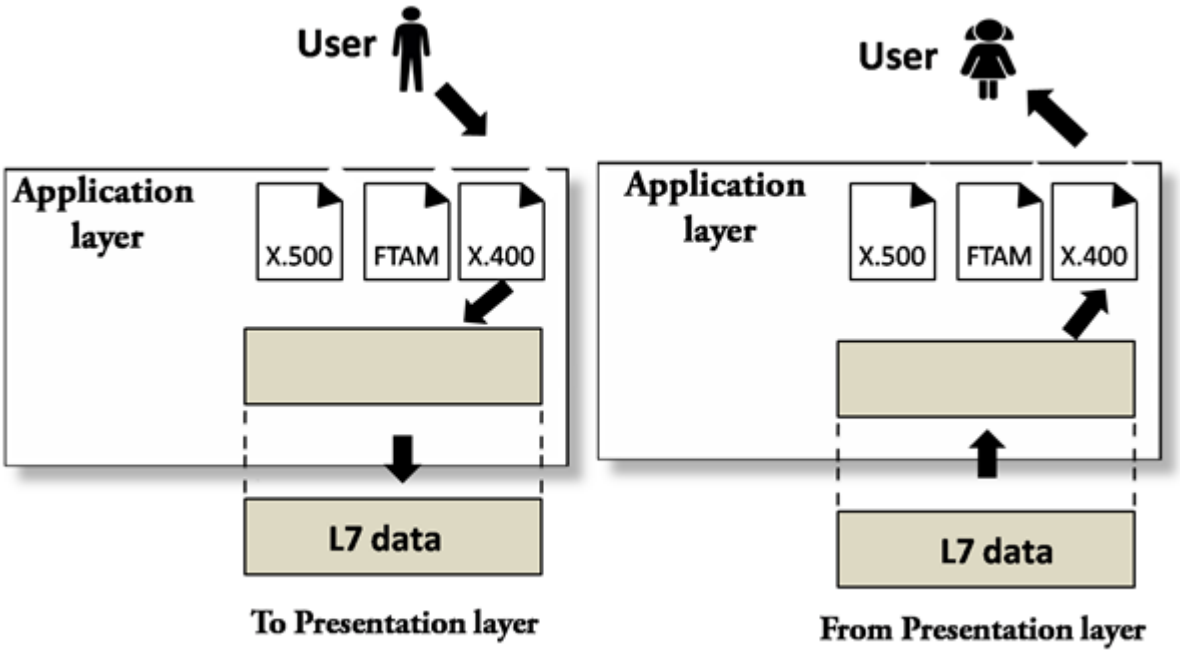
- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation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

7) 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.

Similarities between the TCP/IP model and the OSI model

- Both are logical models.
- Both define standards for networking.
- Both provide a framework for creating and implementing networking standards and devices.
- Both divide the network communication process into layers.
- In both models, a single layer defines a particular functionality and sets standards for that functionality only.
- Both models allow a manufacturer to make devices and network components that can coexist and work with the devices and components made by other manufacturers.
- Both models simplify the troubleshooting process by dividing complex functions into simpler components.
- Instead of defining the already defined standards and protocols, both models referenced them. For example, the Ethernet standards were already defined by IEEE before the creation of these models. So instead of defining them again both models used them as IEEE Ethernet standards.

Differences between the OSI model and the TCP/IP model

- The OSI Layer model has seven layers while the TCP/IP model has four layers.
- The OSI Layer model is no longer used while the TCP/IP is still used in computer networking.
- To define the functionalities of upper layers, the OSI model uses three separate layers (Application, Presentation, and Session) while the TCP/IP model uses a single layer (Application).
- Just like the upper layers, the OSI model uses two separate layers (Physical and Data-link) to define the functionalities of the bottom layers while the TCP/IP uses a single layer (Link layer) for the same.
- To define the routing protocols and standards, the OSI model uses the Network layer while the TCP/IP model uses the Internet layer.
- The OSI model is well documented than the TCP/IP model.
- The OSI model explains every standard and protocol in detail while the TCP/IP model provides a summarized version of the same.

Differences between the original TCP/IP model and the updated TCP/IP model

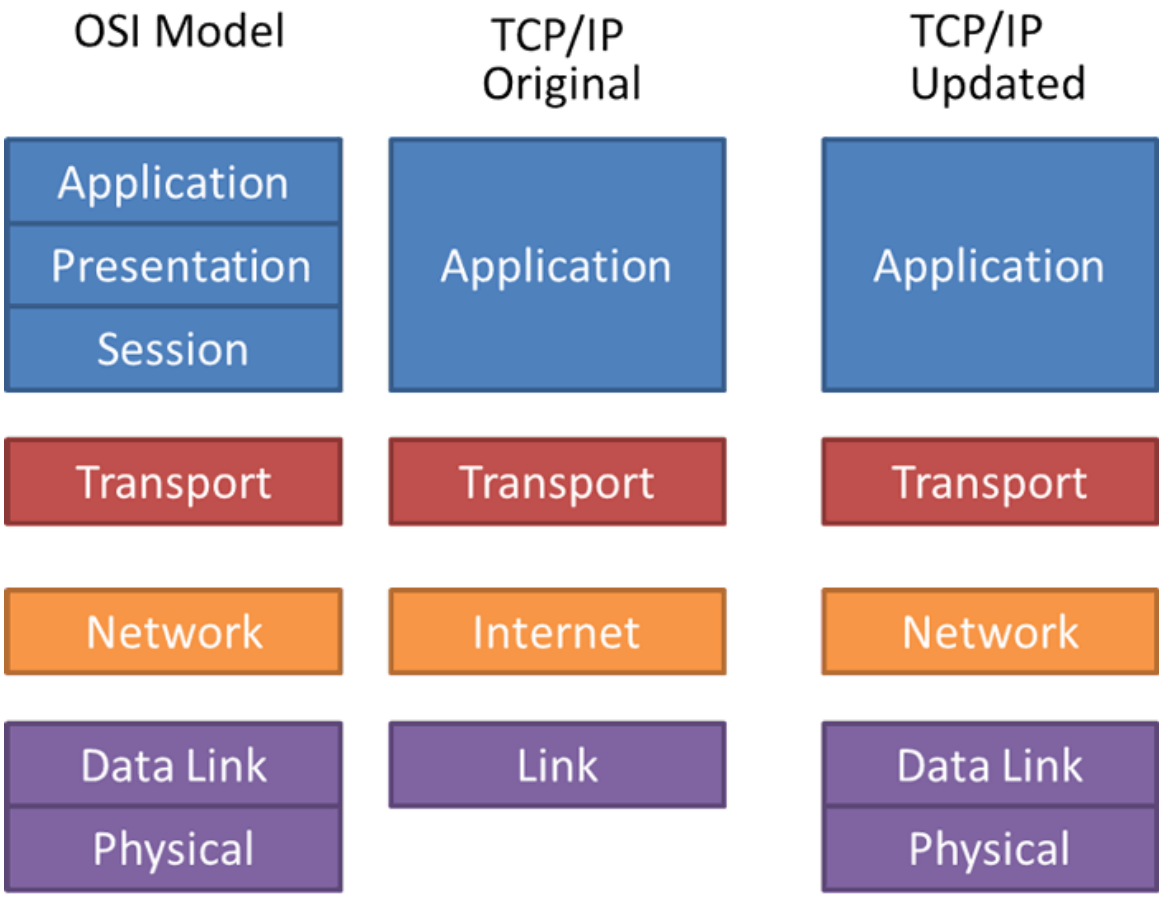
The TCP/IP model which we use nowadays is slightly different from the original TCP/IP model. The original TCP/IP model has four layers while the updated TCP/IP model has five layers.

The original version uses a single layer (Link layer) to define the functionalities and components that are responsible for data transmission. The updated version uses two layers (Data Link and Physical) for the same.

It defines the functions that are directly related to the data transmission in the Physical layer and defines the functions that are indirectly related to the data transmission in the Data-link layer.

In the updated version, the name of the Internet layer is changed to the Network layer.

The following figure compares the OSI reference model, the original TCP/IP model, and the updated TCP/IP model.



Lack of OSI Model's Success :

OSI model drawbacks :

-Many applications do not require/need the data integrity, which is provided by OSI-model.

-In order to fast set up OSI requires agreement b/w three-parties: users & service provider.

-Complex.

-This model is not adapted at all to telecommunication applications on computer.

Why TCP/IP model:

- It can be used to establish/set up connection b/w different types of computers.
- It operates/works independently of the operating system.
- It support for a number of routing-**protocols**.
- It enables the internetworking between the organizations.
- It has a scalable, client-server architecture.

OSI model couldn't compete with TCP/IP model, and failed in getting wider acceptance. One of the main reasons behind the failure of OSI model and wider acceptance of TCP/IP model was because big global networks like internet started running on TCP/IP protocol suite.

7.Physical Layer- Transmission Media

GUIDED MEDIA: Twisted-Pair Cable, Coaxial Cable, Fiber-Optic Cable
UNGUIDED MEDIA: WIRELESS: Radio Waves, Microwaves, Infrared

In transmission media is the way the systems are connected to route data signals in a network.

The telecommunication links are classified into two categories −

- **Guided media (wired)**
- **Unguided media (wireless).**

Both guided and unguided are used for short distance (LANs, MANs) as well as long distance (WANs) communication.

Let us discuss Guided transmission media.

Guided transmission media

Guided transmission media consists of physical connection between source and destination through a wire or a cable.

There are three basic types of guided media which are as follows −

- Twisted pair cable
- Co-axial cable
- Fiber-optic cable

Twisted Pair Copper

Step 1 − It is the most used media across the world. All the local telephone exchanges are made of twisted pair copper. These telephone lines are reused as last mile DSL access links to access the internet from home.

Step 2 − Twisted pair copper wires are also used in Ethernet LAN cables within homes and offices.

Step 3 − It supports low to High Data Rates which is in the order of Gigabytes.

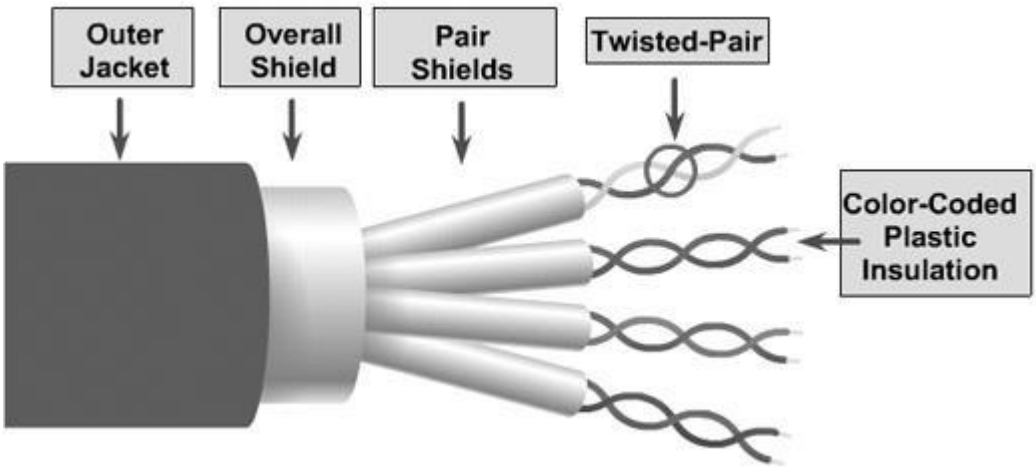
Step 4 − These wires are effective up to a maximum distance of a few kilometres/miles, because the signal strength is lost significantly beyond the distance.

Step 5 − Generally, they come in two variants as follows −

- UTP (unshielded twisted pair)
- STP (shielded twisted pair)

For every variant, there are multiple sub-variants, based on the thickness of the material (like UTP-3, UTP-5, UTP-7 etc.)

The twisted pair copper is diagrammatically represented as follows −



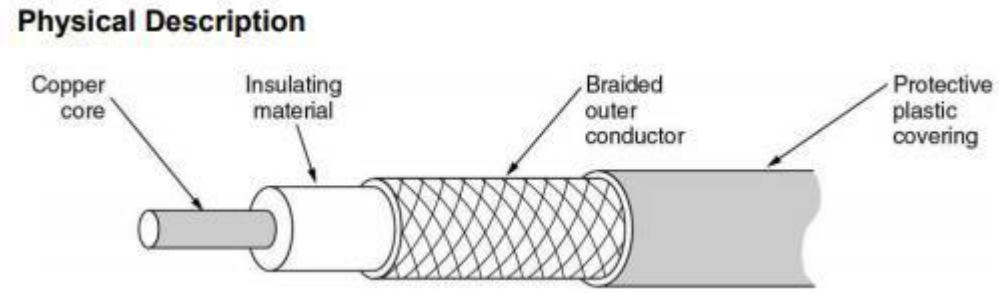
Copper Co-axial Cables

Step 1 − Co-axial copper cables consist of inner copper conductor and an outer copper shield, which are separated by a di-electric insulating material, helpful in preventing signal losses.

Step 2 −: Copper co-axial cables used in cable TV networks and as trunk lines between telecommunication equipments.

Step 3 − It serves as an internet access line from the home and supports medium to high data rates.

The copper co-axial cable is diagrammatically represented as follows −



Fiber Optic Cables

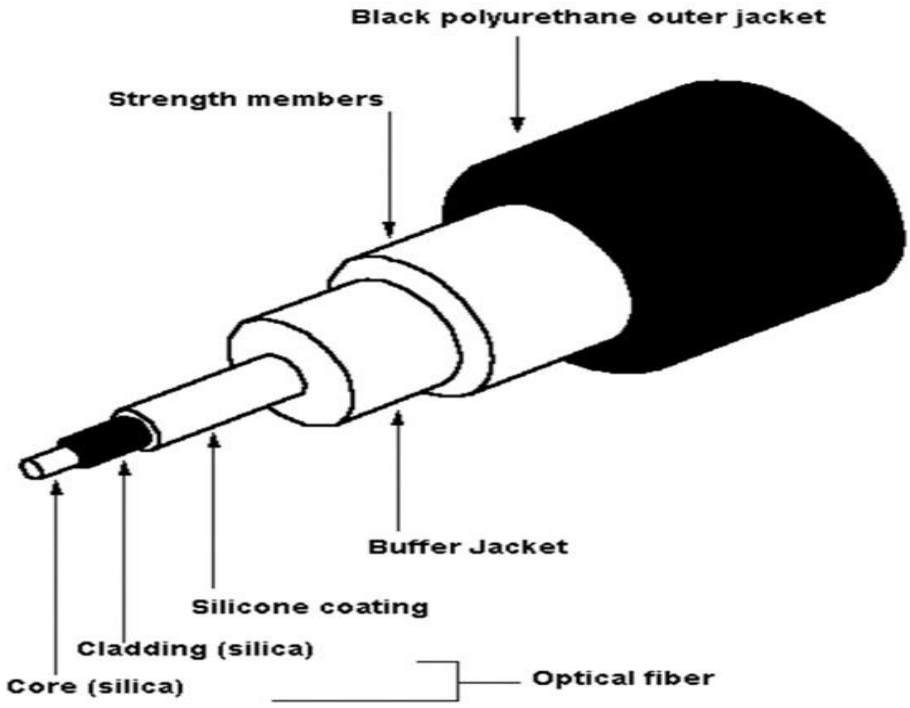
Step 1 − In fiber optic cable the information is transmitted by propagation of optical signals (light) through fiber optic cables and not through the electrical/electromagnetic signals. Because of this, the fiber optics communication supports longer distances as there is no electrical interference.

Step 2 −: The fiber optic cables are made of very thin strands of glass (silica). It supports high data rates.

Step 3 − It is used for accessing the internet from home through FTTH (Fiber-To-The-Home) lines.

Examples − OC-48, OC-192, FTTC, HFC.

The fiber optic cable is diagrammatically represented as follows −



Now let us discuss Unguided Transmission media.

Unguided transmission media

In Unguided transmission media there is no physical connection between source and destination, instead they use air itself. These connections are not bound to a channel to follow.

Unguided transmission media uses two basic types of primary technologies which are as follows −

Microwaves

Step 1 − Microwaves travel in straight lines and therefore the narrow focus concentrates all the energy into a beam.

Step 2 − In microwaves periodic repeaters are necessary for long distances and for transmitting and receiving antennas are aligned accurately.

Example − Bluetooth technology.

Satellite

Step 1 − Use microwave radio to protect from the atmosphere and act as a microwave relay station.

Step 2 − They are situated in space 22,000 miles above the equator, and it appears stationary from the earth as it rotates with specific speed.

Step 3 − They can amplify and relay microwave signals from one transmitter on the ground to another.

Differences

The major differences between guided and unguided transmission media are as follows −

Guided media	Unguided media
The signal requires a physical path for transmission.	The signal is broadcasted through air or sometimes water
It is called wired communication or bounded transmission media.	It is called wireless communication or unbounded transmission media.
It provides direction to signal for travelling. Twisted pair cable, coaxial cable and fibre optic cable are its types.	It does not provide any direction. Radio waves, microwave and infrared are its types.

NOTE :::: The below topics is given in another pdf (named UNIT 1 NOTES part 2)

PPT for CRC problems given.

PPT for Framing Topic given

Data-Link Layer: Introduction to Data-Link Layer [Chapter 9]
INTRODUCTION: Nodes and Links, Services, Two Categories of Links, Two Sublayers
LINK-LAYER ADDRESSING: Three Types of addresses, Address Resolution Protocol (ARP), An Example of Communication

Error Detection and Correction [Chapter 10(10.1,10.3.1-.5)]
INTRODUCTION: Types of Errors, Redundancy, Detection versus Correction, Coding
CYCLIC CODES: Cyclic Redundancy Check, Polynomials, Cyclic Code Encoder Using Polynomials, Cyclic Code Analysis, Advantages of Cyclic Codes

Data Link Control (DLC) [Chapter 11(11.1,11.2)]
DLC SERVICES: Framing, Flow and Error Control, Connectionless and Connection-Oriented
Media Access Control (MAC) [Chapter 12]
RANDOM ACCESS: ALOHA, CSMA, CSMA/CD, CSMA/CA
CONTROLLED ACCESS: Reservation, Polling, Token Passing
CHANNELIZATION: FDMA, TDMA, CDMA