Computer Networks-I (BTCS-403)

Chapter-1: Introduction to Computer Networks.

Notes

Introduction to Computer Networks:

Modern world scenario is ever changing. Data Communication and network have changed the way business and other daily affair works. Now, they highly rely on computer networks and internetwork.

A set of devices often mentioned as nodes connected by media link is called a Network.

A node can be a device which is capable of sending or receiving data generated by other nodes on the network like a computer, printer etc. These links connecting the devices are called **Communication channels**.

Computer network is a telecommunication channel using which we can share data with other computers or devices, connected to the same network. It is also called Data Network. The best example of computer network is Internet.

Computer network does not mean a system with one Control Unit connected to multiple other systems as its slave. That is Distributed system, not Computer Network.

A network must be able to meet certain criteria's, these are mentioned below:

1. Performance
2. Reliability
3. Scalability

Performance

It can be measured in the following ways:

- **Transit time:** It is the time taken to travel a message from one device to another.
- **Response time:** It is defined as the time elapsed between enquiry and response.

Other ways to measure performance are:

1. Efficiency of software
2. Number of users
3. Capability of connected hardware

Reliability

It decides the frequency at which network failure take place. More the failures are, less is the network's reliability.

Security

It refers to the protection of data from any unauthorized user or access. While travelling through network, data passes many layers of network, and data can be traced if attempted. Hence security is also a very important characteristic for Networks.

Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc, all of these are possible because of computer networks.

2. **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.
3. **Sharing files, data:** Authorized users are allowed to share the files on the network.

Basic Communication Model

A Communication model is used to exchange data between two parties. For example: communication between a computer, server and telephone (through modem).

Source

Data to be transmitted is generated by this device, example: telephones, personal computers etc.

Transmitter

The data generated by the source system is not directly transmitted in the form its generated. The transmitter transforms and encodes the data in such a form to produce electromagnetic waves or signals.

Transmission System

A transmission system can be a single transmission line or a complex network connecting source and destination.

Receiver

Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Destination

Destination receives the incoming data from the receiver.

Data Communication

The exchange of data between two devices through a transmission medium is called **Data Communication**. The data is exchanged in the form of **0's** and **1's**. The transmission medium used is wire cable. For data communication to occur, the communication device must be a part of a communication system. Data Communication has two types - **Local** and **Remote** which are discussed below:

Local

Local communication takes place when the communicating devices are in the same geographical area, same building, or face-to-face etc.

Remote

Remote communication takes place over a distance i.e. the devices are farther. The effectiveness of a data communication can be measured through the following features:

1. **Delivery**: Delivery should be done to the correct destination.
2. **Timeliness**: Delivery should be on time.
3. **Accuracy**: Data delivered should be accurate.

Components of Data Communication

1. **Message:** It is the information to be delivered.
2. **Sender:** Sender is the person who is sending the message.
3. **Receiver:** Receiver is the person to whom the message is being sent to.
4. **Medium:** It is the medium through which the message is sent. For example: A Modem.
5. **Protocol:** These are some set of rules which govern data communication.

Uses of Computer Networks

Had it not been of high importance, nobody would have bothered connecting computers over a network. Let's start exploring the uses of Computer Networks with some traditional usecases at companies and for individuals and then move on to recent developments in the area of mobile users and home networking.

Business Applications

- **Resource Sharing:** The goal is to make all programs, equipments, and especially data, available to anyone on the network without regard to the physical location of the resource and the user.
- **Server-Client model:** One can imagine a company's information system as consisting of one or more databases and some number of employees who need to access them remotely. In this model, the data is stored on powerful computers called **servers**. Often these are centrally housed and maintained by a system administrator. In contrast, the employees have simple machines, called **clients**, on their desks, with which they access remote data.
- **Communication Medium:** A computer network can provide a powerful communication medium among employees. Virtually every company that has two or more computers now has e-mail (electronic mail), which employees generally use for a great deal of daily communication

- **E-Commerce:** A goal that is starting to become more important is doing business with consumers over the Internet. Airlines, bookstores and music vendors have discovered that many customers like the convenience of shopping from home. This sector is expected to grow quickly in the future. The most popular forms are listed in the below figure:

Tag and Full Name	Example
B2C - Business-to-Consumer	Ordering books on-line
B2B - Business-to-Business	Car manufacturer ordering tires from supplier
C2C - Consumer-to-Consumer	Auctioning second-hand products on line
G2C - Government-to-Consumer	Government distributing tax forms electronically
P2P - Peer-to-Peer	File sharing

Home Applications

Some of the most important uses of the Internet for home users are as follows:

- **Access to remote information**
- **Person-to-person communication**
- **Interactive entertainment**
- **Electronic commerce**

Mobile Users

Mobile computers, such as notebook computers and Mobile phones, are one of the fastest-growing segments of the computer industry. Although wireless networking and mobile computing are often related, they are not identical, as the below figure shows.

Wireless	Mlobile	Applications
No	No	Desktop computers in offices
No	Yes	A notebook computer used in a hotel room
Yes	No	Networks in older, unwired buildings
Yes	Yes	Portable office; PDA for store inventory

Line Configuration in Computer Networks

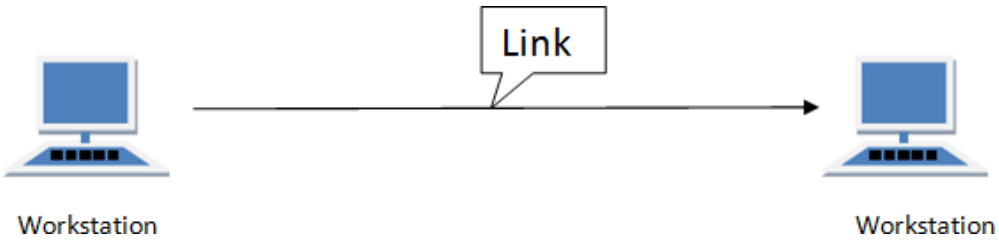
Network is a connection made through connection links between two or more devices. Devices can be a computer, printer or any other device that is capable to send and receive data. There are two ways to connect the devices:

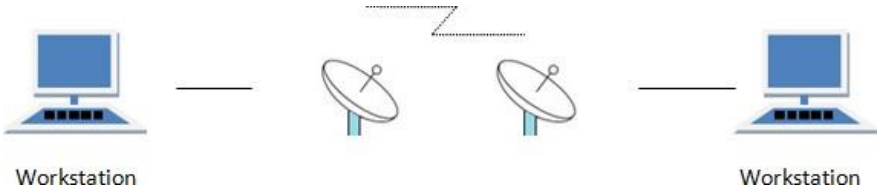
1. Point-to-Point connection
2. Multipoint connection

Point-To-Point Connection

It is a protocol which is used as a communication link between two devices. It is simple to establish. The most common example for Point-to-Point connection (PPP) is a computer connected by telephone line. We can connect the two devices by means of a pair of wires or using a microwave or satellite link.

Example: Point-to-Point connection between remote control and Television for changing the channels.



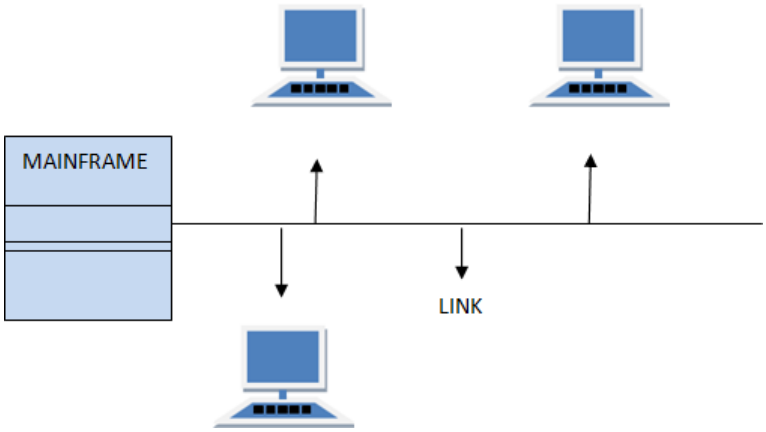


Multi-Point Connection

It is also called Multi-drop configuration. In this connection two or more devices share a single link.

There are two kinds of Multipoint Connections:

- If the links are used simultaneously between many devices, then it is spatially shared line configuration.
- If user takes turns while using the link, then it is time shared (temporal) line configuration.



Network Topologies:

What is Topology?

In communication networks, a topology is usually a schematic description of the setup and the arrangement of a network, including its connecting lines and nodes. There are two ways of defining network geometry: the physical topology and the logical (signal) topology.

Physical Topology: *Physical topology* is the physical layout of the components on a network. The cabling layout used to link devices is known as the physical topology of the network. This refers to the layout of cabling, the locations of nodes, and the interconnections between the nodes and the cabling. The physical topology of a network is determined by the capabilities of the network access devices and media, the level of control or fault tolerance desired, and the cost associated with cabling or telecommunications circuits.

Logical Topology: *Determines how the hosts access the medium to communicate across the network. The logical topology in contrast, is the way that the signals act on the network media, or the way that the data passes through the network from one device to the next without regard to the physical interconnection of the devices. A network's logical topology is not necessarily the same as its physical topology.*

Reasons for Using Network Topology's:

So why does network topology matter? A few reasons are as follows:

- The Network Topology affects the Performance.
- The network topology is a factor in determining the media type used to cable the network.
- The network topology impacts the cost of cabling the network.

•Some access methods may only work with specific topologies. Some of the factors that affect choice of topology for a network are −

- **Cost** − Installation cost is a very important factor in overall cost of setting up an infrastructure. So cable lengths, distance between nodes, location of servers, etc. have to be considered when designing a network.
- **Flexibility** − Topology of a network should be flexible enough to allow reconfiguration of office set up, addition of new nodes and relocation of existing nodes.
- **Reliability** − Network should be designed in such a way that it has minimum down time. Failure of one node or a segment of cabling should not render the whole network useless.
- **Scalability** − Network topology should be scalable, i.e. it can accommodate load of new devices and nodes without perceptible drop in performance.
- **Ease of installation** − Network should be easy to install in terms of hardware, software and technical personnel requirements.
- **Ease of maintenance** − Troubleshooting and maintenance of network should be easy.

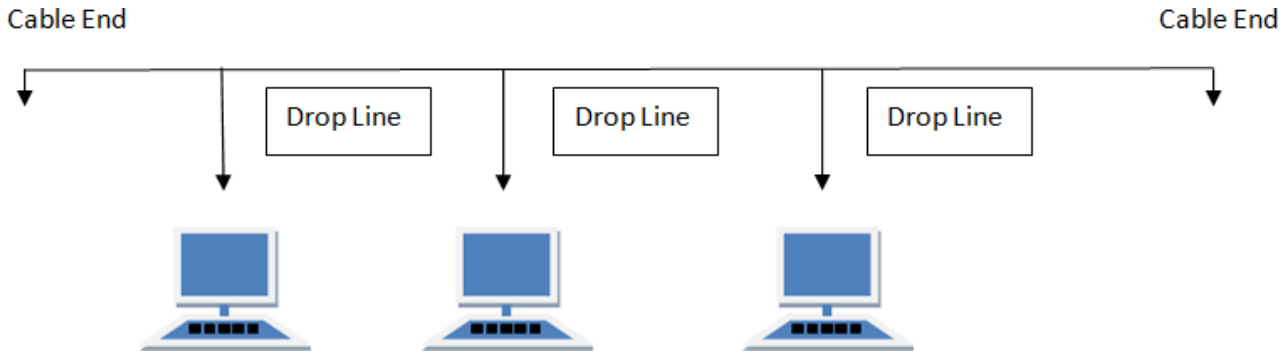
Types of Network Topologies:

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**.

Data network with bus topology has a **linear transmission cable**, usually **coaxial**, to which many **network devices** and **workstations** are attached along the length. **Server** is at one end of the bus. When a workstation has to send data, it transmits **packets** with **destination address** in its header along the bus.



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

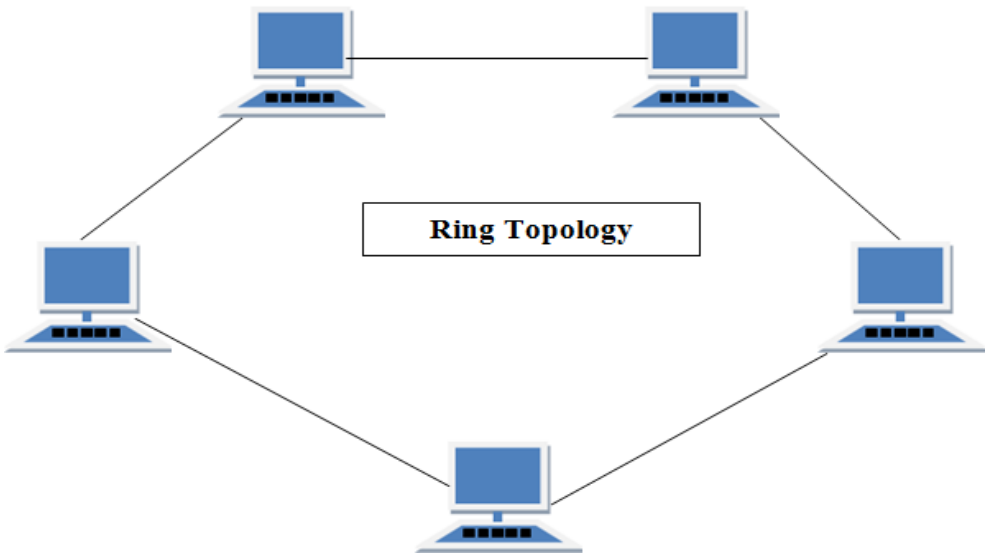
1. It is cost effective.
2. Cable required is least compared to other network topology.
3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

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. Dumb terminals cannot be connected to the bus
5. 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. In **ring topology** each terminal is connected to exactly **two nodes**, giving the network a circular shape. Data travels in only one pre-determined direction.



When a terminal has to send data, it transmits it to the neighboring node which transmits it to the next one. Before further transmission data may be amplified. In this way, data reverses the network and reaches the destination node, which removes it from the network. If the data reaches the sender, it removes the data and resends it later.

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.
3. Small cable segments are needed to connect two nodes
4. Ideal for optical fibers as data travels in only one direction
5. Very high transmission speeds possible

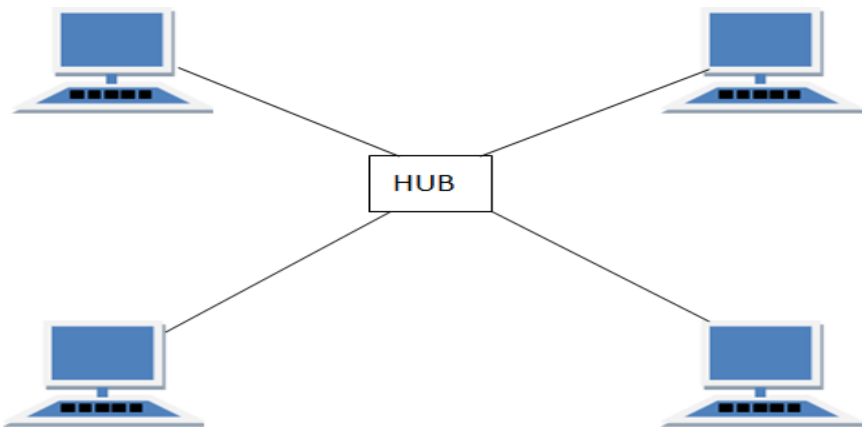
Disadvantages of Ring Topology

1. Adding or deleting the computers disturbs the network activity. Difficult to remove one or more nodes while keeping the rest of the network intact
2. Failure of one computer disturbs the whole network.
3. Troubleshooting is difficult as many nodes may have to be inspected before faulty one is identified

---

STAR Topology

In star topology, server is connected to each node individually. Server is also called the central node. 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. Any exchange of data between two nodes must take place through the server. It is the most popular topology for information and voice networks as central node can process data received from source node before sending it to the destination 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. Failure of one node does not affect the network. 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:

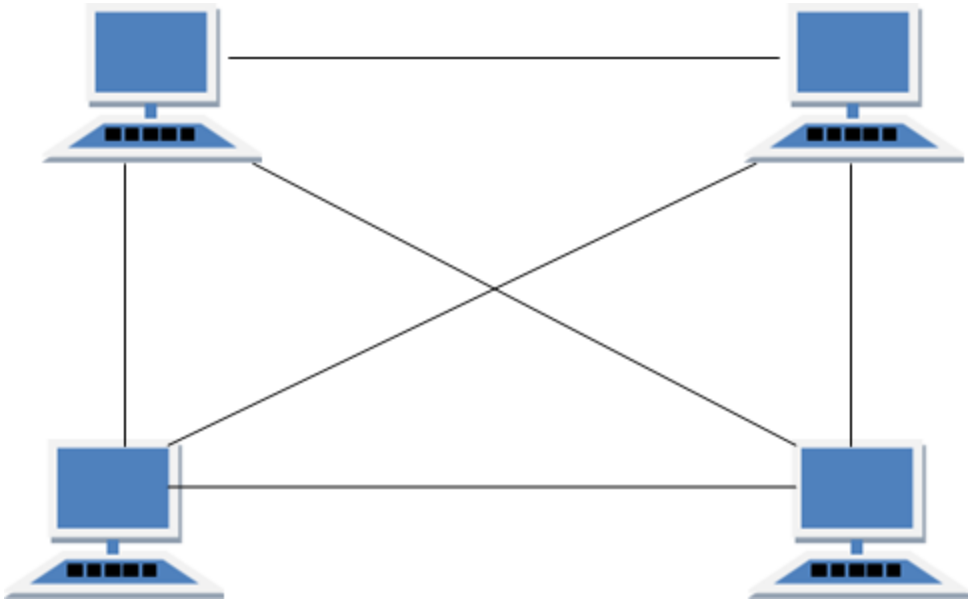
1. Routing
2. Flooding

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 nodes etc. We can even have routing logic, to re-configure the failed nodes.

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 it's 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.

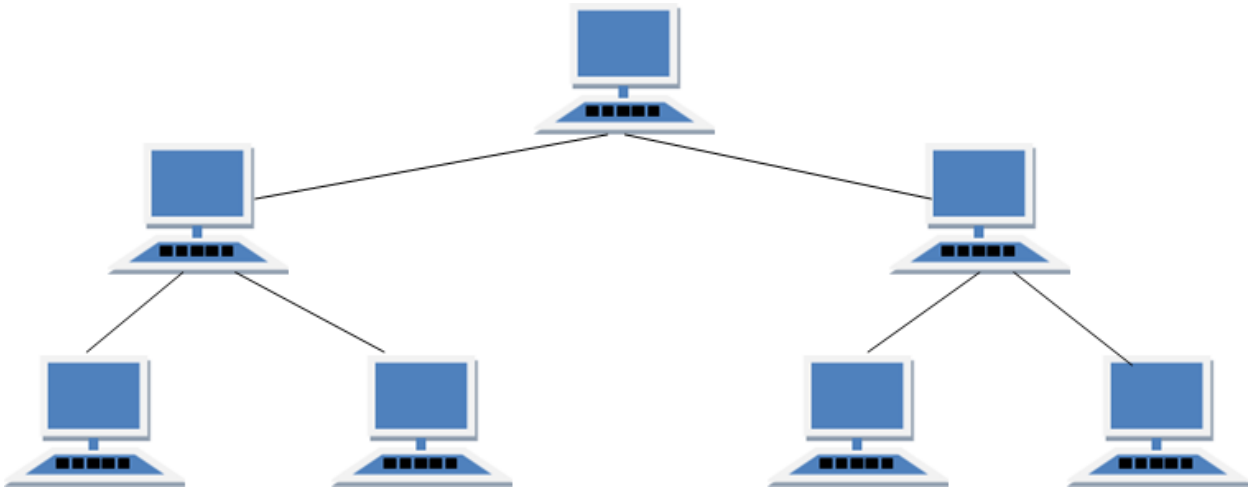
Disadvantages of Mesh Topology

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

TREE Topology

Tree topology has a group of star networks connected to a linear bus backbone cable. It incorporates features of both star and bus topologies.

It has a root node and all other nodes are connected to it forming a hierarchy. It is also called hierarchical topology. It should at least have three levels to the hierarchy.



Features of Tree Topology

1. Ideal if workstations are located in groups.
2. Used in Wide Area Network.

Advantages of Tree Topology

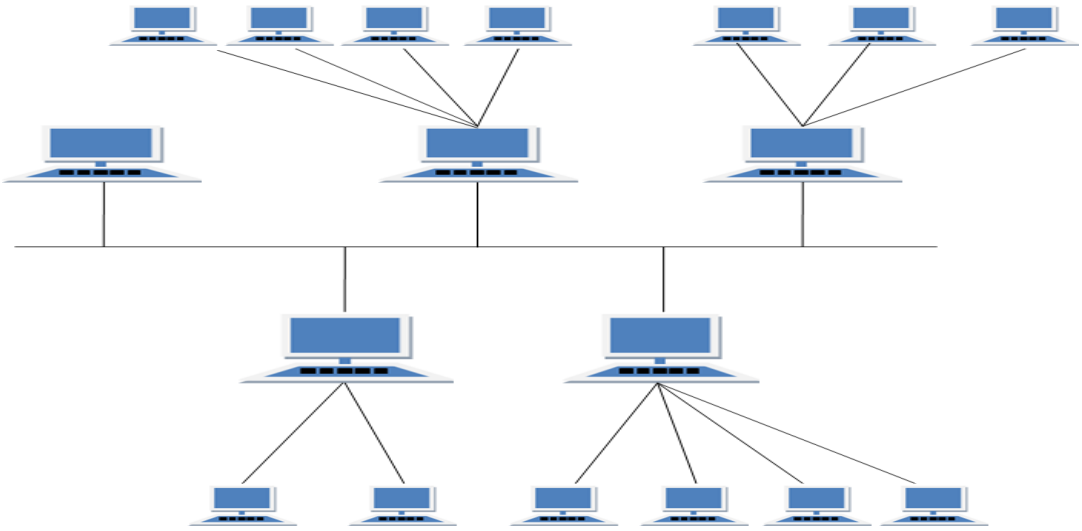
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy. Existing network can be easily expanded
3. Easily managed and maintained. Point-to-point wiring for individual segments means easier installation and maintenance
4. Error detection is easily done.
5. Well suited for temporary networks

Disadvantages of Tree Topology

1. Technical expertise required to configure and wire tree topology
2. Failure of backbone cable brings down entire network
3. Insecure network
4. Heavily cabled.
5. Costly.
6. If more nodes are added maintenance is difficult.
7. Central hub fails, network fails.

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.

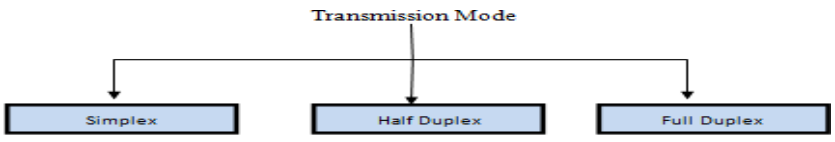
Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.

Transmission Modes in Computer Networks:

Transmission mode means transferring of data between two devices. It is also called communication mode. These modes direct the direction of flow of information. There are three types of transmission mode. They are:

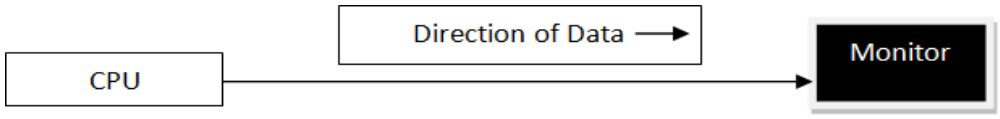
- Simplex Mode
- Half duplex Mode
- Full duplex Mode



SIMPLEX Mode

In this type of transmission mode data can be sent only through one direction i.e. communication is unidirectional. We cannot send a message back to the sender. Unidirectional communication is done in Simplex Systems.

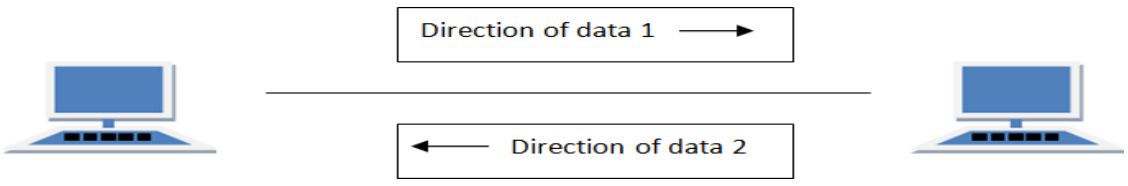
Examples of simplex Mode is loudspeaker, television broadcasting, television and remote, keyboard and monitor etc.



HALF DUPLEX Mode

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time. For example, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one that can carry data in both directions) but data can be sent in only one direction at a time.

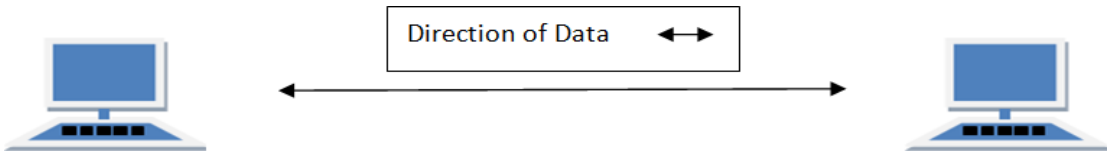
Example of half duplex is a walkie- talkie in which message is sent one at a time and messages are sent in both the directions.



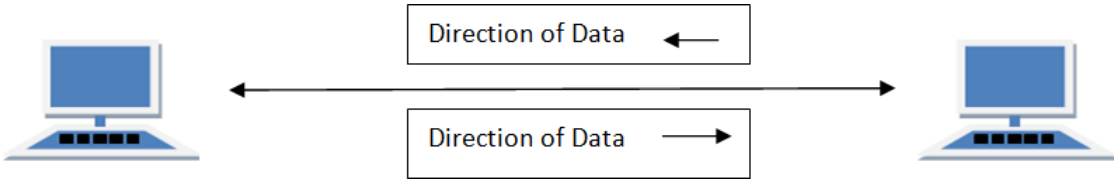
FULL DUPLEX Mode

In full duplex system we can send data in both directions as it is bidirectional. Data can be sent in both directions simultaneously. We can send as well as we receive the data.

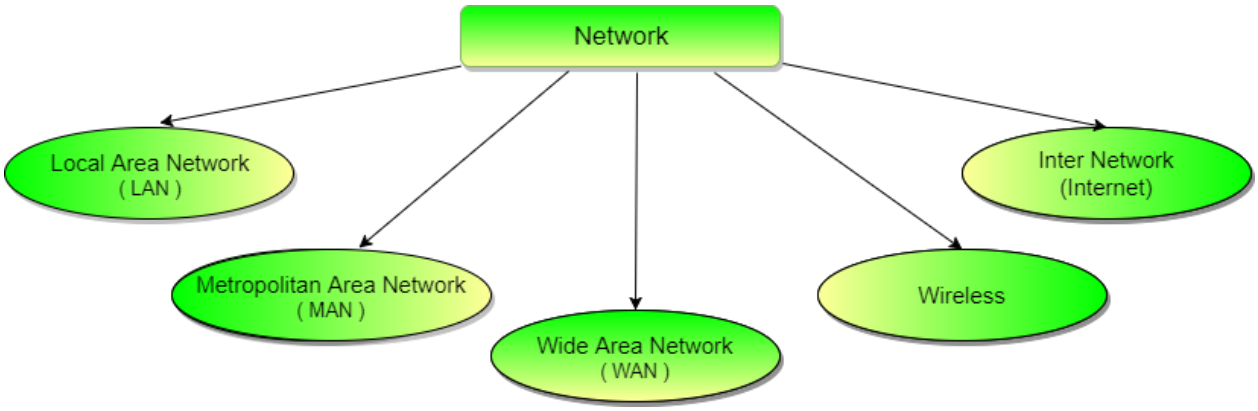
Example of Full Duplex is a Telephone Network in which there is communication between two persons by a telephone line, through which both can talk and listen at the same time.



In full duplex system there can be two lines one for sending the data and the other for receiving data.

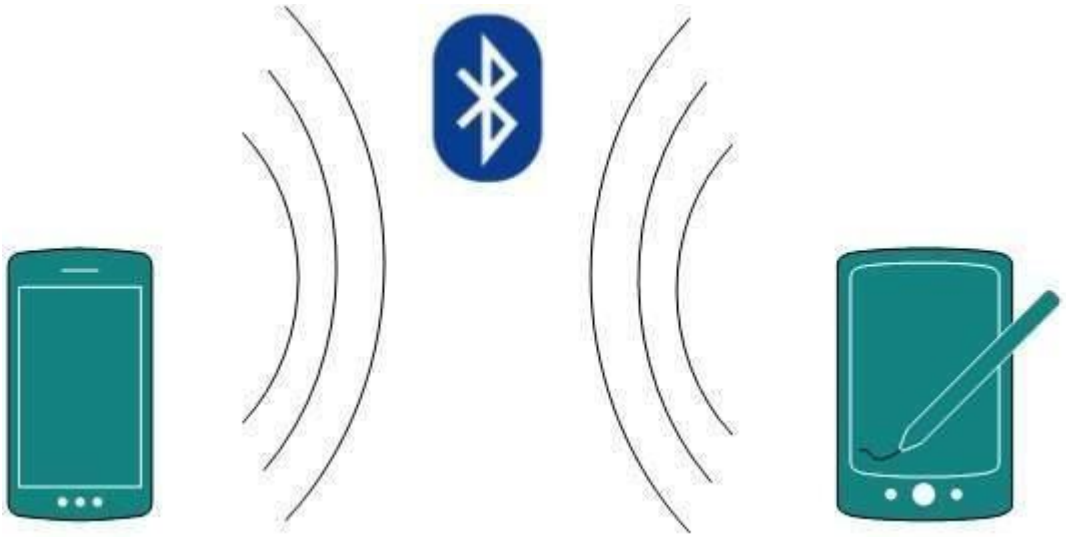


Types of Communication Networks



Personal Area Network:

A Personal Area Network (PAN) is smallest network which is very personal to a user. This may include Bluetooth enabled devices or infra-red enabled devices. PAN has connectivity range up to 10 meters. PAN may include wireless computer keyboard and mouse, Bluetooth enabled headphones, wireless printers and TV remotes.



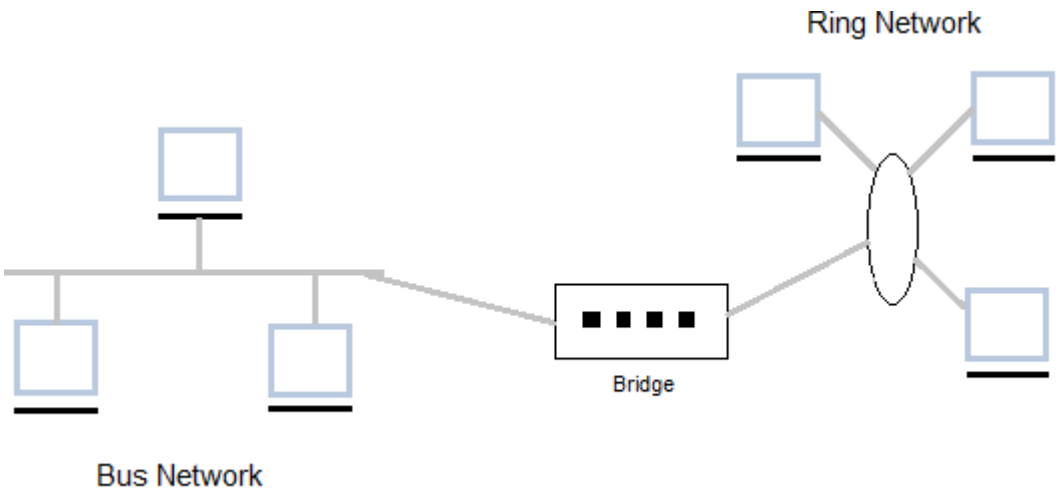
For example, Piconet is Bluetooth-enabled Personal Area Network which may contain up to 8 devices connected together in a master-slave fashion.

Local Area Network (LAN)

It is also called LAN and designed for small physical areas such as an office, group of buildings or a factory. LANs are used widely as it is easy to design and to troubleshoot. Personal computers and workstations are connected to each other through LANs. We can use different types of topologies through LAN, these are Star, Ring, Bus, Tree etc.

LAN can be a simple network like connecting two computers, to share files and network among each other while it can also be as complex as interconnecting an entire building.

LAN networks are also widely used to share resources like printers, shared hard-drive etc.



(Different Topologies interconnected in a Local Area Network)

Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.

Applications of LAN

- One of the computers in a network can become a server serving all the remaining computers called clients. Software can be stored on the server and it can be used by the remaining clients.
- Connecting locally all the workstations in a building to let them communicate with each other locally without any internet access.
- Sharing common resources like printers etc are some common applications of LAN.

Advantages of LAN

- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
- **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate licensed software for each client a network.
- **Easy and Cheap Communication:** Data and messages can easily be transferred over networked computers.
- **Centralized Data:** The data of all network users can be saved on hard disk of the server computer. This will help users to use any workstation in a network to access their data. Because data is not stored on workstations locally.
- **Data Security:** Since, data is stored on server computer centrally, it will be easy to manage data at only one place and the data will be more secure too.
- **Internet Sharing:** Local Area Network provides the facility to share a single internet connection among all the LAN users. In Net Cafes, single internet connection sharing system keeps the internet expenses cheaper.

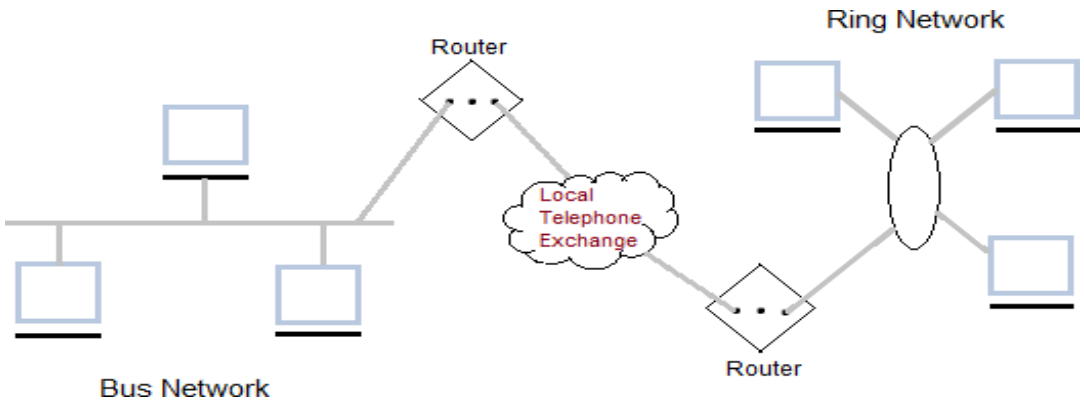
Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
- **Data Security Threat:** Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.

- **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

It was developed in 1980s.It is basically a bigger version of LAN. It is also called MAN and uses the similar technology as LAN. It is designed to extend over the entire city. It can be means to connecting a number of LANs into a larger network or it can be a single cable. It is mainly hold and operated by single private company or a public company.



Characteristics of MAN

- It generally covers towns and cities (50 km)
- Communication medium used for MAN are optical fibers, cables etc.
- Data rates adequate for distributed computing applications.

Advantages of MAN

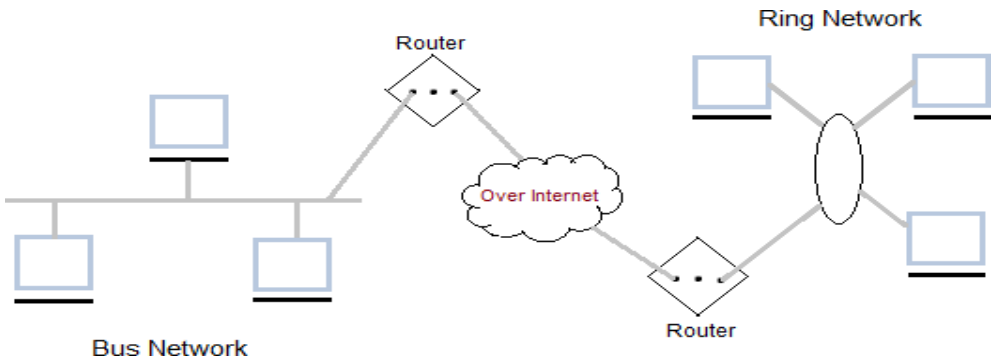
- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually encompasses several blocks of a city or an entire city.

Disadvantages of MAN

- More cable required for a MAN connection from one place to another.
- It is difficult to make the system secure from hackers and industrial espionage(spying) graphical regions.

Wide Area Network (WAN)

It is also called WAN. WAN can be private or it can be public leased network. It is used for the network that covers large distance such as cover states of a country. It is not easy to design and maintain. Communication medium used by WAN are PSTN or Satellite links. WAN operates on low data rates.



Characteristics of WAN

- It generally covers large distances (states, countries, continents).
- Communication medium used are satellite, public telephone networks which are connected by routers.

Advantages of WAN

- Covers a large geographical area so long distance business can connect on the one network.
- Shares software and resources with connecting workstations.
- Messages can be sent very quickly to anyone else on the network. These messages can have picture, sounds or data included with them (called attachments).
- Expensive things (such as printers or phone lines to the internet) can be shared by all the computers on the network without having to buy a different peripheral for each computer.
- Everyone on the network can use the same data. This avoids problems where some users may have older information than others.

Disadvantages of WAN

- Need a good firewall to restrict outsiders from entering and disrupting the network.
- Setting up a network can be an expensive, slow and complicated. The bigger the network the more expensive it is.
- Once set up, maintaining a network is a full-time job which requires network supervisors and technicians to be employed.
- Security is a real issue when many different people have the ability to use information from other computers. Protection against hackers and viruses adds more complexity and expense.

Wireless Network

Digital wireless communication is not a new idea. Earlier, **Morse code** was used to implement wireless networks. Modern digital wireless systems have better performance, but the basic idea is the same.

Wireless Networks can be divided into three main categories:

1. **System interconnection**
2. **Wireless LANs**
3. **Wireless WANs**

System Interconnection

System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.

In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

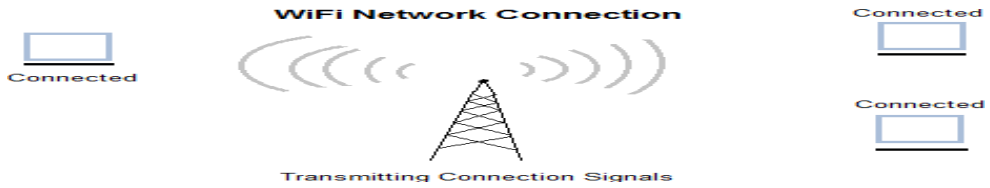
Wireless LANs

These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard for wireless LANs called **IEEE 802.11**, which most systems implement and which is becoming very widespread.

Wireless WANs

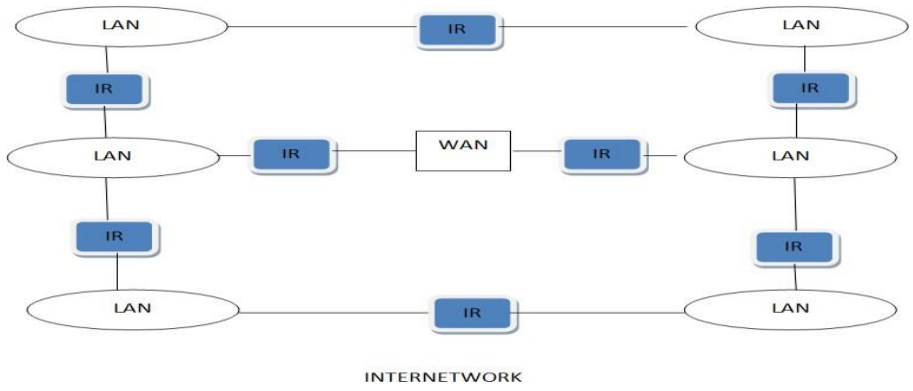
The radio network used for cellular telephones is an example of a low-bandwidth wireless WAN. This system has already gone through three generations.

- The first generation was analog and for voice only.
- The second generation was digital and for voice only.
- The third generation is digital and is for both voice and data.



Inter Network

Inter Network or Internet is a combination of two or more networks. Inter network can be formed by joining two or more individual networks by means of various devices such as routers, gateways and bridges.



Connection Oriented and Connectionless Services

These are the two services given by the layers to layers above them. These services are :

1. Connection Oriented Service
2. Connectionless Services

Connection Oriented Services

There is a sequence of operation to be followed by the users of connection oriented service. These are:

1. Connection is established
2. Information is sent
3. Connection is released

In connection oriented service we have to establish a connection before starting the communication. When connection is established we send the message or the information and then we release the connection.

Connection oriented service is more reliable than connectionless service. We can send the message in connection oriented service if there is an error at the receivers end. Example of connection oriented is TCP (Transmission Control Protocol) protocol.

Connection-Less Services

It is similar to the postal services, as it carries the full address where the message (letter) is to be carried. Each message is routed independently from source to destination. The order of message sent can be different from the order received.

In connectionless the data is transferred in one direction from source to destination without checking that destination is still there or not or if it prepared to accept the message. Authentication is not needed in this. Example of Connectionless service is UDP (User Datagram Protocol) protocol.

Difference between Connection-oriented service and Connectionless service

1. In connection oriented service authentication is needed while connectionless service does not need any authentication.
2. Connection oriented protocol makes a connection and checks whether message is received or not and sends again if an error occurs connectionless service protocol does not guarantees a delivery.
3. Connection oriented service is more reliable than connectionless service.
4. Connection oriented service interface is stream based and connectionless is message based.

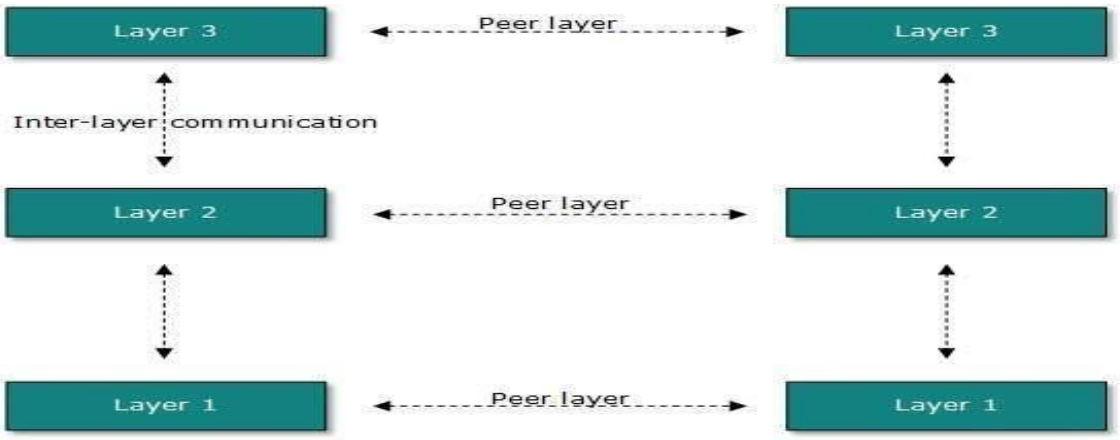
Network Software and Layered Concepts:

Networking engineering is a complicated task, which involves software, firmware, chip level engineering, hardware, and electric pulses. To ease network engineering, the whole networking concept is divided into multiple layers. Each layer is involved in some particular task and is independent of all other layers. But as a whole, almost all networking tasks depend on all of these layers. Layers share data between them and they depend on each other only to take input and send output.

Layered Tasks:

In layered architecture of Network Model, one whole network process is divided into small tasks. Each small task is then assigned to a particular layer which works dedicatedly to process the task only. Every layer does only specific work.

In layered communication system, one layer of a host deals with the task done by or to be done by its peer layer at the same level on the remote host. The task is either initiated by layer at the lowest level or at the top most level. If the task is initiated by the-top most layer, it is passed on to the layer below it for further processing. The lower layer does the same thing, it processes the task and passes on to lower layer. If the task is initiated by lower most layer, then the reverse path is taken.



Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task. All layers identify their counterparts by means of encapsulation header and tail.

Protocols

These are set of rules that govern the format and meaning of frames, messages or packets that are exchanged between the server and client.

A network protocol defines rules and conventions for communication between network devices. Network protocols include mechanisms for devices to identify and make connections with each other, as well as formatting rules that specify how data is packaged into messages sent and received. Some protocols also support message acknowledgment and data compression designed for reliable and/or high-performance network communication.

The key elements of the protocol are Syntax, semantics, and timing.

Syntax:

The term syntax refers to the structure or format of the data, meaning the order in which they are presented, for example, a some 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 are 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.

Layering Concepts and Benefits:

Network architectures define the standards and techniques for designing and building communication systems for computers and other devices. The layered concept of networking was developed to accommodate changes in technology. Each layer of a specific network model may be responsible for a different function of the network. Each layer will pass information up and down to the next subsequent layer as data is processed.

To reduce the design complexity, most of the networks are organized as a series of **layers** or **levels**, each one build upon one below it. The basic idea of a layered architecture is *to divide the design into small pieces*. Each layer adds to the services provided by the lower layers in such a manner that the highest layer is provided a full set of services to manage communications and run the applications. The benefits of the layered models are modularity and clear interfaces, i.e. open architecture and comparability between the different providers' components.

A basic principle is to ensure independence of layers by defining services provided by each layer to the next higher layer without defining how the services are to be performed. This permits changes in a layer without affecting other layers.

The number of layers, functions and contents of each layer differ from network to network. However in all networks, the purpose of each layer is to offer certain services to higher layers, shielding those layers from the details of how the services are actually implemented.

The basic elements of a layered model are **services, protocols and interfaces**.

- A *service* is a set of actions that a layer offers to another (higher) layer.
- *Protocol* is a set of rules that a layer uses to exchange information with a peer entity. These rules concern both the contents and the order of the messages used.
- Between the layers service interfaces are defined. The messages from one layer to another are sent through those interfaces.

Benefits of using layer structure:

By separating the network communications into logical smaller pieces, the OSI model simplifies how network protocols are designed

The benefits to layering networking protocol specifications are many including:

Interoperability

Greater Compatibility

Better Flexibility

Scalability

Mobility

Value Added Features

Cost Effective Quality

Modularity

Standardization and Certification

Task Segmentation

Portability

A five-layer architecture is shown in Fig.

The entities comprising the corresponding layers on different machines are called *peers*. In other words, it is the peers that communicate using protocols. In reality, no data is transferred from layer n on one machine to layer n of another machine. Instead, each layer passes data and control information to the layer immediately below it, until the lowest layer is reached. Below layer-1 is the physical layer through which actual communication occurs. The peer process abstraction is crucial to all network design. Using it, the un-manageable tasks of designing the complete network can be broken into several smaller, manageable, design problems, namely design of individual layers.

Between each pair of adjacent layers there is an interface. The interface defines which primitives operations and services the lower layer offers to the upper layer adjacent to it.

A set of layers and protocols is known as **network architecture**. The specification of architecture must contain enough information to allow an implementation to write the program or build the hardware for each layer so that it will correctly obey the appropriate protocol. Neither the details of implementation nor the specification of interface is a part of network architecture because these are hidden away inside machines and not visible from outside. It is not even necessary that the interface on all machines in a network be same, provided that each machine can correctly use all protocols. A list of protocols used by a certain system, one protocol per layer, is called **protocol stack**.

Why Layered architecture?

1.To make the design process easy by breaking unmanageable tasks into several smaller and manageable tasks (by divide-and-conquer approach).

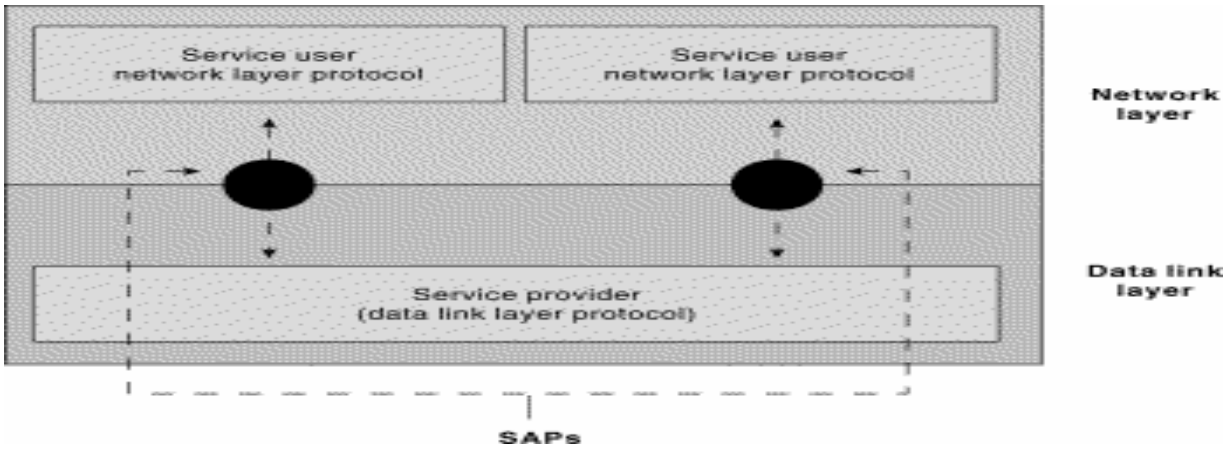
2.Modularity and clear interfaces, so as to provide comparability between the different providers' components.

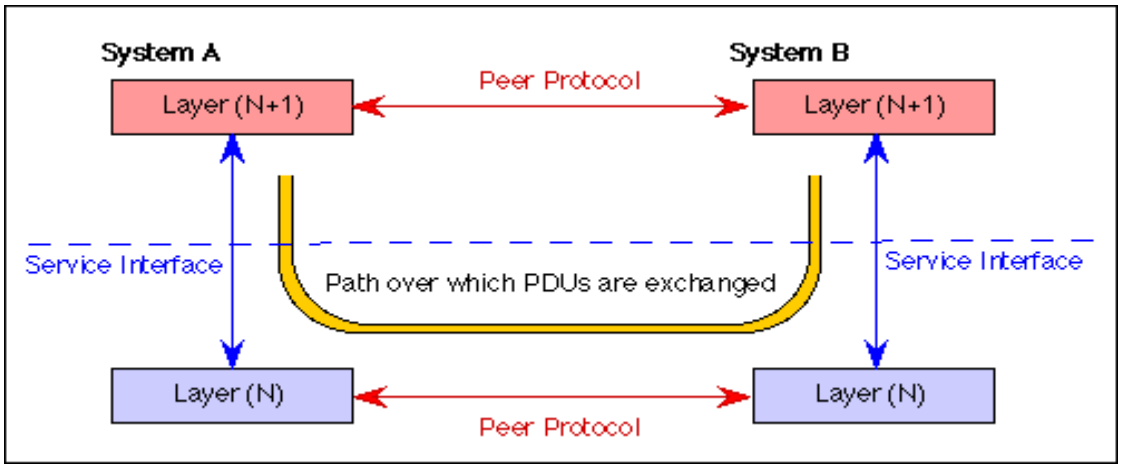
3.Ensure independence of layers, so that implementation of each layer can be changed or modified without affecting other layers.

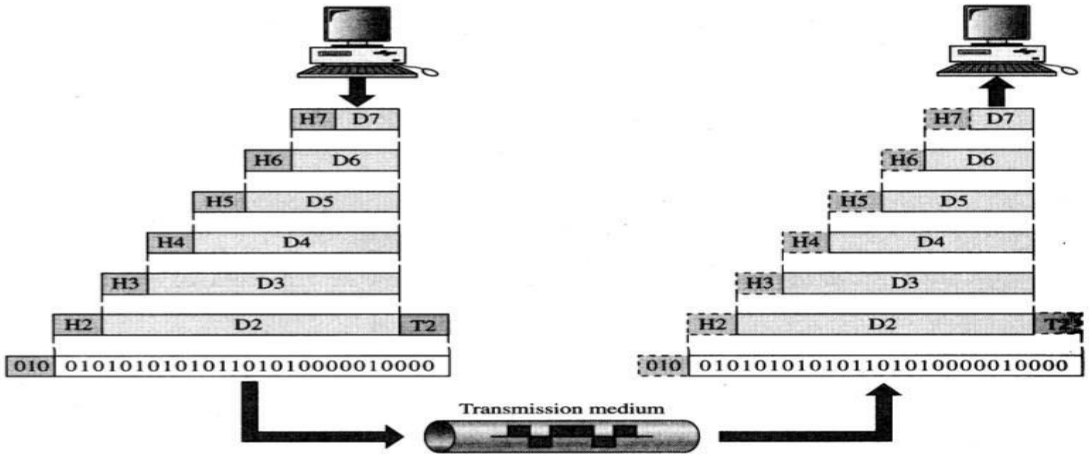
4. Each layer can be analyzed and tested independently of all other layers.

Services and service access points :

One OSI layer communicates with another layer to make use of the services provided by the second layer. The services provided by adjacent layers help a given OSI layer communicate with its peer layer in other computer systems. Three basic elements are involved in layer services: the service user, the service provider, and the service access point (SAP).







In Figure above, which gives an overall view of the OSI network model layers, D7 means the data unit at layer 7, D6 means the data unit at layer 6, and so on. The process starts at layer 7 (the application layer), then moves from layer to layer in descending, sequential order. At each layer, a header, or possibly a trailer, can be added to the data unit. Commonly, the trailer is added only at layer 2. When the formatted data unit passes through the physical layer (layer 1), it is changed into an electromagnetic signal and transported along a physical link.

Upon reaching its destination, the signal passes into layer 1 and is transformed back into digital form. The data units then move back up through the OSI network model layers. As each block of data reaches the next higher layer, the headers and trailers attached to it at the corresponding sending layer are removed, and actions appropriate to that layer are taken. By the time it reaches layer 7, the message is again in a form appropriate to the application and is made available to the recipient.

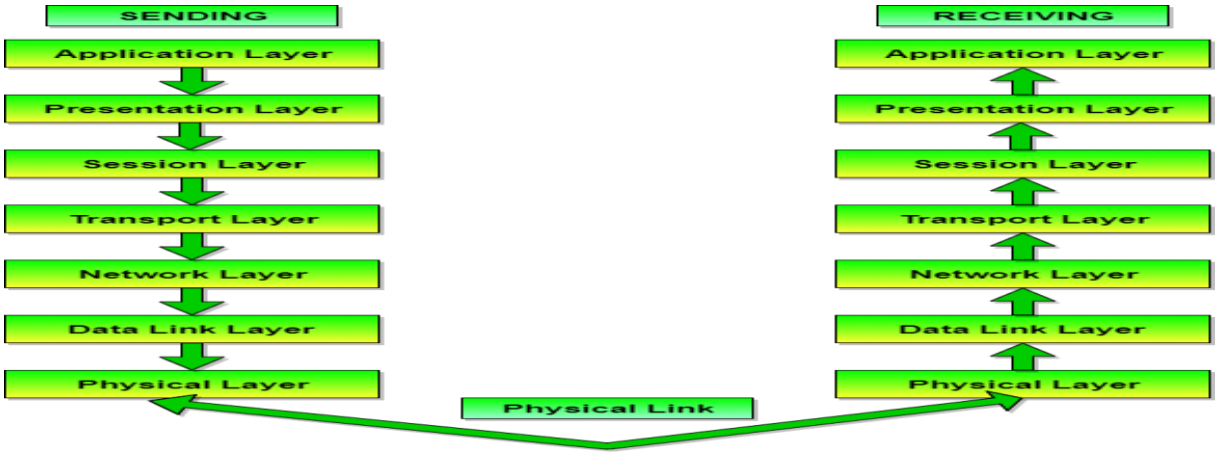
Models in Communication Networks:

The most important reference models are:

1. OSI reference model.
2. TCP/IP model.

Introduction to ISO-OSI Model:

There are many users who use computer network and are located all over the world. To ensure national and worldwide data communication ISO (ISO stands for International Organization of Standardization.) developed this model. This is called a model for open system interconnection (OSI) and is normally called as OSI model.OSI model architecture consists of seven layers. It defines seven layers or levels in a complete communication system. OSI Reference model is explained in other chapter.



It's easy to remember the sequence of OSI Model 7 Layers using this simple sentence:

"All people seem to need data processing."

All = Application Layer

People= Presentation Layer

Seem = Session Layer

To = Transport Layer

Need = Network Layer

Data = Data Link Layer

Processing = Physical Layer

“Please Do Not Throw Salami Pizza Away”

“Please Do Not Tell Secret Passwords Anytime”

“Please Do Not Teach Students Pointless Acronyms”

"Please Do Not Tell Stupid People Anything."

Transport Layer—Segments (SOME)

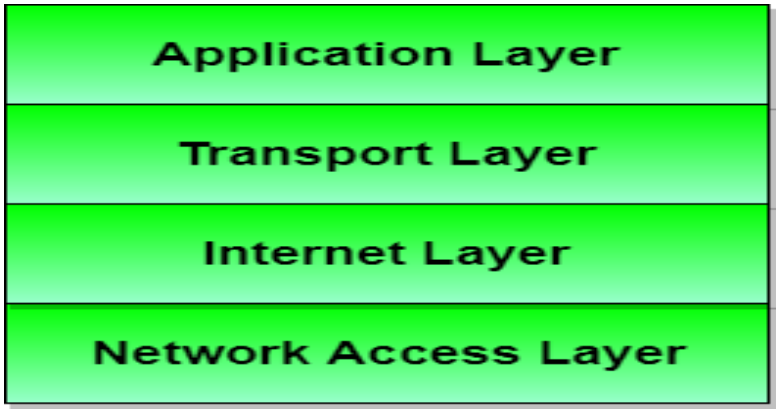
Network Layer—Packets (PEOPLE)

Data Link Layer—Frames (FEAR)

Physical Layer— Bits (BIRTHDAYS)

<u>Introduction to TCP/IP Model:</u>

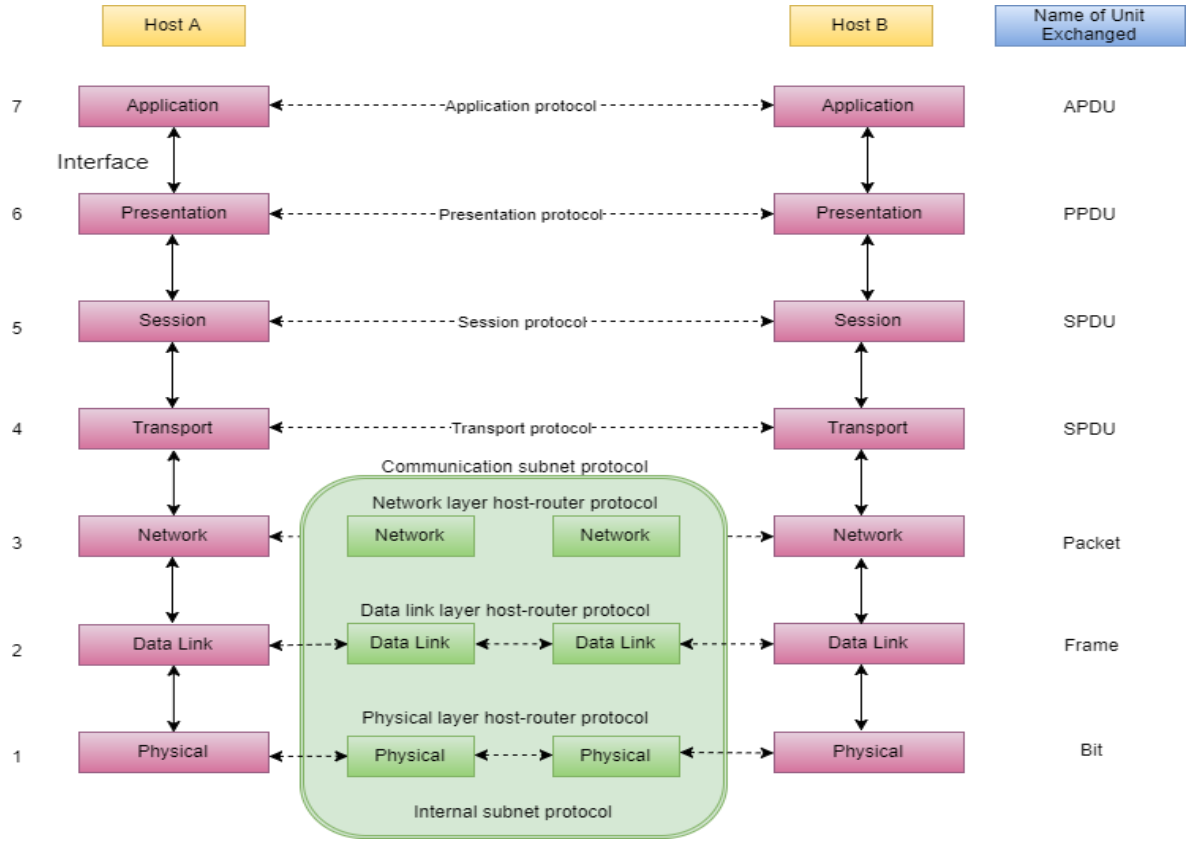
TCP/IP is transmission control protocol and internet protocol. Protocols are set of rules which govern every possible communication over the internet. These protocols describe the movement of data between the host computers or internet and offers simple naming and addressing schemes.



ISO/OSI Model in Communication Networks

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.

The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system.



Layer	Name of Protocol	Name of Unit exchanged
Application	Application Protocol	APDU - Application Protocol Data Unit
Presentation	Presentation Protocol	PPDU - Presentation Protocol Data Unit
Session	Session Protocol	SPDU - Session Protocol Data Unit
Transport	Transport Protocol	TPDU - Transport Protocol Data Unit
Network	Network layer host-router Protocol	Packet
Data Link	Data link layer host-router Protocol	Frame
Physical	Physical layer host-router Protocol	Bit

Feature of OSI Model:

1. Big picture of communication over network is understandable through this OSI model.
2. We see how hardware and software work together.
3. We can understand new technologies as they are developed.
4. Troubleshooting is easier by separate networks.
5. Can be used to compare basic functional relationships on different networks.

Functions of Different Layers:

Layer 1: The Physical Layer:

1. It is the lowest layer of the OSI Model.
2. It activates, maintains and deactivates the physical connection.
3. It is responsible for transmission and reception of the unstructured raw data over network.
4. Voltages and data rates needed for transmission is defined in the physical layer.
5. It converts the digital/analog bits into electrical signal or optical signals.
6. Data encoding is also done in this layer.

Layer 2: Data Link Layer:

1. Data link layer synchronizes the information which is to be transmitted over the physical layer.
2. The main function of this layer is to make sure data transfer is error free from one node to another, over the physical layer.
3. Transmitting and receiving data frames sequentially is managed by this layer.
4. This layer sends and expects acknowledgements for frames received and sent respectively. Resending of non-acknowledgement received frames is also handled by this layer.
5. This layer establishes a logical layer between two nodes and also manages the Frame traffic control over the network. It signals the transmitting node to stop, when the frame buffers are full.

Layer 3: The Network Layer:

1. It routes the signal through different channels from one node to other.
2. It acts as a network controller. It manages the Subnet traffic.
3. It decides by which route data should take.
4. It divides the outgoing messages into packets and assembles the incoming packets into messages for higher levels.

Layer 4: Transport Layer:

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as Multiplexing, Segmenting or Splitting on the data are done by this layer
3. It receives messages from the Session layer above it, convert the message into smaller units and passes it on to the Network layer.
4. Transport layer can be very complex, depending upon the network requirements.

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer:

1. Session layer manages and synchronize the conversation between two different applications.
2. Transfer of data from source to destination session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The Presentation Layer:

1. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data.
2. While receiving the data, presentation layer transforms the data to be ready for the application layer.
3. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role of translator.
4. It performs Data compression, Data encryption, Data conversion etc.

Layer 7: Application Layer:

1. It is the topmost layer.
2. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.
3. This layer mainly holds application programs to act upon the received and to be sent data.

Merits of OSI reference model:

1. OSI model distinguishes well between the services, interfaces and protocols.
2. Protocols of OSI model are very well hidden.
3. Protocols can be replaced by new protocols as technology changes.
4. Supports connection oriented services as well as connectionless service.

Demerits of OSI reference model:

1. Model was devised before the invention of protocols.
2. Fitting of protocols is tedious task.
3. It is just used as a reference model.

OSI Reference Model- Detailed Description:

PHYSICAL Layer - OSI Model

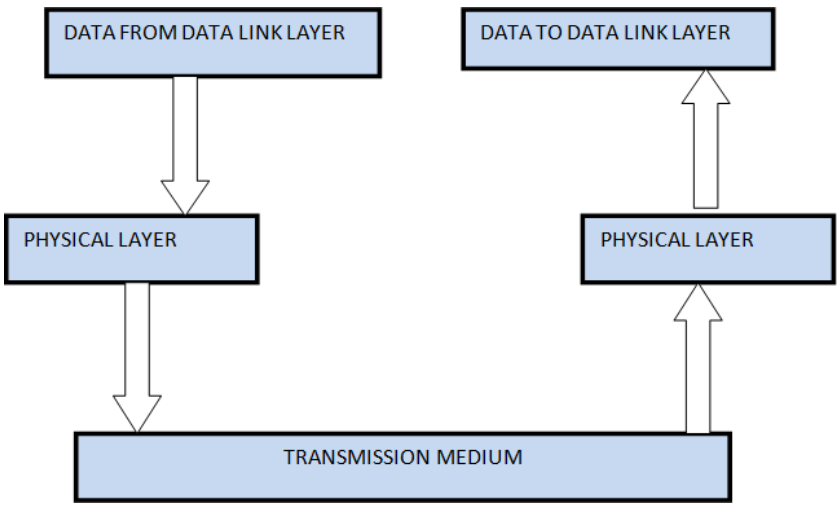
Physical layer is the lowest layer of all. It is responsible for sending bits from one computer to another. This layer is not concerned with the meaning of the bits and deals with the physical connection to the network and with transmission and reception of signals.

This layer defines electrical and physical details represented as 0 or a 1. How many pins a network will contain, when the data can be transmitted or not and how the data would be synchronized.

FUNCTIONS OF PHYSICAL LAYER:

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.

2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.
3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.
4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.
5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.
6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.
7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, and Full Duplex.
8. Deals with baseband and broadband transmission.



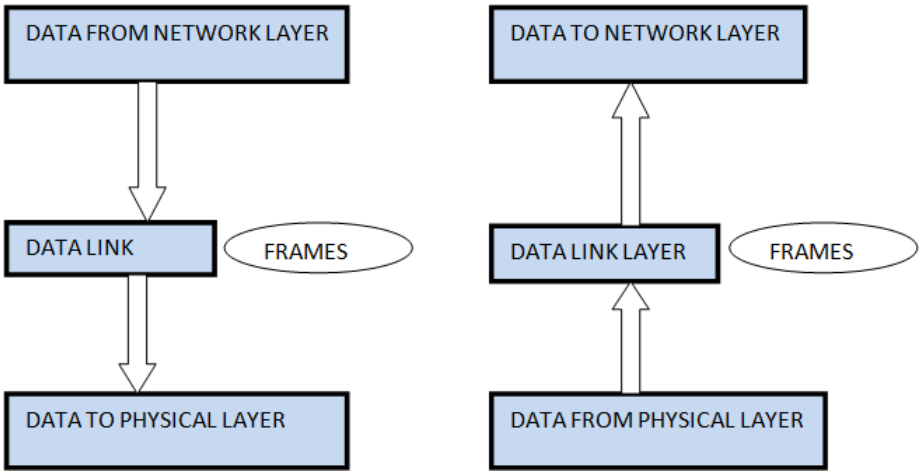
DATA LINK Layer - OSI Model

Data link layer is most reliable node to node delivery of data. It forms frames from the packets that are received from network layer and gives it to physical layer. It also synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical.

Error detection bits are used by the data link layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message.

FUNCTIONS OF DATA LINK LAYER:

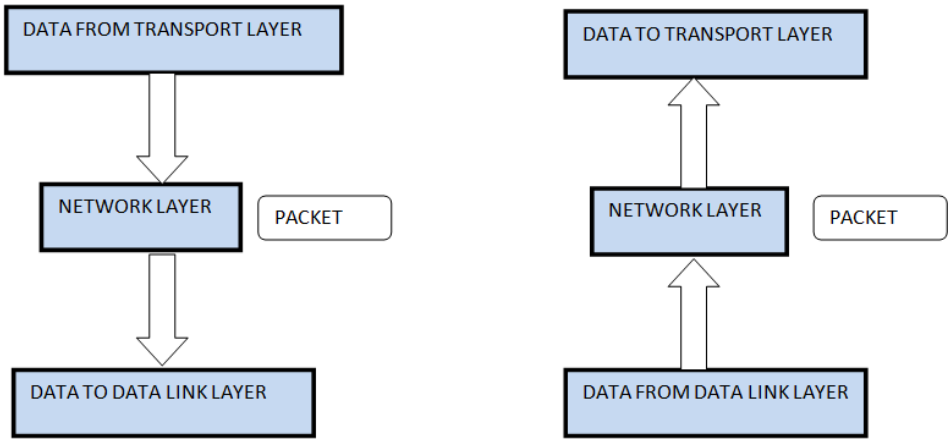
1. **Framing:** Frames are the streams of bits received from the network layer into manageable data units. This division of stream of bits is done by Data Link Layer.
2. **Physical Addressing:** The Data Link layer adds a header to the frame in order to define physical address of the sender or receiver of the frame, if the frames are to be distributed to different systems on the network.
3. **Flow Control:** A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
4. **Error Control:** Error control is achieved by adding a trailer at the end of the frame. Duplication of frames is also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
5. **Access Control:** Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



Network Layer - OSI Model

The main aim of this layer is to deliver packets from source to destination across multiple links (networks). If two computers (system) are connected on the same link then there is no need for a network layer. It routes the signal through different channels to the other end and acts as a network controller.

It also divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.



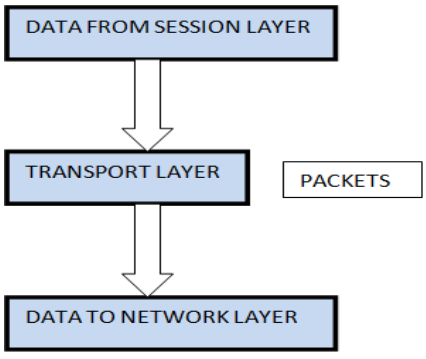
FUNCTIONS OF NETWORK LAYER:

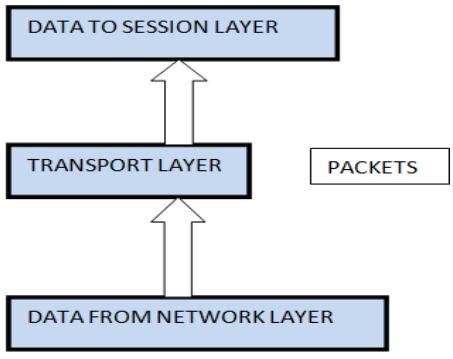
1. It translates logical network address into physical address. Concerned with circuit, message or packet switching.
2. Routers and gateways operate in the network layer. Mechanism is provided by Network Layer for routing the packets to final destination.
3. Connection services are provided including network layer flow control, network layer error control and packet sequence control.
4. Breaks larger packets into small packets.

Transport Layer - OSI Model

The main aim of transport layer is to be delivered the entire message from source to destination. Transport layer ensures whole message arrives intact and in order, ensuring both error control and flow control at the source to destination level. It decides if data transmission should be on parallel path or single path

Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer and ensures that message arrives in order by checking error and flow control.



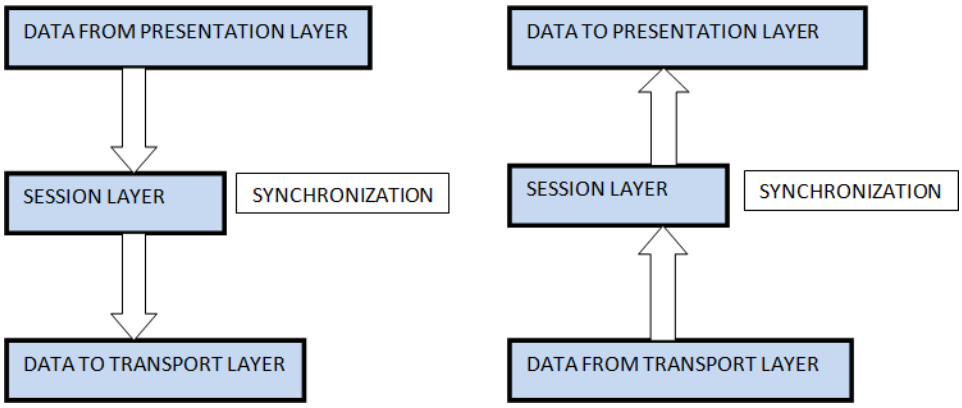


FUNCTIONS OF TRANSPORT LAYER:

1. **Service Point Addressing:** Transport Layer header includes service point address which is port address. This layer gets the message to the correct process on the computer unlike Network Layer, which gets each packet to the correct computer.
2. **Segmentation and Reassembling:** A message is divided into segments; each segment contains sequence number, which enables this layer in reassembling the message. Message is reassembled correctly upon arrival at the destination and replaces packets which were lost in transmission.
3. **Connection Control :** It includes 2 types :
   - Connectionless Transport Layer: Each segment is considered as an independent packet and delivered to the transport layer at the destination machine.
   - Connection Oriented Transport Layer: Before delivering packets, connection is made with transport layer at the destination machine.
4. **Flow Control:** In this layer, flow control is performed end to end.
5. **Error Control:** Error Control is performed end to end in this layer to ensure that the complete message arrives at the receiving transport layer without any error. Error Correction is done through retransmission.

Session Layer - OSI Model

Its main aim is to establish, maintain and synchronize the interaction between communicating systems. Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

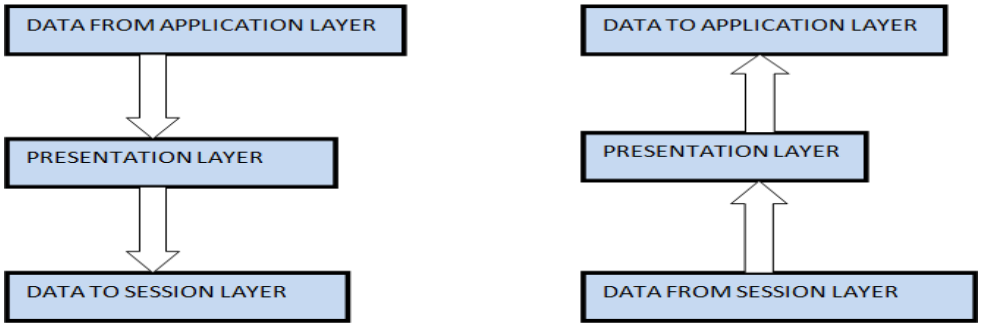


FUNCTIONS OF SESSION LAYER:

1. **Dialog Control:** This layer allows two systems to start communication with each other in half-duplex or full-duplex.
2. **Synchronization:** This layer allows a process to add checkpoints which are considered as synchronization points into stream of data. Example: If a system is sending a file of 800 pages, adding checkpoints after every 50 pages is recommended. This ensures that 50 page unit is successfully received and acknowledged. This is beneficial at the time of crash as if a crash happens at page number 110; there is no need to retransmit 1 to100 pages.

Presentation Layer - OSI Model

The primary goal of this layer is to take care of the syntax and semantics of the information exchanged between two communicating systems. Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

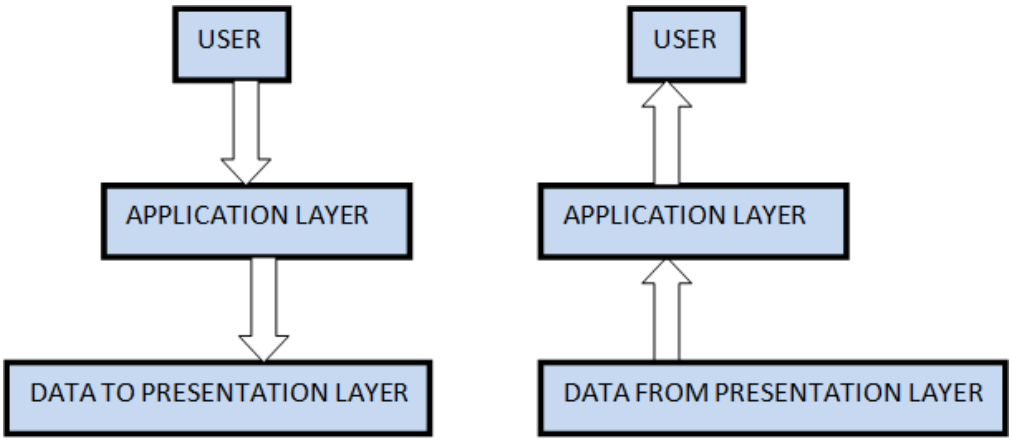


FUNCTIONS OF PRESENTATION LAYER:

1. **Translation:** Before being transmitted, information in the form of characters and numbers should be changed to bit streams. The presentation layer is responsible for interoperability between encoding methods as different computers use different encoding methods. It translates data between the formats the network requires and the format the computer.
2. **Encryption:** It carries out encryption at the transmitter and decryption at the receiver.
3. **Compression:** It carries out data compression to reduce the bandwidth of the data to be transmitted. The primary role of Data compression is to reduce the number of bits to be 0transmitted. It is important in transmitting multimedia such as audio, video, text etc.

Application Layer - OSI Model

It is the top most layer of OSI Model. Manipulation of data (information) in various ways is done in this layer which enables user or software to get access to the network. Some services provided by this layer includes: E-Mail, transferring of files, distributing the results to user, directory services, network resource etc.

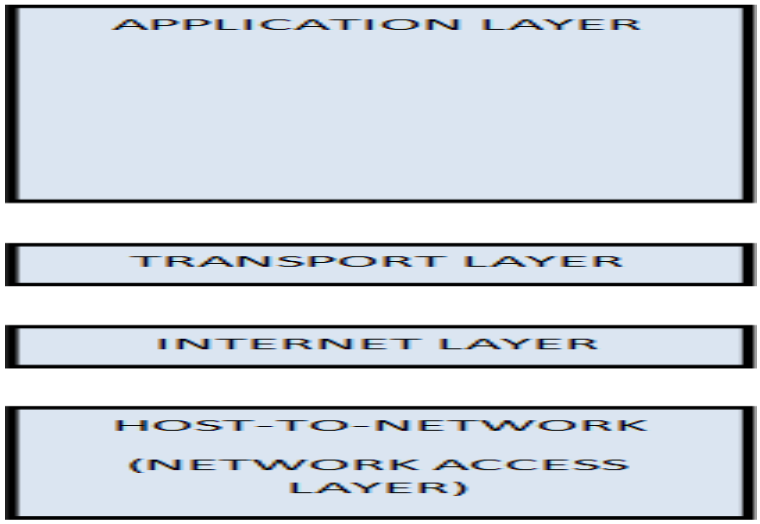


FUNCTIONS OF APPLICATION LAYER:

1. **Mail Services:** This layer provides the basis for E-mail forwarding and storage.
2. **Network Virtual Terminal:** It allows a user to log on to a remote host. The application creates software emulation of a terminal at the remote host. User's computer talks to the software terminal which in turn talks to the host and vice versa. Then the remote host believes it is communicating with one of its own terminals and allows user to log on.
3. **Directory Services:** This layer provides access for global information about various services.
4. **File Transfer, Access and Management (FTAM):** It is a standard mechanism to access files and manages it. Users can access files in a remote computer and manage it. They can also retrieve files from a remote computer.

The TCP/IP Reference Model

TCP/IP means Transmission Control Protocol and Internet Protocol. It is the network model used in the current Internet architecture as well. Protocols are set of rules which govern every possible communication over a network. These protocols describe the movement of data between the source and destination or the internet. These protocols offer simple naming and addressing schemes.



Overview of TCP/IP reference model

TCP/IP that is Transmission Control Protocol and Internet Protocol was developed by Department of Defense's Project Research Agency (ARPA, later DARPA) as a part of a research project of network interconnection to connect remote machines.

The features that stood out during the research, which led to making the TCP/IP reference model were:

- Support for a flexible architecture. Adding more machines to a network was easy.
- The network was robust, and connections remained intact until the source and destination machines were functioning.

The overall idea was to allow one application on one computer to talk to(send data packets) another application running on different computer.

Description of different TCP/IP protocols

Layer 1: Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect to the host, so that the packets can be sent over it.
3. Varies from host to host and network to network.

Layer 2: Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called an internet layer.
2. It is the layer which holds the whole architecture together.
3. It helps the packet to travel independently to the destination.
4. Order in which packets are received is different from the way they are sent.
5. IP (Internet Protocol) is used in this layer.

Layer 3: Transport Layer

1. It decides if data transmission should be on parallel path or single path.
2. Functions such as multiplexing, segmenting or splitting on the data is done by transport layer.

3. The applications can read and write to the transport layer.
4. Transport layer adds header information to the data.
5. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
6. Transport layer also arrange the packets to be sent, in sequence.

Layer 4: Application Layer

The TCP/IP specifications described a lot of applications that were at the top of the protocol stack. Some of them were TELNET, FTP, SMTP, DNS etc.

1. TELNET is a two-way communication protocol which allows connecting to a remote machine and run applications on it.
2. FTP (File Transfer Protocol) is a protocol that allows File transfer amongst computer users connected over a network. It is reliable, simple and efficient.
3. SMTP (Simple Mail Transport Protocol) is a protocol, which is used to transport electronic mail between a source and destination, directed via a route.
4. DNS (Domain Name Server) resolves an IP address into a textual address for Hosts connected over a network.

Merits of TCP/IP model

1. It operated independently.
2. It is scalable.
3. Client/server architecture.
4. Supports a number of routing protocols.
5. Can be used to establish a connection between two computers.

Demerits of TCP/IP

1. In this, the transport layer does not guarantee delivery of packets.
2. The model cannot be used in any other application.
3. Replacing protocol is not easy.
4. It has not clearly separated its services, interfaces and protocols.

Comparison of OSI Reference Model and TCP/IP Reference Model

Following are some major differences between OSI Reference Model and TCP/IP Reference Model, with diagrammatic comparison below.

OSI(Open System Interconnection)	**TCP/IP(Transmission Control Protocol / Internet Protocol)**
1. OSI is a generic, protocol independent standard, acting as a communication gateway between the network and end user.	1. TCP/IP model is based on standard protocols around which the Internet has developed. It is a communication protocol, which allows connection of hosts over a network.
2. In OSI model the transport layer guarantees the delivery of packets.	2. In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
3. Follows vertical approach.	3. Follows horizontal approach.

4. OSI model has a separate Presentation layer and Session layer.	4. TCP/IP does not have a separate Presentation layer or Session layer.
5. OSI is a reference model around which the networks are built. Generally it is used as a guidance tool.	5. TCP/IP model is, in a way implementation of the OSI model.
6. Network layer of OSI model provides both connection oriented and connectionless service.	6. The Network layer in TCP/IP model provides connectionless service.
7. OSI model has a problem of fitting the protocols into the model.	7. TCP/IP model does not fit any protocol
8. Protocols are hidden in OSI model and are easily replaced as the technology changes.	8. In TCP/IP replacing protocol is not easy.
9. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them. It is protocol independent.	9. In TCP/IP, services, interfaces and protocols are not clearly separated. It is also protocol dependent.
10. It has 7 layers	10. It has 4 layers

Diagrammatic Comparison between OSI Reference Model and TCP/IP Reference Model