Computer Networks
UNIT-1 Introduction

Prepared By,
M.Gouthamm, Asst.Prof, CSE, MRUH

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:

Data Communication: Local

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

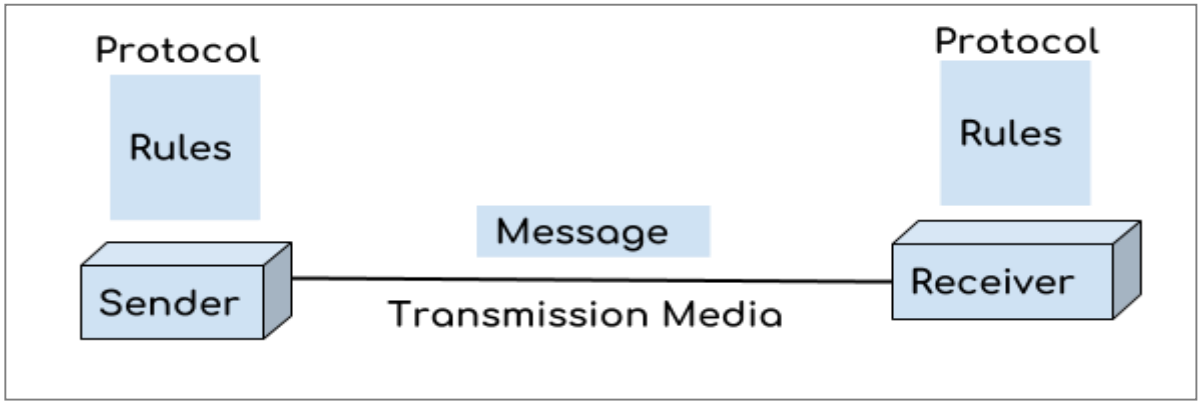
Data Communication: Remote

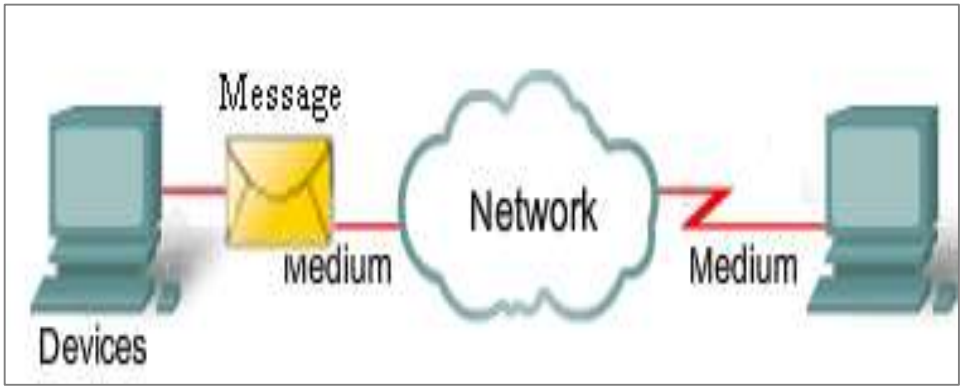
- Remote communication takes place over a distance i.e. the devices are farther.

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





Components of Data Communication

There are **five basic components** of Data Communication.

- **Message**: It is the data or information which needs to be transferred from one device to another device over a computer network.
- **Sender**: Sender is the device that has the data and needs to send the data to other device connected to the network.
- **Receiver**: A receiver is the device which is expecting the data from other device on the network.
- **Transmission media:** In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.
- **Protocol**: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol.

For example, http and https are the two protocols used by web browsers to get and post the data to internet, similarly smtp protocol is used by email services connected to the internet.

Basic Communication Model

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

Communication Model: Source

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

Communication Model: 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.

Communication Model: Transmission System

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

Communication Model: Receiver

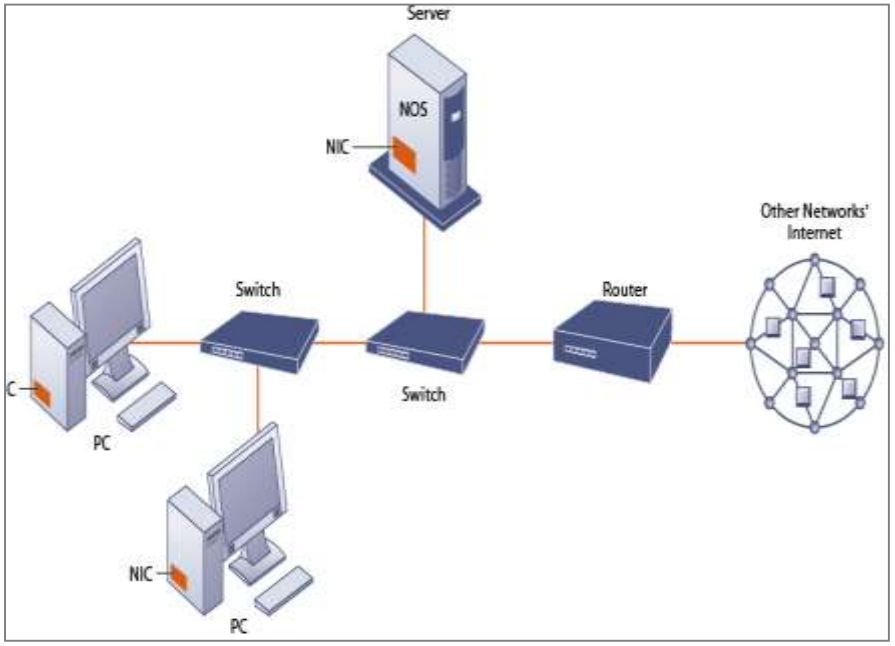
- Receiver accepts the signal from the transmission system and converts it into a form which is easily managed by the destination device.

Communication Model: Destination

- Destination receives the incoming data from the receiver.

Introduction

- A **computer network** is a group of devices connected with each other through a transmission medium such as wires, cables etc.
- These devices can be computers, printers, scanners, Fax machines etc.
- The purpose of having computer network is to send and receive data stored in other devices over the network. These devices are often referred as nodes.



Introduction

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

1. Performance
2. Reliability
3. Scalability

Computer Networks: Performance

It can be measured in the following ways:

1. **Transit time :** It is the time taken to travel a message from one device to another.
2. **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

Introduction

Computer Networks: Reliability

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

Computer Networks: Security

- It refers to the protection of data from any unauthorised 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:** Authorised users are allowed to share the files on the network.

Advantages of Computer Network

A network is very useful for connection and communication purposes. Not just that, it also has many other advantages.

Below are some of the prominent ones:

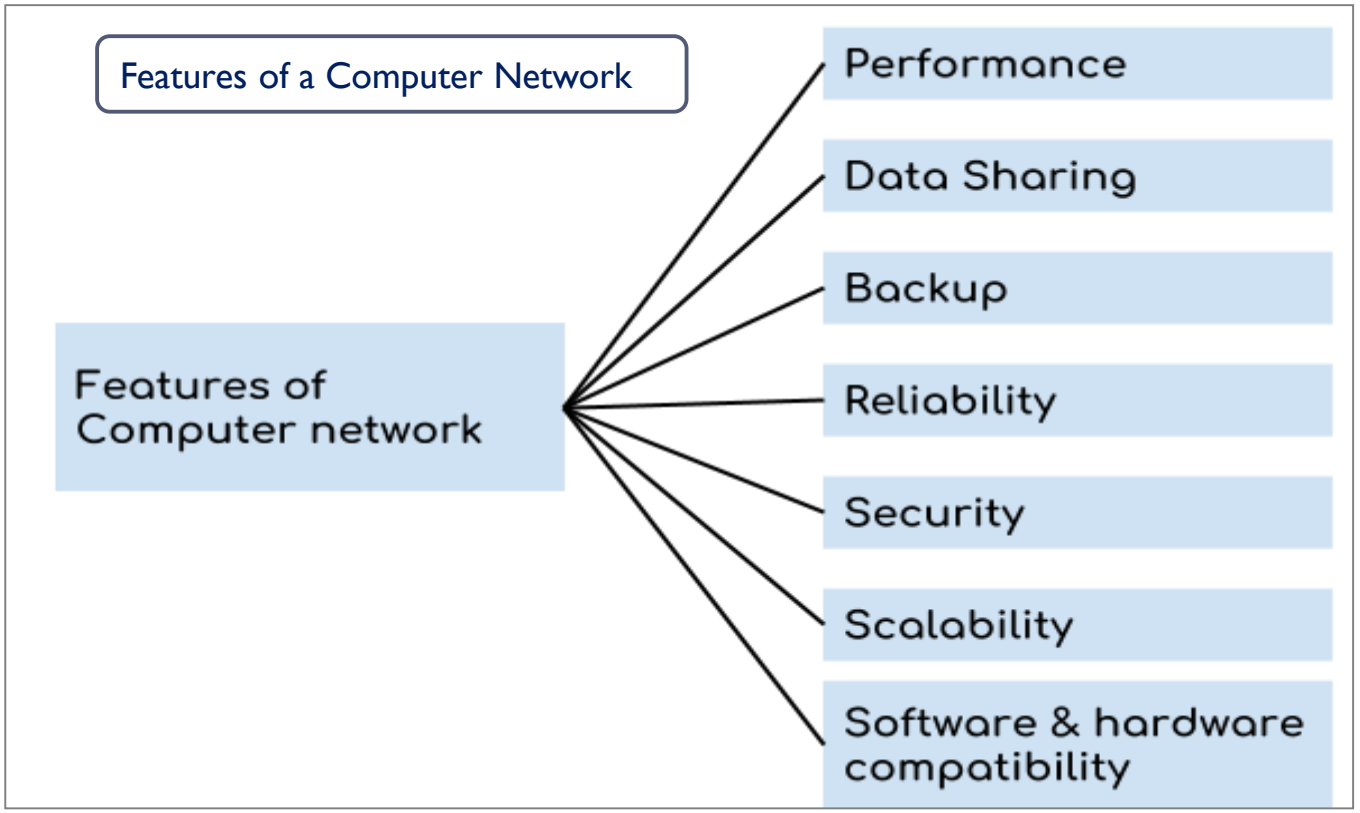
1. Ease of accessibility
2. Flexibility
3. Convenient resource sharing
4. Connectivity
5. Security
6. Great storage capacity
7. Reduced cost

Disadvantages of Computer Network

Disadvantages of computer networks: Various disadvantages include:

1. Lack of robustness
2. Spread of computer virus
3. Independence issues
4. Lack of productivity
5. Health issues

Computer Network Features



Computer Network Features

A computer network has following features:

- **Performance**: Performance of a computer network is measured in terms of response time. The response time of sending and receiving data from one node (computer in a computer network are often referred as node) to another should be minimal.

- **Data Sharing**: One of the reason why we use a computer network is to share the data between different systems connected with each other through a transmission media.

- **Backup**: A computer network must have a central server that keeps the backup of all the data that is to be shared over a network so that in case of a failure it should be able to recover the data faster.

- **Software and hardware compatibility**: A computer network must not limit all the computers in a computer network to use same software and hardware, instead it should allow the better compatibility between the different software and hardware configuration.

Computer Network Features

- **Reliability**: There should not be any failure in the network or if it occurs the recovery from a failure should be fast.

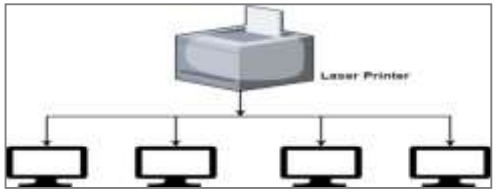
- **Security**: A computer network should be secure so that the data transmitting over a network should be safe from unauthorized access. Also, the sent data should be received as it is at the receiving node, which means there should not be any loss of data during transmission.

- **Scalability**: A computer network should be scalable which means it should always allow to add new computers (or nodes) to the already existing computer network.

For example, a company runs 100 computers over a computer network for their 100 employees, lets say they hire another 100 employees and want to add new 100 computers to the already existing LAN then in that case the local area computer network should allow this.

Uses of Computer Networks

Computer Networks: Business Applications



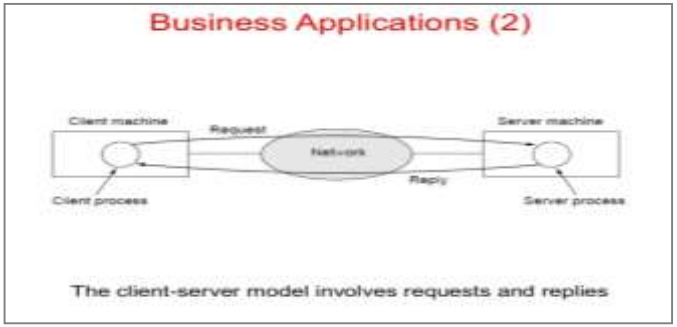
Following are some issues in business applications of computer networks:

1. Resource Sharing:

- The goal is to make all programs, equipment's(like printers etc), and especially data, available to anyone on the network without regard to the physical location of the resource and the user.

2. Server-Client model:

- 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, using which they access remote data.



3. 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

Uses of Computer Networks

4. eCommerce:

- A goal that is starting to become more important in businesses 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

Uses of Computer Networks

Computer Networks: Home Applications

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

1. **Access to remote information**
2. **Person-to-person communication**
3. **Interactive entertainment**
4. **Electronic commerce**

Computer Networks: Mobile Users

- Mobile computers, such as notebook computers and Mobile phones, is one of the fastest-growing segment of the entire 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

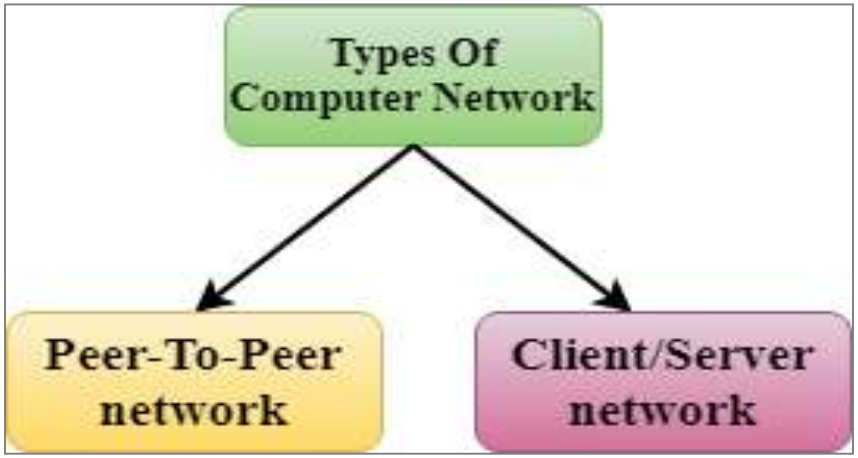
Computer Network Architecture

- A **Computer Architecture** is a design in which all computers in a computer network are organized.

- A architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc.

Simply we can say that how computers are organized and how tasks are allocated to the computer.

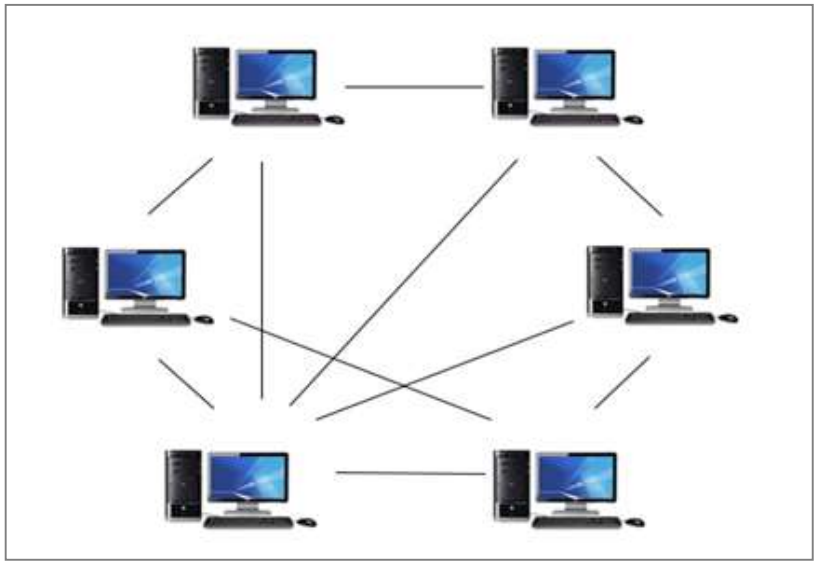
The two most popular computer architectures are **P2P (Peer to Peer)** and **Client-Server architecture**.

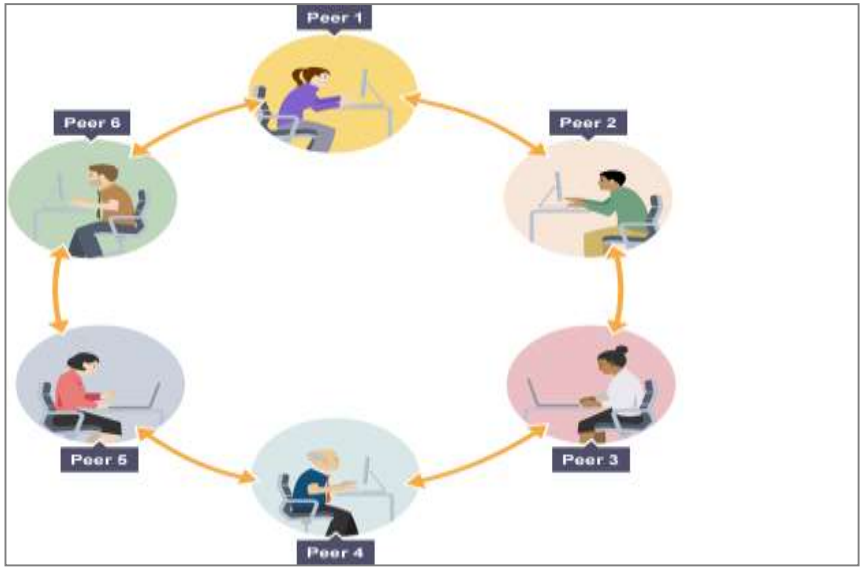


Computer Network Architecture

Peer to Peer Architecture –

- Peer-To-Peer network is a network in which all the computers are linked together with equal privilege and responsibilities for processing the data.
- Peer-To-Peer network is useful for small environments, usually up to 10 computers.
- Peer-To-Peer network has no dedicated server.
- Special permissions are assigned to each computer for sharing the resources, but this can lead to a problem if the computer with the resource is down.





Computer Network Architecture

Peer to Peer Architecture –

Advantages of a Peer to Peer Architecture

1. Less costly as there is no central server that has to take the backup.
2. In case of a computer failure all other computers in the network are not affected and they will continue to work as same as before the failure.
3. Installation of peer to peer architecture is quite easy as each computer manages itself.

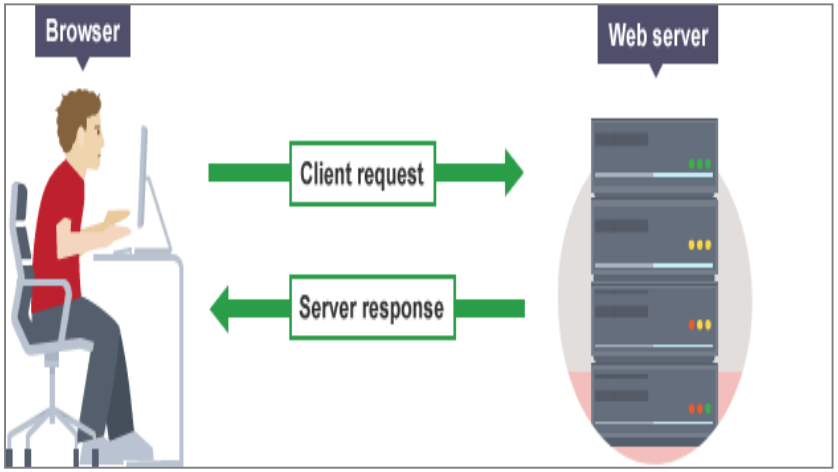
Disadvantages of a Peer to Peer Architecture

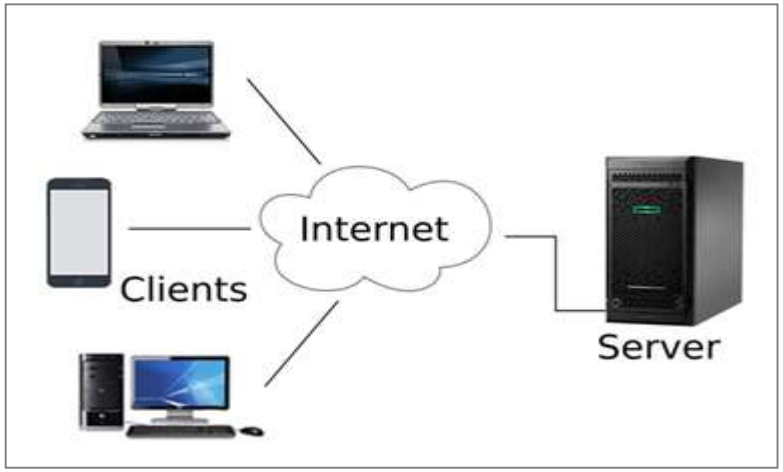
1. Each computer has to take the backup rather than a central computer and the security measures are to be taken by all the computers separately.
2. Scalability is a issue in a peer to Peer Architecture as connecting each computer to every computer is a headache on a very large network.

Computer Network Architecture

Client Server Architecture

- Client/Server network is a network model designed for the end users called clients, to access the resources such as songs, video, etc. from a central computer known as Server.
- The central controller is known as a **server** while all other computers in the network are called **clients**.
- A server performs all the major operations such as security and network management.
- A server is responsible for managing all the resources such as files, directories, printer, etc.
- All the clients communicate with each other through a server. For example, if client1 wants to send some data to client 2, then it first sends the request to the server for the permission. The server sends the response to the client 1 to initiate its communication with the client 2.





Computer Network Architecture

Advantages of Client Server Architecture

1. A Client/Server network contains the centralized system. Therefore we can back up the data easily.
2. A Client/Server network has a dedicated server that improves the overall performance of the whole system.
3. Security is better in Client/Server network as a single server administers the shared resources.
4. It also increases the speed of the sharing resources.

Disadvantages of Client Server Architecture

1. Client/Server network is expensive as it requires the server with large memory.
2. A server has a Network Operating System(NOS) to provide the resources to the clients, but the cost of NOS is very high.
3. It requires a dedicated network administrator to manage all the resources.

Computer Network Architecture

Differences between client-server and P2P networks

	Client-server	P2P
Security	The server controls security of the network.	No central control over security.
Management	The server manages the network. Needs a dedicated team of people to manage the server.	No central control over the network. Anyone can set up.
Dependency	Clients are dependent on the server.	Clients are not dependent on a central server.
Performance	The server can be upgraded to be made more powerful to cope with high demand.	If machines on the network are slow they will slow down other machines.
Backups	Data is all backed up on the main server.	Each computer has to be backed up. Data can easily be deleted by users.

Network Hardware

There is no generally accepted taxonomy into which all computer networks fit, but two dimensions stand out as important: **transmission technology and scale.**

- Broadly speaking, there are two types of transmission technology that are in widespread use:

1. **Point-to-Point line configuration/connection**
2. **Multipoint line configuration/connection**

Point-to-Point connection

- As the name suggests, a point-to-point connection provides a link between exactly two devices/nodes, which implies the link can only be used by the two devices connected to it, i.e. the sender and receiver and no other device can use it.

The important features of the point-to-point connection are as follows:

1. The entire capacity of the link is reserved for data transmission between the two nodes connected to it.
2. Like, if the capacity of a link is 10MBPS, which means 10 megabits of data can be transmitted through it per second, then only the two devices can utilize it, and no other device can claim this.
3. Mostly cables/wires are used to attach the two endpoints in point-to-point line configuration, but microwaves or radiowaves can also be used.
4. It is one of the most basic and simplest configurations to implement.

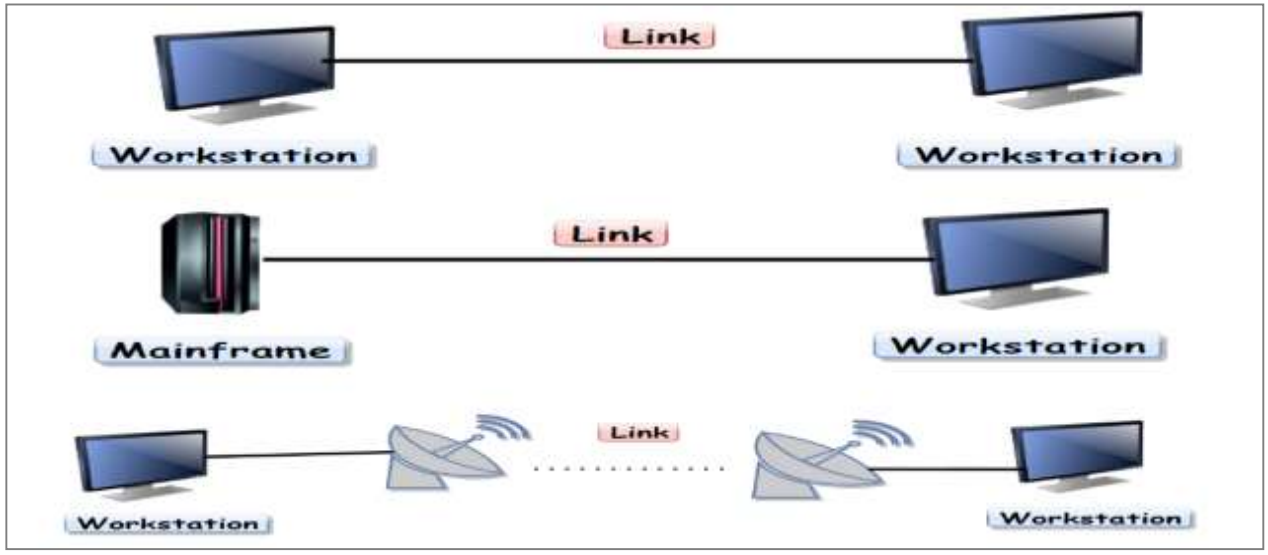
Network Hardware

Point-to-Point connection

Examples

1. One real-life example is controlling a T.V. through an infrared remote, which does nothing but establish a point-to-point connection between the T.V and remote.

2. Another best example is a telephone call in which there is a point-to-point connection between 2 telephones.



Network Hardware

Multipoint connection

- It is also called Multidrop configuration. In this connection, two or more devices share a single link.
- More than two devices share the link that is the capacity of the channel is shared now.

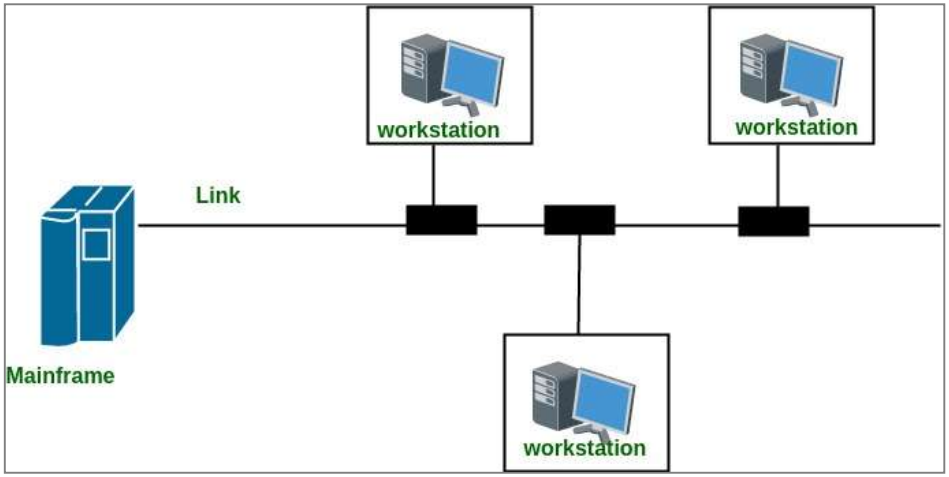
With shared capacity, there can be two possibilities in a Multipoint Line configuration:

Spatial Sharing: If several devices can share the link simultaneously, it's called Spatially shared line configuration.

Temporal (Time) Sharing: If users must take turns using the link, then it's called Temporally shared or Time Shared Line configuration.

Example

- ATM is an example of Multipoint connection



Network Hardware

Transmission Modes

- Data Transmission mode defines the direction of the flow of information between two communication devices. It is also called Data Communication or Directional Mode.
- The data transmission modes can be characterized in the following three types based on the direction of exchange of information:

1. **Simplex**
2. **Half-Duplex**
3. **Full Duplex**

Network Hardware

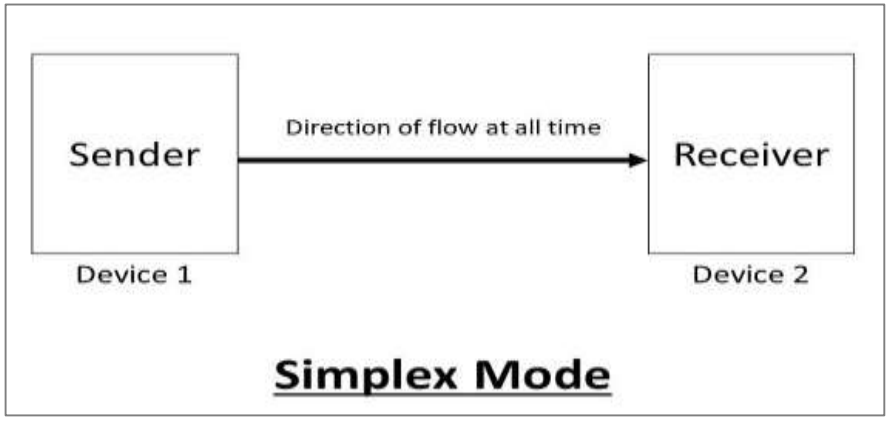
Transmission Modes

According to the Direction of Exchange of Information:

1. Simplex

- **Simplex is the data transmission mode in which the data can flow only in one direction, i.e., the communication is unidirectional.**
- In this mode, a sender can only send data but can not receive it. Similarly, a receiver can only receive data but can not send it.
- This transmission mode is not so popular because we cannot perform two-way communication between the sender and receiver in this mode.
- It is mainly used in the business field as in sales that do not require any corresponding reply. It is similar to a one-way street.

For Example, Radio and TV transmission, keyboard, mouse, etc.



Network Hardware

Following are the advantages of using a Simplex transmission mode:

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

Following are the disadvantages of using a Simplex transmission mode:

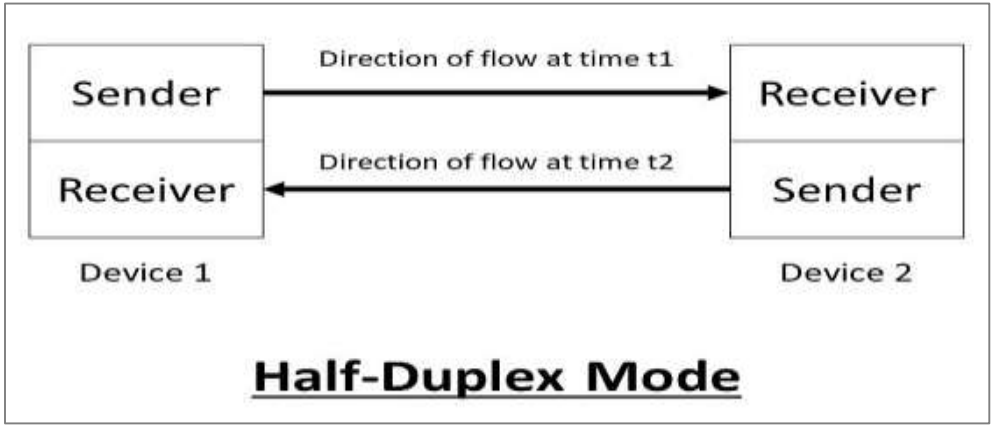
- It is unidirectional in nature having no inter-communication between devices.
- There is no mechanism for information to be transmitted back to the sender(No mechanism for acknowledgement).

Network Hardware

2. Half-Duplex

- **Half-Duplex is the data transmission mode in which the data can flow in both directions but in one direction at a time. It is also referred to as Semi-Duplex.**
- In other words, each station can both transmit and receive the data but not at the same time. When one device is sending the other can only receive and vice-versa.
- In this type of transmission mode, the entire capacity of the channel can be utilized for each direction. Transmission lines can carry data in both directions, but the data can be sent only in one direction at a time.

For Example, Walkie-Talkie, Internet Browsers, etc.



Network Hardware

Following are the advantages of using a half-duplex transmission mode:

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

Following are the disadvantages of using a half-duplex transmission mode:

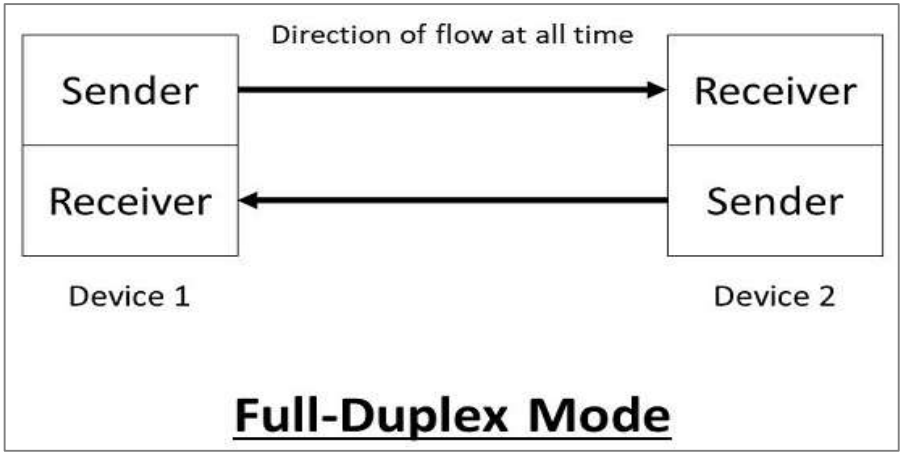
- The two-way communication can not be established simultaneously at the same time.
- Delay in transmission may occur as only one way communication can be possible at a time.

Network Hardware

3. Full-Duplex

- **Full-Duplex is the data transmission mode in which the data can flow in both directions at the same time. It is bi-directional in nature.**
- It is two-way communication in which both the stations can transmit and receive the data simultaneously.
- Full-Duplex mode has double bandwidth as compared to the half-duplex. The capacity of the channel is divided between the two directions of communication. This mode is used when communication in both directions is required simultaneously.

For Example, a Telephone Network, in which both the persons can talk and listen to each other simultaneously.



Network Hardware

Following are the advantages of using a full-duplex transmission mode:

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

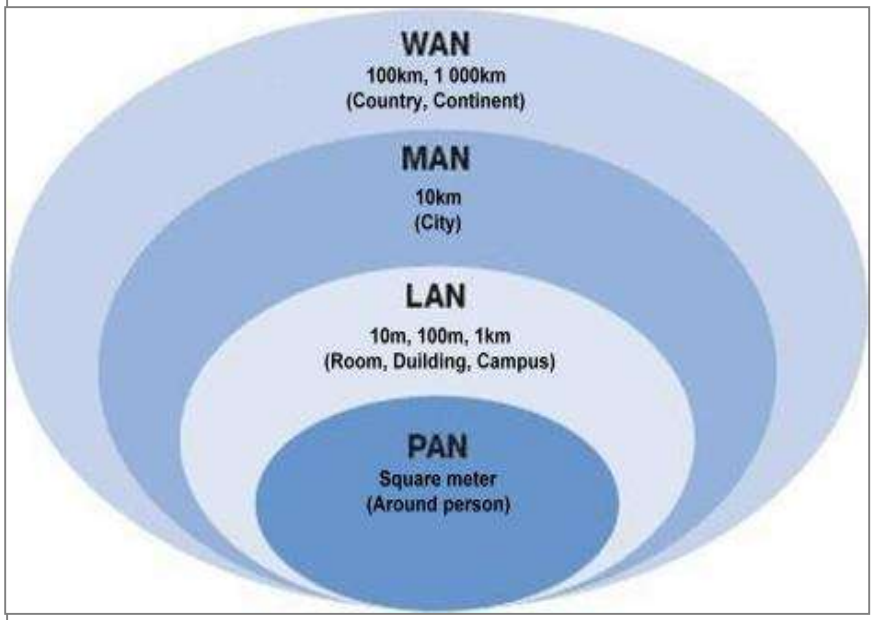
Following are the disadvantages of using a half-duplex transmission mode:

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

Network Hardware

Classification of interconnected processors by scale.

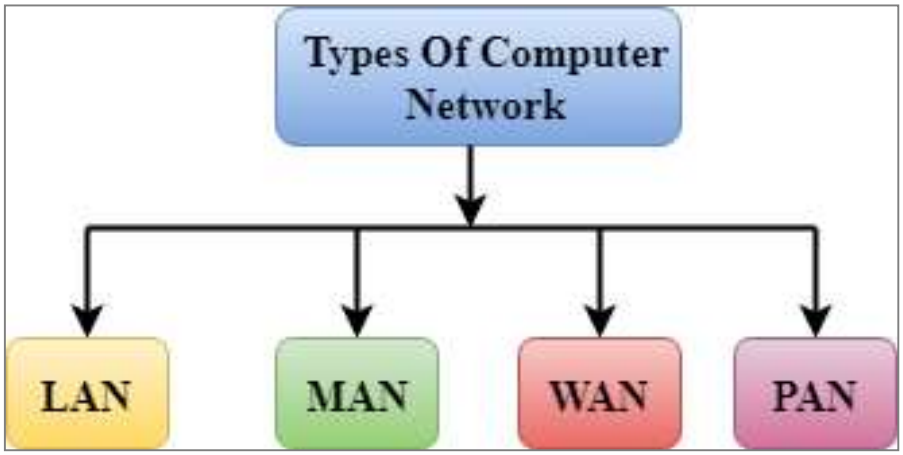
Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet



Network Hardware

- **A computer network is a system in which multiple computers are connected to share information and resources.**
- Computer network varies with each other based on their functionality, geography, ownership, and communication media used.
- ***A computer network can be divided into the following types, based on the geographical area that they cover, they are:***

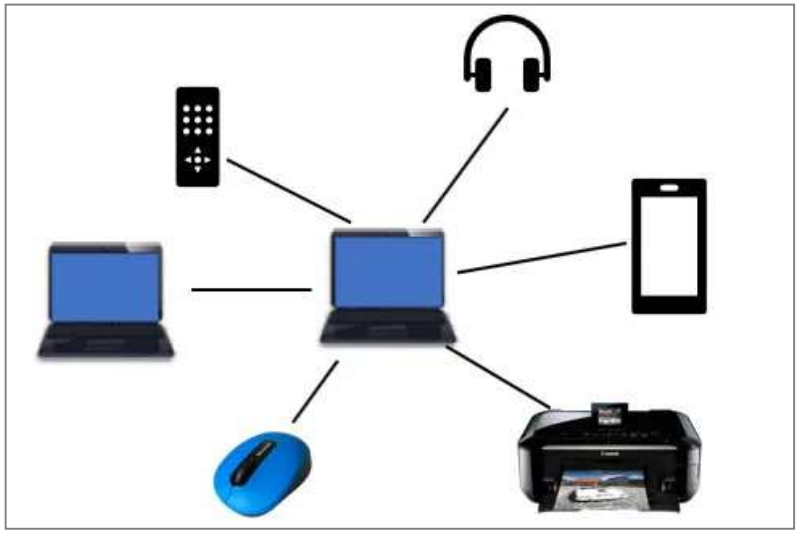
1. **PAN(Personal Area Network)**
2. **LAN(Local Area Network)**
3. **MAN(Metropolitan Area Network)**
4. **WAN(Wide Area Network)**



Network Hardware

1. **PAN(Personal Area Network) –**

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



Network Hardware

PAN(Personal Area Network) – There are two types of Personal Area Network:

1. **Wireless Personal Area Network**
2. **Wired Personal Area Network**

1. Wireless Personal Area Network: Wireless Personal Area Network is configured is based on wireless technologies like Bluetooth and Wi-Fi which falls over a limited range network.

2. Wired Personal Area Network: Wired Personal Area Network is deployed by using USB.

Examples Of Personal Area Network

1. Body Area Network: Body Area Network moves along with a person like a smartphone or a watch that moves with a person. He can also connect with other people to interlink the device for sharing the data.

2. Offline Network: The offline network can be deployed inside the house which is also called a home network. It is planned to connect with television, printers which are not accessible to the internet.

3. Small Home Office: Small Home office is used to link the devices to cyberspace via a VPN that is a virtual private network.

Network Hardware

PAN(Personal Area Network) –

Advantages of PAN

1. Here are the important pros/benefits of PAN network:
2. PAN networks are relatively secure and safe
3. It offers only short-range solution up to ten meters
4. Strictly restricted to a small area

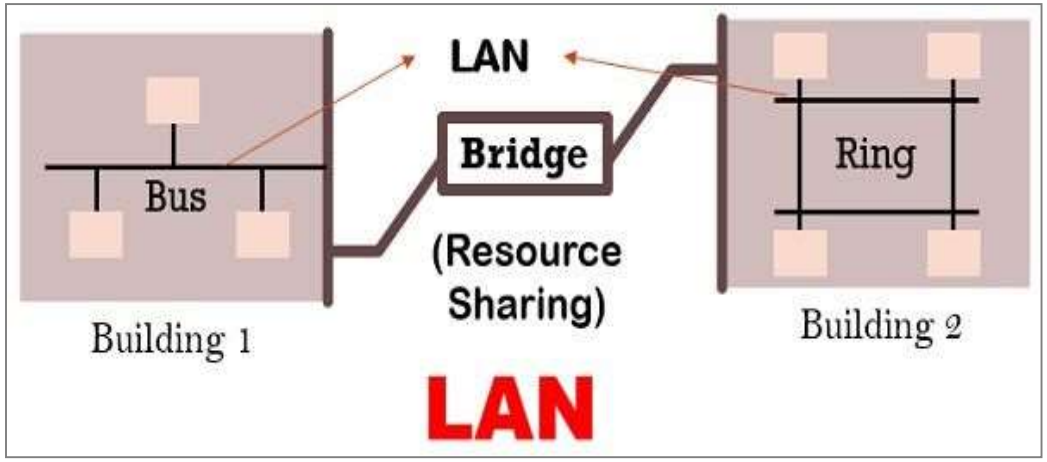
Disadvantages of PAN

1. Here are the cons/drawbacks of using PAN network:
2. It may establish a bad connection to other networks at the same radio bands.
3. Distance limits.

Network Hardware

2. LAN(Local Area Network) –

- A local area network is a network, which is designed to operate over a very small geographical or physical area such as an office, building, a group of buildings, etc.
- Generally, it is used to connect two or more personal computers through a communication medium such as **coaxial, twisted-pair cables,** etc.
- A LAN can use either wired or wireless mode of communication. The LAN which entirely uses wireless media for communication can be termed as **WLAN(Wireless Local Area Network).**
- Ethernet LAN is the most commonly used LAN. The speed of a Local Area Network also depends on the topology used. ***For example,*** a LAN using bus topology has a speed of 10mbps to 100mbps, while in ring topology it is around 4mbps to 16mbps. LAN's are generally privately owned networks.



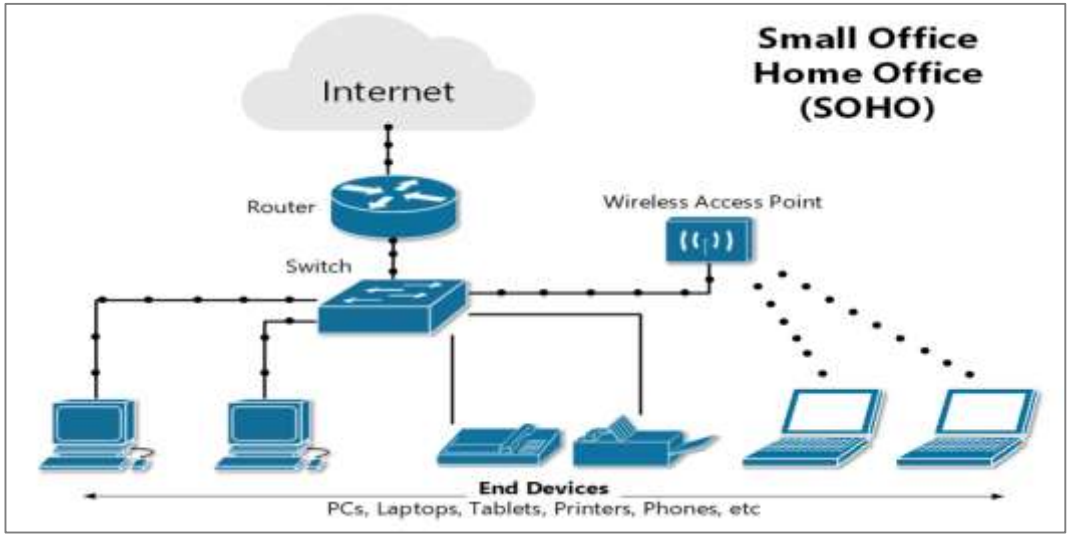
Network Hardware

Functionalities of LAN

1. **File Serving:** In LAN, a large storage disk acts as a central storage repository.
2. **Print Serving:** Printers can be shared very easily in a LAN by various computers.
3. **Academic Support:** A LAN can be used in the classroom, labs, etc. for educational purposes.
4. **Manufacturing Support:** LAN can support the manufacturing and industrial environment.
5. **High Reliability:** Individual workstations might survive the network in case of failures.

Advantages of LAN

1. File transfer and file access
2. Resource or peripherals sharing
3. Personal computing
4. Document distribution
5. Easy to design and troubleshoot
6. Minimum propagation delay
7. High data rate transfer
8. Low error rate & Easily scalable(devices can be added or removed very easily)



Network Hardware

Disadvantages of LAN

Here are the cons/drawbacks of LAN:

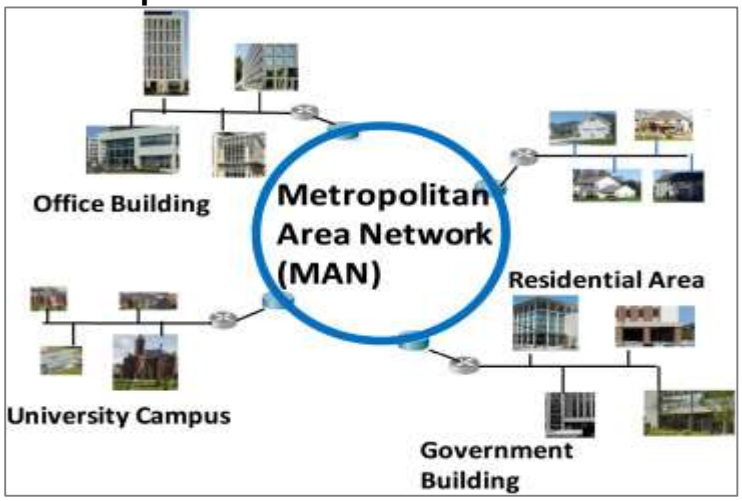
- LAN will indeed save cost because of shared computer resources, but the initial cost of installing Local Area Networks is quite high.
- The LAN admin can check personal data files of every LAN user, so it does not offer good privacy.
- Unauthorized users can access critical data of an organization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

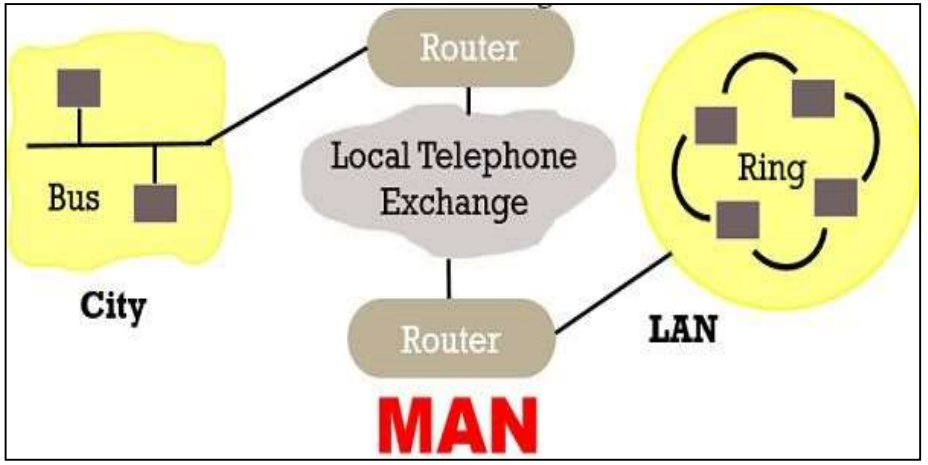
Network Hardware

3. MAN(Metropolitan Area Network)

- A **Metropolitan Area Network** or MAN is consisting of a computer network across an entire city, college campus, or a small region.
- It can be connected using an optical fiber cable as a communication medium. Two or more LAN's can also be connected using routers to create a MAN.
- When this type of network is created for a specific campus, then it is termed as CAN(Campus Area Network).
- A MAN can be either a public or privately owned network. Generally, a telephone exchange line is most commonly used as a communication medium in MAN.
- **The protocols that are used in MAN are RS-232, Frame Relay, ISDN, etc.**

Best example of MAN is the cable television network that spans over the whole city.





Network Hardware

Characteristics of MAN

1. Here are important characteristics of the MAN network:
2. It mostly covers towns and cities in a maximum 50 km range
3. Mostly used medium is optical fibers, cables
4. Data rates adequate for distributed computing applications.

Uses Of Metropolitan Area Network:

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

Network Hardware

Advantages of MAN

Here are the pros/benefits of MAN network:

1. It offers fast communication using high-speed carriers, like fiber optic cables.
2. It provides excellent support for an extensive size network and greater access to WANs.
3. The dual bus in MAN network provides support to transmit data in both directions concurrently.
4. A MAN network mostly includes some areas of a city or an entire city.
5. The Propagation delay of MAN is moderate

Disadvantages of MAN

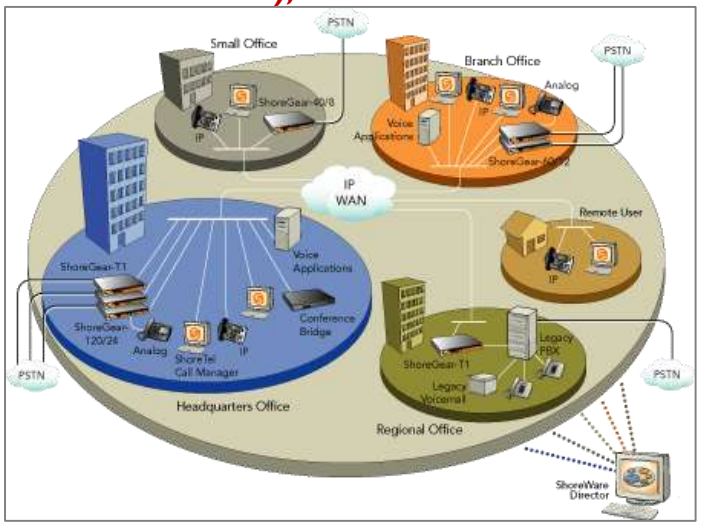
Here are drawbacks/cons of using the MAN network:

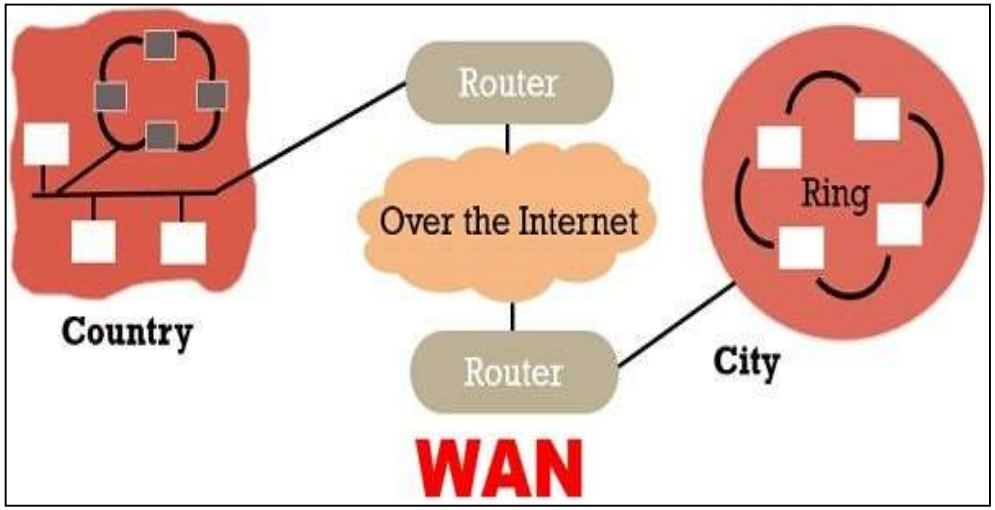
1. You need more cable to establish MAN connection from one place to another.
2. In MAN network it is tough to make the system secure from hackers.
3. It is hard to design and maintain a MAN
4. MAN is less fault-tolerant
5. It is costlier to implement
6. Congestions are more in a MAN

Network Hardware

4. WAN(Wide Area Network)

- A Wide Area Network is the largest spread network. It spans over very large-distances such as a country, continent or even the whole globe. Two widely separated computers can be connected very easily using WAN. For Example, the Internet.
- A WAN may include various Local and Metropolitan Area Network. The mode of communication in a WAN can either be wired or wireless. Telephone lines for wired and satellite links for wireless communication can be used in a wide area network.
- The protocols used in WAN are **ISDN(Integrated Service Digital Network), SMDS(Switched Multi-Megabit Data Service), SONET(Synchronous Optical Network), HDLC(High Data Link Control), SDLC(Synchronous Data Link Control), etc.**





Network Hardware

Characteristics of WAN

Below are the characteristics of WAN:

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

Examples Of Wide Area Network:

1. **Mobile Broadband:** A 4G network is widely used across a region or country.
2. **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fiber.

Network Hardware

Advantages of WAN

Here are the benefits/pros of WAN:

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

Disadvantages of WAN

Here are the drawbacks/cons of WAN network:

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

Network Hardware

COMPARISON CHART LAN, MAN, WAN

BASIS OF COMPARISON	LAN	MAN	WAN
Expands to	Local Area Network	Metropolitan Area Network	Wide Area Network
Meaning	A network that connects a group of computers in a small geographical area.	It covers relatively large region such as cities, towns.	It spans large locality and connects countries together. Example Internet.
Ownership of Network	Private	Private or Public	Private or Public
Design and maintenance	Easy	Difficult	Difficult
Propagation Delay	Short	Moderate	Long
Speed	High	Moderate	Low
Fault Tolerance	More Tolerant	Less Tolerant	Less Tolerant
Congestion	Less	More	More
Used for	College, School, Hospital.	Small towns, City.	Country/Continent.
Allows	Single pair of devices to communicate.	Multiple computers can simultaneously interact.	A huge group of computers communicate at the same time.

Network Hardware

Following are the types of network, based on Ownership:

1. Private Network:

- A private network is a network in which various restrictions are imposed to secure the network, to restrict unauthorized access.
- This type of network is privately owned by a single or group of people for their personal use. Local Area Network(LAN) can be used as a private network.

2. Public Network:

- A public network is a network that has the least or no restrictions on it. It can be freely accessed by anyone, without any restrictions.
- This type of network is publicly owned by the government or NGOs. Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as a public network.

Network Hardware

Following are the types of network, based on Transmission Media:

1. **Bound/Guided Media Network:**

- Bounded/Guided media can also be referred to as wired media.
- This kind of networks provides a physical link between two nodes connected in a network.
- The physical links are directed towards a particular direction in the network. **Co-axial, twisted pair, optical fiber cable, etc.** can be used in such networks for connectivity.
- Local Area Network(LAN) and Metropolitan Area Network(MAN) can be used as a Bound/Guided media network.

2. Unbound/Unguided Media Network:

- Unbounded/Unguided media can also be referred to as wireless media.
- This kind of network does not need any physical link for **electromagnetic transmission. Radio waves, Microwaves, Infrared, etc.** can be used in such networks for connectivity.
- Metropolitan Area Network(MAN) and Wide Area Network(WAN) can be used as an Unbound/Unguided media network.

Network Hardware

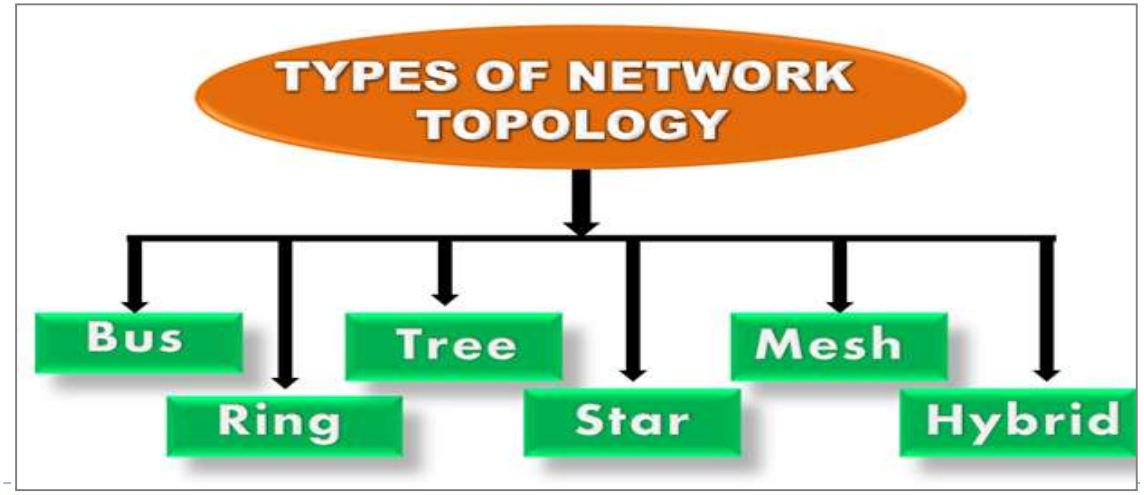
Network Topologies

- In computer networks, a topology is used to explain how a network is physically connected and the logical flow of information in the network.

In computer networks, there are mainly two types of topologies, they are:

Physical Topology: A physical topology describes the way in which the computers or nodes are connected with each other in a computer network. It is the arrangement of various elements(link, nodes, etc.), including the device location and code installation of a computer network.

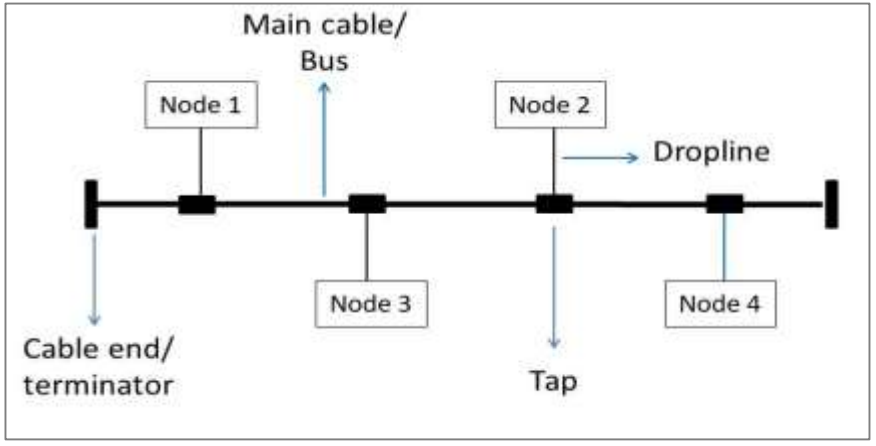
Logical Topology: A logical topology describes the way, data flow from one computer to another.

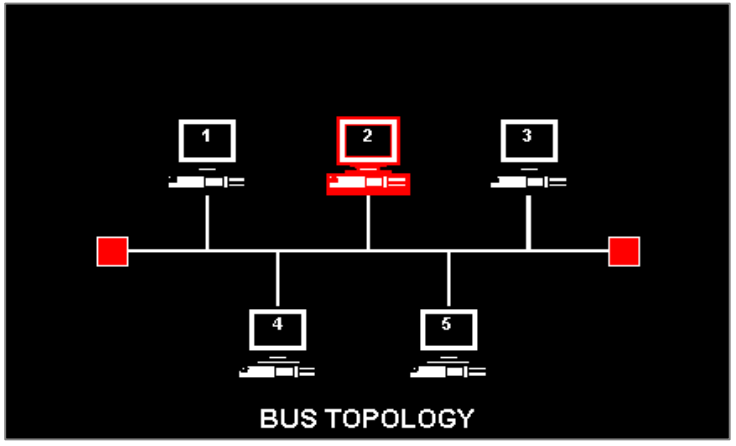


Network Hardware

Bus Topology

- **Bus topology is the simplest kind of topology in which a common bus or channel is used for communication in the network.**
- The bus is connected to various taps and droplines. Taps are the connectors, while droplines are the cables connecting the bus with the computer. In other words, there is only a single transmission line for all nodes.
- The bus topology is mainly used in 802.3 (ethernet) and 802.4 standard networks.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).





Network Hardware

Advantages of Bus topology

1. Simple to use and install.
2. If a node fails, it will not affect other nodes.
3. Less cabling is required.
4. Cost-efficient to implement.

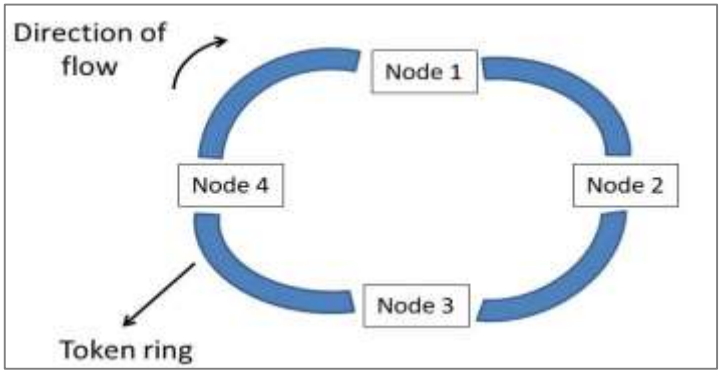
Disadvantages of Bus topology

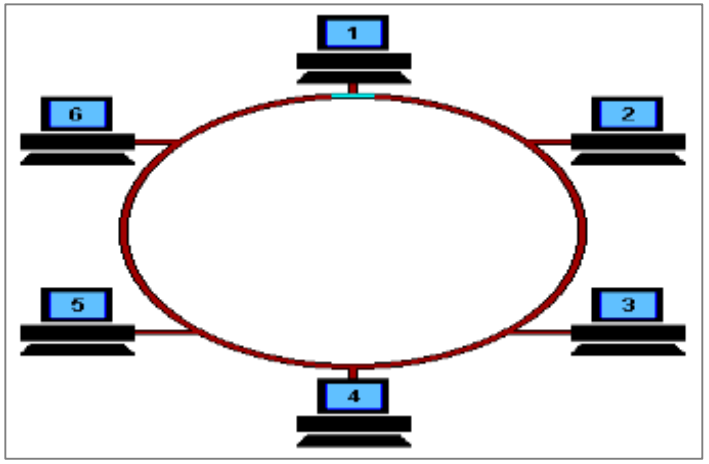
1. Efficiency is less when nodes are more(strength of signal decreases).
2. If the bus fails, the network will fail.
3. A limited number of nodes can connect to the bus due to limited bus length.
4. Security issues and risks are more as messages are broadcasted to all nodes.
5. Congestion and traffic on the bus as it is the only source of communication.

Network Hardware

Ring Topology

- **Ring topology is a topology in which each computer is connected to exactly two other computers to form the ring.** The message passing is unidirectional and circular in nature.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is unidirectional.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a clockwise direction.
- The most common access method of the ring topology is **token passing**.
  - **Token passing:** It is a network access method in which token is passed from one node to another node.
  - **Token:** It is a frame that circulates around the network.





Network Hardware

Advantages of Ring topology:

1. Easy Installation.
2. Less Cabling Required.
3. Reduces chances of data collision(unidirectional).
4. Easy to troubleshoot(the faulty node does not pass the token).
5. Each node gets the same access time.

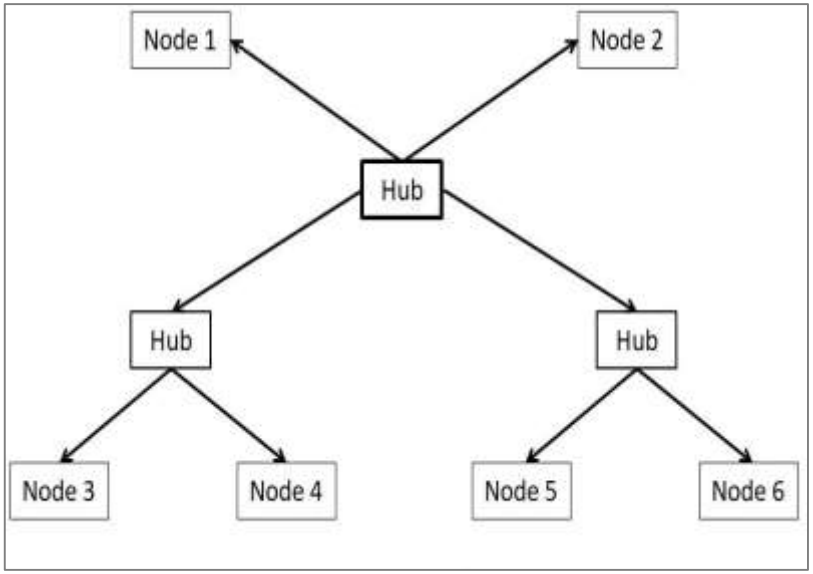
Disadvantages of Ring topology:

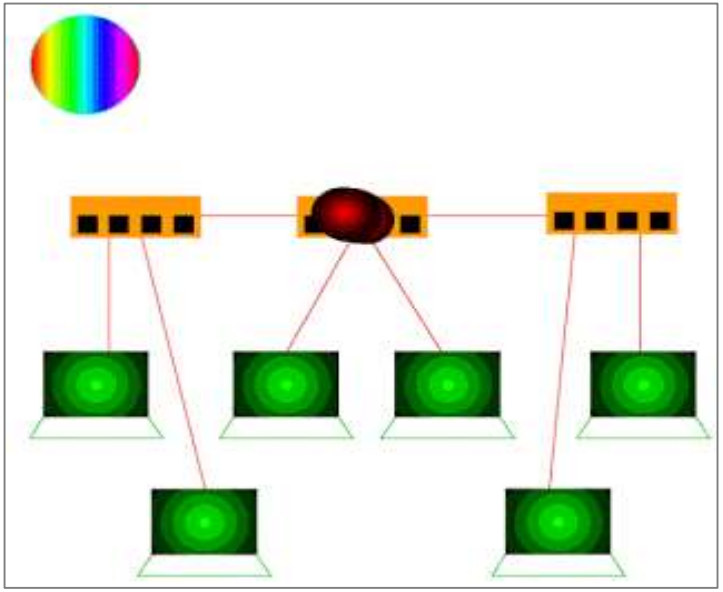
1. If a node fails, the whole network will fail.
2. Slow data transmission speed(each message has to go through the ring path).
3. Difficult to reconfigure(we have to break the ring).

Network Hardware

Tree Topology

- Tree topology combines the characteristics of bus topology and star topology.
- A tree topology is a type of structure in which all the computers are connected with each other in hierarchical fashion.
- Tree topology is a computer network topology in which all the nodes are directly or indirectly connected to the main bus cable.
- There is a main hub and all the other sub-hubs are connected to each other in this topology.





Network Hardware

Advantages of Tree topology

1. Large distance network coverage.
2. Fault finding is easy by checking each hierarchy.
3. Least or no data loss.
4. A Large number of nodes can be connected directly or indirectly.
5. Other hierarchical networks are not affected if one of them fails.

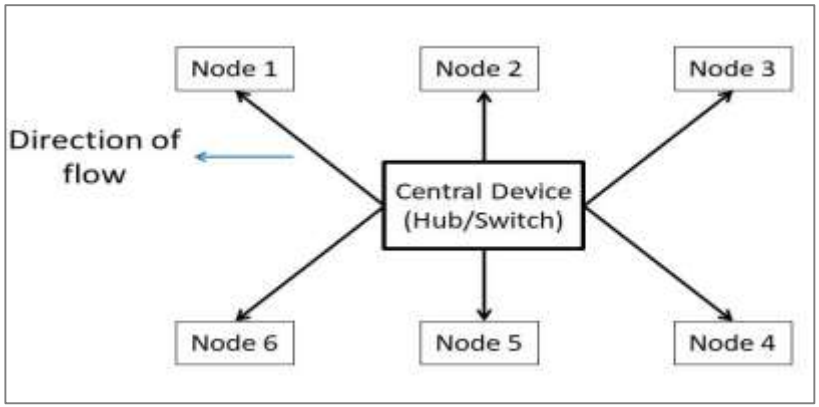
Disadvantages of Tree topology

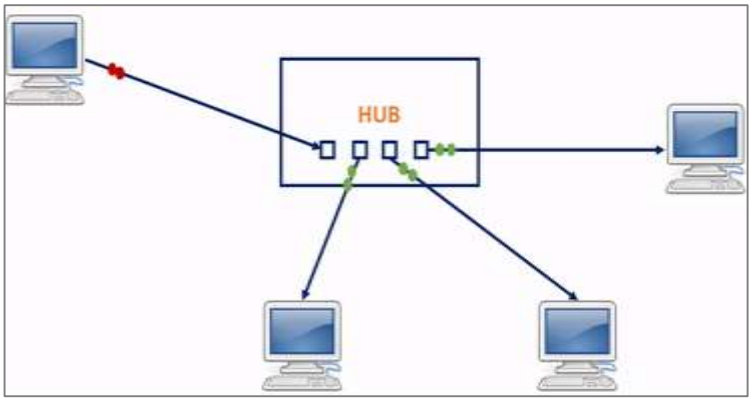
1. Cabling and hardware cost is high.
2. Complex to implement.
3. Hub cabling is also required.
4. A large network using tree topology is hard to manage.
5. It requires very high maintenance.
6. If the main bus fails, the network will fail.

Network Hardware

Star Topology

- **Star topology is a computer network topology in which all the nodes are connected to a centralized hub.**
- The hub or switch acts as a middleware between the nodes. Any node requesting for service or providing service, first contact the hub for communication.
- The central device(hub or switch) has point to point communication link(the dedicated link between the devices which can not be accessed by some other computer) with the devices.
- The central device then broadcast or unicast the message based on the central device used. The hub broadcasts the message, while the switch unicasts the messages by maintaining a switch table.





Network Hardware

Advantages of Star topology

1. Centralized control.
2. Less Expensive.
3. Easy to troubleshoot(the faulty node does not give response).
4. Good fault tolerance due to centralized control on nodes.
5. Easy to scale(nodes can be added or removed to the network easily).
6. If a node fails, it will not affect other nodes.
7. Easy to reconfigure and upgrade(configured using a central device).

Disadvantages of Star topology

1. If the central device fails, the network will fail.
2. The number of devices in the network is limited(due to limited input-output port in a central device).

Network Hardware

Mesh Topology

- **Mesh topology is a computer network topology in which nodes are interconnected with each other.**

There are mainly two types of Mesh:

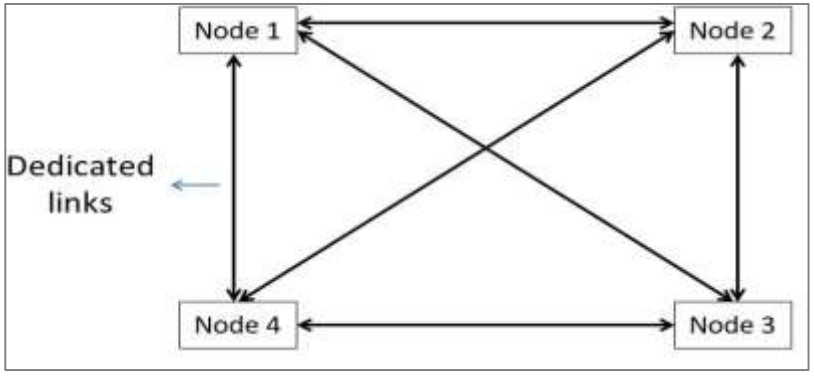
1. **Full Mesh:** In which each node is connected to every other node in the network.
2. **Partial Mesh:** In which, some nodes are not connected to every node in the network.

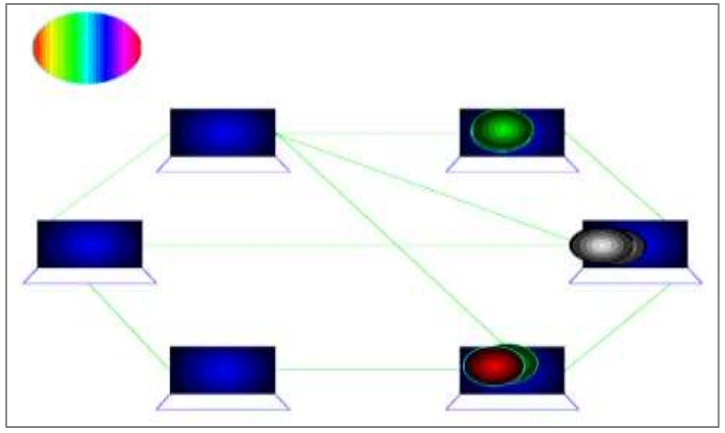
- In a fully connected mesh topology, each device has a point to point link with every other device in the network.
- If we are using,

  simplex links, then the number of communication links will be **'n(n-1)'** for **'n'** devices,

  while it is **'n(n-1)/2'** if we are using duplex links in the mesh topology.

For Example, the Internet(WAN).





Network Hardware

Advantages of Mesh topology

1. Dedicated links facilitate direct communication.
2. No congestion or traffic problems on the channels.
3. Good Fault tolerance due to the dedicated path for each node.
4. Very fast communication.
5. Maintains privacy and security due to a separate channel for communication.
6. If a node fails, other alternatives are present in the network.

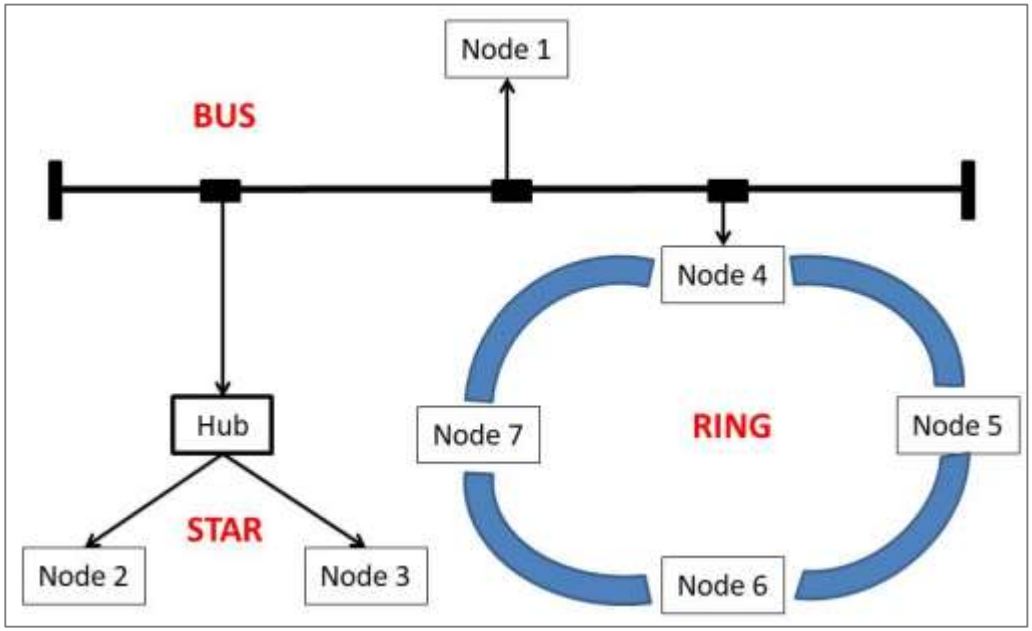
Disadvantages of Mesh topology

1. Very high cabling required.
2. Cost inefficient to implement.
3. Complex to implement and takes large space to install the network.
4. Installation and maintenance are very difficult.

Network Hardware

Hybrid Topology

- **A Hybrid topology is a computer topology which is a combination of two or more topologies.** In practical use, they are the most widely used.
- In this topology, all topologies are interconnected according to the needs to form a hybrid. All the good features of each topology can be used to make an efficient hybrid topology.



Network Hardware

Advantages of Hybrid topology

1. It can handle a large volume of nodes.
2. It provides flexibility to modify the network according to our needs.
3. Very Reliable(if one node fails it will not affect the whole network).

Disadvantages of Hybrid topology

1. Complex design.
2. Expensive to implement.
3. Multi-Station Access Unit(MSAL) required

Network Hardware

Network Topologies Outcomes:

Hence, after learning the various computer network topologies, we can conclude that some points need to be considered when selecting a physical topology:

1. **Ease of Installation.**
2. **Fault Tolerance.**
3. **Implementation Cost.**
4. **Cabling Required.**
5. **Maintenance Required.**
6. **Reliable Nature.**
7. **Ease of Reconfiguration and upgradation.**

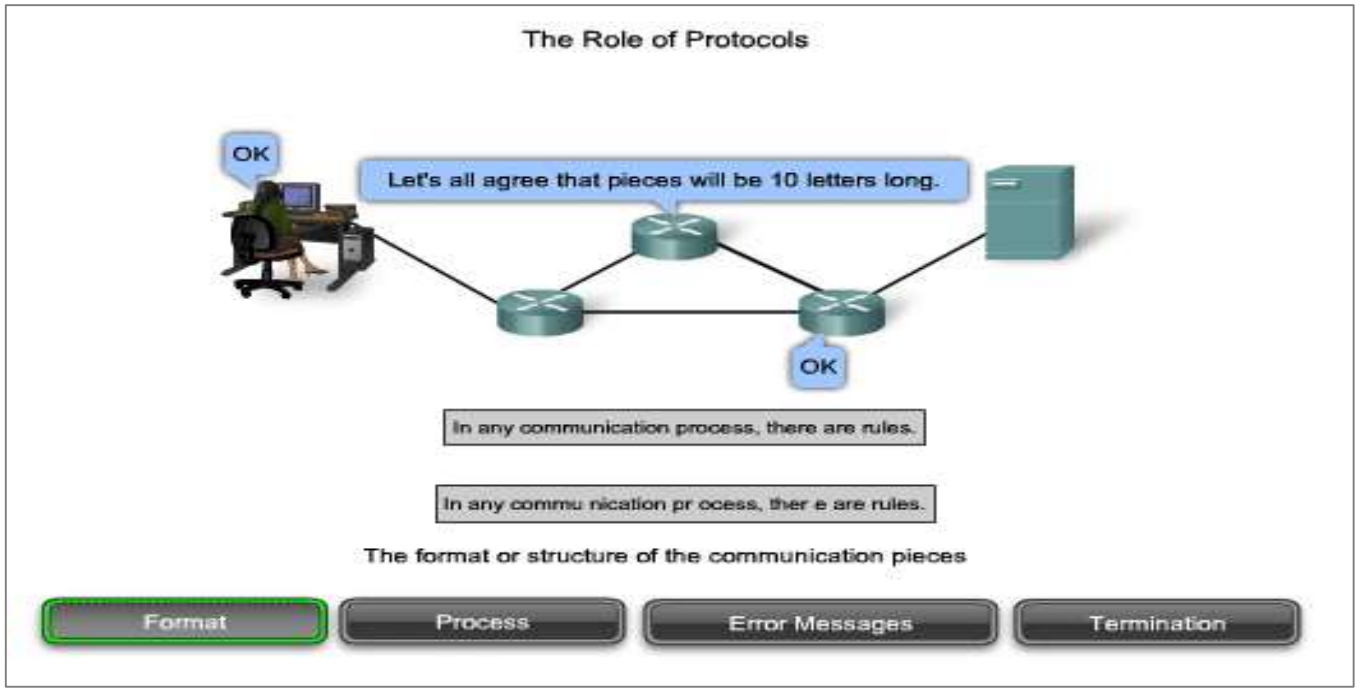
Network Software

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

Network Software

There are three aspects of protocols given below :

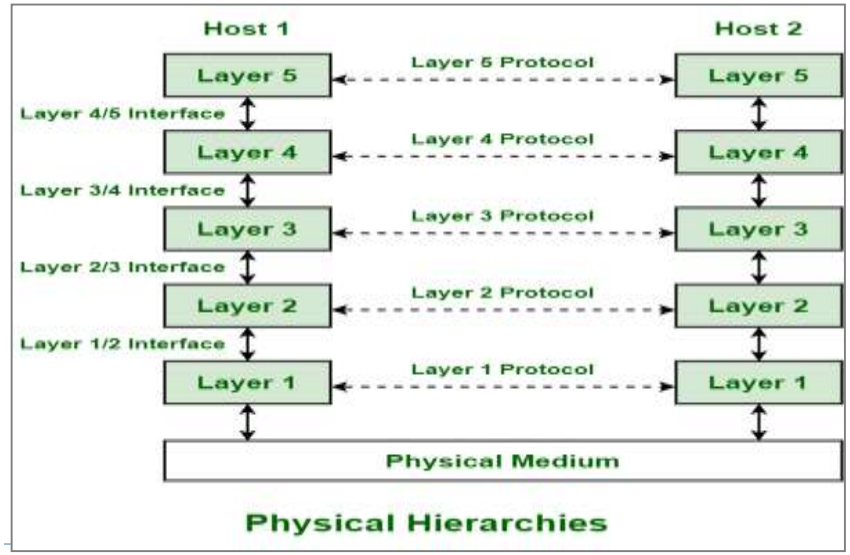
1. **Syntax –** It is used to explain data format that is needed to be sent or received.
2. **Semantics –** It is used to explain exact meaning of each of sections of bits that are usually transferred.
3. **Timings –** It is used to explain exact time at which data is generally transferred along with speed at which it is transferred.



Network Software

1. Protocol Hierarchies

- To reduce their design complexity, most networks are organized as a stack of layers or levels, each one built upon the one below it.
- The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network.
- The purpose of each layer is to offer certain services to the higher layers, shielding those layers from the details of how the offered services are actually implemented.
- In a sense, each layer is a kind of virtual machine, offering certain services to the layer above it.

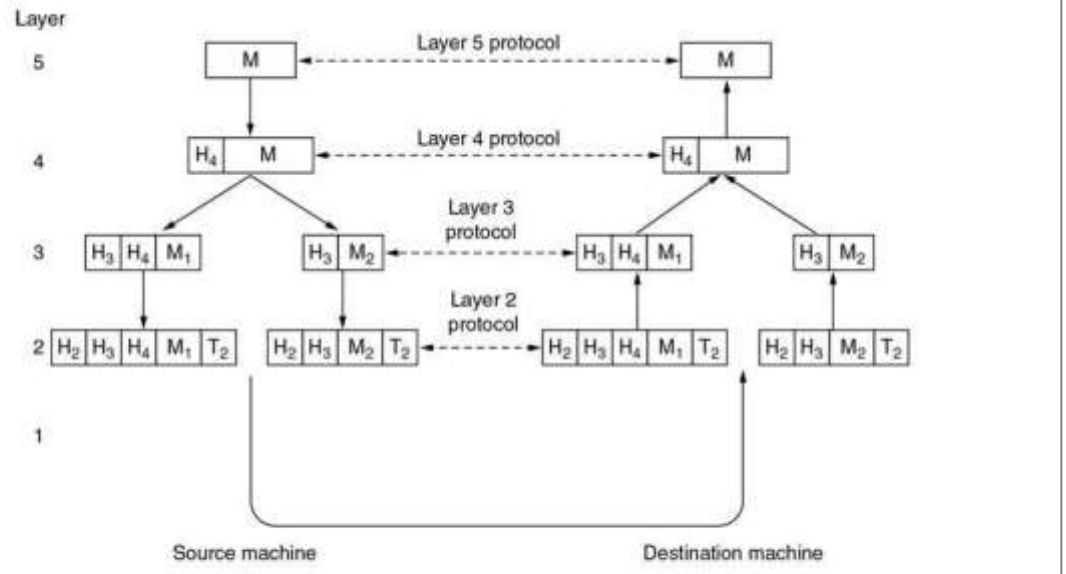


Physical Hierarchies

Network Software

1. Protocol Hierarchies

Now, consider how to provide communication to the top layer of five-layer network



Example information flow supporting virtual communication in layer 5.

Network Software

2. Design Issues for the Layers

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

1. Reliability
2. Scalability
3. Addressing
4. Error Control
5. Flow Control
6. Resource Allocation
7. Statistical Multiplexing
8. Routing
9. Security

Network Software

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

1. **Reliability**

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

2. **Scalability**

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

3. **Addressing**

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

4. **Error Control**

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

Network Software

5. Flow Control

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

6. Resource Allocation

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

7. Statistical Multiplexing

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

8. **Routing**

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

9. **Security**

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

Network Software

3. Connection Oriented Vs Connectionless Service

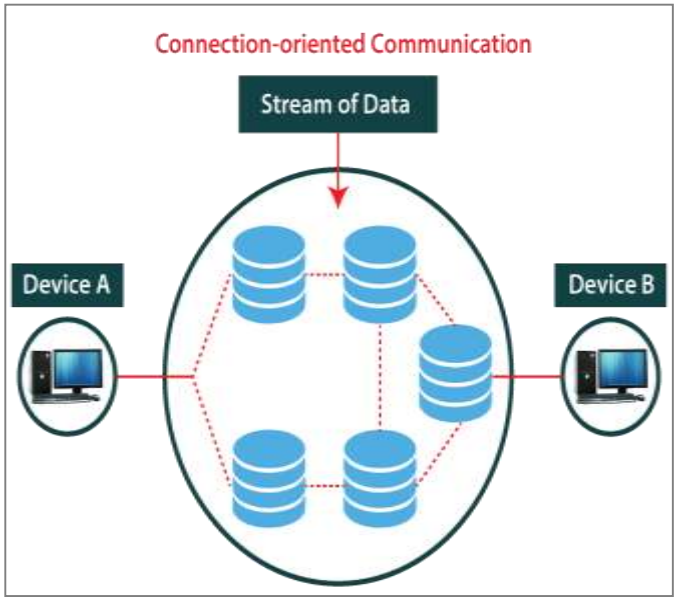
- Data communication is a telecommunication network to send and receive data between two or more computers over the same or different network.

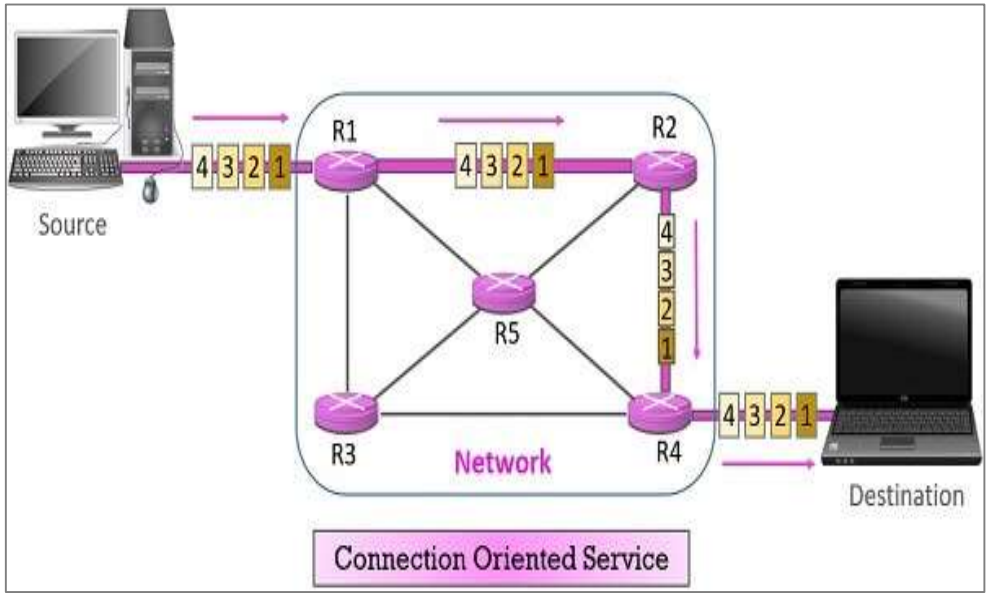
- There are two ways to establish a connection before sending data from one device to another, that are **Connection-Oriented** and **Connectionless Service**.

Network Software

Connection Oriented

- A connection-oriented service is a network service that was designed and developed after the telephone system.
- A connection-oriented service is used to create an end to end connection between the sender and the receiver before transmitting the data over the same or different networks.
- In connection-oriented service, packets are transmitted to the receiver in the same order the sender has sent them.
- It uses a handshake method that creates a connection between the user and sender for transmitting the data over the network. Hence it is also known as a reliable network service.

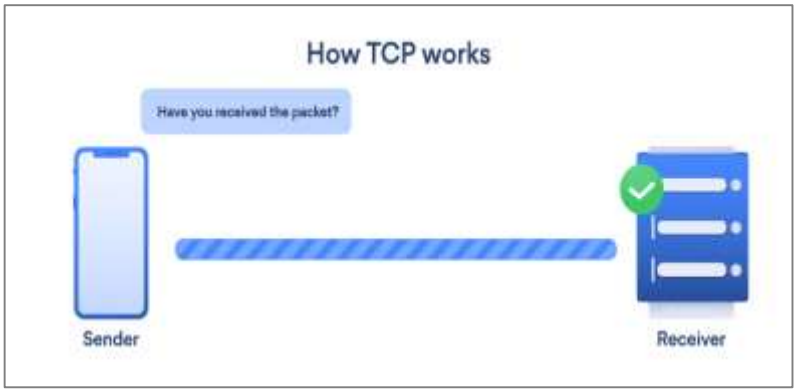


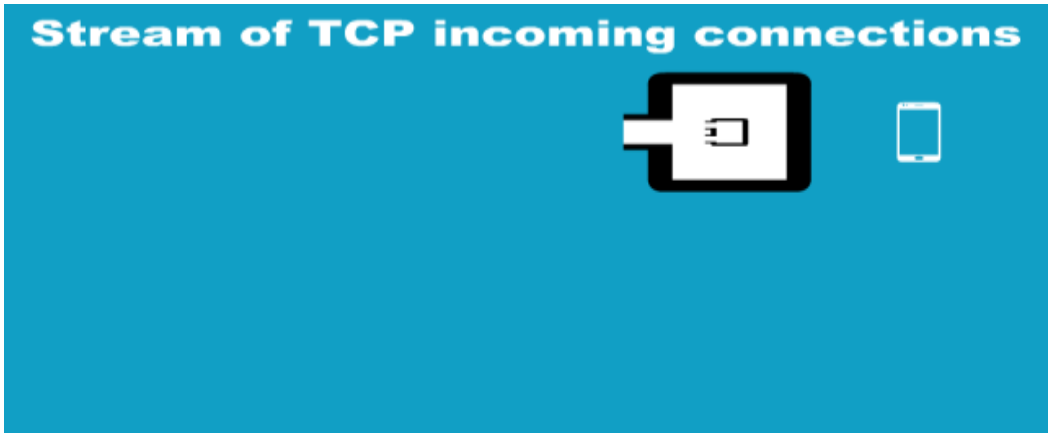


Network Software

TCP (Transmission Control Protocol) -

is a connection-oriented protocol that allows communication between two or more computer devices by establishing connections in the same or different networks.

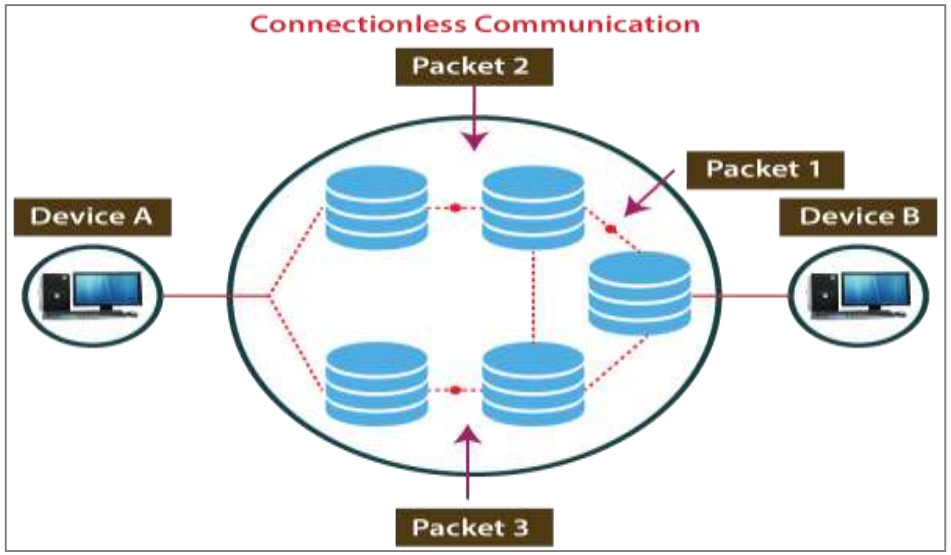




Network Software

Connectionless Service

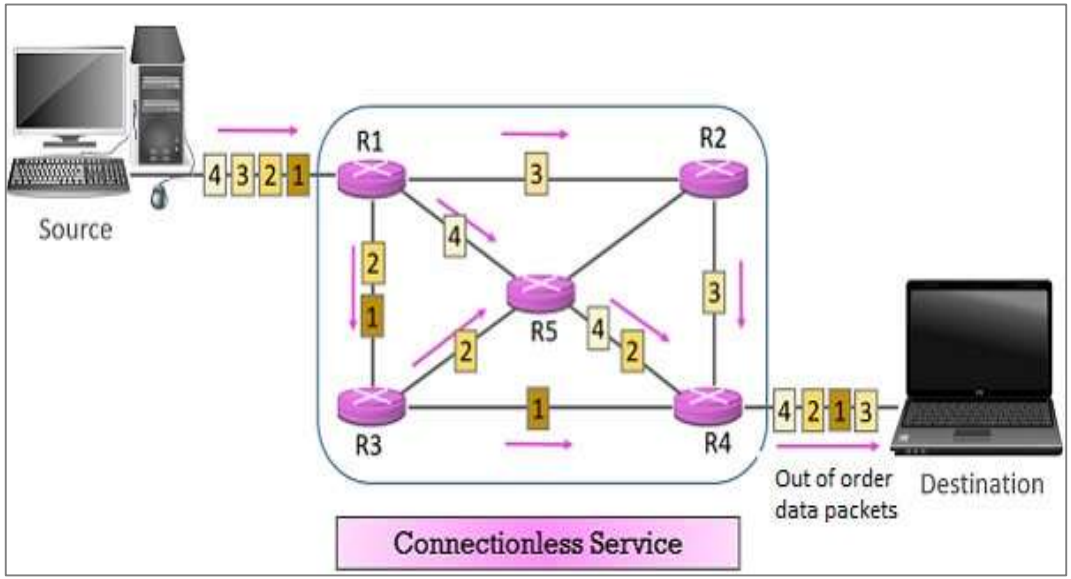
- A connection is similar to a **postal system**, in which each letter takes along different route paths from the source to the destination address.
- Connectionless service is used in the network system to transfer data from one end to another end without creating any connection.
- So it does not require establishing a connection before sending the data from the sender to the receiver.



Network Software

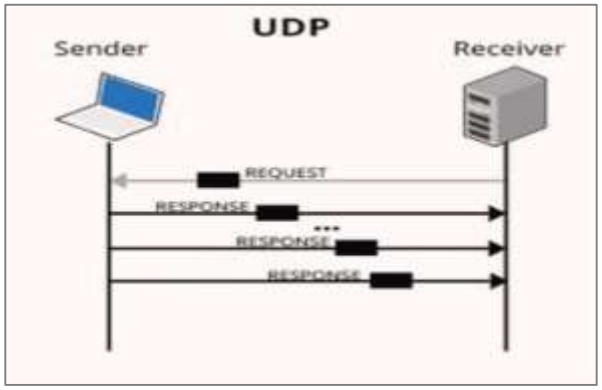
Connectionless Service

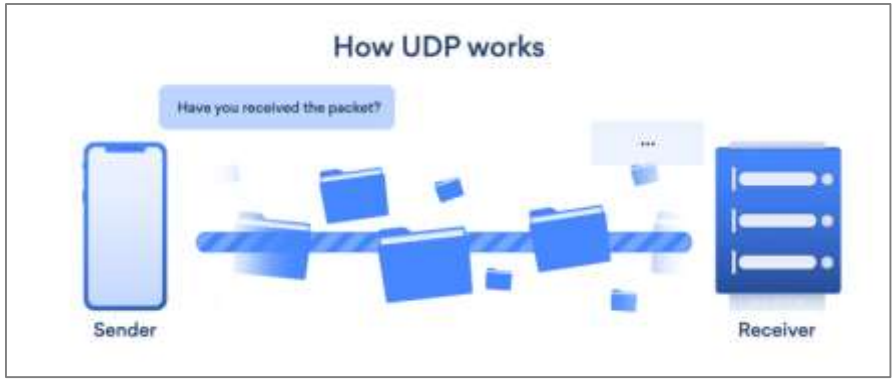
- It is not a reliable network service because it does not guarantee the transfer of data packets to the receiver, and data packets can be received in any order to the receiver.
- Therefore we can say that the data packet does not follow a **defined** path. In connectionless service, the transmitted data packet is not received by the receiver due to network congestion, and the data may be lost.

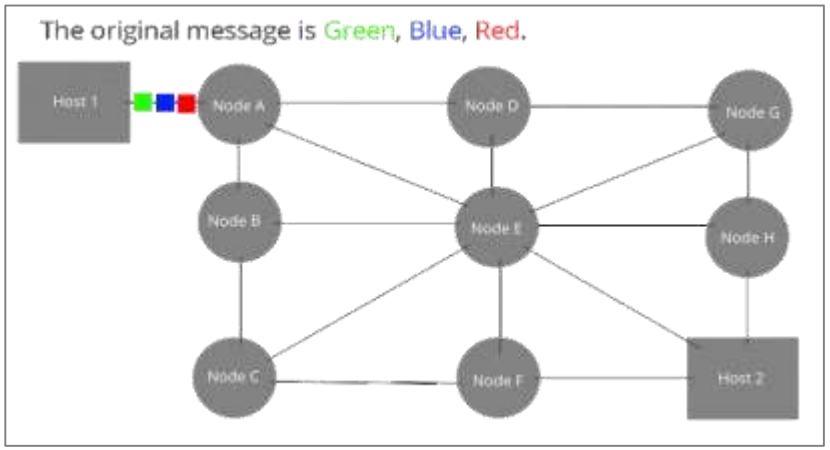


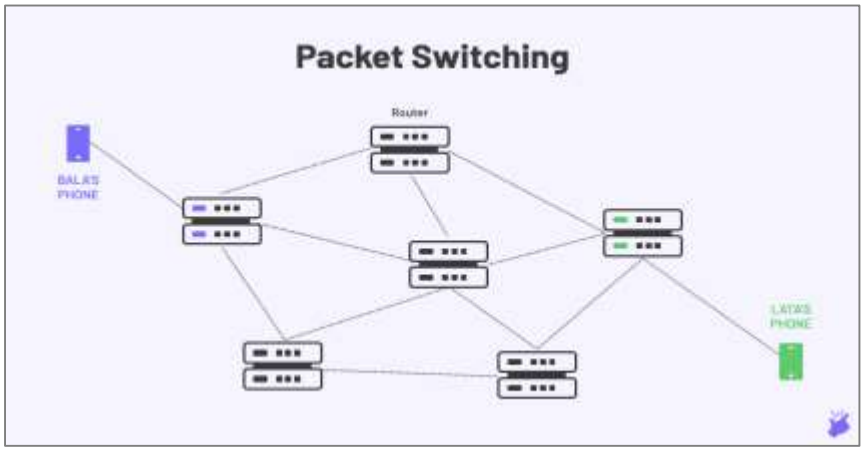
Network Software

UDP (User Datagram Protocol) - is a connectionless protocol that allows communication between two or more devices without establishing any connection. In this protocol, a sender sends the data packets to the receiver that holds the destination address.









Network Software

Connection Oriented Vs Connectionless Service

S. No	Comparison Parameter	Connection-oriented Service	Connection Less Service
1.	**Related System**	It is designed and developed based on the telephone system.	It is service based on the postal system.
2.	**Definition**	It is used to create an end to end connection between the senders to the receiver before transmitting the data over the same or different network.	It is used to transfer the data packets between senders to the receiver without creating any connection.
3.	**Virtual path**	It creates a virtual path between the sender and the receiver.	It does not create any virtual connection or path between the sender and the receiver.
4.	**Authentication**	It requires authentication before transmitting the data packets to the receiver.	It does not require authentication before transferring data packets.
5.	**Data Packets Path**	All data packets are received in the same order as those sent by the sender.	Not all data packets are received in the same order as those sent by the sender.
6.	**Bandwidth Requirement**	It requires a higher bandwidth to transfer the data packets.	It requires low bandwidth to transfer the data packets.
7.	**Data Reliability**	It is a more reliable connection service because it guarantees data packets transfer from one end to the other end with a connection.	It is not a reliable connection service because it does not guarantee the transfer of data packets from one end to another for establishing a connection.
8.	**Congestion**	There is no congestion as it provides an end-to-end connection between sender and receiver during transmission of data.	There may be congestion due to not providing an end-to-end connection between the source and receiver to transmit of data packets.
9.	**Examples**	Transmission Control Protocol (TCP) is an example of a connection-oriented service.	User Datagram Protocol (UDP), Internet Protocol (IP), and Internet Control Message Protocol (ICMP) are examples of connectionless service.

Reference Models

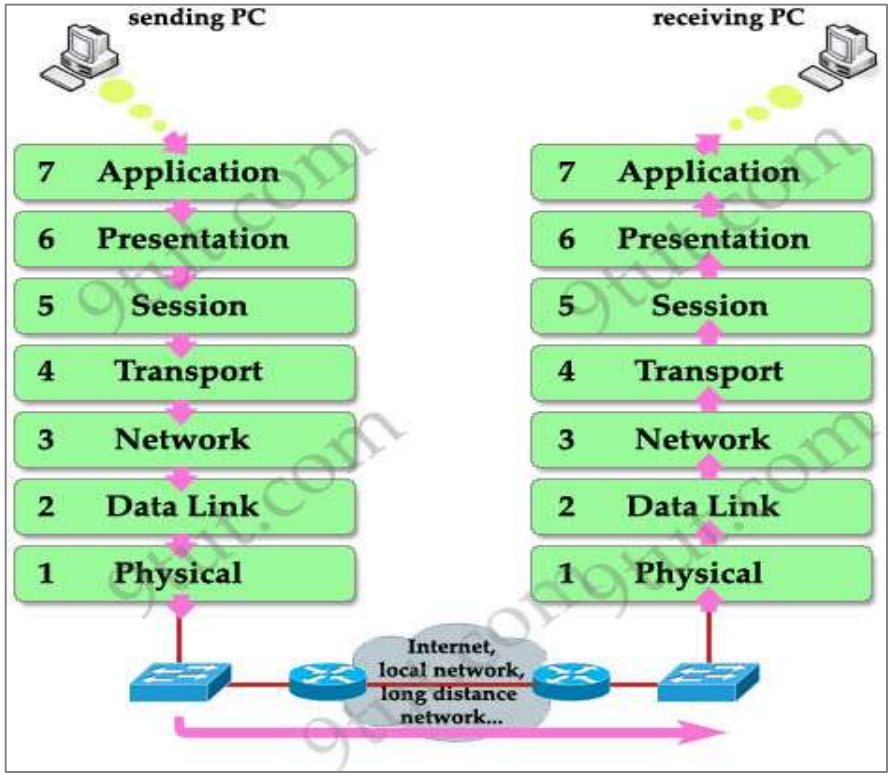
OSI Reference Model:

- **OSI model is a layered framework that allows communication between all types of the computer system. It has seven layers.**
- OSI model is introduced by ISO(International Organization for Standardization) in 1984.
- Each layer has its own functionalities and calls upon the services of the layer just below it.
- These layers are a package of protocols that are implemented by computers to connect in the network.
- **In other words, the OSI model defines and is used to understand how two computers connect with each other in a computer network.**

OSI Reference Model

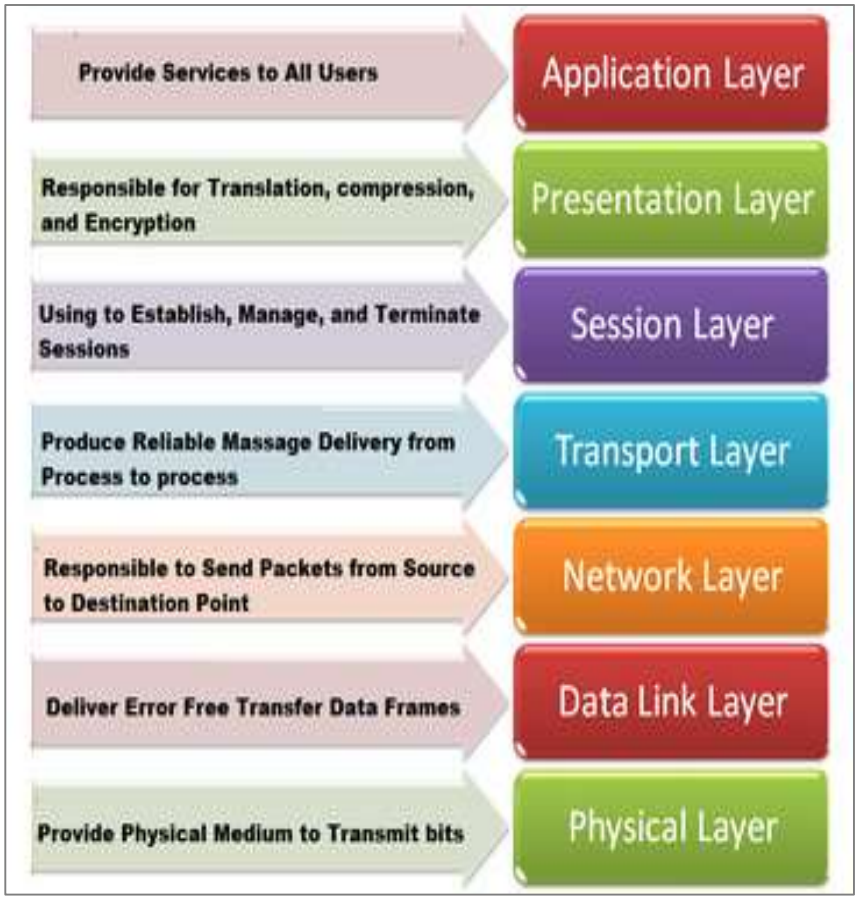
The seven layers of the OSI model, are as follows:

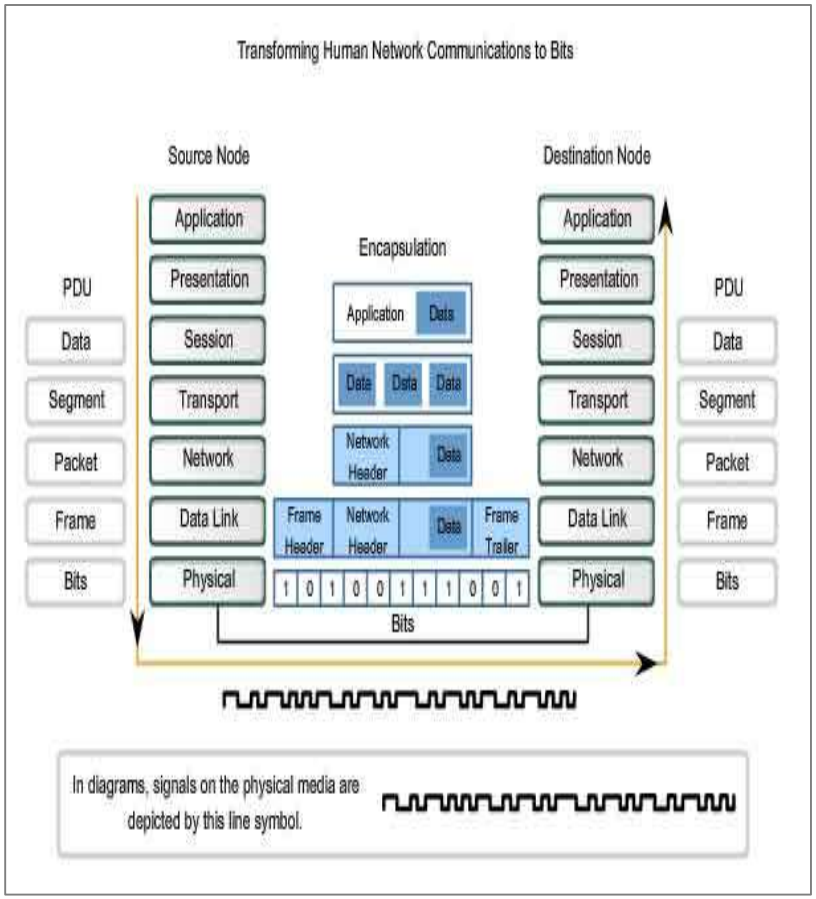
1. **Physical –** How to transmit the signals (mainly coding)
2. **Datalink –** Two-party communication – Ethernet
3. **Network –** Routing, Addressing IP
4. **Transport –** End to end communications – TCP
5. **Session –** Establish/Manage connections
6. **Presentation –** ASCII conversion
7. **Application –** Actual file transfer, emails, remote login



OSI Reference Model

The seven layers of the OSI model, are as follows:

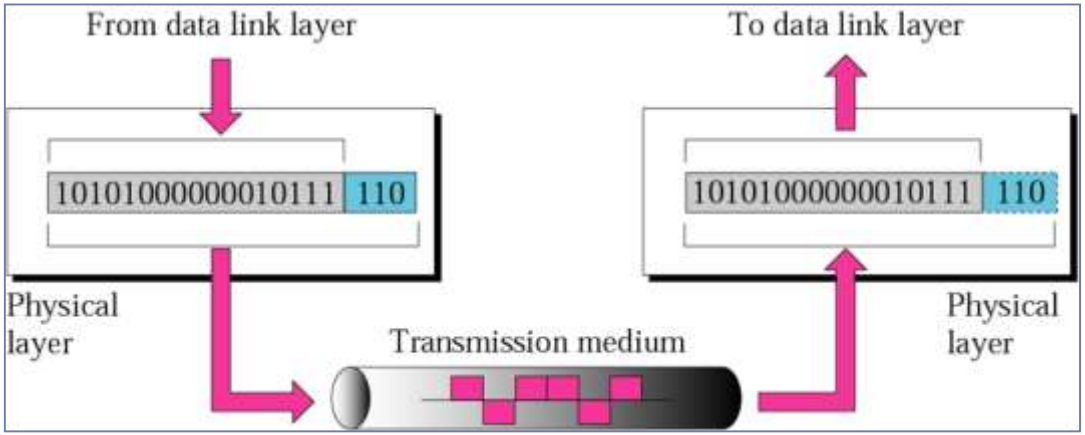




OSI Reference Model

1. **Physical Layer**

- **The Physical Layer is the lowest layer of the OSI model and it deals with data in the form of bits or signals.**
- The type of signal being generated depends upon the transmission medium. For example, if we are using copper wire or LAN cable, the output signal will be an electrical signal. Likewise, the output signal will be a light signal for optical fibre cable, and radio signal for air as a transmission medium.
- At the sender's side, the physical layer will get the data from the upper layer and convert it into bitstreams(0's and 1's) and send it through a physical channel. At the receiver's side, it will convert the bitstreams into frames to be passed to the data-link layer.



OSI Reference Model

1. **Physical Layer**

Physical Media - Characteristics

Ethernet Media

	10BASE-T	100BASE-TX	100BASE-FX	1000BASE-CX	1000BASE-T	1000BASE-SX	1000BASE-LX	1000BASE-ZX	10GBASE-ZR
Media	EIA/TIA Category 3, 4, 5 UTP - four pair	EIA/TIA Category 5 UTP - two pair	50/62.5 mmulti mode fiber	STP	EIA/TIA Category 5 (or greater) UTP, four pair	50/62.5 micron multimode fiber	50/62.5 micron multimode fiber or 9 micron single mode fiber	9m single mode fiber	9m single mode fiber
Maximum Segment Length	100m (328 feet)	100m (328 feet)	2 km (6562 ft)	25 m (82 feet)	100 m (328 feet)	Up to 550 m (1,804 ft) depending on fiber used	550 m (MMF)10 km (SMF)	Approx. 70 km	Up to 80 km
Topology	Star	Star	Star	Star	Star	Star	Star	Star	Star
Connector	ISO 8877 (RJ-45)	ISO 8877 (RJ-45)		ISO 8877 (RJ-45)	ISO 8877 (RJ-45)				

OSI Reference Model

Following are the functionalities of a physical layer:

1. It defines the transmission media between two connecting devices.
2. It also specifies the data rate(number of bits sent each second) over the defined media.
3. It defines the topology of the network. The topology may be Bus, Ring, Star, Mesh, Tree, or Hybrid.
4. It defines a data transmission mode. It can be Simplex, Half-Duplex, or Duplex.
5. It defines the type of data encoding used in the transmission.
6. It defines the line configuration of the network. It can be point-to-point or multipoint.

OSI Reference Model

2. Data Link Layer

- **The Data-Link Layer is the second layer of the OSI model. It performs the physical addressing of data.**

- Physical addressing is the process of adding the physical(MAC) address to the data. MAC(Media Access Control) Address is a 48-bit alpha-numeric number that is embedded in NIC(Network Interface Card) by the manufacturer.

- In other words, the data-link layer is embedded as software in the NIC which provides a means for data transfer from one computer to another via a local media. Thus, the data-link layer facilitates the transmission of data within the same network only.

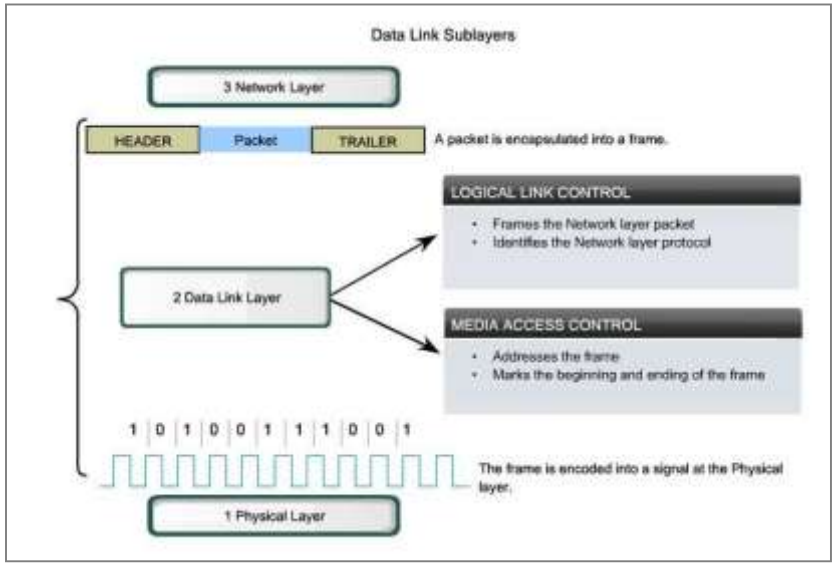
The data link layer is subdivided into two types of sublayers:

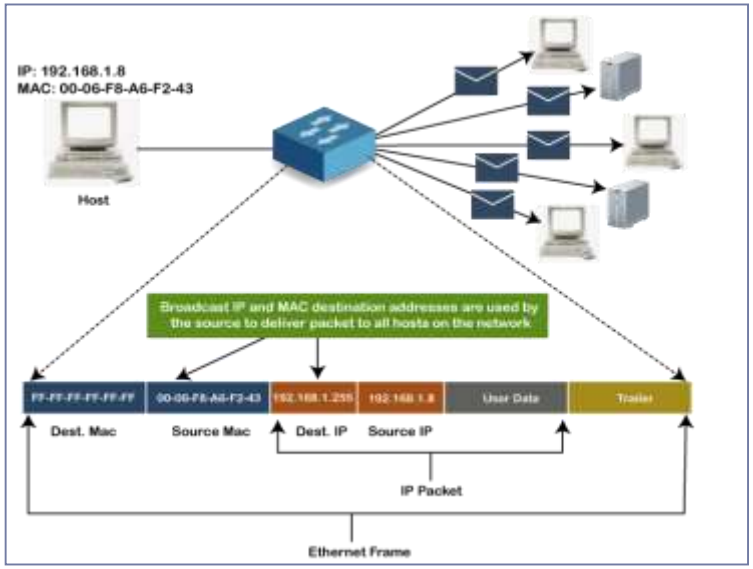
- **Media Access Control (MAC) layer-** It is responsible for controlling how device in a network gain access to medium and permits to transmit data.
- **Logical link control layer-** This layer is responsible for identity and encapsulating network-layer protocols and allows you to find the error.

OSI Reference Model

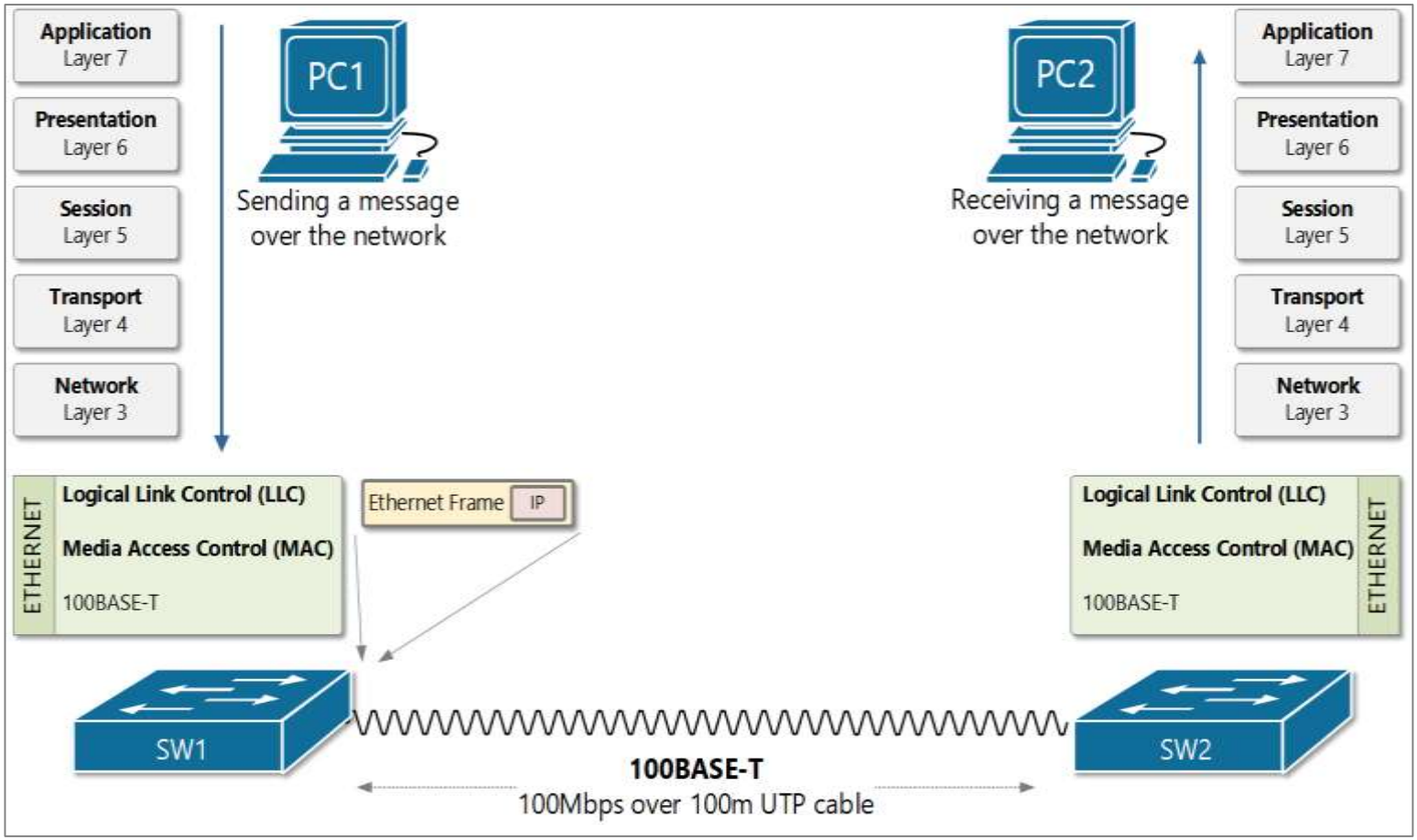
Important Functions of Datalink Layer:

1. Framing which divides the data from Network layer into frames.
2. Allows you to add header to the frame to define the physical address of the source and the destination machine
3. Adds Logical addresses of the sender and receivers
4. It is also responsible for the sourcing process to the destination process delivery of the entire message.
5. It also offers a system for error control in which it detects retransmits damage or lost frames.
6. Datalink layer also provides a mechanism to transmit data over independent networks which are linked together.





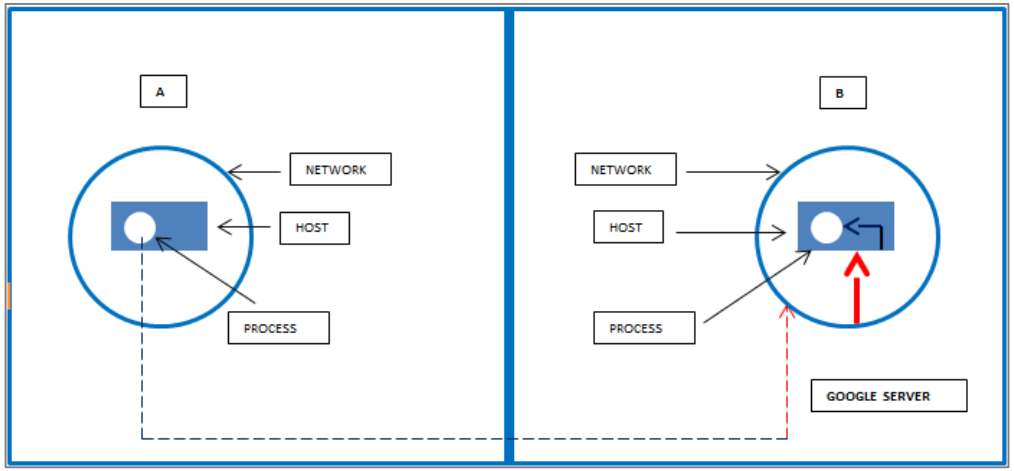
OSI Reference Model

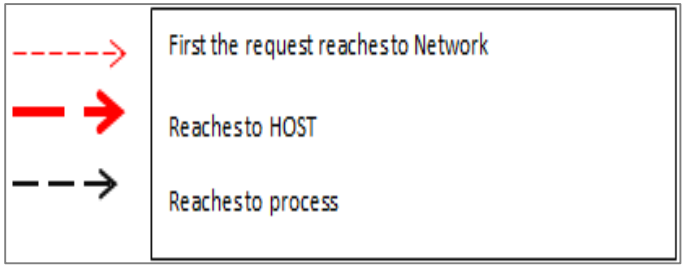


OSI Reference Model

Understanding the Process

- So now we are going to learn the computer network process.
- The network segment is very huge and has a greater need to work on its improvement. It allows computing devices to exchange data over wired or wireless networks.
- Within a network, there is a host (many hosts can be there) and within a host, there is a process (many processes can be there).





- Now with using only the domain name, we have to identify the network, the host and the process which is the entire thing we will see happening.
- The domain name (i.e. www.google.com) must be converted to IP address so that it can be understood by the receiving host and networks.
- So, IP address has 2 parts 1. HOST ID 2. NETWORK ID.

OSI Reference Model

3. Network Layer

- **It mainly performs the transmission of data from one computer to another in different networks.**
- This layer may not be so beneficial if we are transmitting the data in the same network. **The network layer performs logical addressing(IP addressing) of the data.**
- The source and destination IP addresses are included in the data header file by the network layer. The data is in the form of packets in this layer.
- At the sender side, the network layer breaks the data segments received from the upper layer into smaller units, called data packets.
- Similarly, at the receiver's side, it reassembles the data packets into segments for the upper layer, i.e., the transport layer.
- Routers are mainly used in the network layer for routing purposes.
- **Some of the protocols that are mostly used in this layer are OSPF(Open Shortest Path First), BGP(Border Gateway Protocol), IS-IS(Intermediate System to Intermediate System), etc.**

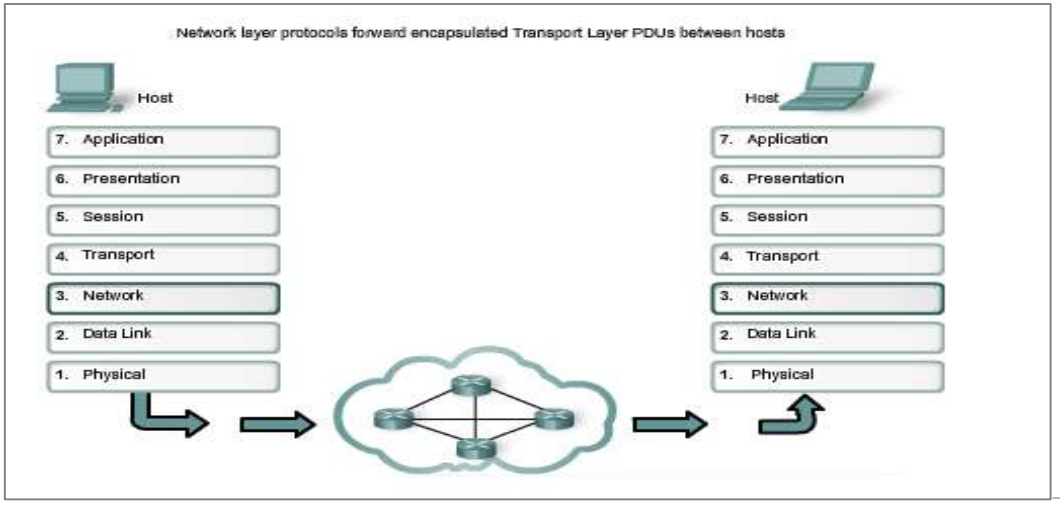
OSI Reference Model

Following are the main functionalities of a network layer:

- **Logical Addressing:** Every computer in a network has a unique IP(Internet Protocol) address. The network layer attaches the source and destination IP address to the data so that it can be transmitted even in different networks. Internet Protocol Version 4(IPv4) and Internet Protocol Version 6(IPv6) addressing are used by the network layer for logical addressing.

- **Routing:** Routing is a process through which the data packets can travel from one node to another in a computer network. In the network layer, the routing decisions are mainly based on IP addresses or logical addressing.

- **Path Determination:** Path determination is the process of selecting a path from various available paths based on the routing information. Path determination is done by the network layer for finding the most optimum path for data transmission.



OSI Reference Model

4. Transport Layer

- **It is mainly responsible for the process-to-process delivery of the data. It performs flow and error control in the data for its proper transmission.**
- The transport layer controls the reliability of communication through various functionalities.
- At the sender's side, the transport layer receives the data from the upper layer and performs segmentation.
- The source and destination port numbers are also included in the header file of the data before forwarding it to the network layer.
- At the receiver's side, the transport layer performs the reassembly and sequencing of data. It reads the port number of the data from the header file, and then direct it towards the proper application.

OSI Reference Model

Following are the main functionalities of a transport layer:

- **Segmentation:** Dividing the data received into multiple data segments can be termed as segmentation. The transport layer performs the **assembly as well as reassembly** of data at the sender's and receiver's side respectively. Each segment has the source and destination 'port' and 'sequence' number. The port number helps to direct each data segment to the correct application, while the sequence number keeps them in a correct sequence when the segmented data is received at the receiver's side.

- **Flow Control:** The transport layer controls the **flow of the data** being transmitted. It is mainly done to avoid any data loss and enhance data transmission efficiency.

- **Error Control:** The transport layer checks for any kind of errors in the data using the **checksum bits** that are present in the data header. It can also request for retransmission of some data if it is not received at the receiver's end.

- **Connection Control:** The transport layer also maintains the connection between the devices in a proper way.

For connection-oriented transmission, **TCP(Transmission Control Protocol)** is used. TCP is quite slow but is reliable in nature. It can be used for long-distance transmissions.

For connection-less transmission, **UDP(User Datagram Protocol)** is used. UDP is fast but not reliable in nature. It is mainly preferred for short-distance transmissions.

OSI Reference Model

5. Session Layer

- **It mainly helps in setting up, closing and managing the connection in the network.**
- Actually, whenever two devices get connected, a session is created, which is terminated as soon the connection is no longer required.
- The termination of the session is important to avoid the unnecessary wastage of resources. In other words, the session layer performs session management.
- The session layer enables the devices to send and receive the data by establishing connections and also terminates the connection after the data transfer.
- It mainly performs authentication and authorization for establishing a secure connection in the network.

OSI Reference Model

Following are the main functionalities of a session layer:

- **Authentication:** Authentication is a process of **verifying the user**. The session layer may ask the devices to enter valid login credentials, so as to maintain a secure data connection.

- **Authorization:** Authorization is the process of determining the **user's authority to access the data**. The session layer determines whether the device has permission to access those data elements or not.

- **Synchronization:** The session layer synchronizes the sender and receiver. It adds various **checkpoints with the data to synchronize data** at the sender's and receiver's side. In case of any crash or transfer failure, the data transmission can be resumed from the last checkpoint. There is no need to retransfer the whole data.

OSI Reference Model

6. Presentation Layer

- **It mainly performs data translation, encryption & decryption, and compression in the network.** The presentation layer deals with the syntax and semantics of the information exchanged between two systems.
- At the sender's side, it receives the data from the application layer and performs **data encryption and compression to it**.
- At the receiver's side, it receives the data from the transport layer and performs **data translation, decryption, and uncompresses** data.

Following are the main functionalities of a presentation layer:

- **Data Translation:** Data translation refers to transforming data from one form to the other. The presentation layer transforms the high-level **user language data to the equivalent low-level machine-level language**, and vice versa. Some of the standards used by this layer for translation are ASCII, EBCDIC, etc.
- **Data Encryption and Decryption:** Data encryption is the process of converting a **plain text into cypher text for security**. Encryption is applied to the data at the sender's side. Data decryption is the process of converting a **ciphertext into plain text**. It is applied to the data at the receiver's side. The presentation layer uses the SSL(Secure Socket Layer) for data encryption and decryption.
- **Data Compression:** Data compression is the process of **reducing the number of bits in the data.** It can either be lossy or lossless in nature. Lossless compression is mostly preferred for some important data items.

OSI Reference Model

7. Application Layer

- **The Application layer is the topmost layer of the OSI model. This layer is mostly used by the network applications, that use the network.**
- It mainly acts as an interface between the user and the network services. The Application layer provides services for network applications with the help of protocols.

Some of the most widely used application layer protocols are HTTP, HTTPS, FTP, NFS, DHCP, FMTP, SNMP, SMTP, Telnet, etc.

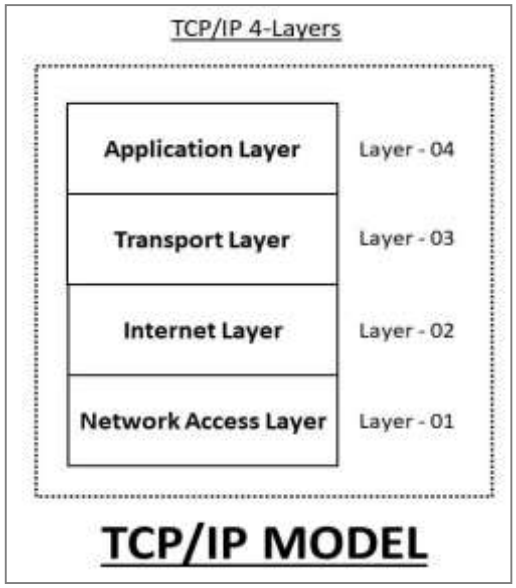
Following are the main functionalities of an application layer:

- **File Transfer:** The Application layer mainly facilitates the file transfer between two network devices with the help of FTP(File Transfer Protocol).
- **Web Surfing:** Web surfing is possible only in the application layer. Some protocols like HTTP(Hypertext Transfer Protocol), HTTPs(Hypertext Transfer Protocol Secure), etc. enables web surfing.
- **Emails:** Electronic-mails can be sent from one device to another on the network only through the application layer. Some protocols like SMTP(Simple Mail Transfer Protocol), etc. are used for sending emails over the network.
- **Network Virtual Terminal:** The Application layer facilitates the remote host login in the network with the help of protocols like Telnet, etc. It can also be referred to as the software version of the physical terminal in the network.

TCP/IP Reference Model

- The TCP/IP reference model is a layered model developed by the Defense Project Research Agency(ARPA or DARPA) of the United States as a part of their research project in 1960.
- Initially, it was developed to be used by defense only. But later on, it got widely accepted.
- The main purpose of this model is to connect two remote machines for the exchange of information. These machines can be operating in different networks or have different architecture.

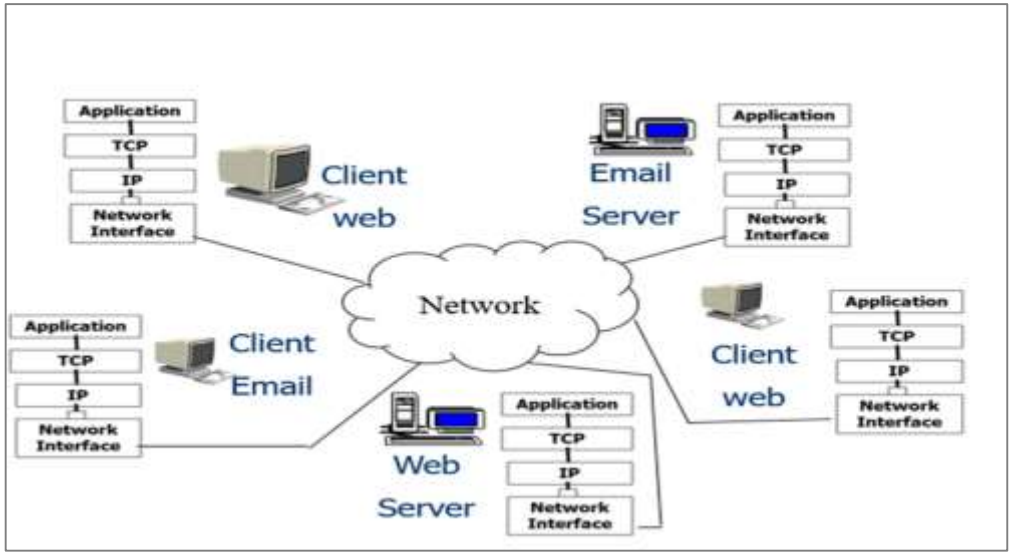
In the early days, the TCP/IP reference model has four layers, as described below.

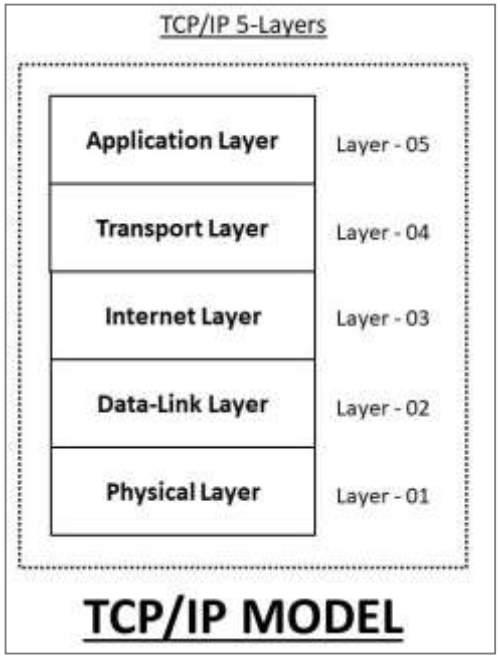


TCP/IP Reference Model

- These layers are much similar to the layers of the **OSI model**.
- The Application layer in the TCP/IP model has approximately the same functionality as the upper three layers(Application, Presentation, and Session layer) of the OSI model.
- Also, the Internet layer acts as the Network layer, and the Network Access layer acts as the lower two layers(Physical and Data-Link layer) of the OSI model.
- TCP/IP network model is named after two main protocols(TCP and IP) and is widely used in current internet architecture.

But nowadays, we generally use a five-layer TCP/IP model, as shown below.





TCP/IP Reference Model

1. **Physical Layer**

- The Physical Layer is the lowest layer of the TCP/IP model.
- It deals with data in the form of bits. This layer mainly handles the host to host communication in the network.
- It defines the transmission medium and mode of communication between two devices. The medium can be wired or wireless, and the mode can be simplex, half-duplex, or full-duplex.
- It also specifies the line configuration(point-to-point or multiport), data rate(number of bits sent each second), and topology in the network.
- There are no specific protocols that are used in this layer. The functionality of the physical layer varies from network-to-network.

TCP/IP Reference Model

2. Data-Link Layer

- The Data-Link Layer is the second layer of the TCP/IP layer.
- It deals with data in the form of data frames.
- It mainly performs the data framing in which, it adds some header information to the data packets for the successful delivery of data packets to correct destinations.
- For this, it performs physical addressing of the data packets by adding the source and the destination address to it.
- The data-link layer facilitates the delivery of frames within the same network.
- It also facilitates the flow and error control of the data frames. The flow of the data can be controlled through the data rate.
- Also, the errors in the data transmission and faulty data frames can be detected and retransmitted using the checksum bits in the header information.

TCP/IP Reference Model

3. Internet Layer

- The Internet layer of the TCP/IP model is approximately the same as the Network layer of the OSI model.
- It deals with data in the form of datagrams or data packets.
- This layer mainly performs the logical addressing of the data packets by adding the IP(Internet Protocol) address to it.
- The IP addressing can be done either by using the Internet Protocol Version 4(IPv4) or Internet Protocol Version 6(IPv6).
- The Internet layer also performs routing of data packets using the IP addresses. The data packets can be sent from one network to another using the routers in this layer.
- This layer also performs the sequencing of the data packets at the receiver's end. In other words, it defines the various protocols for logical transmission of data within the same or different network.
- The protocols that are used in the Internet layer are IP(Internet Protocol), ICMP(Internet Control Message Protocol), IGMP(Internet Group Management Protocol), ARP(Address Resolution Protocol), RARP(Reverse Address Resolution Protocol), etc.

TCP/IP Reference Model

4. Transport Layer

- The Transport layer is the fourth layer of the TCP/IP model. It deals with data in the form of data segments. It mainly performs segmentation of the data received from the upper layers.
- It is responsible for transporting data and setting up communication between the application layer and the lower layers.
- This layer facilitates the end-to-end communication and error-free delivery of the data. It also facilitates flow control by specifying data rates.
- The transport layer is used for process-to-process communication with the help of the port number of the source and the destination.

The Transport layer facilitates the congestion control using the following protocols:

TCP:

- TCP stands for Transmission Control Protocol. It is a connection-oriented protocol. It performs sequencing and segmentation of data.
- It also performs flow and error control in data transmission. There is an acknowledgement feature in TCP for the received data. It is a slow but reliable protocol. It is suitable for important and non-real time data items.

UDP:

- UDP stands for User Datagram Protocol. It is a connection-less protocol. It does not perform flow and error control in data transmission.
- There is no acknowledgement feature in UDP for the received data. It is a fast but unreliable protocol. It is suitable for real-time data items.

TCP/IP Reference Model

5. ApplicationLayer

- The Application layer in the TCP/IP model is equivalent to the upper three layers(Application, Physical, and Session Layer) of the OSI model.
- It deals with the communication of the whole data message. The Application layer provides an interface between the network services and the application programs.
- It mainly provides services to the end-users to work over the network.

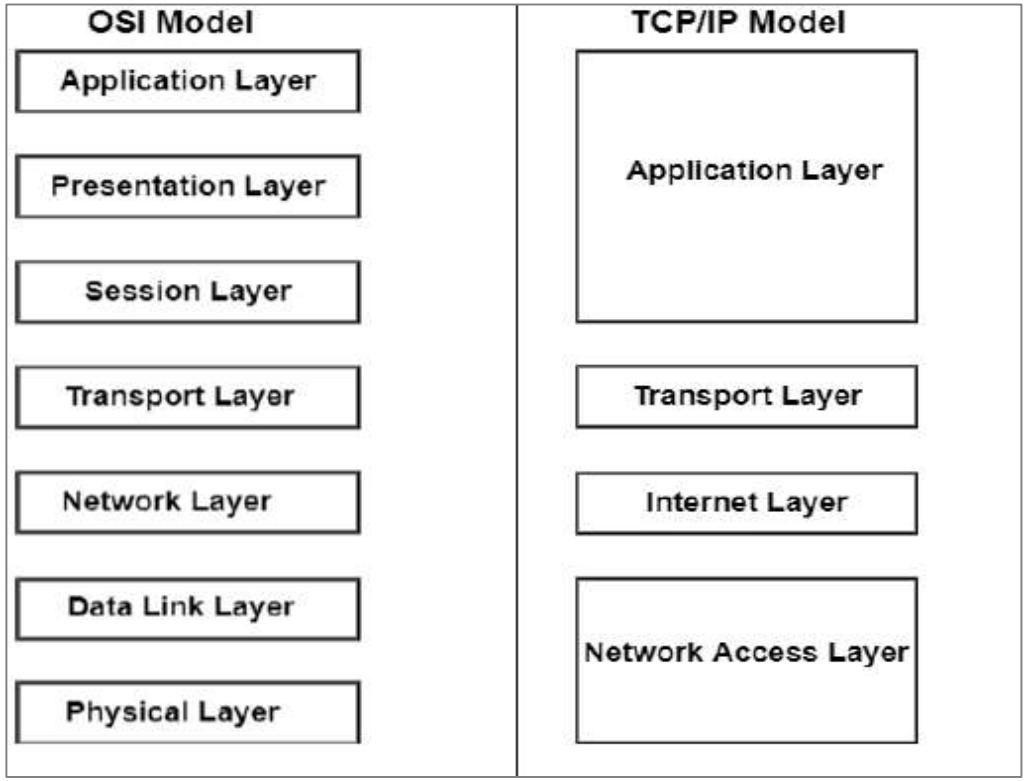
For Example, file transfer, web browsing, etc.

This layer uses all the higher-level protocols like HTTP, HTTPS, FTP, NFS, DHCP, FMTP, SNMP, SMTP, Telnet, etc.

- The application layer helps in setting up and managing the network connections.
- It also checks for the user's program authentication and authorization for the data.
- It also performs some complex operations like data translation, encryption and decryption, and data compression.
- The application layer synchronizes the data at the sender's and the receiver's end.
- In other words, it is the topmost layer and defines the interface for application programs with transport layer services.

OSI Vs TCP/IP Model

Following are the differences between OSI and TCP/IP Reference Model –



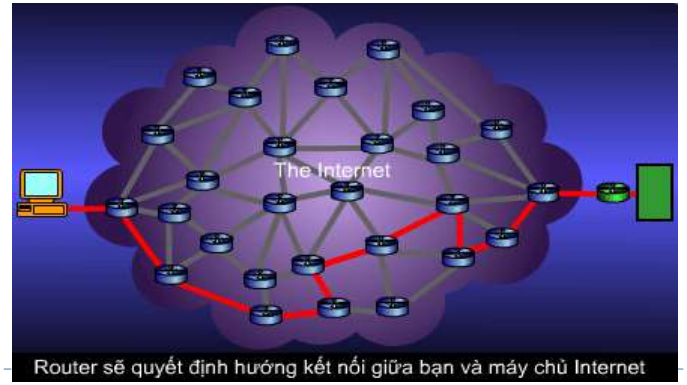
OSI Vs TCP/IP Model

Following are the differences between OSI and TCP/IP Reference Model –

OSI	TCP/IP
OSI represents **Open System Interconnection**.	TCP/IP model represents the Transmission Control Protocol / Internet Protocol.
OSI is a generic, protocol independent standard. It is acting as an interaction gateway between the network and the final-user.	TCP/IP model depends on standard protocols about which the computer network has created. It is a connection protocol that assigns the network of hosts over the internet.
The OSI model was developed first, and then protocols were created to fit the network architecture's needs.	The protocols were created first and then built the TCP/IP model.
It provides quality services.	It does not provide quality services.
The OSI model represents defines administration, interfaces and conventions. It describes clearly which layer provides services.	It does not mention the services, interfaces, and protocols.
The protocols of the OSI model are better unseen and can be returned with another appropriate protocol quickly.	The TCP/IP model protocols are not hidden, and we cannot fit a new protocol stack in it.
It is difficult as distinguished to TCP/IP.	It is simpler than OSI.
It provides both connection and connectionless oriented transmission in the network layer; however, only connection-oriented transmission in the transport layer.	It provides connectionless transmission in the network layer and supports connecting and connectionless-oriented transmission in the transport layer.
It uses a horizontal approach.	It uses a vertical approach.
The smallest size of the OSI header is 5 bytes.	The smallest size of the TCP/IP header is 20 bytes.
Protocols are unknown in the OSI model and are returned while the technology modifies.	In TCP/IP, returning protocol is not difficult.

Network Examples

- **INTERNET**
- **ARPANET**
- **Internet –** Internet is a global network that connects billions of computers across the world with each other and to the World Wide Web.
- It uses standard internet protocol suite (TCP/IP) to connect billions of computer users worldwide.
- It is set up by using cables such as optical fibers and other wireless and networking technologies.
- At present, internet is the fastest mean of sending or exchanging information and data between computers across the world.
- It is believed that the internet was developed by "Defense Advanced Projects Agency" (DARPA) department of the United States. And, it was first connected in 1969.



Network Examples

Why is the Internet Called a Network?

- Internet is called a network as it creates a network by connecting computers and servers across the world using routers, switches and telephone lines, and other communication devices and channels.
- So, it can be considered a global network of physical cables such as copper telephone wires, fiber optic cables, tv cables, etc.
- Furthermore, even wireless connections like 3G, 4G, or Wi-Fi make use of these cables to access the Internet.

Internet is different from the World Wide Web

- The World Wide Web is a network of computers and servers created by connecting them through the internet.
- So, the internet is the backbone of the web as it provides the technical infrastructure to establish the WWW and acts as a medium to transmit information from one computer to another computer.
- It uses web browsers to display the information on the client, which it fetches from web servers.

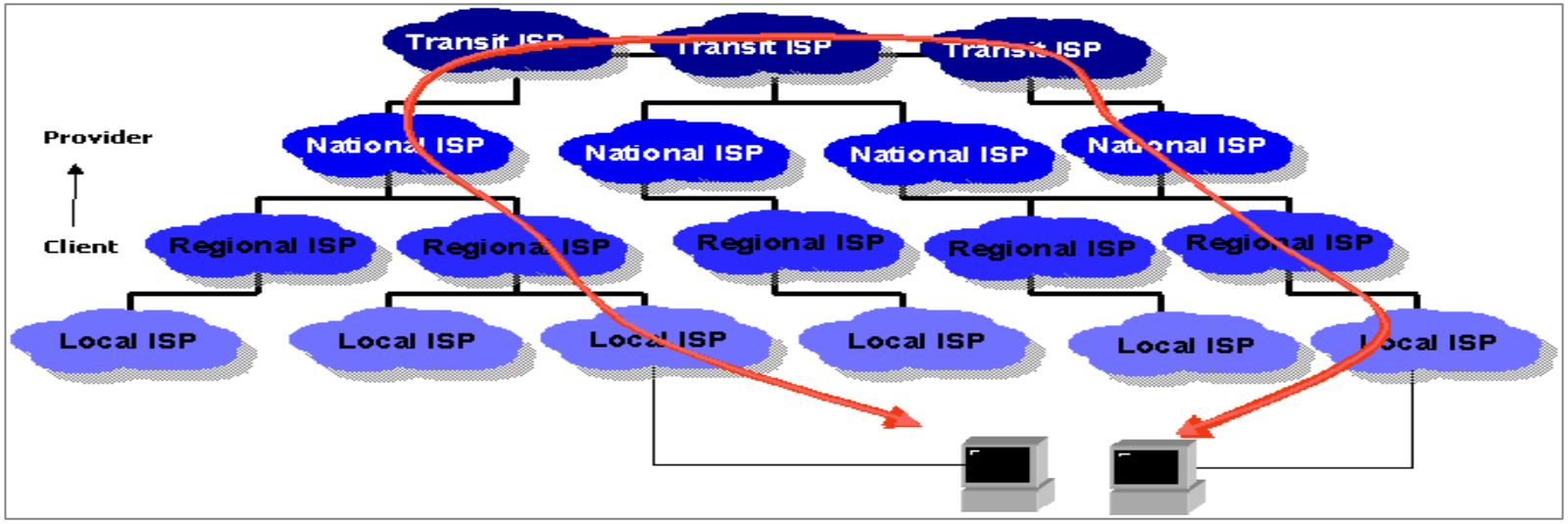
Network Examples

Internet is defined as an Information super Highway, to access information over the web.

However, It can be defined in many ways as follows:

- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name **http://www.google.com** to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.

Network Examples



Network Examples

- ARPANET stands for Advanced Research Projects Agency NET.
- ARPANET was first network which consisted of distributed control. It was first to implement TCP/IP protocols.
- It was basically beginning of Internet with use of these technologies.
- It was designed with a basic idea in mind that was to communicate with scientific users among an institute or university.

History of ARPANET :

- ARPANET was introduced in the year 1969 by Advanced Research Projects Agency (ARPA) of US Department of Defense.
- It was established using a bunch of PCs at various colleges and sharing of information and messages was done.
- It was for playing as long separation diversions and individuals were asked to share their perspectives.
- In the year 1980, ARPANET was handed over to different military network, Defense Data Network.

Network Examples

Characteristics of ARPANET :

- It is basically a type of WAN.
- It used concept of Packet Switching Network.
- It used Interface Message Processors(IMPs) for sub-netting.
- ARPANETs software was split into two parts- a host and a subnet.

Advantages of ARPANET :

- ARPANET was designed to service even in a Nuclear Attack.
- It was used for collaborations through E-mails.
- It created an advancement in transfer of important files and data of defense.

Limitations of ARPANET :

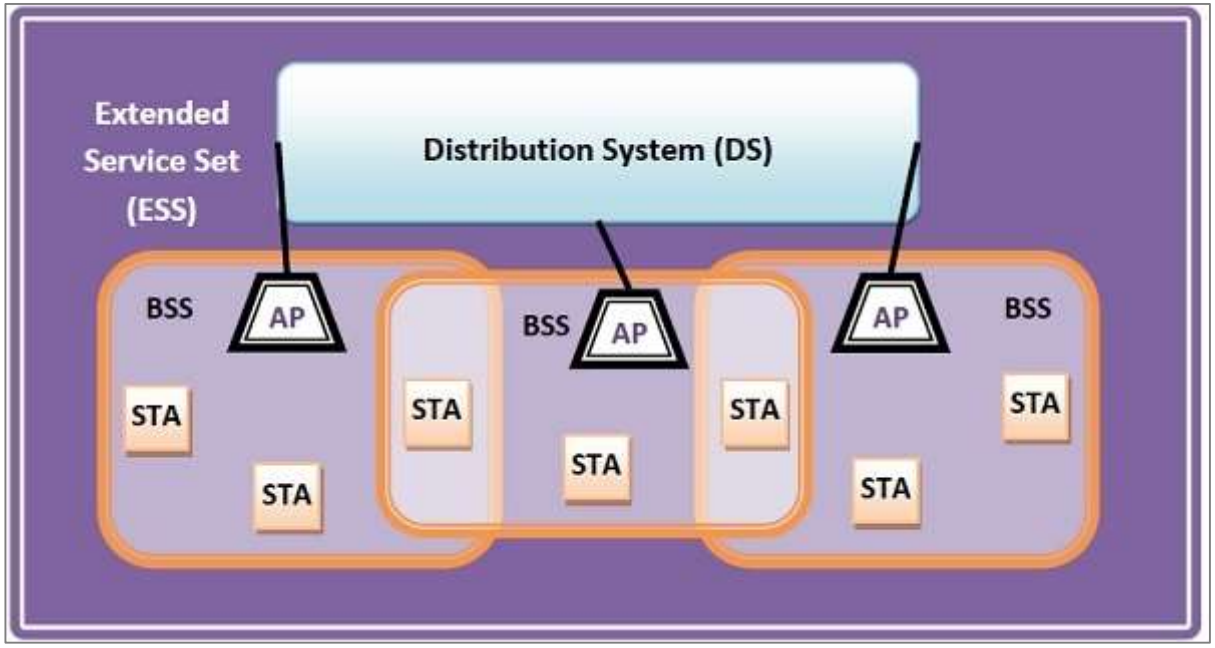
- Increased number of LAN connections resulted in difficulty handling.
- It was unable to cope-up with advancement in technology.

Network Examples

IEEE 802.11

- IEEE 802.11 standard, popularly known as WiFi, lays down the architecture and specifications of wireless LANs (WLANs). WiFi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.

IEEE 802.11 Architecture



Network Examples

The components of an IEEE 802.11 architecture are as follows −

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
  - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
  - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.

Each station has a wireless network interface controller.

- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level.

BSS can be of two categories depending upon the mode of operation−

- **Infrastructure BSS −** Here, the devices communicate with other devices through access points.
- **Independent BSS −** Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.

- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.

Network Examples

IEEE 802.11 Mac Frame

- MAC layer provides functionality for several tasks like control medium access, can also offer support for roaming, authentication, and power conservation.
- The basic services provided by MAC are the **mandatory asynchronous data service and optional time-bounded service**.

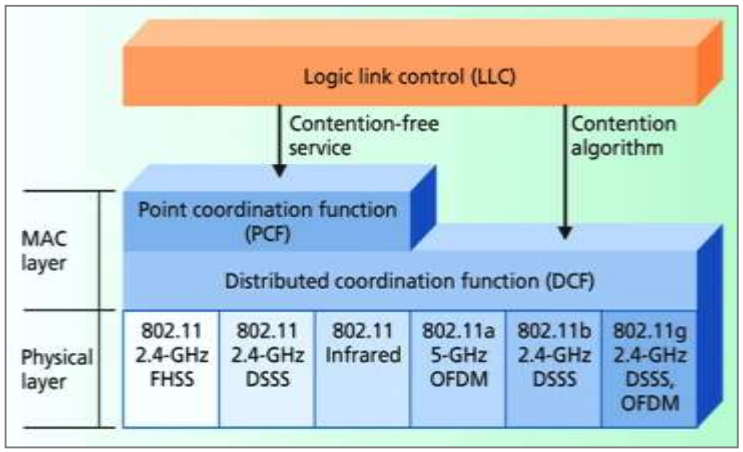
IEEE 802.11 defines two MAC sub-layers:-

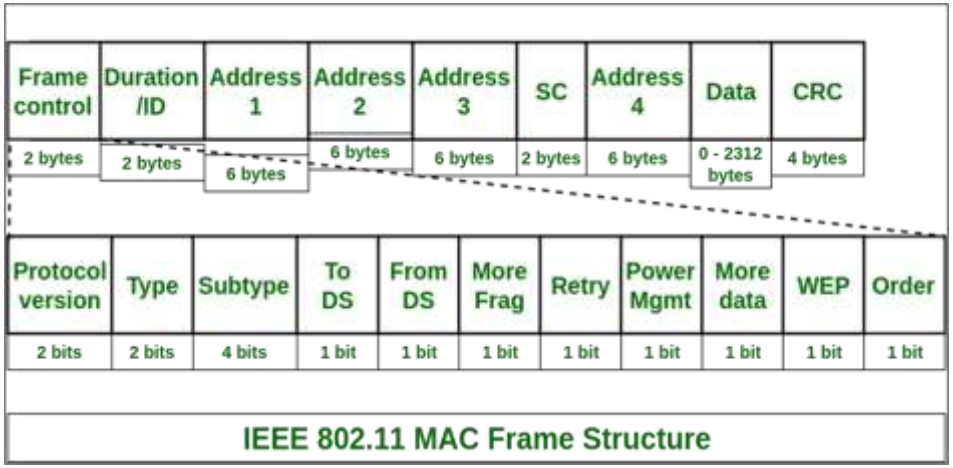
- **Distributed Coordination Function (DCF) –**
  DCF uses **CSMA/CA as access method** as wireless LAN can't implement CSMA/CD. It only offers asynchronous service.

- **Point Coordination Function (PCF) –**
  PCP is implemented on top of DCF and mostly used **for time-service transmission**. It uses a centralized, contention-free polling access method. It offers both **asynchronous and time-bounded service**.

MAC Frame:

The MAC layer frame consists of 9 fields. The following figure shows the basic structure of an IEEE 802.11 MAC data frame along with the content of the frame control field.





Network Examples

- **Frame Control** – It is a 2 bytes starting field composed of 11 subfields. It contains control information of the frame.

1. **Version:** It is a 2 bit long field which indicates the current protocol version which is fixed to be 0 for now.
2. **Type:** It is a 2 bit long field which determines the function of frame **i.e management(00), control(01) or data(10).** The value 11 is reserved.
3. **Subtype:** It is a 4 bit long field which indicates sub-type of the frame like 0000 for association request, 1000 for beacon.
4. **To DS:** It is a 1 bit long field which when set indicates that destination frame is for DS(distribution system).
5. **From DS:** It is a 1 bit long field which when set indicates frame coming from DS.
6. **More frag (More fragments):** It is 1 bit long field which when set to 1 means frame is followed by other fragments.
7. **Retry:** It is 1-bit long field, if the current frame is a retransmission of an earlier frame, this bit is set to 1.
8. **Power Mgmt (Power management):** It is 1-bit long field that indicates the mode of a station after successful transmission of a frame. Set to 1 the field indicates that the station goes into power-save mode. If the field is set to 0, the station stays active.
9. **More data:** It is 1-bit long field that is used to indicate receiver that a sender has more data to send than the current frame. This can be used by an access point to indicate to a station in power-save mode that more packets are buffered or it can be used by a station to indicate to an access point after being polled that more polling is necessary as the station has more data ready to transmit.
10. **WEP:** It is 1 bit long field which indicates that the standard security mechanism of 802.11 is applied.
11. **Order:** It is 1 bit long field, if this bit is set to 1 the received frames must be processed in strict order.

Network Examples

- **Duration/ID** –

  It is 4 bytes long field which contains the **value indicating the period of time** in which the medium is occupied(in μs).

- **Address 1 to 4 –**

  These are 6 bytes long fields which contain standard IEEE 802 MAC addresses (48 bit each). The meaning of each address depends on the DS bits in the frame control field.

- **SC (Sequence control) –**

  It is 16 bits long field which consists of 2 sub-fields, i.e., **Sequence number (12 bits) and Fragment number (4 bits)**. Since acknowledgement mechanism frames may be duplicated hence, a sequence number is used to filter duplicate frames.

- **Data –**

  It is a variable length field which contain information specific to individual frames which is transferred transparently from a sender to the receiver(s).

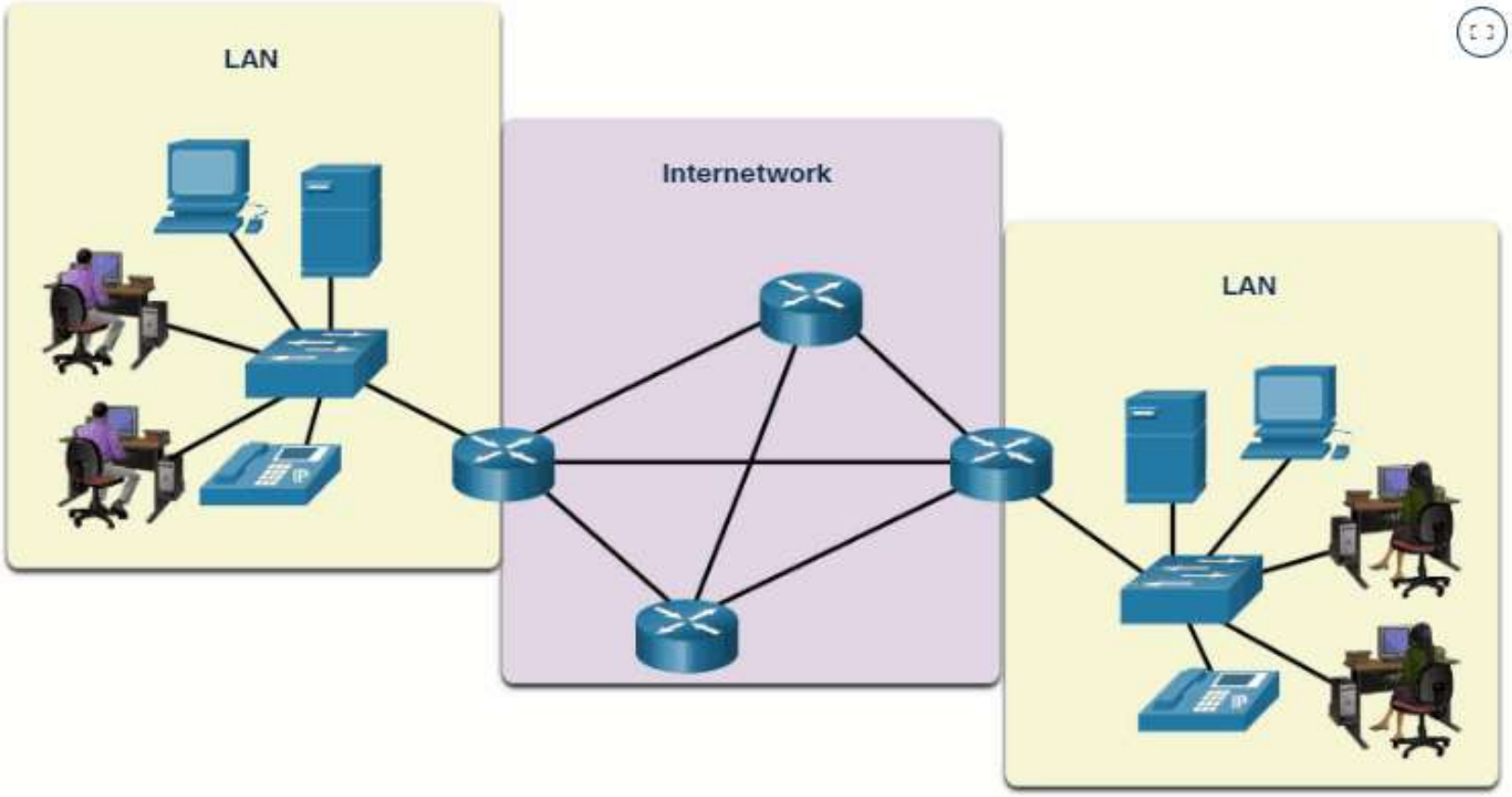
- **CRC (Cyclic redundancy check) –**

  It is 4 bytes long field which contains a **32 bit CRC error detection sequence** to ensure error free frame.

Internet Based Applications

Internet is used for different purposes by different people. Some uses of the Internet are listed below:

1. E-Commerce (auction, buying, selling products etc.)
2. Research (on-line journals, magazines, information etc.)
3. Education (e-learning courses, virtual classroom, distance learning)
4. E-Governance (online filing of application (Income Tax), on-line application forms etc.)
5. On-line ticket booking (airplane tickets, rail tickets, cinema hall tickets etc.)
6. On-line payments (credit card payments etc.)
7. Video conferencing
8. Exchange of views, music, files, mails, folders, data, information etc.
9. Outsourcing jobs (work flow software)
10. Social networking (sites like facebook, linkedin, twitter)
11. E-Telephony (sites like skype)



Data originates with an end device, flows through the network, and arrives at an end device.

CN: UNIT-1 Network Devices

Prepared By,
M.Gouthamm, Asst.Prof, CSE, MRUH

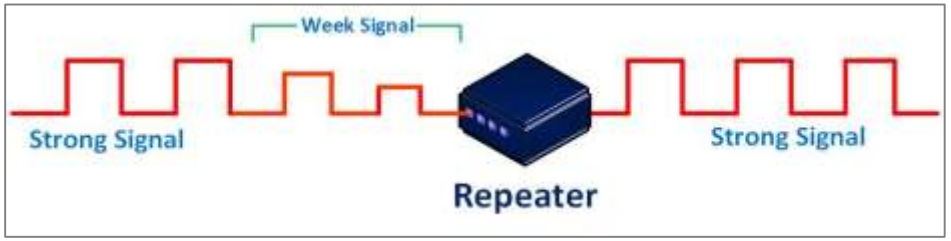
Network Devices

- To communicate data through different transmission media and to configure networks with different functionality, we require different devices like Modem, Hub, Switch, Repeater, Router, Gateway, etc. Let us explore them in detail.

Network Devices

1. REPEATER

- A repeater is a two-port device that operates at the physical layer .
- It is used to regenerate the signal over the same network before it becomes too weak or corrupted, allowing the signal to be transmitted for a longer distance over the same network.
- It is important to understand that repeaters do not amplify the signal. When the signal weakens, repeaters copy it bit by bit and regenerate it at its original strength.

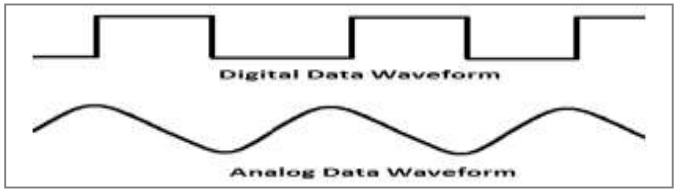


Types of Repeater

On the basis of signals that repeaters generate.

- **Analog Repeaters :**

In an analog repeater, data is transmitted through analog signals to increase its amplitude. These repeaters are used in trunk lines to help broadcast multiple signals using **frequency division multiplexing** (FDM). It houses the linear amplifier as well as the filters.



- **Digital Repeaters :**

In a digital repeater, data is transmitted in the form of binary digits such as 0s and 1s. While transmitting data, 0 and 1 values are generated, and it is capable of transmitting data over long distance.

Network Devices

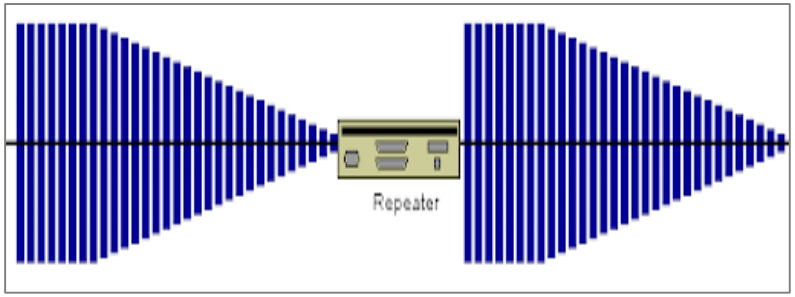
Based on the types of connected networks.

- **Wired Repeaters :**

  These repeaters are commonly used in wired Local Area Networks .

- **Wireless Repeaters :**

  They are commonly used in wireless LANs and cellular networks .



Advantages of Repeater

- Repeaters can increase the overall distance of a network.
- Repeaters are easy to set up and can easily increase network length or coverage area.
- Repeaters have no significant impact on network performance.
- It is a cost-effective network device.

Disadvantages of Repeater

- Repeaters are unable to connect disparate networks.
- Repeaters cannot reduce network traffic.
- Most repeaters on a network generate noise on the wire, increasing the possibility of packet collisions.

Network Devices

2. BRIDGE

- A **bridge** is a network device that operates at the data link layer device.
- A bridge is a repeater with the added functionality of filtering content by reading the MAC addresses of the source and destination.
- It is also used to connect two LANs that use the same protocol. It has a **single input** and **output port**, making it a two-port device.

Types of Bridges

There are generally two types of bridges used in networking :

Transparent Bridges :

- A transparent bridge is a type of bridge that monitors incoming network traffic to determine **media access control** (MAC) addresses.
- These bridges operate in a manner that is transparent to all networked hosts. A transparent bridge stores MAC addresses in a table similar to a routing table and uses that information to route packets to their destination.

Source Routing Bridges :

- The source station performs the routing operation in these bridges, and the frame specifies which route to take.
- The host can find the frame by sending a special frame known as the **discovery frame**, which propagates throughout the network using all possible paths to the destination.

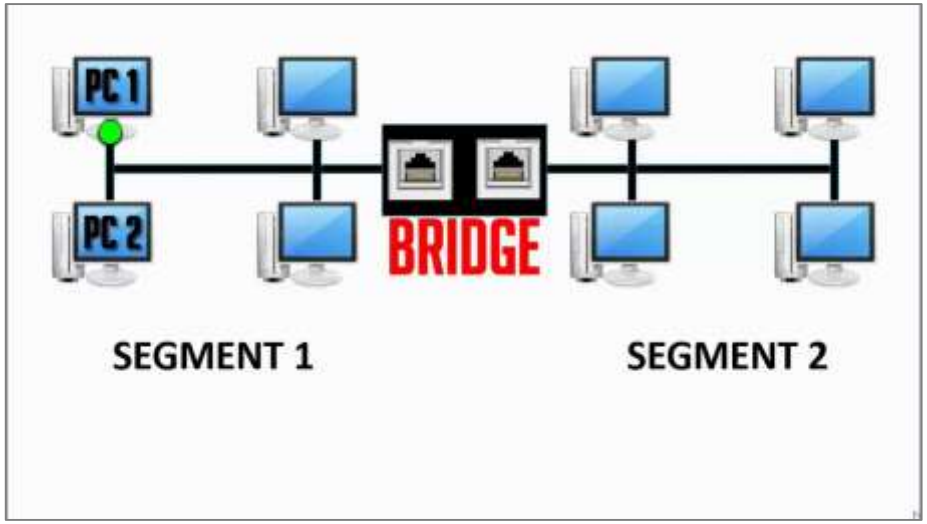
Network Devices

Advantages of Bridge

- Bridges reduce network traffic with minor segmentation.
- Bridges can also help to reduce network traffic on a segment by splitting up network communications.
- Bridge expands the number of connected **workstations** and **network segments**.
- It reduces collisions.

Disadvantages of Bridge

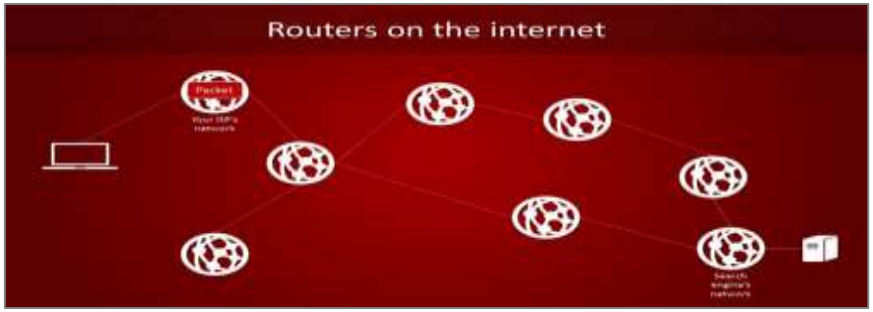
- It is slower than repeaters due to the filtering process.
- A bridge is more expensive than repeaters or hubs.
- Bridges are not scalable to an extremely large network.



Network Devices

3. ROUTERS

- Routers are networking devices operating at layer 3 or a network layer of the OSI model.
- They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks.
- When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.



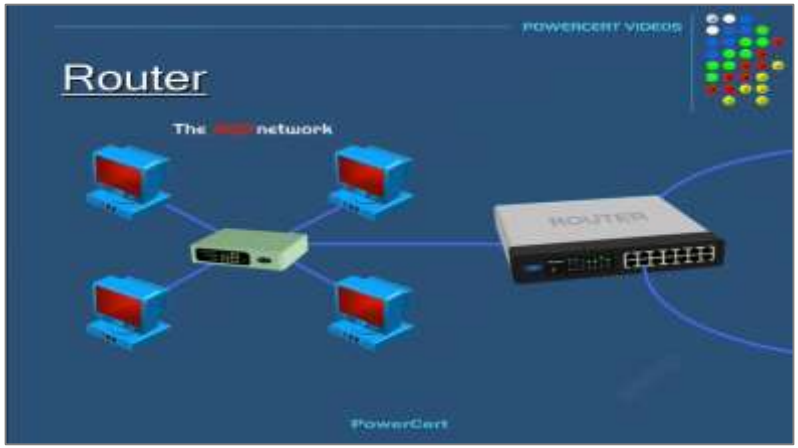
Features of Routers

- A router is a layer 3 or network layer device.
- It connects different networks together and sends data packets from one network to another.
- A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
- It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
- Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.
- Routers are manufactured by some popular companies like −Cisco, D-Link, HP, 3Com, Juniper, Nortel

Network Devices

Routing Table

- The functioning of a router depends largely upon the routing table stored in it.
- The routing table stores the available routes for all destinations.
- The router consults the routing table to determine the optimal route through which the data packets can be sent.



A routing table typically contains the following entities −

- IP addresses and subnet mask of the nodes in the network
- IP addresses of the routers in the network
- Interface information among the network devices and channels

Routing tables are of two types −

- **Static Routing Table −** Here, the routes are fed manually and are not refreshed automatically. It is suitable for small networks containing 2-3 routers.
- **Dynamic Routing Table −** Here, the router communicates with other routers using routing protocols to determine the available routes. It is suited for larger networks having large number of routers.

Network Devices

Types of Routers

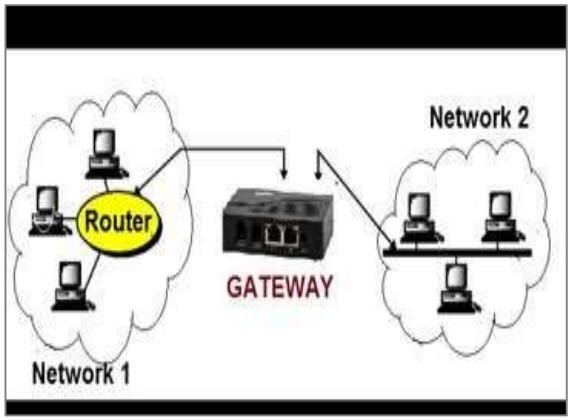
A variety of routers are available depending upon their usages. The main types of routers are −

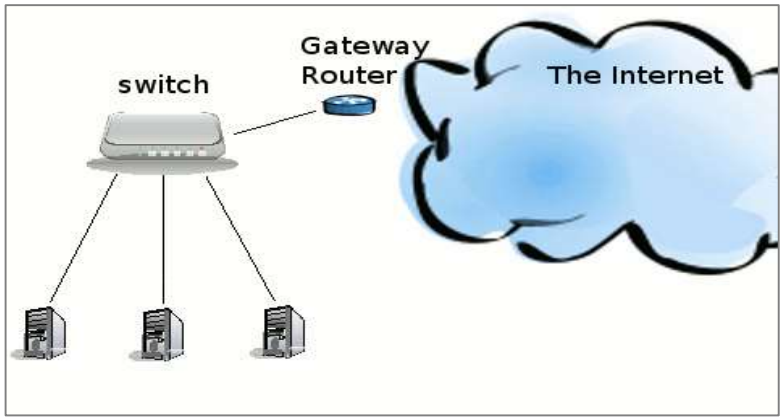
1. **Wireless Router** − They provide **WiFi connection** WiFi devices like laptops, smartphones etc. They can also provide standard Ethernet routing. For indoor connections, the range is 150 feet while its 300 feet for outdoor connections.
2. **Broadband Routers** − They are used to connect to the **Internet through telephone** and to use voice over Internet Protocol (VoIP) technology for providing high-speed Internet access. They are configured and provided by the Internet Service Provider (ISP).
3. **Core Routers** − They can **route data packets within a given network**, but cannot route the packets between the networks. They helps to link all devices within a network thus forming the backbone of network. It is used by ISP and communication interfaces.
4. **Edge Routers** − They are low-capacity routers placed at the periphery of the networks. They **connect the internal network to the external networks**, and are suitable for transferring data packets across networks. They use Border Gateway Protocol (BGP) for connectivity. There are two types of edge routers, subscriber edge routers and label edge routers.
5. **Brouters** − Brouters are specialised routers that can **provide the functionalities of bridges as well**. Like a bridge, brouters help to transfer data between networks. And like a router, they route the data within the devices of a network.

Network Devices

4. GATEWAYS

- As the term "Gateway" suggests, it is a key access point that acts as a "gate" between an organisation's network and the outside world of the Internet.
- Gateway serves as the entry and exit point of a network, as all data coming in or going out of a network must first pass through the gateway in order to use routing paths.
- Besides routing data packets, gateways also maintain information about the host network's internal connection paths and the identified paths of other remote networks.
- If a node from one network wants to communicate with a node of a foreign network, it will pass the data packet to the gateway, which then routes it to the destination using the best possible route





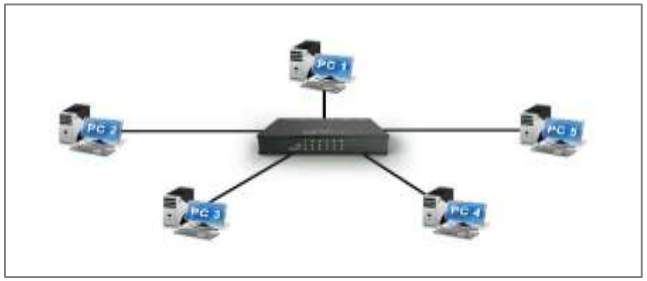
Network Devices

5.HUBS

- A hub is a basically multi-port repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations.
- Hubs cannot filter data, so data packets are sent to all connected devices.
- Also, they do not have the intelligence to find out the best path for data packets which leads to inefficiencies and wastage.

Types of Hub

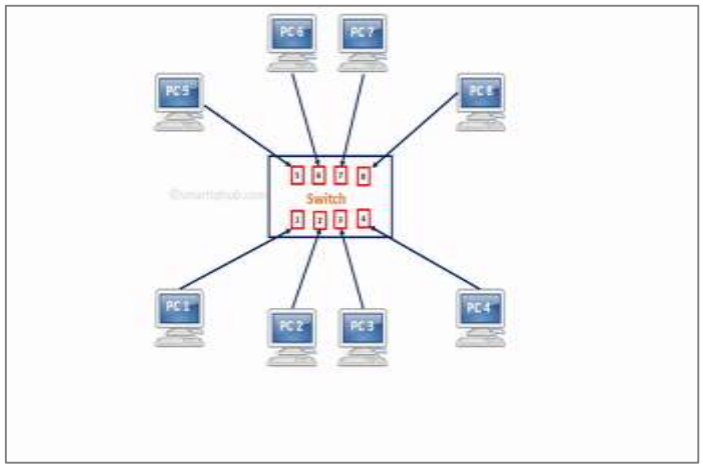
- **Active Hub:-** These are the hubs that have their power supply and **can clean, boost, and relay the signal along with the network**. It serves both as a repeater as well as a wiring center. These are used to extend the maximum distance between nodes.
- **Passive Hub:-** These are the hubs that **collect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

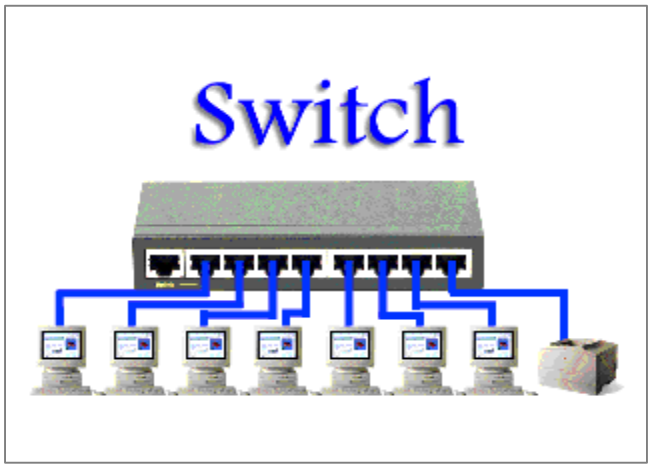


Network Devices

6.SWITCHES

- **Switch** is a network device that connects other devices to **Ethernet** networks through **twisted pair** cables.
- It uses **packet switching** technique to **receive, store** and **forward data packets** on the network.
- The switch maintains a list of network addresses of all the devices connected to it.
- On receiving a packet, it checks the destination address and transmits the packet to the correct port.
- Before forwarding, the packets are checked for collision and other network errors.
- The data is transmitted in full duplex mode



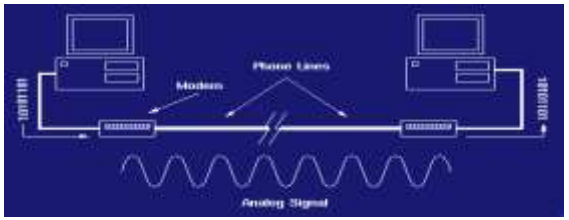


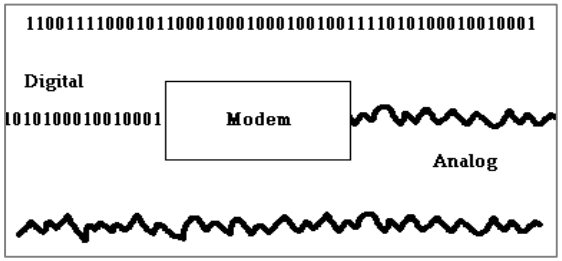
Network Devices

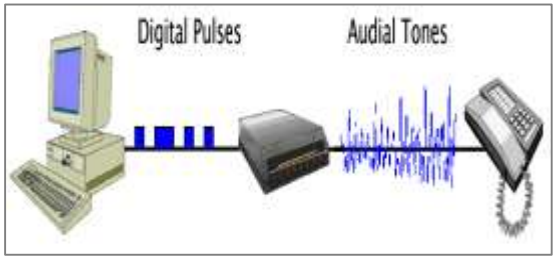
7. MODEMS

Modem is a device that enables a computer to send or receive data over telephone or cable lines. The data stored on the computer is digital whereas a telephone line or cable wire can transmit only analog data.

- The main function of the modem is to convert digital signal into analog and vice versa. Modem is a combination of two devices − **modulator** and **demodulator**. The **modulator** converts digital data into analog data when the data is being sent by the computer.The **demodulator** converts analog data signals into digital data when it is being received by the computer.







Types of Modem

- Modem can be categorized in several ways like direction in which it can transmit data, type of connection to the transmission line, transmission mode, etc.
- Depending on direction of data transmission, modem can be of these types −
- **Simplex** − A simplex modem can transfer data in only one direction, **from digital device to network (modulator) or network to digital device (demodulator)**.
- **Half duplex** − A half-duplex modem has the capacity to transfer data in both the directions but only one at a time.
- **Full duplex** − A full duplex modem can transmit data in both the directions simultaneously.

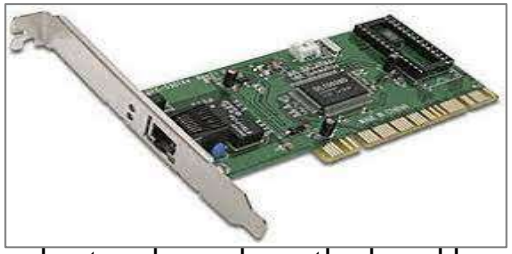
Network Devices

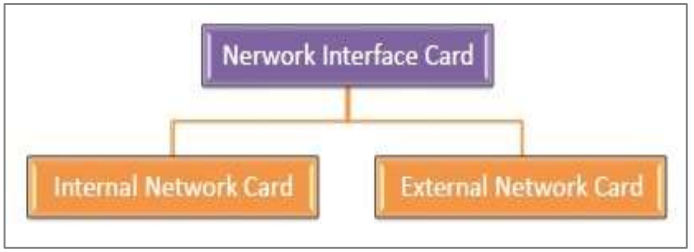
8. NIC

A network interface card (NIC) is a hardware component without which a computer cannot be connected over a network. It is a circuit board installed in a computer that provides a dedicated network connection to the computer. It is also called network interface controller, network adapter or LAN adapter.

Purpose

- NIC allows both wired and wireless communications.
- NIC allows communications between computers connected via local area network (LAN) as well as communications over large-scale network through Internet Protocol (IP).
- NIC is both a physical layer and a data link layer device, i.e. it provides the necessary hardware circuitry so that the physical layer processes and some data link layer processes can run on it.



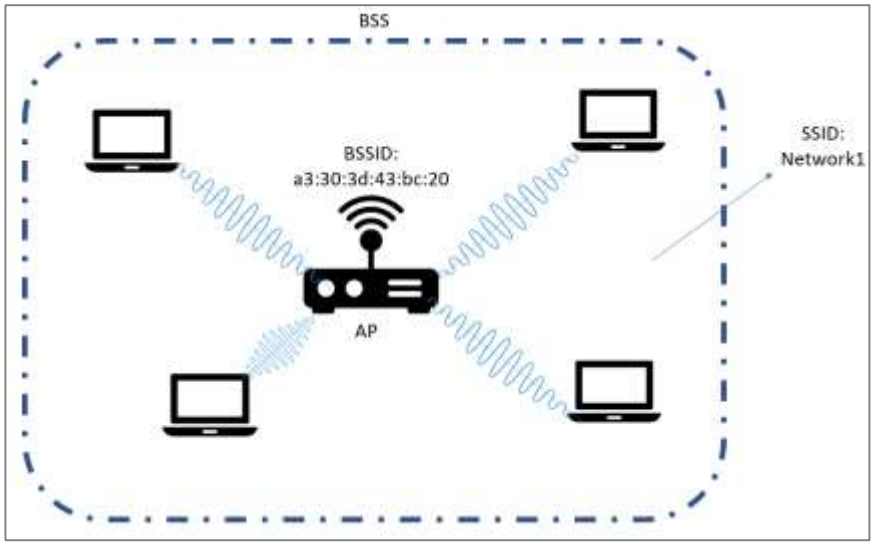


- In internal networks cards, motherboard has a slot for the network card where it can be inserted. It requires network cables to provide network access.
- In laptops that do not have an internal NIC, external NICs are used. External network cards are of two types: Wireless and USB based.

Network Devices

9. WIRELESS ACCESS POINTS

- A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.
- It is easier and simpler to understand and implant the device. It can be fixed, mobile or hybrid proliferated in the 21st century. The availability, confidentiality, and integrity of the communication and network are a responsibility and to be ensured about that.
- A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.



Advantages of Wireless Access Point (WAP):

1. More User Access
2. Broader Transmission Range

Disadvantages of Wireless Access Point (WAP):

1. High cost
2. Poor stability
3. Less Secure

Network Devices

10. FIREWALLS

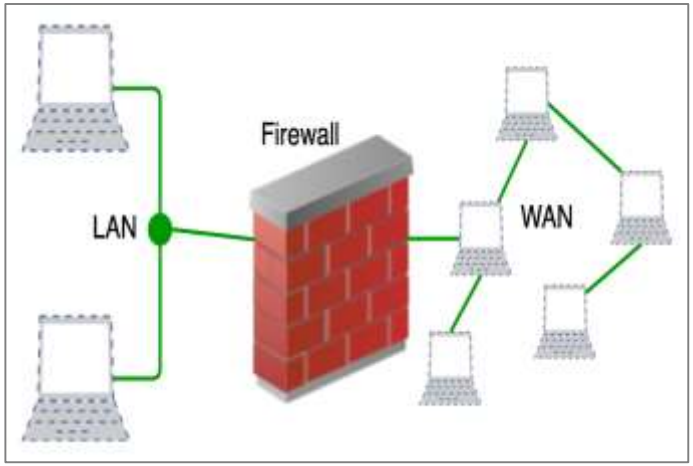
- A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules it accepts, rejects or drops that specific traffic.

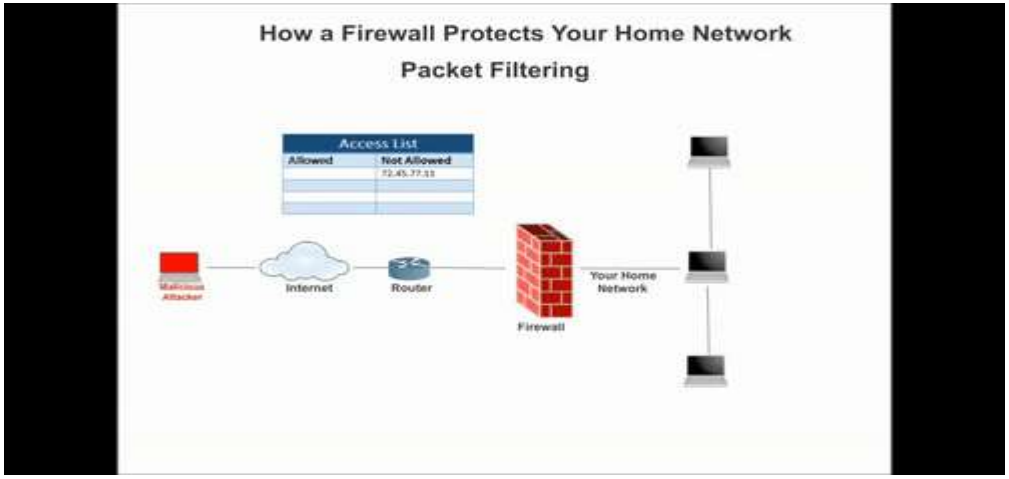
  Accept : allow the traffic

  Reject : block the traffic but reply with an "unreachable error"

  Drop : block the traffic with no reply

- A firewall establishes a barrier between secured internal networks and outside untrusted network, such as the Internet.





Network Devices

11. PROXIES

- The **proxy server** is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server.
- It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.
- In other words, we can say that the proxy server allows us to access any websites with a different IP address.
- It plays an intermediary role between users and targeted websites or servers.
- It collects and provides information related to user requests.
- The most important point about a proxy server is that it does not **encrypt traffic**.

There are two main purposes of proxy server:

- To keep the system behind it anonymous.
- To speed up access to a resource through caching.