CHAPTER5 DATA COMMUNICATION & COMPUTER NETWORK

Computer Network

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

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

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

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

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

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

1. **Performance**
2. **Reliability**
3. **Scalability**

Computer Networks: Performance

It can be measured in the following ways:

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

Other ways to measure performance are:

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

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

Properties of a Good Network

1. **Interpersonal Communication:** We can communicate with each other efficiently and easily. Example: emails, chat rooms, video conferencing etc., all of these are possible because of computer networks.
2. **Resources can be shared:** We can share physical resources by making them available on a network such as printers, scanners etc.
3. **Sharing files, data:** Authorized users are allowed to share the files on the network.

Basic Communication Model

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

Communication Model: Source

Data to be **transmitted is generate**d 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.

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.

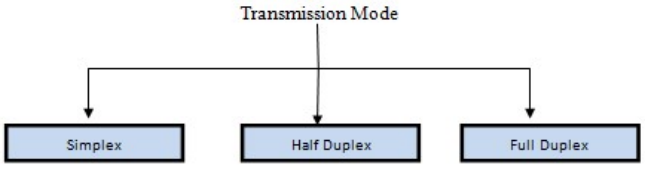
Components of Data Communication

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

Transmission Modes in Computer Networks

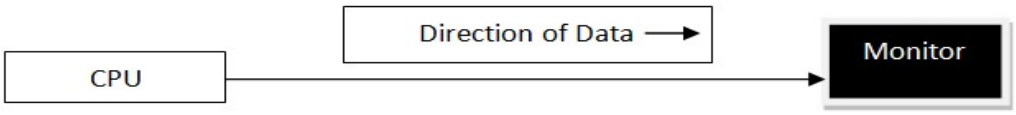
Transmission mode refers to the mechanism of transferring of data between two devices connected over a network. It is also called **Communication Mode**. These modes direct the direction of flow of information. There are three types of transmission modes. They are:

1. Simplex Mode
2. Half duplex Mode
3. Full duplex Mode



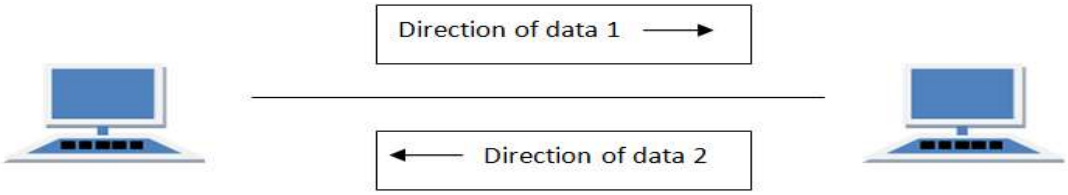
SIMPLEX Mode

In this type of transmission mode, **data can be sent only in one direction** i.e. **communication is unidirectional. We cannot send a message back to the sender.** Unidirectional communication is done in Simplex Systems where we just need to send a command/signal, and do not expect any response back.
Examples of simplex Mode are **loudspeakers, television broadcasting, television and remote, keyboard and monitor etc.**



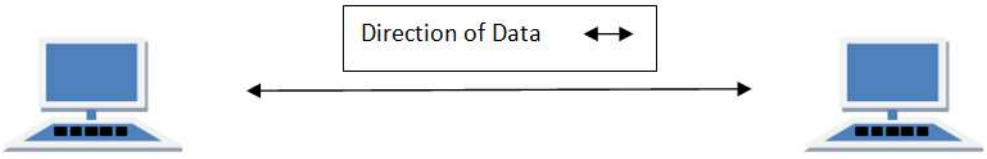
HALF DUPLEX Mode

Half-duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time.
For example, on a local area network using a technology that has half-duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. Hence half-duplex transmission implies a bidirectional line (one that can carry data in both directions) but data can be sent in only one direction at a time.
Example of half duplex is a **Walkie- talkie, Fax Machine, ATM, credit card verification system** in which message is sent one at a time but messages are sent in both the directions.

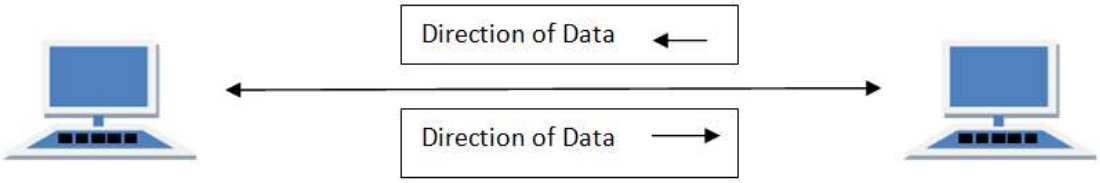


FULL DUPLEX Mode

In full duplex system we can send data in **both the directions** as it **is bidirectional at the same time in other words, data can be sent in both directions simultaneously.**
Example of Full Duplex is a **Telephone Network, satellite communication, mobile communication, etc** in which there is communication between two persons by a telephone line, using which both can talk and listen at the same time.



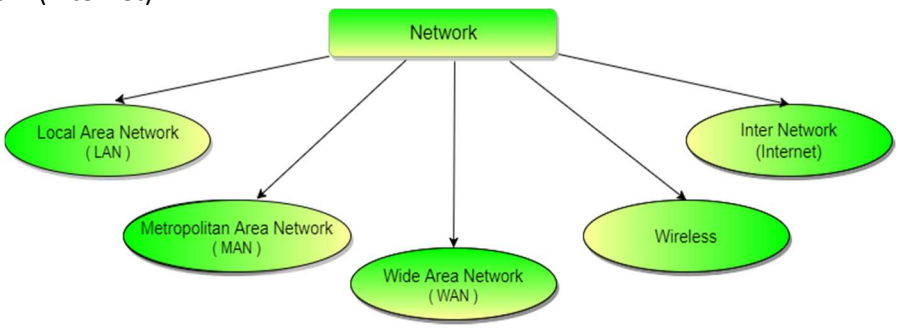
In full duplex system there can be two lines one for sending the data and the other for receiving data.



Types of Communication Networks

Communication Networks can be of following 5 types:

1. Local Area Network (LAN)
2. Metropolitan Area Network (MAN)
3. Wide Area Network (WAN)
4. Wireless
5. Inter Network (Internet)

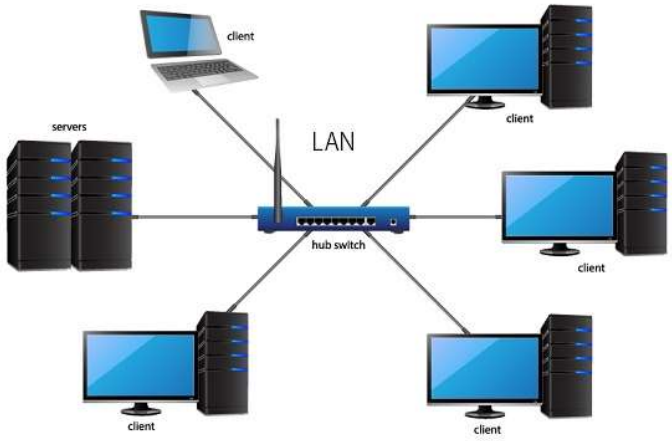


Local Area Network (LAN)

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

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

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



Characteristics of LAN

- LAN's are private networks, not subject to tariffs or other regulatory controls.
- LAN's operate at relatively high speed when compared to the typical WAN.
- There are different types of Media Access Control methods in a LAN, the prominent ones are Ethernet, Token ring.
- It connects computers in a single building, block or campus, i.e. they work in a restricted geographical area.
- No special security is needed.

Applications of LAN

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

Advantages of LAN

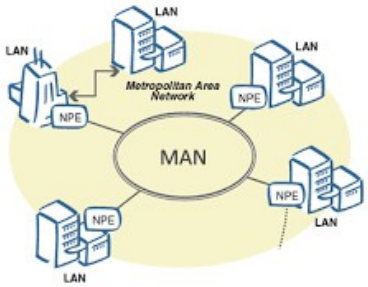
- **Resource Sharing:** Computer resources like printers, modems, DVD-ROM drives and hard disks can be shared with the help of local area networks. This reduces cost and hardware purchases.
- **Software Applications Sharing:** It is cheaper to use same software over network instead of purchasing separate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

Disadvantages of LAN

- **High Setup Cost:** Although the LAN will save cost over time due to shared computer resources, but the initial setup costs of installing Local Area Networks is high.
- **Privacy Violations:** The LAN administrator has the rights to check personal data files of each and every LAN user. Moreover he can check the internet history and computer use history of the LAN user.
- **Data Security Threat:** Unauthorized users can access important data of an organization if centralized data repository is not secured properly by the LAN administrator.
- **LAN Maintenance Job:** Local Area Network requires a LAN Administrator because, there are problems of software installations or hardware failures or cable disturbances in Local Area Network. A LAN Administrator is needed at this full time job.
- **Covers Limited Area:** Local Area Network covers a small area like one office, one building or a group of nearby buildings.

Metropolitan Area Network (MAN)

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



Characteristics of MAN

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

Advantages of MAN

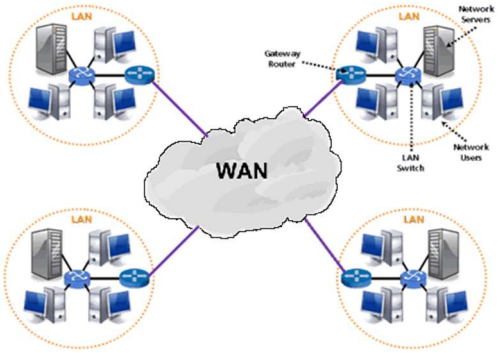
- Extremely efficient and provide fast communication via high-speed carriers, such as fibre optic cables.
- It provides a good back bone for large network and provides greater access to WANs.
- The dual bus used in MAN helps the transmission of data in both directions simultaneously.
- A MAN usually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

Disadvantages of MAN

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

Wide Area Network (WAN)

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



Characteristics of WAN

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

Advantages of WAN

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

Disadvantages of WAN

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

DIFFERENCES BETWEEN LAN AND WAN

	LAN	WAN
Stands/Definition	**LOCAL AREA NETWORK**	**WIDE AREA NETWORK**
Covers	Local Areas only (e.g. homes, offices, schools)	**Large Geographic Area (e.g. cities, states, nations, global)**
Speed	High Speed (10mbps to 1gbps)	Less Speed (150mbps)
Data Transfer rates	Much higher data transfer rates	Lower data transfer rates
Example	The Network in an office building can be a LAN.	The internet is the good example of WAN.
Technology	Ethernet and Token Ring are the connectivity technologies.	MPLS, ATM, Frame Relay and X.25 are the connectivity technologies for longer distances.
Components/Layers	LAYER1 devices like HUB, repeaters and LAYER2 devices like switch and bridges	LAYER1, LAYER2 as well as LAYER3 devices like routers, multilayer switch and ATM are used.
Setup Cost	Setup cost is less as compared to WAN.	Setup cost is more as compared to LAN.
Maintenance cost	Maintenance cost is less as compared to WAN.	Maintenance cost is more as compared to LAN.
Bandwidth	High bandwidth is available for transmission.	Low bandwidth is available for transmission.
Network Congestion	Network congestion is not more seen in LAN.	There can be more chance of network congestion in WAN.
Technical Experts	No more technical experts like Network/System admins are required.	It requires more technical experts like Network/System admins are required.

Wireless Network

Digital wireless communication is not a new idea.
Modern digital wireless systems have better performance, but the basic idea is the same.
Wireless Networks can be divided into three main categories:

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

System Interconnection

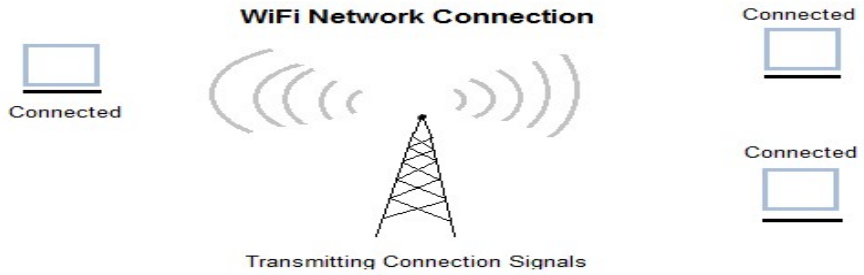
System interconnection is all about interconnecting the components of a computer using **short-range radio**. Some companies got together to design a short-range wireless network called **Bluetooth** to connect various

components such as monitor, keyboard, mouse and printer, to the main unit, without wires. Bluetooth also allows digital cameras, headsets, scanners and other devices to connect to a computer by merely being brought within range.
In simplest form, system interconnection networks use the master-slave concept. The system unit is normally the **master**, talking to the mouse, keyboard, etc. as **slaves**.

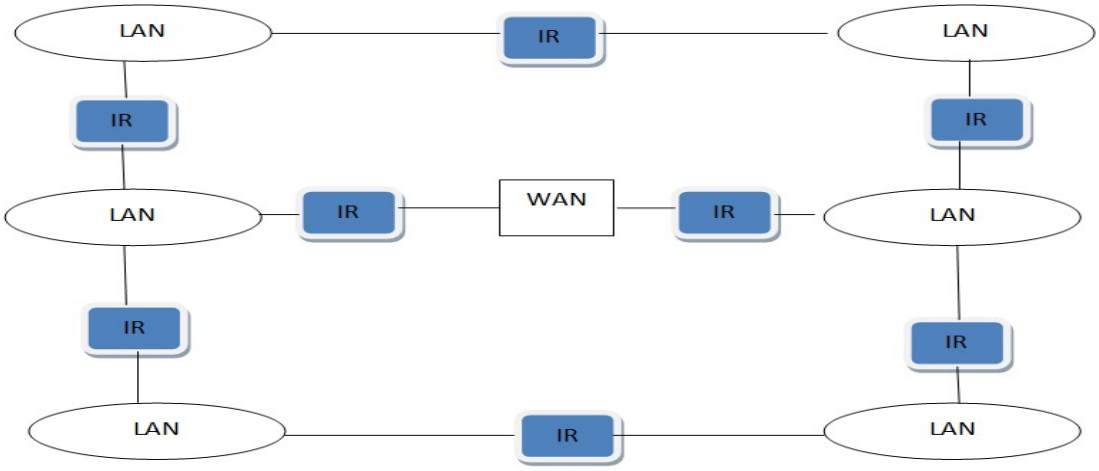
Wireless LANs
These are the systems in which every computer has a **radio modem** and **antenna** with which it can communicate with other systems. Wireless LANs are becoming increasingly common in small offices and homes, where installing **Ethernet** is considered too much trouble. There is a standard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

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

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



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



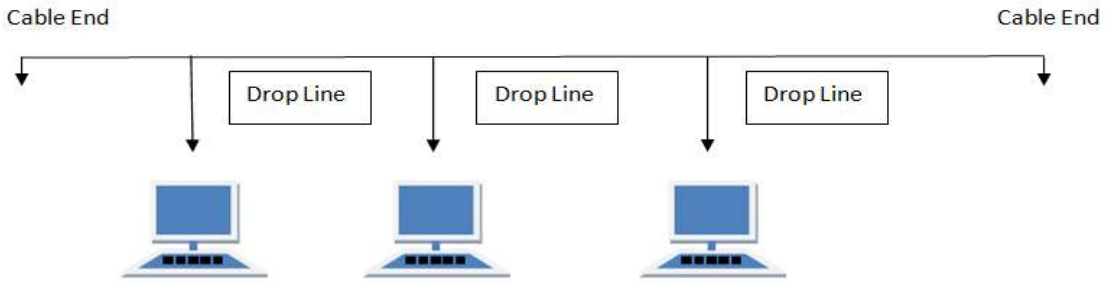
INTERNETWORK

Types of Network Topology

Network Topology is the schematic description of a **network arrangement, connecting various nodes (sender and receiver) through lines of connection.** Network topology refers to the **physical or logical layout of a network**. It defines the way **different nodes are placed and interconnected with each other**. Alternately, network topology may describe **how the data is transferred between these nodes.**

BUS Topology

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



Features of Bus Topology

1. It transmits data only in one direction.
2. Every device is connected to a single cable
3. The data signal is available to all computers connected to the bus.
4. The data signal on the bus does not get destroyed and still transmits along the bus, and is finally absorbed by the terminator to the end of the network.
5. It is good for connecting few (15-20) computers.
6. A single coaxial cable is generally used in bus topology, to which the computers or devices are connected.
7. Ethernet is a commonly used protocol in networks connected by the bus topology.

Advantages of Bus Topology

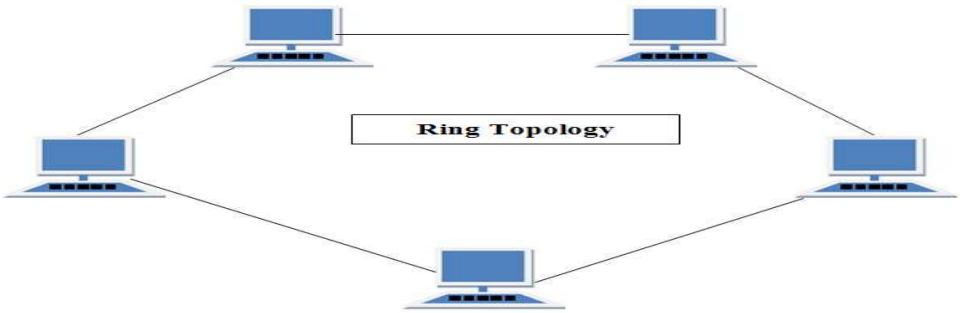
1. It is cost effective.
2. It is simple, reliable and easy to use.
3. Cable required is least compared to other network topology.
4. Used in small networks.
5. Failure of one computer does not affect other.
6. It is easy to understand.
7. Easy to expand joining two cables together.
8. Easiest network topology for connecting computers or peripherals in a linear fashion.\

Disadvantages of Bus Topology

1. If Cables fails then whole network fails.
2. If network traffic is heavy or nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.
5. Not preferable for large network.
6. Additional devices slow the network down.

RING Topology

It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbors for each device. In this type of network topology, each node is exactly connected to two other nodes, forward and backward, thus forming a single continuous path for signal transmission.



Features of Ring Topology

1. All the devices in the network are connected in the form of a ring.
2. Each device has a receiver and transmitter to receive the data signals and to send them to the next computer respectively.
3. Ring network does not have terminated ends, thus data signals travel in a circle
4. Ring topology uses token passing method to provide the access to the devices in the network.
5. The computer or devices are connected to the ring using twisted pair cables, coaxial cables or the optic fibers.
6. The protocol used to implement ring topology are Token Ring.

Advantages of Ring Topology

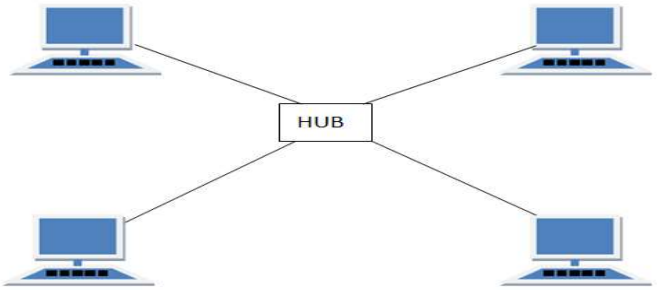
1. All data flows in one direction, reducing the chance of packet collisions.
2. A network server is not needed to control network connectivity between each workstation.
3. Data can transfer between workstations at high speeds.
4. Additional workstations can be added without impacting performance of the network.
5. Because of every computer is given equal access to the token, no one computer can monopolize the network.

Disadvantages of Ring Topology

1. Troubleshooting is difficult in ring topology.
2. Adding or deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.
4. More cabling is required than Bus Network.
5. The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and Hubs/switches.

STAR Topology

In this type of topology all the computers are connected to a **single hub through a cable**. This **hub is the central node** and all others nodes are connected to the central node. This type of topology is best suited for smaller network and works efficiently when there are a limited number of nodes.



Features of Star Topology

1. Every node has its own dedicated connection to the hub.
2. Hub acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fiber or coaxial cable.
4. All devices are connected through the central link forming a star-like structure.
5. The computers are connected to the central hub or switch using twisted pair cables, coaxial cables or optic fibers.
6. Most popular topology to connect computers and devices in network.
7. The common protocols used in star topology are Ethernet, Token Ring and Localtalk.

Advantages of Star Topology

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

Disadvantages of Star Topology

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

MESH Topology

It is a point-to-point connection to other nodes or devices. All the network nodes are connected to each other. It is the least used network topology and most expensive to implement. In mesh environment, a cable runs from every computer to every other computer.

Mesh has **[n * (n—1) / 2]** physical channels to link n devices. That is: 4 devices will have **(4*3)/2= 6 links.**

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

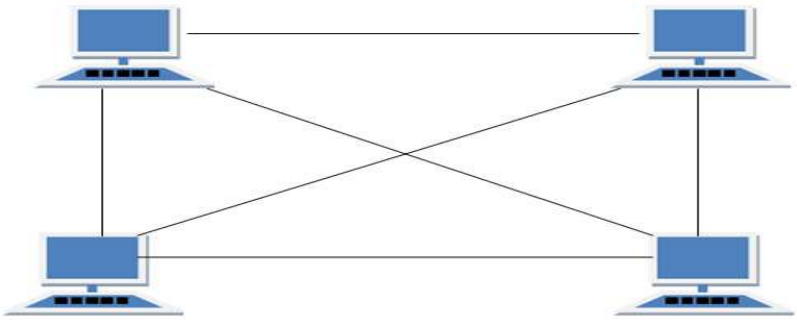
1. Routing
2. Flooding

MESH Topology: Routing

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

MESH Topology: Flooding

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



Types of Mesh Topology

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

Features of Mesh Topology

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

Advantages of Mesh Topology

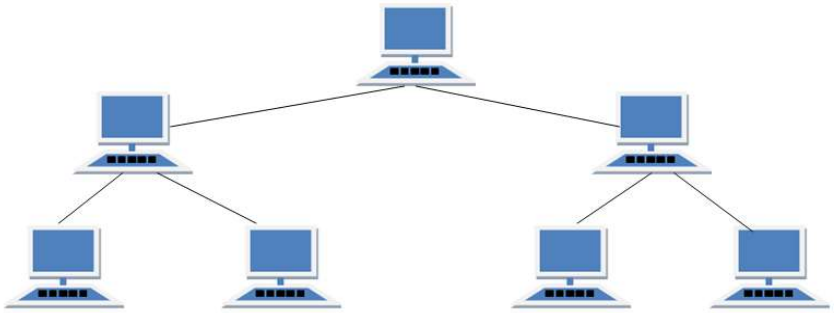
1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.
5. No traffic problem as nodes has dedicated links.
6.

Disadvantages of Mesh Topology

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.
4. Every system has its privacy and security
5. It requires more space for dedicated links.

TREE Topology

It has a **root node and all other nodes are connected to it forming a hierarchy**. It is also called **hierarchical topology.** It should at least have three levels to the hierarchy. This topology integrates various star topologies together in a single bus, so it is known as a Star Bus topology. Tree topology is a very common network which is similar to a bus and star topology.



Features of Tree Topology

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

Advantages of Tree Topology

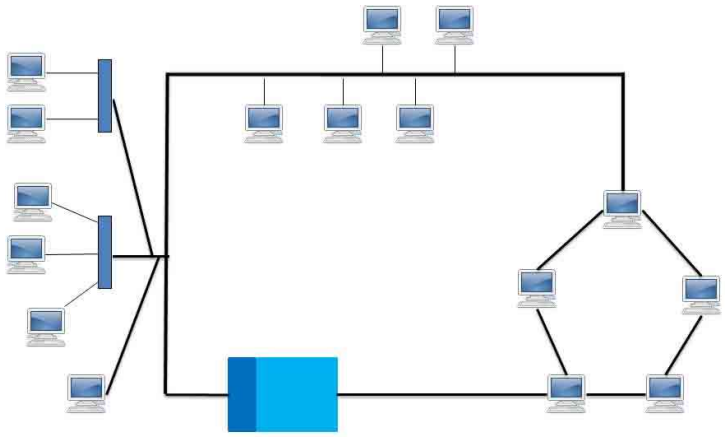
1. Extension of bus and star topologies.
2. Expansion of nodes is possible and easy.
3. Easily managed and maintained.
4. Error detection is easily done.

Disadvantages of Tree Topology

1. Heavily cabled.
2. Costly.
3. If more nodes are added maintenance is difficult.
4. Central hub fails, network fails.

HYBRID Topology

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



Features of Hybrid Topology

1. It is a combination of two or topologies
2. Inherits the advantages and disadvantages of the topologies included
3. Bigger and complex design or arrangement.

Advantages of Hybrid Topology

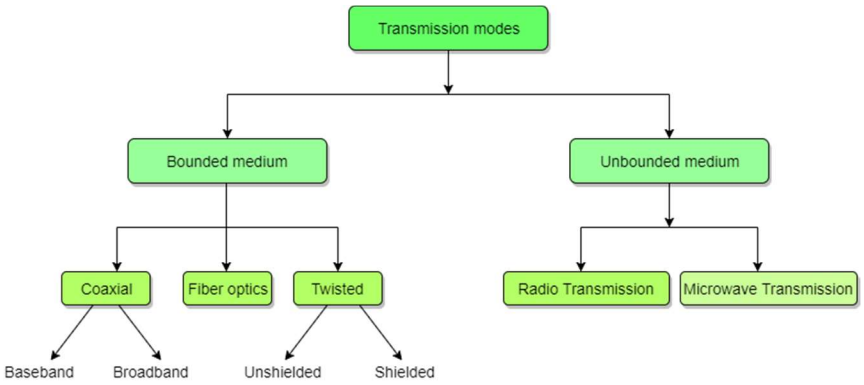
1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology

1. Complex in design.
2. Costly.
3. Sound technical team to operate.

Transmission Mediums in Computer Networks

Data is represented by computers and other telecommunication devices using **signals.** Signals are transmitted in the **form of electromagnetic energy** from one device to another. Electromagnetic signals travel through vacuum, air or other transmission mediums to move from one point to another **(from sender to receiver).**
Electromagnetic energy (includes e**lectrical and magnetic fields**) consists of **power, voice, visible light, radio waves, ultraviolet light, gamma rays etc.**
Transmission medium is the means through which we send our data from one place to another. The first layer **(physical layer) of Communication Networks** OSI Seven layer model is dedicated to the transmission media; we will study the OSI Model later.



Factors to be considered while selecting a Transmission Medium

1. **Transmission Rate**
2. **Cost and Ease of Installation**
3. **Resistance to Environmental Conditions**
4. **Distances**

Bounded or Guided Transmission Media

Guided media, which are those that provide a **conduit** from one device to another, include **Twisted-Pair Cable**, **Coaxial Cable**, and **Fiber-Optic Cable**.
A signal travelling along any of these media is **directed and contained by the physical limits of the medium.** Twisted-pair and coaxial cable use **metallic (copper)** conductors that accept and transport signals in the **form of electric current. Optical fiber** is a cable that accepts and transports signals in the **form of light.**

Twisted Pair Cable

This cable is the most **commonly used** and is **cheaper than others.** It is **lightweight, cheap, can be installed easily,** and they s**upport many different types of network**. Some important points:

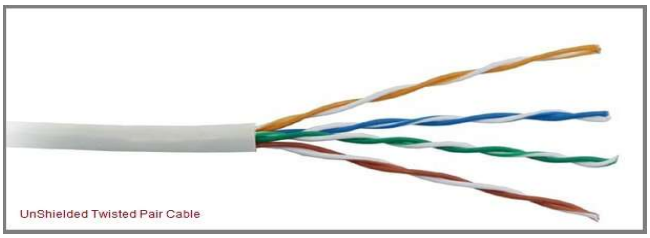
- Its frequency range is 0 to 3.5 kHz.
- Typical attenuation is 0.2 dB/Km @ 1kHz.
- Typical delay is 50 µs/km.
- Repeater spacing is 2km.

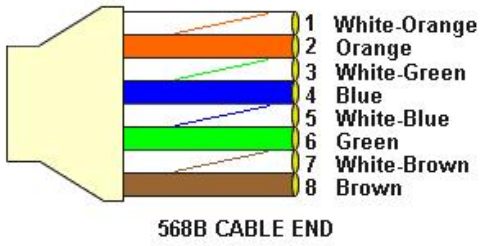
A twisted pair consists of **two conductors (normally copper), each with its own plastic insulation, twisted together.** One of these wires is used to carry **signals to the receiver**, and the other is used only **as ground reference.** The receiver uses the difference between the two. In addition to the signal sent by the sender on one of the wires, interference (noise) and crosstalk may affect both wires and create unwanted signals. **If the two wires are parallel,** the effect of these unwanted signals is not the same in both wires because they are at different locations relative to the **noise or crosstalk** sources. This results in a difference at the receiver.
Twisted Pair is of two types:

- **Unshielded Twisted Pair (UTP)**
- **Shielded Twisted Pair (STP)**

Unshielded Twisted Pair Cable

It is the most common type of telecommunication when compared with Shielded Twisted Pair Cable which consists of two conductors usually copper, each with its **own color plastic insulator.** Identification is the reason behind **colored plastic insulation.** The commonly used standard during the cabling connection **is 568b.**
UTP cables consist of 2 or 4 pairs of twisted cable. Cable with 2 pair use **RJ-11** connector and 4 pair cable use **RJ-45** connector.





Advantages of Unshielded Twisted Pair Cable

- Installation is easy
- Flexible
- Cheap
- It has high speed capacity,
- 100 meter limit
- Higher grades of UTP are used in LAN technologies like Ethernet.

It consists of two insulating copper wires (1mm thick). The wires are twisted together in a helical form to reduce electrical interference from similar pair.

Disadvantages of Unshielded Twisted Pair Cable

- Bandwidth is low when compared with Coaxial Cable
- Provides less protection from interference.

Shielded Twisted Pair Cable

This cable has a **metal foil** or braided-mesh covering which encases each pair of insulated conductors. Electromagnetic noise penetration is prevented by **metal casing.** Shielding also **eliminates crosstalk.**

It has same attenuation as unshielded twisted pair. It is **faster the unshielded and coaxial cable.** It is more expensive than coaxial and unshielded twisted pair.

Advantages of Shielded Twisted Pair Cable

- Easy to install
- Performance is adequate
- Can be used for Analog or Digital transmission

CATEGORY	SPEED	
CATEGORY 3	10 Mbps	
CATEGORY 5	100 Mbps	
CATEGORY 5e	1 Gbps	Enhanced
CATEGORY 6	1 Gbps	10 Gbps (cable length under 100 meters)
CATEGORY 6a	10 Gbps	Augmented
CATEGORY 7	10 Gbps	Added shielding to the wires.

- Increases the signaling rate
- Higher capacity than unshielded twisted pair
- Eliminates crosstalk

Disadvantages of Shielded Twisted Pair Cable

- Difficult to manufacture
- Heavy
- More Costly

Applications of Shielded Twisted Pair Cable

- In telephone lines to provide voice and data channels. The DSL lines that are used by the telephone companies to provide high-data-rate connections also use the high-bandwidth capability of unshielded twisted-pair cables.
- Local Area Network, such as 10Base-T and 100Base-T, also use twisted-pair cables.

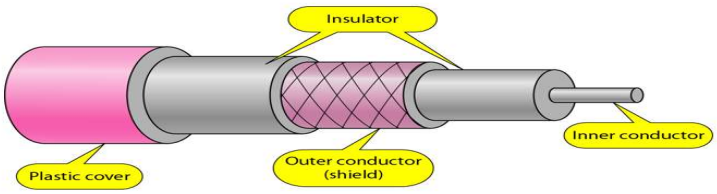
Coaxial Cable

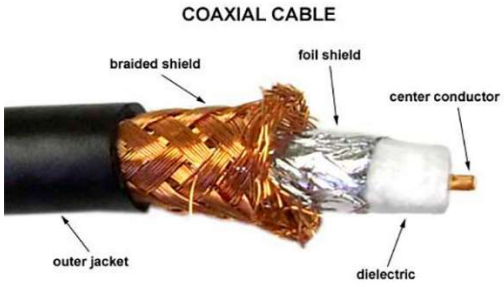
Coaxial is called by this name because it contains **two conductors that are parallel to each other.** Copper is used in this as center conductor which can be a solid wire or a standard one. It is surrounded by **PVC installation,** a sheath which is encased in an **outer conductor of metal foil, braid or both.**

Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

Here the most common coaxial standards.

- 50-Ohm RG-7 or RG-11 : used with thick Ethernet.
- 50-Ohm RG-58 : used with thin Ethernet
- 75-Ohm RG-59 : used with cable television
- 93-Ohm RG-62 : used with ARCNET.





Coaxial Cable Standards

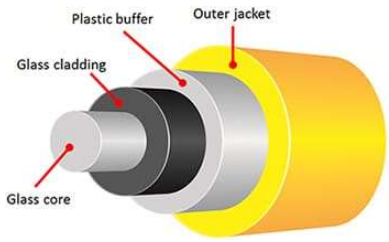
Coaxial cables are categorized by their Radio Government (RG) ratings. Each RG number denotes a unique set of physical specifications, including the wire gauge of the inner conductor, the thickness and the type of the inner insulator, the construction of the shield, and the size and type of the outer casing. Each cable defined by an RG rating is adapted for a specialized function, as shown in the table below:

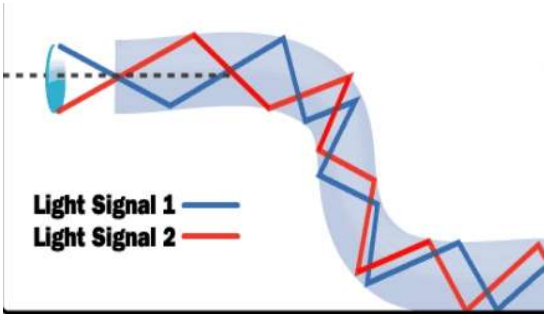
Category	*Impedance*	*Use*
RG-59	75 Ω	Cable TV
RG-58	50 Ω	Thin Ethernet
RG-11	50 Ω	Thick Ethernet

Characteristics of Coaxial Cable

- A coaxial cable has a single **inner conductor that transmits electrical signals**; the **outer conductor** acts a **ground.** The two conductor are separated by insulation. The inner conductor, insulator and the outer conductor are wrapped in a sheath of Teflon or PVC.
- The **copper wire** is used for both inner and outer conductor. The signal is transmitted over the surface of the inner conductor.
- A **thicker coaxial cable can transmit more data than a thinner one.**
- The commonly used coaxial cable is **10base2 that transmits over a 185m**, and **10base5** transmits over a distance of **500m**
- The **part around the centre** is called **dielectric**, whose main mission is to **isolate the conductor centre**. It is usually made from the composition for **plastic or foam.**

Fiber Optic Cable





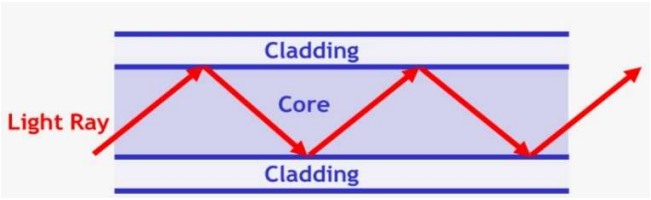


*Fig: passing light through core in fiber optic via **total internal Reflection***

A fiber-optic cable is made of **glass or plastic** and **transmits signals in the form of light**. For better understanding we first need to explore several aspects of the **nature of light**. Light travels in a straight line as long as it is mobbing through a single uniform substance. If ray of light travelling through one substance suddenly enters another substance (of a different density), **the ray changes direction.** The below figure shows how a ray of light changes direction when going from a more dense to a less dense substance.

Advantages of Fiber Optic Cable

Fiber optic has several advantages over metallic cable:

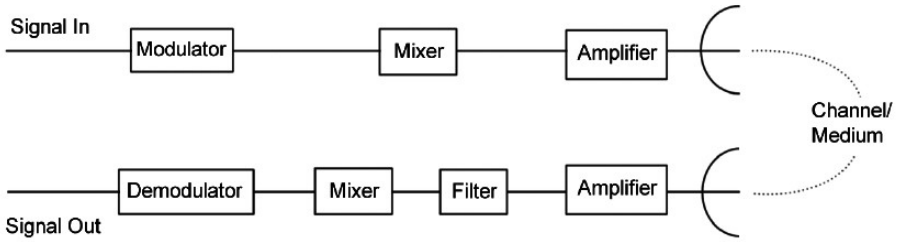
- **Higher bandwidth** is mainly possible via optical fiber.
- Optical fibers **do not cause electrical interference** in the other cables, since they use light signals.
- It carries pulse of light **much farther distance** than copper wire.
- Since **signals** in optical **fiber degrades less, so lower-power transmitters can be used** instead of the high voltage electrical transmitters needed for copper wires.
- **Less signal attenuation and interference**, they are **used for long-distance and high-demand applications.**
- **Resistance to corrosive materials.**
- **Light weight and highly portable.**
- **Greater immunity to tapping** (TAP-Terminal Access Point).

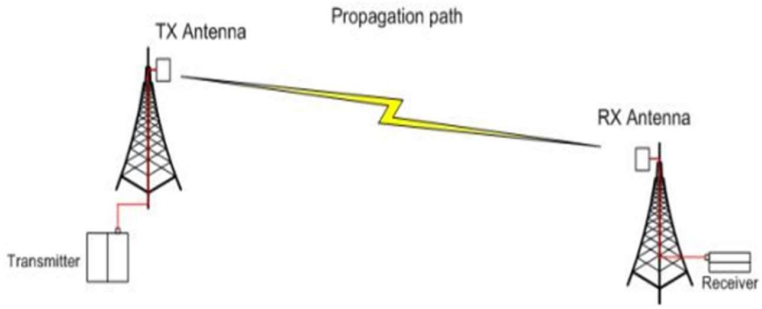
Disadvantages of Fiber Optic Cable

There are some disadvantages in the use of optical fiber:

- **Installation and maintenance requires special equipment.**
- If a fiber breaks, **finding the broken location is difficult.**
- **High Cost** for **repairing the optical fiber**. As this requires special equipment. **(splicing machine)**

Radio Transmission





The **electromagnetic radio waves that operates at the audio frequency** are also **used to transmit computer data.** This transmission is also known as Radio Frequency RF transmission. The computer using RF transmission **do not require a direct physical connection like wires and cables**. Each computers attaches to an antenna that can both send and receive radio transmission. **Radio technology**, transmission and detection of communication signals consisting of **electromagnetic waves that travel through the air in a straight line or by reflection from the ionosphere.** They are widely used for communications **since they are easy to generate, can travel long distances and can penetrate buildings.** Radio waves have **omnidirectional antennas**, i.e. antennas that can send signals in **all directions.**

High Frequency Radio Waves

High frequency radio waves travel in straight lines and have sky propagation. However, they are affected by interferences and are affected by rains. The military communicates in the HF and VHF bands. They are also used for long distance broadcasting and FM radio.

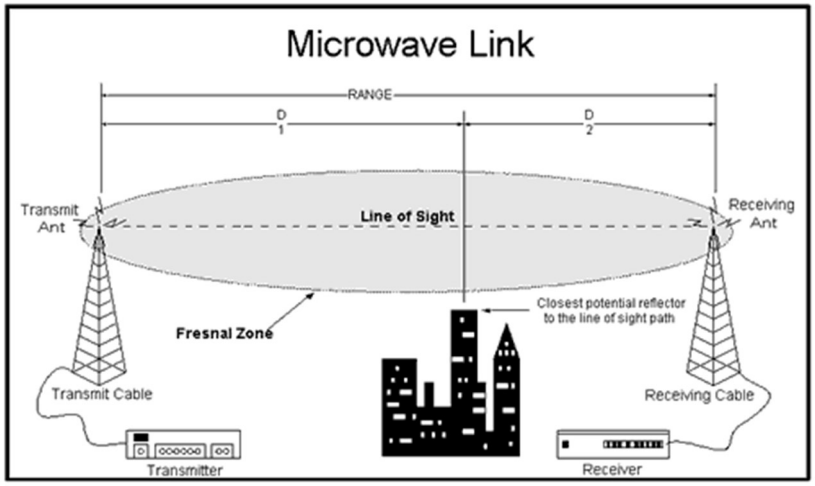
Applications

Some of the areas of applications of radio waves are −

- Broadcasting and multicasting
- Fixed and mobile radio communications
- AM and FM radio
- Television

- Marine communication
- Wireless computer networks
- Cordless phones

Microwave Transmission



Microwave is a **line-of-sight** wireless communication technology that uses **high frequency beams of radio waves** to provide **high speed wireless connections** that can **send and receive voice, video, and data information. Microwave links** are widely used for point-to-point communications because their **small wavelength** allows conveniently-sized antennas to direct them in narrow beams, which can be pointed directly at the receiving antenna.

Features of Microwaves

- Microwaves travel in **straight lines,** and so the transmitter and receiver stations should be **accurately aligned to each other.**
- Microwave propagation is **line – of – sight propagation**. So, towers hoisting the stations should be placed so that the curvature of the earth or any **other obstacle does not interfere with the communication.**
- Since it is **unidirectional,** it allows multiple receivers in a row to receive the signals without interference.
- Microwaves do **not pass through buildings.** So, **indoor receivers cannot be used effectively**.
- Microwaves are often **refracted by the atmospheric layers**. The refracted rays take longer time to reach the destination than the direct rays. This causes out of phase transmission, called **multipath fading.**
- Microwaves need **unidirectional antennas** to send out signals. Two types of antennas are needed
    - **Parabolic Dish Antenna** − It is used by the receiving station. It is parabolic in shape, which concentrates all energy to a **small beam** thus achieving a **strong signal with high SNR.**
    - **Horn Antenna** − It has a stem with a curved head. In sending stations, outgoing waves from the stem are broadcast by the curved head as a **series of parallel beams**. In the receiving station, the rays are collected by the curved head and deflected in the stem.

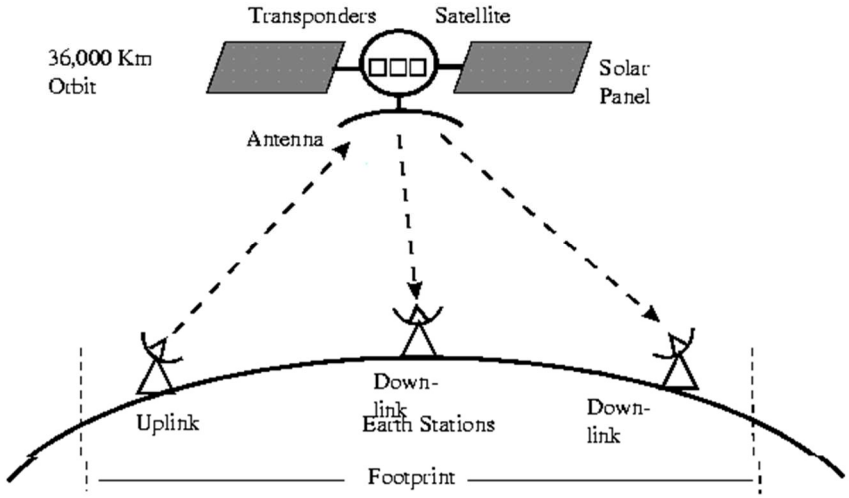
Applications

- Long distance telephone communication
- Cellular phones
- Television networks
- Satellites
- Wireless LANs

Disadvantages:

- Needing expensive towers and repeaters
- Subject to interference from passing airplanes and rain. Because microwave system are line of sight media, radio towers must be spaced approximately every 42km along the route.
- Dedicated network admin is required.
- Security must be concerned while sending the signal. I.e. it must be encrypted.

Satellite Transmission or Communication



Satellite communication is also a kind of **line of sight communication.** The communication across the **longer distances** can be provided by combining radio frequency transmission with satellites. Satellites are set in the **geostationary orbits directly over the equator**, which **rotates synchronous to earth** and hence look stationary from any point on the earth. The geostationary orbits are placed **36000km above the earth surface**. The communication is carried through uplinks and downlinks. The **uplink transfers** the date to the satellite and **downlink receives** the data from the satellite. Uplinks and Downlinks are **also called earth stations** because they are locked on the earth. The area shadowed by the satellite in which the information and data can be transmitted and received is called the **footprint.**

Microwaves and radio waves are used to communicate with satellites.

Satellite Communication – Advantages

There are many Advantages of satellite communications such as −

- Flexibility
- Ease in installing new circuits
- Distances are easily covered and cost doesn't matter

- Broadcasting possibilities
- Each and every corner of earth is covered
- User can control the network

Satellite Communication – Disadvantages

Satellite communication has the following drawbacks –

- The initial costs such as segment and launch costs are too high.
- Congestion of frequencies
- Interference and propagation

Satellite Communication – Applications

Satellite communication finds its applications in the following areas −

- In Radio broadcasting.
- In TV broadcasting such as DTH. **(Direct to Home)**
- In Internet applications such as providing Internet connection for data transfer, GPS applications, Internet surfing, etc.
- For voice communications.
- For research and development sector, in many areas.
- In military applications and navigations.

Reference Models in Communication Networks

The most important reference models are:

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

Introduction to ISO-OSI Model

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

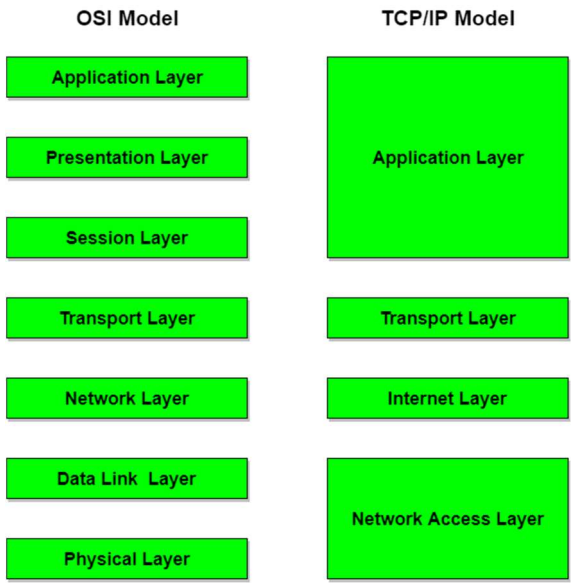
Introduction to TCP/IP Reference Model

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

Internet Protocols are the rules set established for network communication. TCP/IP is considered a robust networking protocol model. It is the condensed version of the OSI Model.

1. **Network Access Layer:** Network Access Layer is the combination of Data Link Layer and Physical Layer available in the OSI model. Physical Addressing is done in this layer i.e. MAC Address of source and destination is assigned to the data packets. Hence this layer is responsible for the physical transmission of data.
2. **Internet Layer:** The Internet layer is used to send an independent packet to a network to the destination. All the machines, Web servers, nodes that are attached to the TCP/IP network are assigned in this layer.
3. **Transport layer**: It allows the information to be delivered in information chart format from the source to the destination host without defects.
4. **Application Layer:** Application layer performs the tasks of the OSI model in three layers: Application, Presentation and Session Layer. It is required for the interaction between node and node and handles the requirements of the user interface. Protocols available in the Application Layer are TFTP, HTTP, Telnet, SSH, NTP, DNS, NFS, FTP, SNMP, DHCP, SMTP.

Both, OSI vs TCP/IP are the most popular and widely used communication networking protocols. The main difference between them is that OSI is a **conceptual model that is not practically used for communication**. It defines how the data is transferred in a network or different architectures. Whereas TCP/IP is widely used for link establishment and network interaction. The TCP/IP also allows the connection mode on the network layer only, but these two methods are on the transport layer. **With the OSI model, it promotes connection-free and connection-oriented network communication, but connection-oriented communication is only permitted in the transport layer.**



The OSI Model - Features, Principles and Layers

There are n numbers of users who use computer network and are located over the world. So to ensure, national and worldwide data communication, systems must be developed which are compatible to communicate with each other ISO has developed a standard. ISO stands for **International organization of Standardization**. This is called a model for **Open System Interconnection** (OSI) and is commonly known as OSI model.
The ISO-OSI model is a seven layer architecture. It defines seven layers or levels in a complete communication system. They are:

1. **Application Layer**
2. **Presentation Layer**
3. **Session Layer**
4. **Transport Layer**
5. **Network Layer**
6. **Datalink Layer**
7. **Physical Layer**

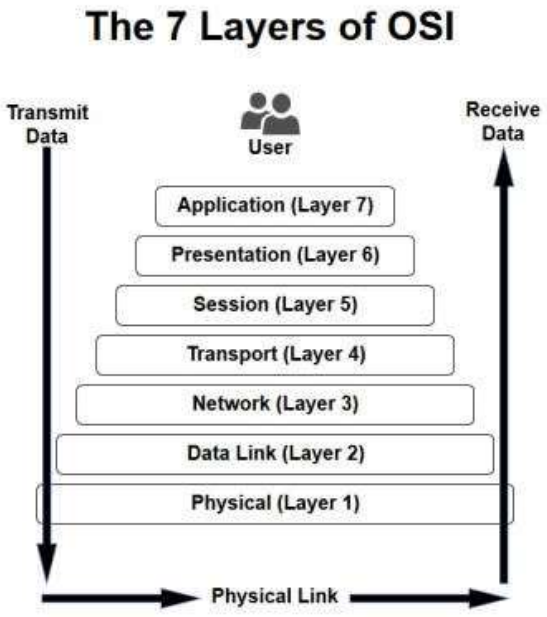
Below we have the complete representation of the OSI model, showcasing all the layers and how they communicate with each other.

In the table below, we have specified the **protocols** used and the **data unit** exchanged by each layer of the OSI Model.

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

Feature of OSI Model

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



Application (Layer 7)

OSI Model, Layer 7, supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer **provides application services for file transfers, e-mail, and other network software services**. **Telnet and FTP** are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

- *Layer 7 Application examples include **WWW browsers, NFS, SNMP, Telnet, HTTP, FTP***

Presentation (Layer 6)

This layer provides independence from differences in **data representation (e.g., encryption) by translating from application to network format, and vice versa.** The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.

- *Layer 6 Presentation **examples include encryption, ASCII, EBCDIC, TIFF, GIF, PICT, JPEG, MPEG, MIDI.***

Session (Layer 5)

This layer **establishes, manages and terminates connections between applications**. The session layer **sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications** at each end. It deals with session and connection coordination.

- *Layer 5 Session examples include **NFS, NetBios names, RPC, SQL.***

Transport (Layer 4)

OSI Model, Layer 4, provides t**ransparent transfer of data between end systems, or hosts**, and is responsible for **end-to-end error recovery and flow control**. It **ensures complete data transfer**.

- *Layer 4 Transport examples include **SPX, TCP, UDP.***

Network (Layer 3)

Layer 3 provides **switching and routing technologies, creating logical paths,** known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as **addressing, internetworking, error handling, congestion control and packet sequencing.**

- *Layer 3 Network examples include **AppleTalk DDP, IP, IPX.***

Data Link (Layer 2)

At OSI Model, Layer 2, **data packets are encoded and decoded into bits**. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, **flow control and frame synchronization.** The data link layer is divided into two sub layers: **The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer.** The **MAC sub layer** controls **how a computer on the network gains access to**

the data and permission to transmit it. The **LLC layer** controls **frame synchronization, flow control and error checking.**

- *Layer 2 Data Link examples include **PPP, FDDI, ATM, IEEE 802.5/ 802.2, IEEE 802.3/802.2, HDLC, Frame Relay.***

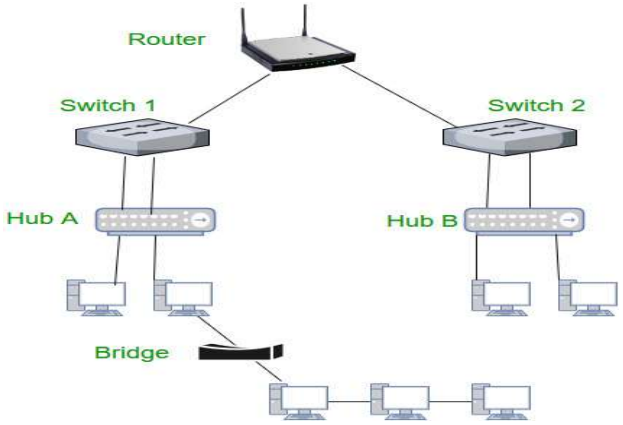
Physical (Layer 1)

OSI Model, Layer 1 conveys the **bit stream - electrical impulse, light or radio signal** — through the network at the electrical and mechanical level. It provides the **hardware means of sending and receiving data on a carrier,** including **defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM** are protocols with physical layer components.

OSI MODEL	TCP/IP MODEL
It is reference model	It is the implementation of OSI model
It is just the theoretical model.	It is the model around which the internet is developed.
It has 7 layers	It has 4 layers.
It is considered as reference tool	It is considered more reliable.
Functionalities described in each layer are perfectly optimized	Functionalities described in each layer are not perfectly optimized.
It is developed by ISO (International Standard Organization)	It is developed by DoD (Department of Defence)
It is never used, just theoretical model.	It is widely used model
It obeys vertical approach.	It obeys horizontal approach.
In OSI model the transport layer guarantees the delivery of packets.	In TCP/IP model the transport layer does not guarantees delivery of packets. Still the TCP/IP model is more reliable.
Network Layer is both Connection Oriented and Connection less.	Network Layer is Connection less.

Network Connecting Devices (Hub, Repeater, Bridge, Switch, Router and Gateways)

Mostly the network devices are connected to each other for the purpose of sharing data or resources from a network.



1. Repeater – A repeater operates at the **physical layer**. Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network. An important point to be noted about repeaters is that **they do not amplify the signal.** When the signal becomes weak, **they copy the signal bit by bit and regenerate it at the original strength**. It is a 2 port device.

2. Hub – A hub is basically a **multiport 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.** In other words, collision domain of all hosts connected through Hub remains one. Also, they do not **have intelligence to find out best path for data packets** which leads to inefficiencies and wastage.

Types of Hub

- **Active Hub: -** These are the hubs which have **their own power supply and can clean , boost and relay the signal along the network**. It serves both as a repeater as well as wiring center. These are used to **extend maximum distance between nodes.** It **amplifies the signal.**
- **Passive Hub: -** These are the hubs which collect wiring from nodes and power supply from active hub. These hubs relay **signals onto the network without cleaning and boosting them** and **can't be used to extend distance between nodes.** It **doesn't amplify the signal.**

3. Bridge – A bridge operates at **data link layer**. **A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.** It is also used for interconnecting **two LANs working on the same protocol.** It has a **single input and single output port**, thus making it **a 2 port device. The** major difference between bridge and repeater is that **bridge has a filtering capacity.**

Types of Bridges

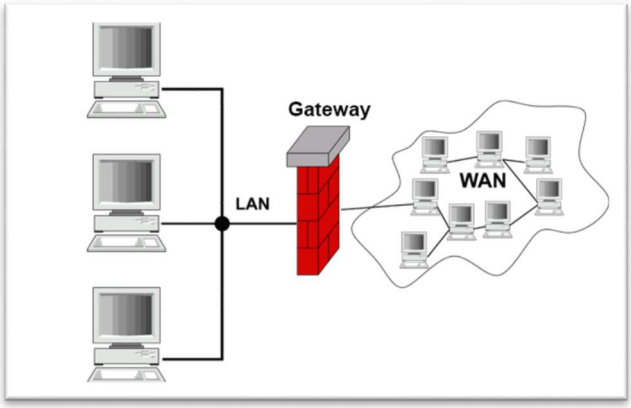
- **Transparent Bridges: -** These are the bridge in which the stations are **completely unaware of the bridge's existence i.e. whether or not a bridge is added or deleted from the network**, reconfiguration of the stations is unnecessary. These bridges makes use of **two processes i.e. bridge forwarding and bridge learning.**

- **Source Routing Bridges: -** In these bridges, **routing operation is performed by source station and the frame specifies which route to follow.** The hot can discover frame by sending a special frame called discovery frame, which spreads through the entire network using all possible paths to destination.

4. Switch – A switch is a **multi-port bridge with a buffer and a design that can boost its efficiency** (large number of ports imply less traffic) and performance. Switch is **data link layer device**. Switch can **perform error checking before forwarding data** that makes it very efficient as it **does not forward packets that have errors** and forward good packets selectively to correct port only. In other words, **switch divides collision domain of hosts, but broadcast domain remains same.**

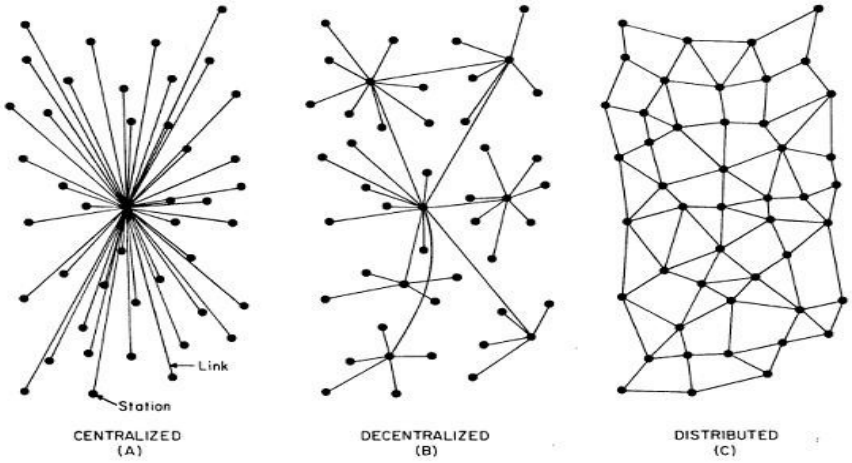
5. Routers – A router is a device like a switch that routes **data packets based on their IP addresses**. Router is mainly a **Network Layer device**. Routers normally **connect LANs and WANs together** and have a dynamically updating **routing table based** on which they **make decisions on routing the data packets.** Router divide **broadcast domains of hosts connected through it.**

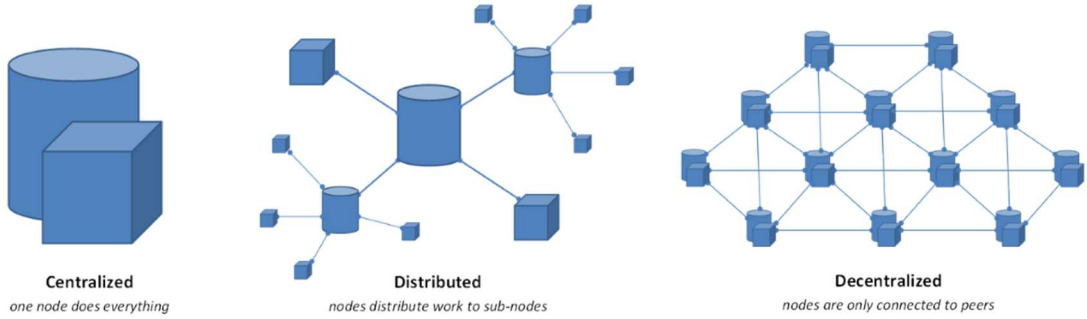
6. **Gateway** – A gateway, as the name suggests, is a **passage to connect two networks together** that may work upon different **networking models or protocols**. They basically works as the **messenger agents** that take data from **one system, interpret it, and transfer it to another system.** Gateways are also **called protocol converters and can operate at any network layer.** Gateways are generally **more complex than switch or router.** For e.g. **Firewall, UTM(Unified Treat Management)**



Centralized vs Decentralized vs Distributed Networks

A network is a collection of devices or systems that are connected to each other that allows them to share resources between them.





There are broadly three different kinds of network as highlighted in the diagram:

- **Centralized Network**: In case of a centralized network, we have a central network owner. The central network owner is a single point of contact for information sharing. The biggest issue with a centralized network is with a single central owner it also becomes a single point of failure. Further, with a single copy stored with the owner, every instance of access to the resource leads to an access issue with time.

- **Decentralized Network**: As for the decentralized network, we have multiple central owners that have the copy of the resources. This eliminates the biggest problem of single point of failure with centralized network. With multiple owners, if a particular central node fails, the information can still be accessed from the other nodes. Further, with multiple owners the speed of access to the information is also reduced.

- **Distributed Network:** The distributed network is the decentralized network taken to the extreme. It avoids the centralization completely. The main idea for the distributed network lies in the concept that everyone gets access, and everyone gets equal access. A distributed system is a network that consists of autonomous computers that are connected using a distribution middleware. They help in sharing different resources and capabilities to provide users with a single and integrated coherent network.

KEY DIFFERENCES BETWEEN THESE NETWORK TYPES

- **Points of Failure / Maintenance**: Centralized systems are easy to maintain as there is only a single point of failure. Decentralized have more but still finite. Distributed systems are the most difficult to maintain.
- **Fault Tolerance / Stability**: Centralized can be highly unstable. Decentralized systems are moderately stable. Distributed systems are very stable and a single failure doesn't do much harm.
- **Scalability / Max Population**: Centralized — low scalability, Decentralized — Moderate, Distributed — Infinite.
- **Ease of development / Creation**: Centralized systems can be created really fast, you pick up a framework and apply it everywhere. For Decentralized and Distributed, you have to first work out the lower level details like resource sharing (trade) and communications (transport).
- **Evolution / Diversity**: Since centralized systems follow a single framework, they don't have diversity and evolve slowly. But for Decentralized and Distributed systems, once the basic infrastructure is in place, evolution is tremendous.

Network Protocol: Simply, a protocol is a set of rules. A network protocol is a set of rules followed by the network. Network protocols are formal standards and policies made up of rules, procedures and formats that defines communication between two or more devices over a network. Network protocols conducts the action, policies, and affairs of the end-to-end process of timely, secured and managed data or network communication. They define rules and conventions for communication. They incorporate all the processes requirement and constraints of initiating and accomplishing communication between computers, routers, servers and other network enabled devices. Network protocols must be confirmed and installed by the sender and receiver to ensure network\data communication. It also applies software and hardware nodes that communicate on a network. There are several types of network protocols.

There are many properties of a transmission that a protocol can define. Common ones include: packet size, transmission speed, error correction types, handshaking and synchronization techniques, address mapping, acknowledgement processes, flow control, packet sequence controls, routing, address formatting

Popular protocols include: **File Transfer Protocol (FTP), TCP/IP, User Datagram Protocol (UDP), Hypertext Transfer Protocol (HTTP), Post Office Protocol (POP3), Internet Message Access Protocol (IMAP), Simple Mail Transfer Protocol (SMTP).**

SMTP - 25

SMTP is known as the **Simple Mail Transfer Protocol.** It is associated with the **TCP port number 25.** The primary purpose of this protocol is to make sure that email messages are communicated over the network securely. This port usually comes into being during the Application layer. Not only does this protocol carry out the task of delivering messages within networks, i can also successfully deliver messages between different networks. This makes it one of the most important ports for the communication of messages over the network due to the security and it provides along with other features. However, you do not have the privilege to download the emails in order to read them; it is just intended for the purpose of transferring them over the network.

HTTP - 80

Port 80 is associated with HTTP, **Hypertext Transfer Protocol**. It comes under the category of a **TCP protocol.** It is one of the most famous and widely used ports in the world. The main purpose of port 80 is to allow the browser to connect to the web pages on the internet. Port 80 basically expects or waits for the web client to ask for a

connection. Once this connection has been made, you will get the privilege to connect to the World Wide Web and get access to various web pages out there. In fact, HTTP - 80 is one of the most important ports associated with the TCP protocol. Moreover, this port is generally used during the application layer of the TCP/IP Model.

HTTPS - 443

HTTPS - 443 is also associated with the **TCP protocol. HTTPS port 443** also lets you connect to the internet by establishing a connection between the webpages and the browser. This lets you connect to the World Wide Web. However, this port has an added feature of security to it, which HTTP port 80 does not have. This port is intended for establishing secure connections to make sure that the data is transmitted over a secure network. The use receives a warning if the browser is trying to access a webpage which is not secure. This port comes into being during the application layer. It basically encrypts and authenticates the network packets before transferring them over the network to increase the security. This feature of security is introduced by the use of SSL, which can also be referred to as Secure Socket Layer.

FTP - 20, 21

FTP is the abbreviation of **"File Transfer Protocol".** The purpose of FTP is to transfer files over the internet. It basically lays down all the rules which are to be followed during the transfer of data. Due to the concern of security, it also asks for authentication by the user before the transfer of data. It is associated with the **TCP protocol** and corresponds to two ports, port 20 and 21. Both of these ports function during the application layer.

Port 20 performs the task of forwarding and transferring of data. It takes over the task of transferring FTP data when it is in active mode. **Port** 21 performs the task of signaling for FTP. It listens to all of the commands and provides a flow control for data. It is quite essential for maintaining the flow of data.

TELNET 23

TELNET port 23 comes under the category of TCP Protocols. Its main function is to establish a connection between a server and a remote computer. It establishes a connection once the authentication method has been approved. However, this port is not suitable to establish secure connections and does not cater to the concern of security. It enables the remote connection of a computer to be established with routers and switches as well. It makes use of a virtual terminal protocol to make a connection with the server. It comes into existence during the application layer of the TCP/IP protocol.

IMAP 143

IMAP is the abbreviation of **Internet Message Access Protocol.** The **IMAP -143 Port lies** under the category of **TCP** protocol. The primary purpose of this port is to retrieve emails from a remote server without having the need to download the email. You have the liberty to access the emails from anywhere by connecting to the server and viewing your email after providing authentication. This opportunity has been provided to you because of the existence of this port. It reserves a virtual memory for the email which enables you to read it by connecting to the

server. However, you may also download the mail if you wish to. It also provides you the ability to search for your messages from a bunch of them to get to your desired one. IMAP 143 Port generally operates at the Application Layer of a TCP/IP Model. In addition to this, it also makes sure that the data remain secure during this connection.

RDP 3389

RDP is also known as the **Remote Desktop Protocol.** It operates on the **port 3389 of the TCP protocol**. This port has been developed by Microsoft. It enables you to establish a connection with a remote computer. With the help of this connection, you get the liberty to control the desktop of this remote computer. This will provide you the ease to access you home desktop system from anywhere in the world just by proper authentication. In order to connect to your remote computer, you will have to forward the connection to the TCP Port 3389 which will then make available to you all the files which you have kept on your remote computer. However, since this port have been developed by Microsoft, it is essential to have a Windows operating system running on your computer in order to access it remotely. Please keep in mind that you might have to do manual settings in order to remotely access your desktop using this port. It operates on the Application layer of the TCP/IP Model. It is used worldwide for the purpose of accessing your desktop remotely.

SSH 22

SSH is also referred to as Secure Shell. It operates on the port number **22 of the TCP protocol**. It carries out the task of remotely connecting to a remote server or host. It allows you to execute a number of commands and move your files remotely as well. However, it is one of the most secure ways of accessing your files remotely. Using this port, you can remotely connect to a computer and move your files with ease. This port sends the data over the network in an encrypted form which adds an extra layer of security on it. In addition to this, only authorized people will be able to remotely log on to their systems using the Port 22 which makes sure that the information does not get into unauthorized hands. It provides the chance to move files within networks as well as gives the privilege to move files between different networks securely. It operates at the Application Layer of the TCP/IP Model and is considered as one of the most secure and reliable ports for accessing files remotely.

DNS 53

DNS is referred to as **Domain Name System.** It operates on the **port 53 of TCP and UDP protocols**. DNS makes use of relational databases to link the host names of the computers or networks to their respective IP Addresses. The port 53 waits for requests from DHCP to transfer the data over the network. It operates on the Application Layer of the TCP/IP Model.
TCP protocol is used by the Zone Transfer function of the DNS server. Once the connection is established, the zone data will be sent by the server using the TCP 53 port. However, when the query has to be transferred from the client computer, it will be sent using the port 53 on UDP protocol. However, if no response is received from the server within 5 seconds, the DNS query will be sent using the port 53 of TCP Protocol.

DHCP 67, 68

DHCP is also known as **Dynamic Host Configuration Protocol.** It basically runs on the **UDP protocol**. The basic purpose of DHCP is to assign IP Address related information to the clients on a network automatically. This information may comprise of subnet mask, IP Address etc. Many of the devices are automatically configured to

look for IP Addresses using DHCP when they connect on a network. It makes it quite reliable to assign all the devices on a network with automatically produced IP Addresses. It generally operates on the Application layer of the TCP/IP Model. DHCP basically makes use of 2 ports; Port 67 and Port 68.
UDP **Port 67** performs the task of accepting address requests from DHCP and sending the data to the server. On the other hand, UDP **Port 68** performs the task of responding to all the requests of DHCP and forwarding data to the client.

POP3-110

POP3 is also referred to as **Post Office Protocol Version 3**. It operates on the **port 110 of TCP Protocol**. It allows the email messages to be retrieved from the SMTP servers. Using this port, you can download the messages from the server and then read them. However, this means that you will not be able to access the messages and read them without downloading them. Furthermore, the messages are also deleted from the server once they are downloaded. However, this port does not cater to the issue of security. The authentication details transferred over the network are not encrypted and sent in plain text. This means that any hacker can easily intercept this information and misuse it. Port 110 generally operates on the Application layer of the TCP/IP Model.