INTRODUCTION

The term ***telecommunication,*** means communication at a distance which includes telephony, telegraphy, and television.

The word ***data*** refers to information presented in whatever form is agreed upon by the parties creating and using the data.

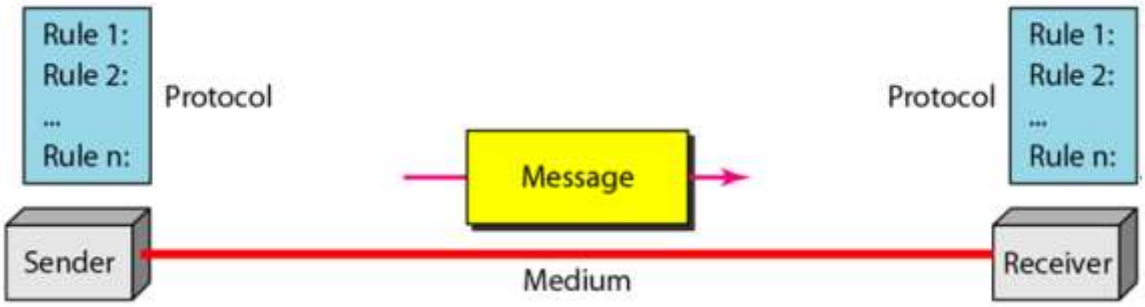
Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

The effectiveness of a data communications system depends on four fundamental characteristics: delivery, accuracy, timeliness and jitter.

1. ***Delivery***: The system must deliver data to the correct destination. Data must be received by the intended device or user and only by that device or user.
2. ***Accuracy***: The system must deliver the data accurately. Data that have been altered in transmission and left uncorrected are unusable.
3. ***Timeliness***: The system must deliver data in a timely manner. Data delivered late are useless. In the case of video and audio, timely delivery means delivering data as they are produced, in the same order that they are produced, and without significant delay. This kind of delivery is called real-time transmission.
4. ***Jitter***: refers to the variation in the packet arrival time. It is the uneven delay in the delivery of audio or video packets. For example, let us assume that video packets are sent every 3D-ms. If some of the packets arrive with 3Dms delay and others with 4D-ms delay, an uneven quality in the video is the result.

Components

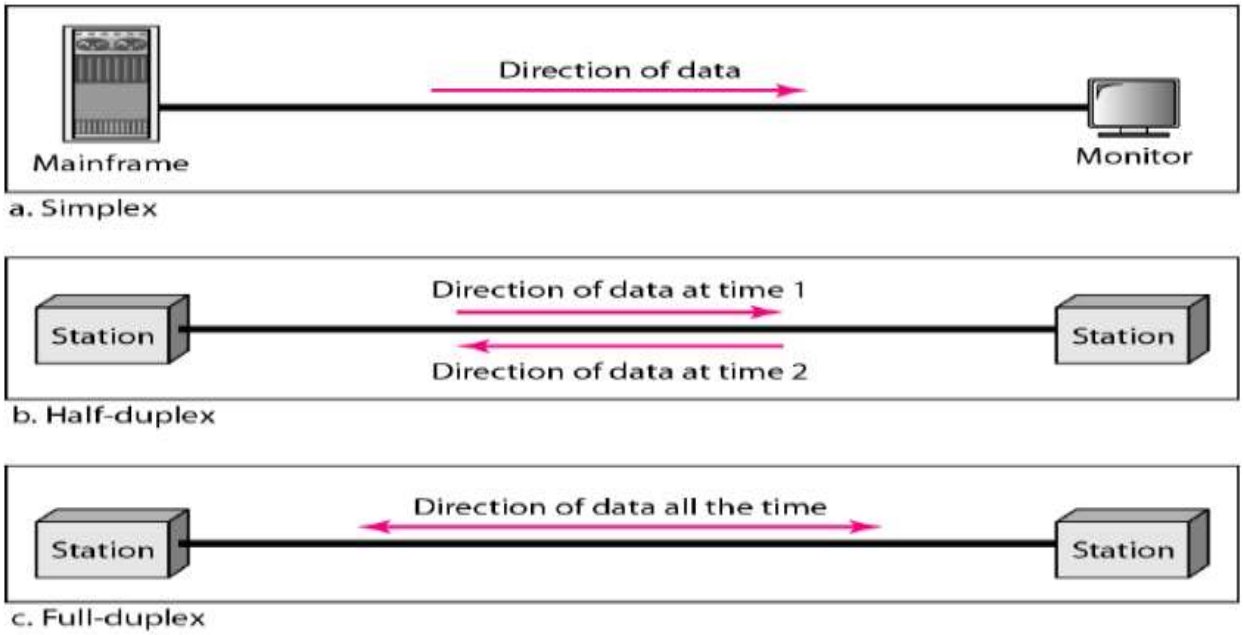
A data communications system has five components:



1. ***Message***: The message is the information (data) to be communicated. Popular forms of information include text, numbers, pictures, audio, and video.
2. ***Sender***: The sender is the device that sends the data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. ***Receiver***: The receiver is the device that receives the message. It can be a computer, workstation, telephone handset, television, and so on.
4. ***Transmission medium***: The transmission medium is the physical path by which a message travels from sender to receiver. Some examples of transmission media include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
5. ***Protocol:*** A protocol is a set of rules that govern data communications. It represents an agreement between the communicating devices. Without a protocol, two devices may be connected but not communicating, just as a person speaking French cannot be understood by a person who speaks only Japanese.

Data Flow

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



Simplex In simplex mode, the communication is unidirectional, as on a one way street. Only one of the two devices on a link can transmit; the other can only receive (Figure a). Keyboards and traditional monitors are examples of simplex devices.

Half-Duplex

In half-duplex mode, each station can both transmit and receive, but not at the same time. When one device is sending, the other can only receive, and vice versa (Figure b). Walkie-talkies and CB (citizens band) radios are both half-duplex systems.

Full-Duplex

In full-duplex, both stations can transmit and receive simultaneously (Figure c). One common example of full-duplex communication is the telephone network.

When two people are communicating by a telephone line, both can talk and listen at the same time. The full-duplex mode is used when communication in both directions is required all the time.

NETWORKS

A *network* is a set of devices (often referred to as nodes) connected by communication links. A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.

Uses of Computer Network:

A. ***Resource Sharing:*** The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user.

B. ***High Reliability:*** By Having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable (due to a hardware failure), the other copies could be used.

C. ***Saving Money:*** Small Computers have a much better price/performance ratio than large ones. Mainframes are roughly a factor of ten faster than personal computers, but they cost a thousand times more.

D. ***Scalability:*** is the ability to increase system performance gradually as the workload grows just by adding more processors.

E. ***Computer network delivering services to private individuals at home, like***: (access to remote information, Person -To- Person communication, Interactive entertainment).

Advantages

- Connectivity and Communication
- Data Sharing
- Hardware Sharing
- Internet Access
- Internet Access Sharing
- Data Security and Management
- Performance Enhancement and Balancing
- Entertainment

Disadvantages

- Security Issues
- Rapid Spread of Computer Viruses
- Illegal or Undesirable Behavior
- Expensive Set Up
- Managing a large network is complicated.
- Dependency on the Main File Server (If the file server breaks down the files on the file server become inaccessible)

Applications

- Marketing and sales.
- Financial services.
- Manufacturing.
- Electronic messaging.
- Information services.
- Cellular telephone.
- Cable television.

NETWORK CRITERIA

A network must be able to meet a certain number of criteria. The most important of these are: ***Performance***; ***Reliability***; ***Security***.

1. *Performance*: can be measured in many ways, including transit time and response time.

- *Transit time* is the amount of time required for a message to travel from one device to another.
- *Response time* is the elapsed time between an inquiry and a response.

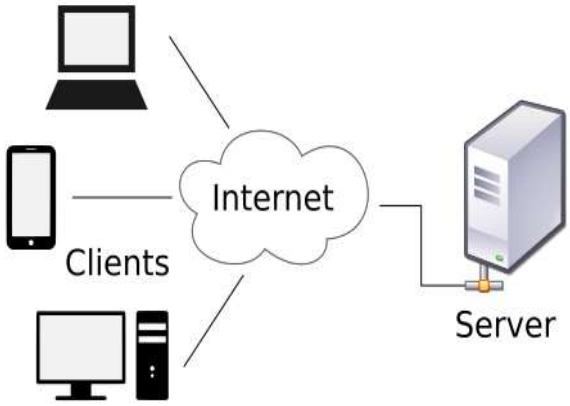
The performance of a network depends on a number of factors which are:

- The number of users
- The type of transmission medium
- The connected hardware
- The efficiency of the software

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

3.*Security*: Network security issues include protecting data from unauthorized access, protecting data from damage and development.

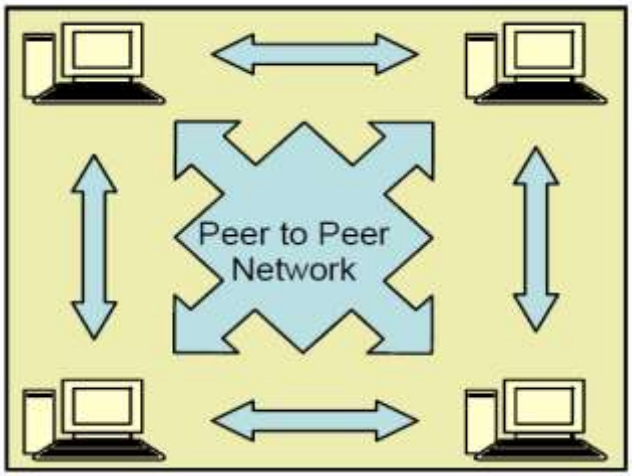
A client is a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network. The term applies to the role that programs or devices play in the client–server model.



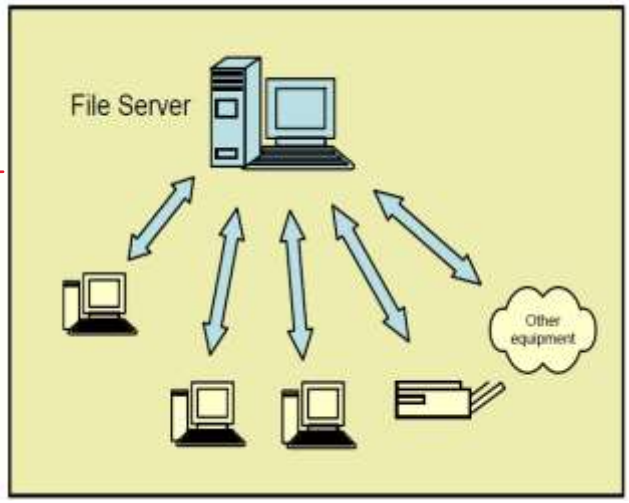
A server is a computer designed to process requests and deliver data to other (client) computers over a local network or the internet. Although any computer running special software can function as a server, the most typical use of the word references the very large, high-powered machines that function as the pumps pushing and pulling data across the internet. Most computer networks support one or more servers that handle specialized tasks.

Network configuration: There are two types of network configuration, peer-to-peer networks and client/server networks.

Peer-to-peer networks: are more commonly implemented where less then ten computers are involved and where strict security is not necessary. All computers have the same status, hence the term 'peer', and they communicate with each other on an equal footing. Files, such as word processing or spreadsheet documents, can be shared across the



network and all the computers on the network can share devices, such as printers or scanners, which are connected to any one computer.



Client/server networks: are more suitable for larger networks. A central computer, or 'server', acts as the storage location for files and applications shared on the network. Usually the server is a higher than average performance computer. The server also controls the network access of the other computers which are referred to as the 'client' computers. Typically, teachers and students in a school will use the client computers for their work and only the network administrator (usually a designated staff member) will have access rights to the server.

Peer-to-Peer Networks vs Client/Server Networks	
Peer-to-Peer Networks	**Client/Server Networks**
• Easy to set up	• More difficult to set up
• Less expensive to install	• More expensive to install
• Can be implemented on a wide range of operating systems	• A variety of operating systems can be supported on the client computers, but the server needs to run an operating system that supports networking
• More time consuming to maintain the software being used (as computers must be managed individually)	• Less time consuming to maintain the software being used (as most of the maintenance is managed from the server)
• Very low levels of security supported or none at all. These can be very cumbersome to set up, depending on the operating system being used	• High levels of security are supported, all of which are controlled from the server. Such measures prevent the deletion of essential system files or the changing of settings
• Ideal for networks with less than 10 computers	• No limit to the number of computers that can be supported by the network
• Does not require a server	• Requires a server running a server operating system
• Demands a moderate level of skill to administer the network	• Demands that the network administrator has a high level of IT skills with a good working knowledge of a server operating system

Components of a Network

A computer network comprises the following components:

1. A minimum of at least 2 computers(nodes).
2. Cables that connect the computers to each other.
3. A network interface device on each computer (this is called a network interface card or NIC)
4. Network operating system software.

Basic Concepts of Networking

- Major network components (devices).
- Line configuration.
- Topology.
- Categories of networks.
- Transmission mode.
- Internetworks.
- Protocols.

Major computer network components

Computer network requires the following devices (some of them are optional):

1. Network Interface Card (NIC)
2. Modem
3. Repeater
4. Hub
5. Bridge
6. Switch
7. Router
8. Getaway

1. Network Interface Card: ***Network adapter*** is a device that enables a computer to talk with other computer/network. Using unique **hardware addresses** encoded on the card chip, the data-link protocol employs these addresses to discover other systems on the network so that it can transfer data to the right destination. NIC's job to translate the data from the computer into signals that can flow easily along the cable.

There are **two types of network cards**: **wired** (e.g., Ethernet) **and wireless** (e.g., WiFi). For two computers to send and receive data, the cards must agree on several things. These include the following:

- The maximum size of the data frames
- The amount of data sent before giving confirmation
- The time needed between transmissions
- The amount of time needed to wait before sending confirmation
- The amount of data a card can hold
- The speed at which data transmits

In order to successfully send data on the network, you need to make sure the network cards are of the same type and they are connected to the same piece of cable.



2. Modems: enables you to connect your computer to the available internet connection over the existing telephone line**.** Like NIC, **Modem is not integrated with a computer motherboard**. It comes as separate part which can be installed on the PCI slots found on motherboard. A modem is not necessary for LAN, but required for internet connection such as dial-up and DSL.

3. Repeaters: is an electronic device that receives a signal and retransmits it. Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction. Important features of a repeater are as follows:

- A repeater connects different segments of a LAN
- A repeater forwards every frame it receives
- A repeater is a regenerator, not an amplifier
- It can be used to create a single extended LAN
- It is a 2 port device.
- Repeater range is roughly 500 m.
- Repeater is considered as a level-1in ISO model (physical layer)

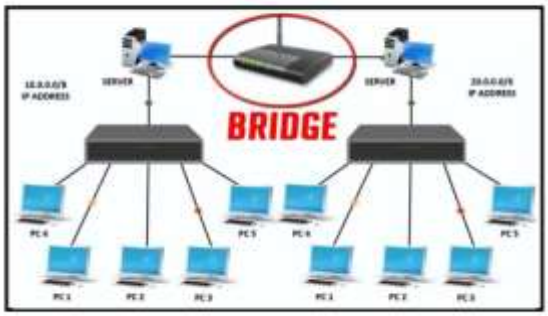
4. Hub: is a central network device that connects network nodes such as workstation and servers in a star topology. A hub is basically a multiport repeater. A hub connects multiple wires coming from different branches, for example, the connector in star topology which connects different stations. Important features of a hub are as follows:

- Hubs cannot filter data
- Hubs do not have intelligence to find out best path for data packets which leads to inefficiencies and wastage.
- The stations connect to the hub with RJ-45 connector having maximum segment length is 100 meters.
- Hub is considered as a level-1in ISO model (physical layer)

5. Bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. This function is

called network bridging. Bridging is distinct from routing. Routing allows multiple networks to communicate independently and yet remain separate, whereas bridging connects two separate networks as if they were a single network. Important features of a bridge are as follows:

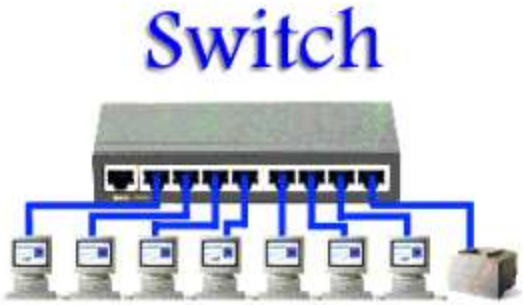
- A bridge operates both in physical and data-link layer (layer 1and 2)
- A bridge uses a table for filtering/routing
- A bridge does not change the physical (MAC) addresses in a frame
- A bridge must contain addressing and routing capability.



6. Switch :is a telecommunication device grouped as one of computer network components. Switch is like a Hub but built in with advanced features. It uses ***physical device addresses*** in each incoming messages so that it can deliver the message to the right destination or port.

Like Hub, switch don't broadcast the received message to entire network, rather before sending it checks to which system or port should the message be sent. In other words switch connects the source and destination directly which increases the speed of the network. Important features of a switch are as follows:

- A switch is essentially a fast bridge having additional sophistication that allows faster processing of frames.
- Switch can perform error checking before forwarding data.
- Both switch and hub have common features: ***Multiple RJ-45 ports***, ***power supply*** and ***connection lights***.
- Switch is data link layer device (layer 2)



7. Router: is a device like a switch that routes data packets based on their IP addresses. Router is mainly ***a Network Layer device*** (layer 3). 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. Router can be found in two products: ***wired*** **and** ***wireless***. The choice depends on your physical office/home setting, **speed** and **cost**. There are two types of routers:

1. ***Static routers*** - Are configured manually and route data packets based on information in a router table.
2. ***Dynamic routers*** - Use dynamic routing algorithms.

8. ***Gateways:*** a piece of networking hardware that joins two networks so the devices on one network can communicate with the devices on another network. 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. Gateways will start at the lower level and strip information until it gets to the required level and repackage the information and work its way back toward the hardware layer of the OSI model.

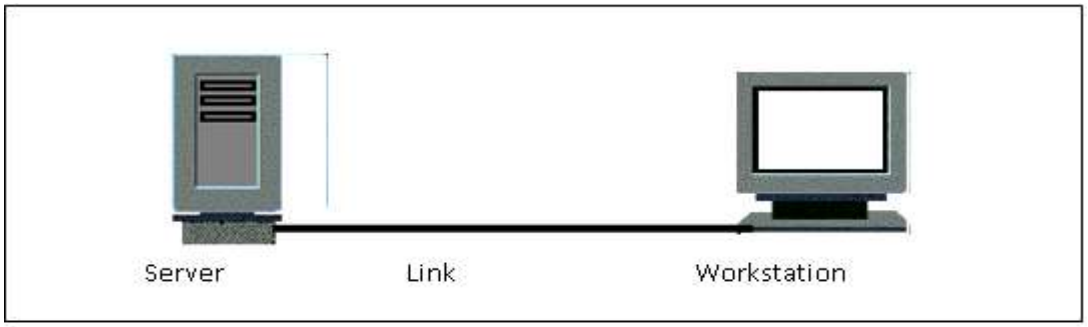
Networking software is a key component of today's computer networks, including the Internet. Understanding the types of networking software is the first step in understanding how your computer network really works.

Network Operating Systems (NOS) can be embedded in a router or hardware firewall that operates the functions in the network layer (layer 3).

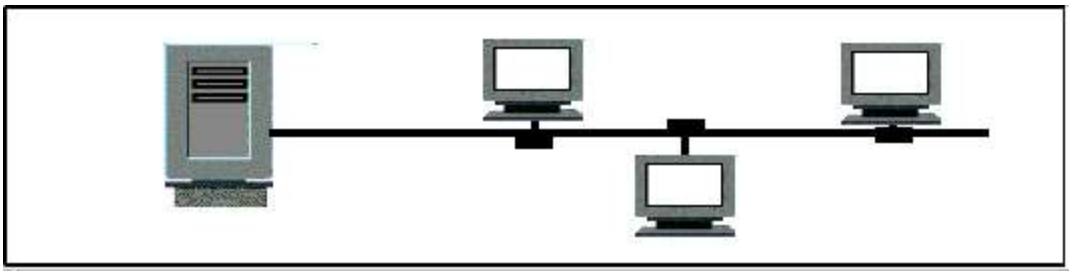
An operating system oriented to computer networking, to allow shared file and printer access among multiple computers in a network, to enable the sharing of data, users, groups, security, applications, and other networking functions, typically over a local area network (LAN), or private network.

Line Configuration:

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



• **Multipoint:** A multipoint (also called multi-drop) connection is one in which more than two specific devices share a single link. In a multipoint environment, the capacity of the channel is shared, either spatially or temporally. If several devices can use the link simultaneously, it is a spatially shared connection. If users must take turns, it is a timeshared connection.

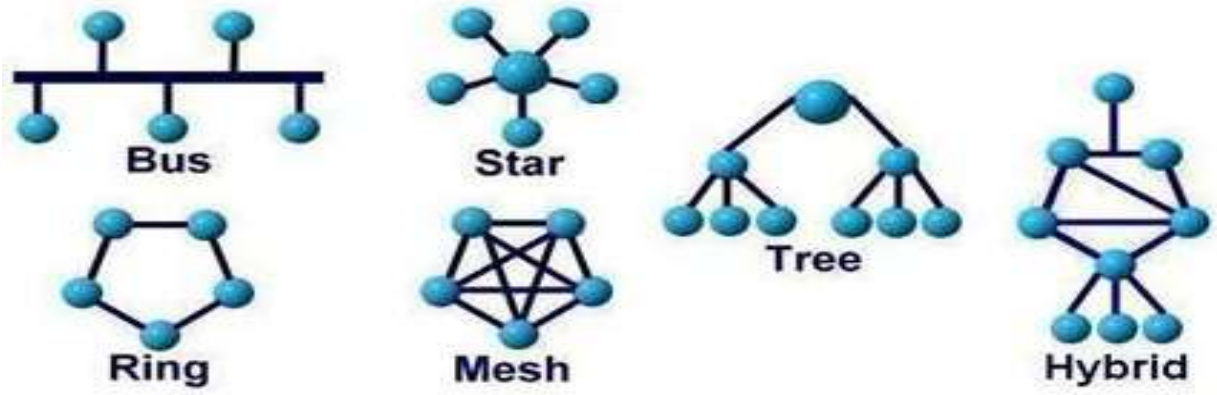


Topology

The term **physical topology** refers to the way in which a network is laid out physically one or more devices connect to a link; two or more links form a topology. The topology of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.

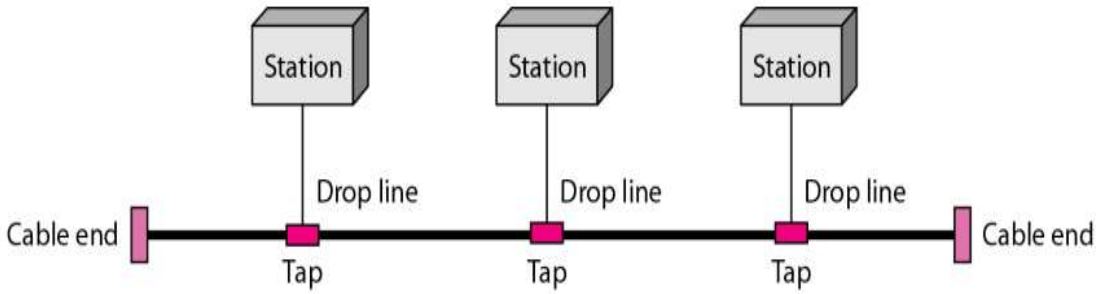
There are many basic topologies possible:

1. Bus topology
2. Star topology
3. Ring topology
4. Tree topology
5. Mesh topology
6. Hybrid topology



BUS:

A **line topology**, a **bus topology** is a network setup in which each computer and network device are connected to a single cable or backbone.



Advantages of bus topology

- It works well when you have a small network.
- It's the easiest network topology for connecting computers or peripherals in a linear fashion.
- It requires less cable length than a star topology.

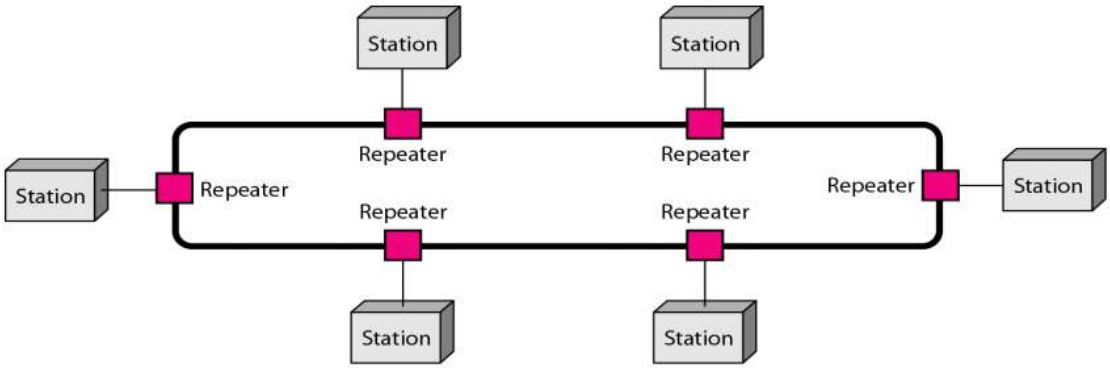
Disadvantages of bus topology

- It can be difficult to identify the problems if the whole network goes down.
- It can be hard to troubleshoot individual device issues.
- Bus topology is not great for large networks.
- Terminators are required for both ends of the main cable.
- Additional devices slow the network down.
- If a main cable is damaged, the network fails or splits into two.

RING:

A **ring topology** is a network configuration in which device connections create a circular data path. In a ring network, packets of data travel from one device to the next until they reach their destination. Most ring topologies allow packets to travel only in one direction, called a ***unidirectional*** ring network. Others permit data to move in either direction, called ***bidirectional***.

Ring topologies may be used in either local area networks (LANs) or wide area networks (WANs).



Advantages of ring topology

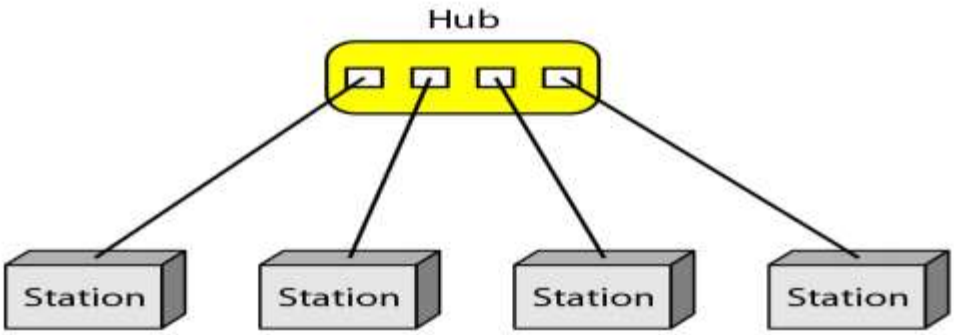
- All data flows in one direction, reducing the chance of packet collisions.
- A network server is not needed to control network connectivity between each workstation.
- Data can transfer between workstations at high speeds.
- Additional workstations can be added without impacting performance of the network.

Disadvantages of ring topology

- All data being transferred over the network must pass through each workstation on the network, which can make it slower than a star topology.
- The entire network will be impacted if one workstation shuts down.
- The hardware needed to connect each workstation to the network is more expensive than Ethernet cards and hubs/switches.

STAR:

A star network, **star topology** is one of the most common network setups. In this configuration, every node connects to a central network device, like a hub, switch, or computer. The central network device acts as a server and the peripheral devices act as clients. Depending on the type of network card used in each computer of the star topology, a coaxial cable or a ***RJ-45*** network cable is used to connect computers together.



Advantages of star topology

- Centralized management of the network, through the use of the central computer, hub, or switch.
- Easy to add another computer to the network.
- If one computer on the network fails, the rest of the network continues to function normally.
- The star topology is used in local-area networks (LANs), High-speed LANs often use a star topology with a central hub.

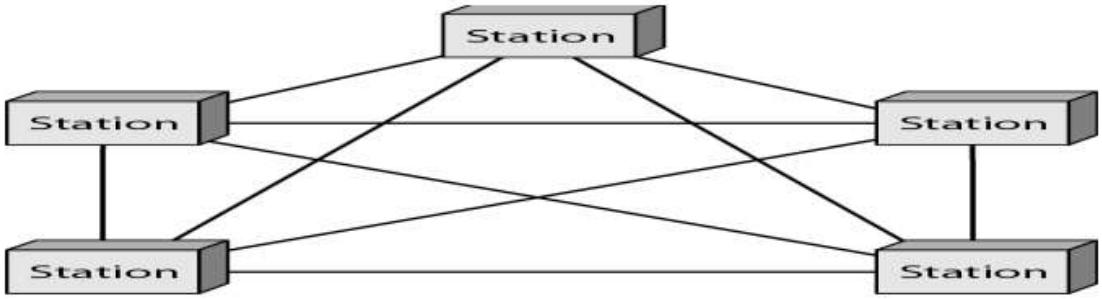
Disadvantages of star topology

- ❖ Can have a higher cost to implement, especially when using a switch or router as the central network device.
- ❖ The central network device determines the performance and number of nodes the network can handle.
- ❖ If the central computer, hub, or switch fails, the entire network goes down and all computers are disconnected from the network

MESH:

A mesh topology is the one where every node is connected to every other node in the network. A mesh topology can be a **full mesh topology** or a **partially connected mesh topology**.

In a full mesh topology, every computer in the network has a connection to each of the other computers in that network. The number of connections in this network can be calculated using the following formula (**n** is the number of computers in the network): **n(n-1)/2.** In a partially connected mesh topology, at least two of the computers in the network have connections to multiple other computers in that network. It is an inexpensive way to implement redundancy in a network. In the event that one of the primary computers or connections in the network fails, the rest of the network continues to operate normally.



Advantages of a mesh topology

- Can handle high amounts of traffic, because multiple devices can transmit data simultaneously.
- A failure of one device does not cause a break in the network or transmission of data.
- Adding additional devices does not disrupt data transmission between other devices.

Disadvantages of a mesh topology

- The cost to implement is higher than other network topologies, making it a less desirable option.
- Building and maintaining the topology is difficult and time consuming.
- The chance of redundant connections is high, which adds to the high costs and potential for reduced efficiency.

Networks Types /Categories of Networks:

1. Personal Area Networks:

PANs (Personal Area Networks) let devices communicate over the range of a person. A common example is a wireless network that connects a computer with its peripherals. Almost every computer has an attached monitor, keyboard, mouse, and printer. Without using wireless, this connection must be done with cables.

To help these users, some companies got together to design a short-range wireless network called ***Bluetooth*** to connect these components without wires. The idea is that if your devices have Bluetooth, then you need no cables. You just put them down, turn them on, and they work together.

2. Local Area Network (LAN):

LANs, are privately-owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other networks by three characteristics:

1. **Their size**: LANs are restricted in size, which means that the worst-case transmission time is bounded and known in advance. Knowing this makes it possible to use certain kinds of designs that would not otherwise be possible .it also simplifies network management.
2. **Their transmission technology:** LANs often use a transmission technology consisting of a single cable to which all the machines are attached, like the telephone company party lines once used in rural areas. LANs are:
   - Run at speed of 10 to 100 Mbps.
   - Make very few errors.
   - Have low delay (tens of microseconds).

The new LAN operate at higher speed, up to hundred of megabits/sec.

3. **Their topology:** Various topologies are possible for broadcast LAN which are bus and ring.

3. Metropolitan Area Network (MAN):

Is basically a bigger version of a LAN and normally covers a city. The best-known examples of MANs are the cable television networks available in many cities. A metropolitan area network (MAN) is a network with a size between a LAN and a WAN. It normally covers the area inside a town or a city.

It is designed for customers who need a high-speed connectivity, normally to the Internet, and have endpoints spread over a city or part of city.

A good example of a MAN is:

1. The part of the telephone company network that can provide a high-speed DSL line to the customer.
2. Another example is the cable TV network that originally was designed for cable TV, but today can also be used for high-speed data connection to the Internet, which has been standardized as IEEE 802.16 and is popularly known as WiMAX.

4. Wide Area Network (WAN):

A WAN spans a large geographical area, often a country or continent. We will begin our discussion with wired WANs, using the example of a company with branch offices in different cities.

We will follow traditional usage and call these machines hosts. The rest of the network that connects these hosts is then called the communication subnet, or just subnet for short. The job of the subnet is to carry messages from host to host, just as the telephone system carries words (really just sounds) from speaker to listener.

In most WANs, the subnet consists of two distinct components:

- **Transmission lines**
- **Switching elements.**

Transmission lines move bits between machines. They can be made of ***copper wire***, ***optical fiber***, or even ***radio links***.

Switching elements, or just switches, are specialized computers that connect two or more transmission lines. These switching computers have been called by various names in the past; the name ***router*** is now most commonly used.

5. Wireless Networks:

Wireless networks can be divided into three main categories:

- System interconnection.
- Wireless LANs.
- Wireless WANs.

1. System interconnection:

Is all about interconnecting the components of a computer using short-range radio . Almost every computer has a monitor, keyboard, mouse, and printer connected to the main unit by cables. So many new users have a hard time plugging all the cables into the right little holes (even though they are usually color coded) that most computer vendors offer the option of sending a technician to the user's home to do it.

2. Wireless LANs:

The next step up in wireless networking are the wireless LANs. These are systems in which every computer has a ***radio modem*** and ***antenna*** with which it can communicate with other systems. Often there is an antenna on the ceiling that the machines talk to. However, if the systems are close enough, they can communicate directly with one another in ***a peer-to-peer configuration***. There is a standard for wireless LANs, called IEEE 802.11.

3. Wireless WANs:

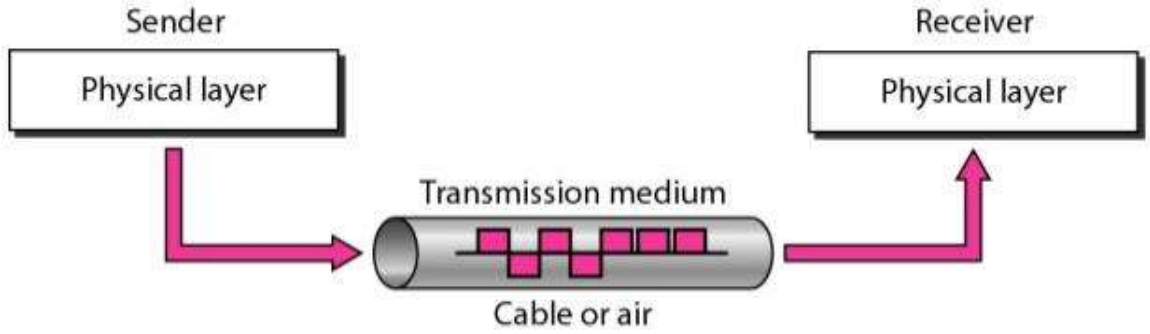
The third kind of wireless network is used in wide area systems. The radio network used for cellular telephones is an example of a low-bandwidth wireless system.

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.

Transmission Media

A transmission medium can be defined as anything that can carry information from a source to a destination.

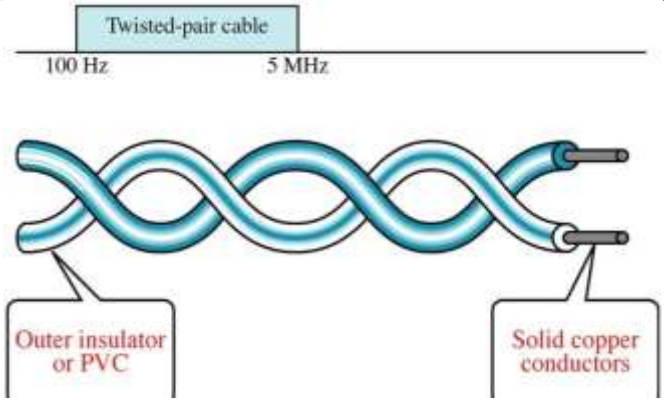


In telecommunications, transmission media can be divided into two broad categories: ***guided*** and ***unguided***. Guided media include ***twisted-pair cable***, ***coaxial cable***, and ***fiber-optic cable***. Unguided medium is ***free space.***

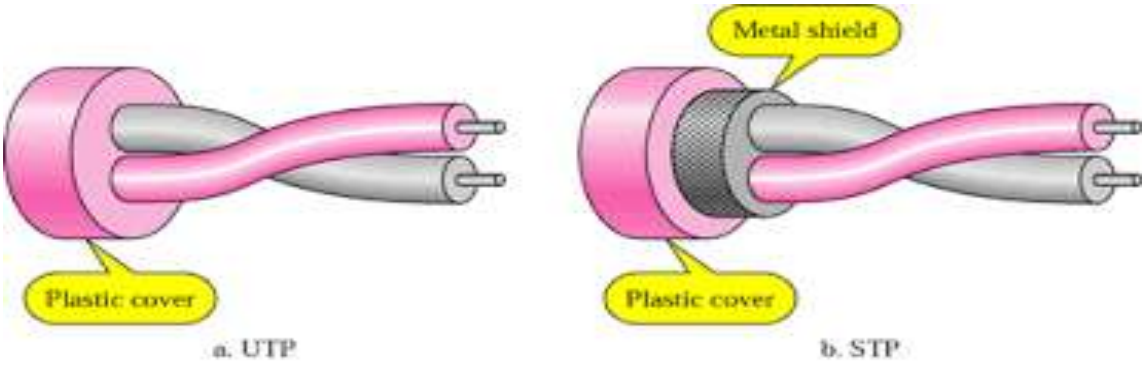
GUIDED MEDIA

Guided media (***Networking cables***) are networking hardware used to connect one network device to other network devices or to connect two or more computers to share printers, scanners etc. Different types of network cables, such as ***coaxial cable***, ***optical fiber cable***, and ***twisted pair cables***, are used depending on the network's ***physical layer***, ***topology***, and ***size***.

Twisted Pair: The pair of twisted is the simplest transmission medium. It consists of one or more pairs of electrical son arranged spiral. This type of support is suitable for transmission both analog and digital.



The twisted pairs may be shielded (***Shielded Twisted Pair (STP)***), that has a metal sheath surrounding completely metallic pairs or unshielded (***Unshielded Twisted Pair (UTP)***).



Why to twist the wires?

- Twisting of wires will reduce the effect of noise or external interference.
- Number of twists per unit length will determine the quality of cable. More twists means better quality.

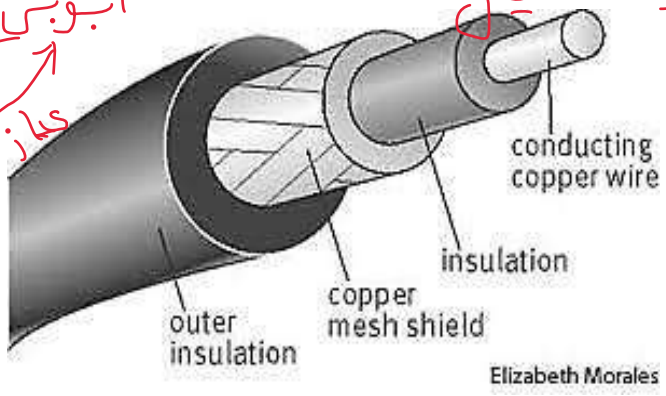
Advantages

1. Cheaper and easier to repair.
2. Easy to handle and install
3. Less susceptible to electrical interference caused by nearby equipment or wires.
4. Less likely to cause interference themselves.
5. Because it is electrically "cleaner", STP wire can carry data at a faster speed

Disadvantages

1. Attenuation is very high.
2. It supports lower bandwidth as compared to other Medias. It supports 10 mbps upto a distance of 100 meters on a 10BASE-T.
3. It offers very poor security and is relatively easy to tap.
4. Being thin in size, they are likely to break easily.

Coaxial cable: is a type of electrical cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath or jacket.



Coaxial cable is used as a transmission line for radio frequency signals. Its applications include feedlines connecting radio transmitters and receivers with their antennas, computer network (Internet) connections, digital audio and distributing cable television signals.

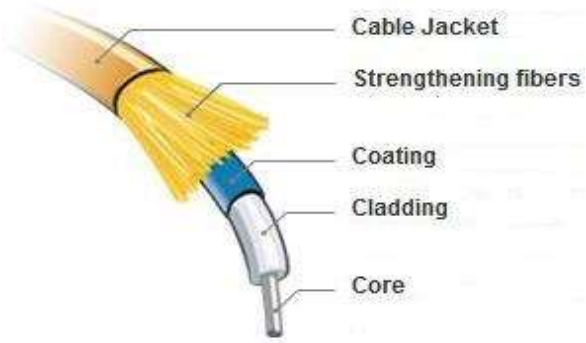
Advantages

1. Coaxial cable can support greater cable lengths between network devices than twisted pair cable.
2. Thick coaxial cable has an extra protective plastic cover that help keep moisture away.

Disadvantages

1. More expensive to install compare to twisted pair cable.
2. The thicker the cable, the more difficult to work with

Optical fiber cable: is an assembly similar to an electrical cable, but containing one or more optical fibers that are used to carry light. It consists of a center glass core surrounded by several layers of protective material. The outer insulating jacket is made of Teflon or PVC to prevent interference. Optical fiber deployment is more expensive than copper but offers higher bandwidth and can cover longer distances.



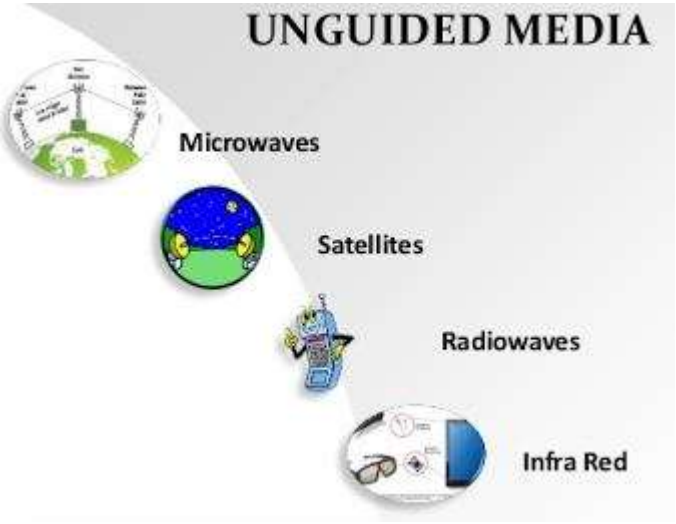
Advantages

3. It can handle much higher bandwidth than copper.
4. Providing a high-speed data connection between different parts of a building.
5. Immunity to electromagnetic interference.
6. Fiber is lighter than copper.
7. Fibers do not leak light and are quite difficult to tap.
8. Excellent security against potential wire-tappers.

Disadvantages

1. Fiber required skills which may not be easily available.
2. Unidirectional, two-way communication requires either two fiber cables or two frequency bands on one fiber.
3. Fiber is costly.

UNGUIDED MEDIA: WIRELESS



Unguided media transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them.

Infrared

Infrared (IR) is a wireless mobile technology used for device communication over short ranges. IR communication has major limitations because it requires line-of-sight, has a short transmission range and is unable to penetrate walls. It extends from the nominal red edge of the visible spectrum at 700 nanometers (frequency 430 THz), to 1 mm (300 GHz). It covers distance of 10 to 30 meters. Data rate of upto 4 Mbps can be achieved.

Advantages

1. The devices are very cheap.
2. The devices are compact, lightweight and consume low power.
3. The technology based devices are easy to use.
4. It is non interfering from RF waves.
5. It is more secure compare to RF technologies.

Disadvantages

1. It requires both transmitter and receiver to be in line of sight.
2. Devices can't move around while transmission is in progress.
3. Used for very short distance applications.

Radio Waves

Is a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared light. Radio waves have frequencies as high as 300 GHz to as low as 3 kHz. They are easy to generate, have same velocity in vacuum, may traverse long distances and they are omni-directional.

Advantages

1. They are easy to generate.
2. It has different penetration through the walls of the buildings or houses based on the frequency.
3. Used in various medical applications..
4. It is used in radar for object detection.

Disadvantages

1. Uncontrolled radiation of RF affects humans.
2. The areas near RF cellular towers have been observed with more lightening compare to other areas.
3. It also affects some of the fruits grown near the RF (Radio Frequency) tower areas.
4. Not very secure.

Satellite

Is any object that revolves around a planet in a circular or elliptical path. Satellite transmission requires an unobstructed line of sight. The line of site will be between the orbiting satellite and a station on Earth. Satellite signals must travel in straight lines but do not have the limitations of ground based wireless transmission, such as the curvature of the Earth.

Advantages

1. High bandwidth
2. Coverage over a large geographical area
3. Can be cheaper over long distances

4. It is used for mobile and wireless communication applications independent of location.
5. It is easy to install and manage the ground station sites.
6. It is used for voice, data, video and any other information transmission.

Disadvantages

1. Propagation delay
2. Satellite design and development requires higher cost.
3. Requires to be monitored and controlled on regular periods so that it remains in the orbit.
4. Satellite has life which is about 12-15 years. Due to this fact, another launch need to be planned before it becomes un-operational.
5. Redundant components are used in the network design.

Microwave

Is well suited for wireless transmission of signals having large bandwidth. This portion of the RF electromagnetic radiation spectrum encompasses many thousands of megahertz. It extends from 3 MHz to 30 MHz, and whose total available bandwidth is only 27 MHz.

Advantages

1. The microwave spectrum has larger bandwidth.
2. Multiple channels available.
3. Microwave radio communication systems propagate signals through the earth's atmosphere.

Disadvantages

1. Line-of-sight will be disrupted if any obstacle, such as new buildings, are in the way.
2. Signal absorption by the atmosphere. Microwaves suffer from attenuation due to atmospheric conditions.
3. Towers are expensive to build.

Important Terminology

Bandwidth is the bit-rate of available or consumed information capacity expressed typically in metric multiples of bits per second.

Throughput is the maximum rate of production or the maximum rate at which something can be processed.

Bandwidth	Throughput
Bandwidth is the maximum amount of data that can travel through a link or network	Throughput is the actual amount of data that can be transferred through a network
Bandwidth is always measured a physical layer property	Throughput can be measured at any layer OSI model
A data rate measured in bits per second	Average rate of successful message delivery over a communication channel.
Bandwidth does not depend on latency on link	Throughput depend on latency on link

Internetworks:

Internet

The network formed by the co-operative interconnection of a large number of computer networks.

- Network of Networks
- Every person who makes a connection owns a slice of the Internet.
- There is no central administration of the Internet.

Applications of Internet

- Download programs and files
- E-Mail
- Voice and Video Conferencing
- E-Commerce
- File Sharing
- Information browsing
- Search the web addresses for access through search engine

Disadvantages of Internet

- Theft of personal information such as name, address, credit card number etc.
- Virus threats nothing but a program which disrupts the normal functioning of your system.
- Spamming refers to receiving unwanted e-mails in bulk, which provide no purpose and needlessly obstruct the entire system.
- Pornography This is perhaps the biggest threat related to children's healthy mental life. A very serious issue concerning the Internet.

Intranet

An intranet is a set of networks that are under the control of a single administrative entity. The intranet uses the IP protocol and IP-based tools such as web browsers and file transfer applications.

Applications of Intranet

- Sharing of company policies/rules & regulations
- Access employee database
- Distribution of circulars/Office Orders
- Access product & customer data
- Sharing of information of common interest
- Launching of personal/departmental home pages
- Submission of reports
- Corporate telephone directories

Disadvantages of Intranet

- A company may not have person to update their Intranet on a routine basis
- Fear of sharing information and the loss of control
- Limited bandwidth for the business
- Unauthorized access, Abuse of access, Denial of service
- Information overload lowers productivity
- True purpose of the Intranet is unknown to many employees/departments
- Hidden or unknown complexity and costs

Extranet

An extranet is a network that is also under the administrative control of a single organization, but supports a limited connection to a specific external network. For example, an organization may provide access to some aspects of its intranet to share data with its business partners or customers.

Benefits of Extranet

- Improved quality.
- lower travel costs.
- lower administrative & other overhead costs.
- reduction in paperwork.
- delivery of accurate information on time.
- improved customer service.
- better communication.
- overall improvement in business effectiveness.

Disadvantages of Extranet

- The suppliers & customer who don't have technical knowledge feel problem.
- Faceless contact.
- Information can be misused by other competitors.
- Fraud may be possible.
- Technical Employees are required.

Network Protocols

A **protocol** is a set of rules that govern data communications. It represents an agreement between the communicating devices. For devices to communicate on a network, they must follow different protocols that perform the many tasks to be completed. The protocols define the following:

- The format of the message, such as how much data to put into each segment
- The way intermediary devices share information about the path to the destination
- The method to handle update messages between intermediary devices
- The process to initiate and terminate communications between hosts

There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. These are:

1. **Transmission Control Protocol (TCP):** TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.

2. **Internet Protocol (IP):** IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.

3. **User Datagram Protocol (UDP):** UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.

4. **Post office Protocol (POP):** POP3 is designed for receiving incoming E-mails.

5. **Simple mail transport Protocol (SMTP):** SMTP is designed to send and distribute outgoing E-Mail.

6. **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.

7. **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.

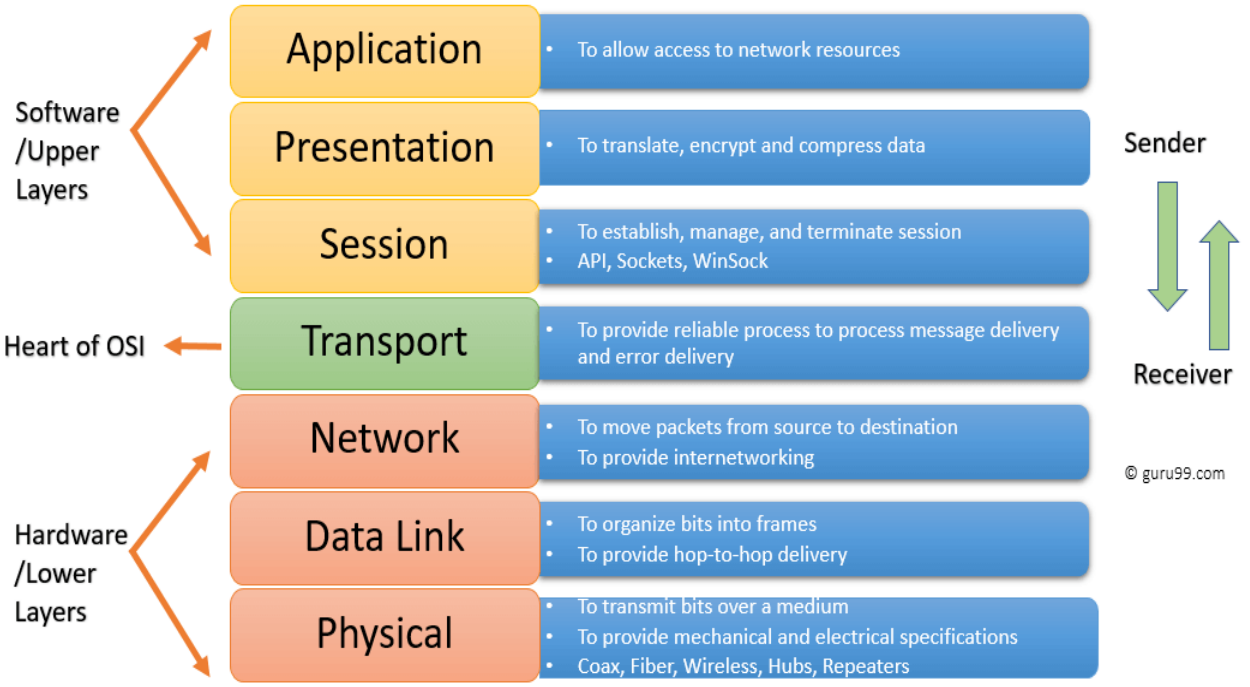
NETWORKING MODELS

A networking model, sometimes also called either a networking architecture or networking blueprint, refers to a comprehensive set of documents. Individually, each document describes one small function required for a network; collectively, these documents define everything that should happen for a computer network to work. the OSI reference model and the TCP/IP reference model.

The ***Open Systems Interconnection (OSI) model*** defines a networking framework to implement protocols in layers, with control passed from one layer to the next. It conceptually divides computer network architecture into 7 layers in a logical progression. The lower layers deal with electrical signals, chunks of binary data, and routing of these data across networks. Higher levels cover network requests and responses, representation of data, and network protocols as seen from a user's point of view.

The **principles** that were applied to arrive at the seven layers can be briefly summarized as follows:

- A layer should be created where a different abstraction is needed.
- Each layer should perform a well-defined function.
- The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
- The layer boundaries should be chosen to minimize the information flow across the interfaces.



1. **Physical Layer:** is responsible for ultimate transmission of digital data bits from the source to the destination. At the Physical layer, data are transmitted using the type of signals are supported by the physical medium: electric voltages, radio frequencies, or pulses of infrared or ordinary light. The physical layer is also concerned with the following: ***Representation of bits***, ***Data rate***, ***Synchronization of bits***, ***Line configuration*** , ***Physical topology*** and ***Transmission mode***
2. **Data Link Layer:** checks for physical transmission errors and packages bits into data "frames". The Data Link layer also manages physical addressing schemes such as MAC addresses for Ethernet networks, controlling access of any various network devices to the physical medium. Other responsibilities of the data link layer include the following: ***Framing***, ***Physical addressing***, ***Flow control*** , ***Error control*** and ***Access control.***

3. **Network Layer:** maintains logical addresses such as IP addresses for devices on the network. The Network layer also manages the mapping between these logical addresses and physical addresses. Other responsibilities of the network layer include the following: ***Logical addressing*** and ***Routing***
4. **Transport Layer:** delivers data across network connections. The transport layer decides on the type of whether it was reliable or unreliable type of communication. Transport layer provides error checking, data recovery and provides port numbers for services. Other responsibilities of the transport layer include the following: ***Service-point addressing, Segmentation and reassembly***, ***Connection control***, ***Flow control*** and ***Error control***.
5. **Session Layer:** is the network ***dialog controller***. It establishes, maintains, and synchronizes the interaction among communicating systems. The session layer is responsible for dialog control and synchronization. Specific responsibilities of the session layer include the following: ***Dialog control*** and ***Synchronization*.**
6. **Presentation Layer:** is concerned with the **syntax and semantics** of the information exchanged between two systems. Specific responsibilities of the presentation layer include the following: ***Translation***, ***Encryption*** and ***Compression***.
7. **Application Layer:** supplies network services to end-user applications. Its contains a variety of protocols that are commonly needed by users. One widely used application protocol is **HTTP** (**Hyper Text Transfer Protocol**), which is the basis for the World Wide Web. Specific services provided by the application layer include the following: ***Network virtual terminal***, ***File transfer***, ***Mail services*** and ***Directory services***.

Protocols supported at various levels

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN

Advantages of the OSI Model

- It helps you to standardize router, switch, motherboard, and other hardware
- Reduces complexity and standardizes interfaces
- Facilitates modular engineering
- Helps you to ensure interoperable technology
- Helps you to accelerate the evolution
- Protocols can be replaced by new protocols when technology changes.
- Provide support for connection-oriented services and connectionless service.
- Supports connectionless and connection-oriented services.
- Offers flexibility to adapt to various types of protocols

Disadvantages of the OSI Model

- Fitting of protocols is a tedious task.
- You can only use it as a reference model.
- Doesn't define any specific protocol.
- In the OSI network layer model, some services are duplicated in many layers such as the transport and data link layers
- Layers can't work in parallel as each layer need to wait to obtain data from the previous layer.