NETWORK
UNIT I

DATA COMMUNICATION

When we want to communicate we need sharing of information. The sharing can be local or remote. Between individuals local communication usually occurs face to face. But remote communication takes place over distance. The term telecommunication, which includes telephony , telegraph and television which means communication at a distance.

The word data refers to facts, concepts an instructions in whatever from which agreed by many parties which uses the data. In computer information system, data are represented by binary information units (or bits) produced and consumed in the form of 0's and 1's.

DATA COMMUNICATION:

Data communication is the exchange of data between two devices through some form of transmission medium like cable. Data communication is considered local if the communicating devices lies in same building or considered as remote if the devices are farther apart.

To achieve data communications to occur, the communicating devices must be part of a communication system made up of a combination of hardware and software. The data communication system depends upon three fundamental characteristics. They are :

(i) 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.

(ii) **Accuracy :** The system must deliver data accurately. Data that have been alerted in transmission and left uncorrected are unusable.

(iii)Timeliness: The system must deliver data in a timely manner. Data delivered late are useless.

Components : A data communication system is made up of five components. They are :

(i) **Message :** The message is the information to be communicated. It consist of text, numbers, pictures, audio , video, etc.. or combination of these.

(ii) Sender : The **sender** is the device that sends the data message . It can be a computer, workstation, video camera , etc..

(iii) Receiver : The receiver is the device that receives the message. It can be a computer, workstation , television, etc…

(iv) Medium : The transmission medium is the physical path by which a message travels from sender to receiver. Examples are twisted pair, coaxial cable, fiber optic cable, etc…

(v) Protocol : A protocol is a set of rules that govern data communication. It represents an agreement between the communicating devices. Without protocol, two devices may be connected but not communicating.

NETWORKS

A network is set of devices connected by the media links. A node can be a computer, printer or any other device capable of sending or receiving data generated by other nodes on the network.

DISTRUBUTED PROCESSING

Network use distributed processing, in which a task is divided among multiple computers. Instead of a single large machine being responsible for all aspects of a process , each separate computer handles a subset. The advantage of distributed processing are :

(i) Security/Encapsulation : A system designer can limit the kinds of interactions that a give user can have with the entire system. For example, the bank can allow users access to their own accounts through an automated teller machine(ATM). But not allow them to access Bank's entire database.

(ii) Distributed databases : No one system needs to provide storage capacity for the entire database. For example, the world wide web gives users access to information that may be actually stored and manipulated anywhere on the Internet.

(iii)Faster problem solving : Multiple computers working on parts of a problem concurrently often can solve the problem faster than single machine working alone. For example, networks of PCs have broken encryption codes that were supposed to be unbreakable because of the amount of time it would take a single computer to crack them.

(iv)Security through redundancy : Multiple computers running the same program at the same time can provide security through redundancy

(v) Collaborative processing : Both multiple components and multiple users may interact on a task. **For example,** in multiuser network games the actions of each player are visible to and affect all the others.

NETWORK CRITERIA

To be considered effective and efficient, a network must meet a number of criteria. They are (i) Performance, (ii) Reliability, (iii) Security.

PERFORMANCE

The 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 other device. Response time is the elapsed(beyond) time between an inquiry and response. The performance of a network depends on number of factors. That includes the number of users, type of transmission medium, hardware and efficiency of a software. Here define each factors as follows :

(i) Number of Users: Having a large number of concurrent users can slow response time in a network not designed to coordinate heavy traffic loads. The design of a given network is based on an assessment of the average number of users that will be communicating at any one time. In a peak time, the actual number of users exceed the average and decrease the performance

(ii) Type of transmission medium: The medium defines the speed at which data can travel through a connection . Today's networks are moving to faster and faster transmission media like fiber optic cables. A medium that can carry at a at 100 megabits per second is 10 time more than the medium that can carry only 10 megabits per second.

(iii) Hardware : The types of hardware included in a network affect both the speed and capacity of the transmission.

(iv) Software : The software used to process data the sender, receiver and intermediate nodes also affects the network performance. Moving a message from one node to node through a network requires processing to transform the raw data into transmittable signals, and to route these signals to the proper destination. Well designed software can speed the process and make transmission more effective and efficient.

RELIABILITY

The network reliability is measure by frequency of failure, the time it takes a link to recover from failure.

(i) Frequency of failure : All networks fail occasionally. A network that fails often , however, is the little value to a user.

(ii) Recovery time of a network after a failure A network that recovers quickly is more useful than one that does not.

(iii) Catastrophe : Networks must be protected from catastrophic events such as fire, earthquake or theft. One protection against unforeseen damage, is reliable system to back up network software.

SECURITY

The network security issues include protecting data from unauthorized access and viruses. They are defined as follows :

(i) Unauthorized Access : For a network to be useful, data must be protected from unauthorized users. Protection can be accomplished at a number of levels. At the lowest level are user identification codes and passwords. At a higher level are encryption is used.

(ii) Viruses : Network is accessible from many points. Hence it is affected by viruses. A virus is illicitly introduced code that damages the system. A good network is protected form viruses by hardware and software designed for this purpose.

Applications

Network applications in different fields are the following :

(i) Marketing and sales: Computer networks are used extensively in both marketing and sales organizations. **Marketing** professionals use them to collect, exchange, and analyze data relating to customer needs and product development cycles. Sales applications include teleshopping which uses order-**entry computers or telephones which are connected to an order processing network.**

(ii) Financial Services : Financial services today are dependent on computer networks. Applications include credit searches, foreign exchange and investment services. **Other important one is Electronic Funds Transfer(EFT) ,** which allows user to transfer money without going to bank.

(iii) Manufacturing : Computer networks are used in many aspects of manufacturing. It includes manufacturing process. To applications use network to provide essential services are (a) computer assisted design(CAD) and (b) Computer assisted manufacturing.

(iv) Electronic messaging : Most wide used network application is electronic mail.

(v) Directory Services : Directory services allow lists of files to be stored in a central location to speed the search operation.

(vi) Information Services : Network information services include bulletin boards and data banks. The WWW offering technical specification for a new product is a information service.

(vii) Electronic Data Interchange(EDI) : EDI allows business information to be transferred without using paper.

(viii) Teleconferencing : Teleconferencing allows conferences to occur without the participants being in the same place. Applications that includes simple text conferencing, video conferencing , voice conferencing.

(ix) Cellular Telephone : Previous years , two parties wishing to use the services of the telephone company had to be linked by physical connection. But now a days cellular networks make it possible to maintain wireless phone connections even while **travelling over large distances.**

(x) Cable television: Future services provided by cable television networks may include video on request, as well as same information. Financial and communications services currently provided by the telephone networks and computer networks.

PROTOCOL AND STANDARDS

Protocols

In networks communication occurs between entities in different systems. AN entity is anything capable of sending or receiving information. Examples are application programs, file transfer packages, browsers, database management systems, and e-mail software. A system is a physical object that contains one or more entities.

But two entities cannot just send bit streams to each other and expect to be understood. For communication to occur, the entities must agree on a protocol. Protocol is a set of rules that govern data communication. A protocol defines what is communicated, how its communicated, and when its communicated. The key elements of a protocol are ,(i) Syntax, (ii) Semantics and (iii) Timing.

(i) Syntax: The syntax refers to the structure or format of data. The meaning is that the order in which they are presented. For example, simple protocol might expect the first eight bits of data to be address of the sender, the second eight bits to be the address of the receiver. The rest of the stream is message.

(ii) Semantics : It refers to the meaning of the each section of bits. It defines particular pattern to be interpreted and what action is to be taken. For example, does an address identify the route to be taken or the final destination of the message?

(iii) Timing : It refers to two characteristics , that is when data should be sent and how fast they can be sent.

STANDARDS

There are number of factors to synchronize, a great deal of coordination across the nodes of a network is necessary if communication is to occur at all. Standards is one among them. For example automobiles are an example of nonstandardized products. A steering wheel from one make or model of car will not fit into another model without modification.

A standard provides a model for development that makes it possible for a product to work regardless of the manufacturers.

Standards are essential in creating and maintaining an open and competitive market for equipment manufacturers and guaranteeing national and international interoperability of data and telecommunications technology and processes. They provide guidelines to manufacturers, vendors, government agencies , and other service providers to ensure the kind of interconnectivity necessary in today's marketplace and in international communications.

Today's pragmatism(practicality) and consumer pressure have forced the industry to recognize the need for general model and there is growing agreement as to what those models are.

Data communication standards fall into two categories , (i) de facto ,(ii) de jure categories.

(i) De jure standards : The de jure standards are those that have been legislated by an officially recognized body. Standards that have not been approved by an organized body but have been adopted as standards through widespread use are de facto standards. De facto standards are often established originally by manufacturers seeking to define the functionality of new product or technology.

(ii) De facto standards : This standard can be further subdivided into two classes, they are (i) **proprietary and (ii) nonproprietary.** Proprietary standards are those originally invented by a commercial organizations as a basis for the operation its products. They are called as proprietary because they are wholly owned by the company that invented them. These standards are also called closed standards.

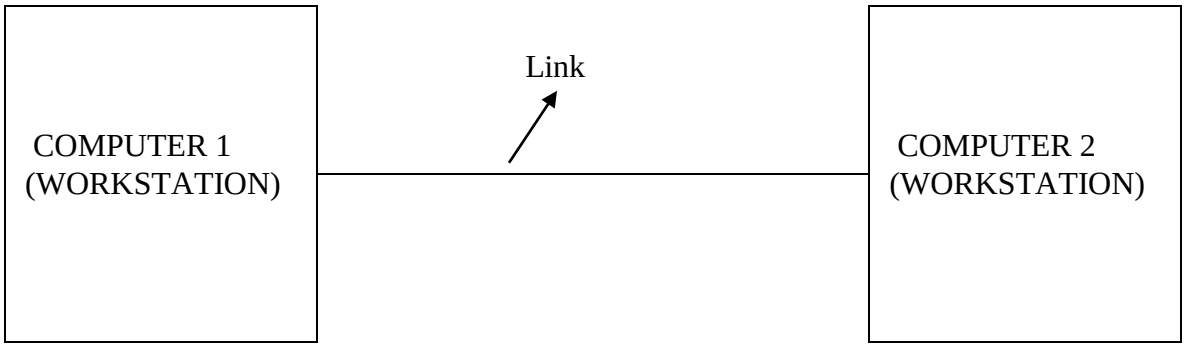
Non proprietary standards are those originally developed by groups or committees that have passed them into the public domain. They are also called open standards. Because they open communication between the different systems.

Line configurations.

The line configuration refers to the way two or more communication devices attach to a link. A link is a physical communication pathway that transfers data from one device to other device. For communication to occur, two devices must be connected in some way to the link at the same time.

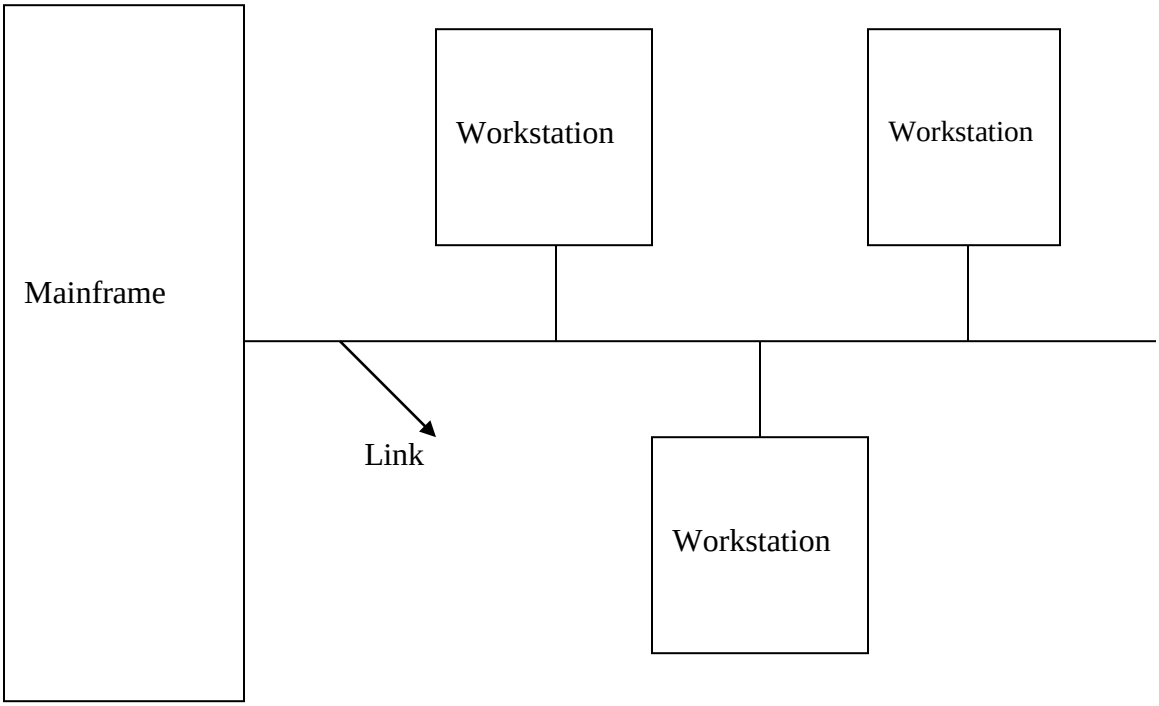
There are two types of line configurations (i) Point-to-point and (ii) Multipoint.

Point-to-point : It provides a dedicated link between two devices. The entire capacity of the channel is reserved for transmission between two devices. Most point-to-point line configurations use actual length of wire or cable to connection two ends.



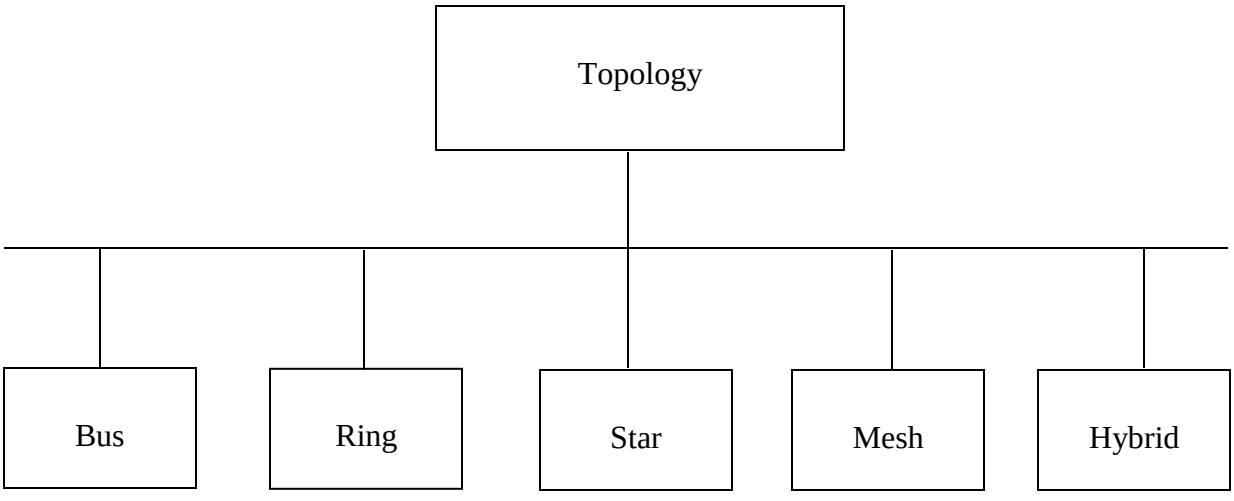
Example is when the user change television channels by infrared remote control, the user are establishing a point to point line configuration between remote control and television control system.

Multipoint : A multipoint is also called a l multidrop is a line configuration is one in which more than two specific devices share a link. In a multipoint environment the capacity of the channel is shared in spatial and temporal manner. If several devices can use a link simultaneously, it is called spatial share and if users must take turns s a time shared line configuration. The following diagram is an example of multidrop.



TOPOLOGY

The term topology refers to the way a network is lid out. It is done through either physically or logically. Two or more devices connected to a link. Then two or more links form a topology. It is defined as the geometric representation of the relationship of all the links and linking devices. There are five types of topologies, they are (i) Bus, (ii) Ring, (iii) Star, (iv) Mesh, (v) Hybrid.

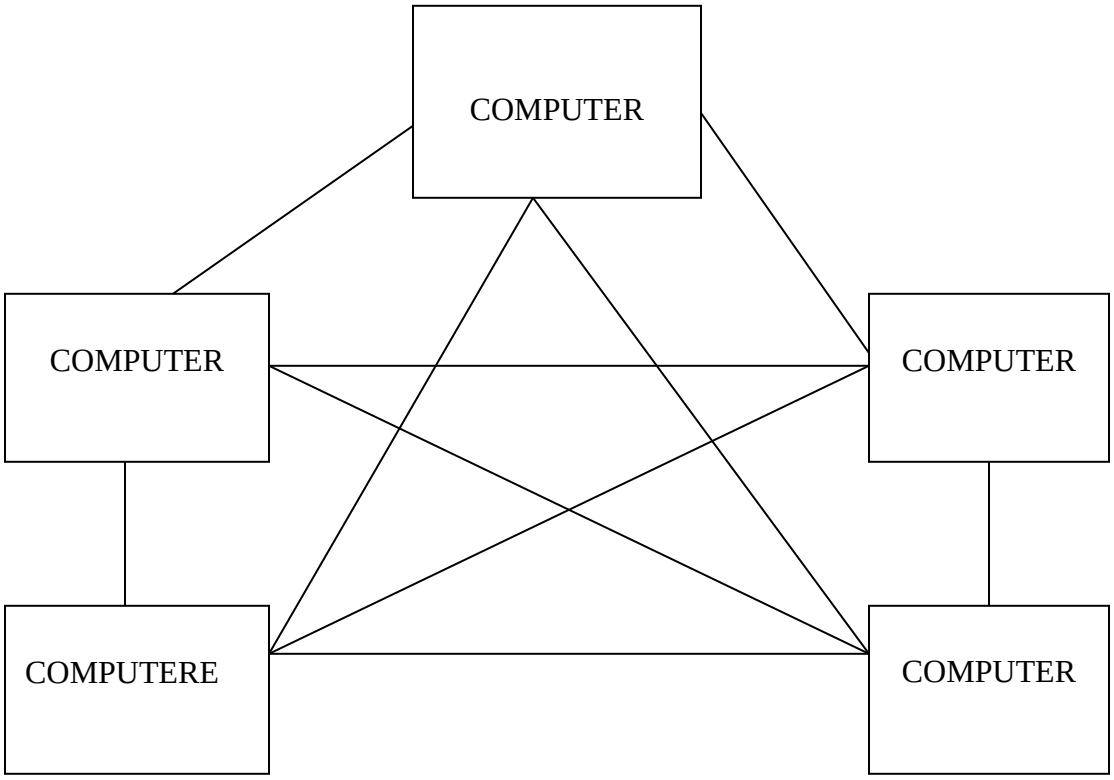


From the above diagram , we have five labels which represents the name of the topology and they describe how the devices in a network are interconnected rather than physical arrangement. In topology we consider the relationship between devices as a link. The two relationships are used, they are (i) Peer-to-peer, (ii) Primary-Secondary.

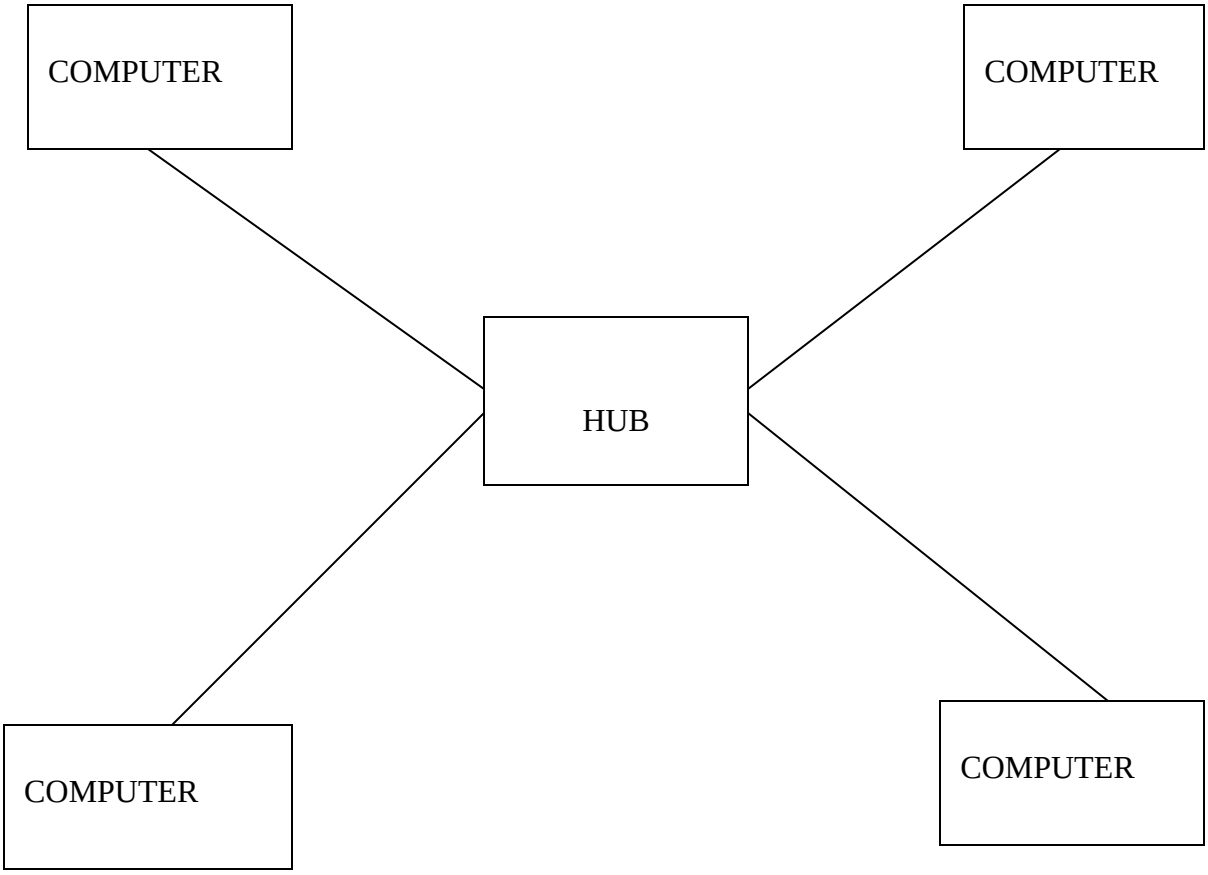
Mesh : In this topology every device has a dedicated point to point link to every other device. The term dedicated is that the link carry traffic only between two devices that it connects. A fully connected mesh network has n(n-1)/2 physical connection. A mesh offers several advantages over other network topologies. The first is the use of dedicated links which guarantees each connection can carry its own data load and eliminate the traffic problem.
The second is it is robust, which means when a link is not used , it cannot participate the entire network system.
The third one is privacy and security. That is when a message is travel along the link , it is going to only the intended receiver. The fourth one is physical boundary which prevents other user can access this network.

The fourth one is point to point link which is easy to found error and find fault isolation.

There are few disadvantages of mesh topology, they are (i) Amount of cabling and number of I/O ports are used. (ii) Device must be connected to every device in the network which causes the configuration to be difficult and difficult to troubleshoot, (iii) Require greater amount of space for wiring , (iv) Hardware required to connect each link , which are expensive. The block diagram of Mesh topology is as shown below :

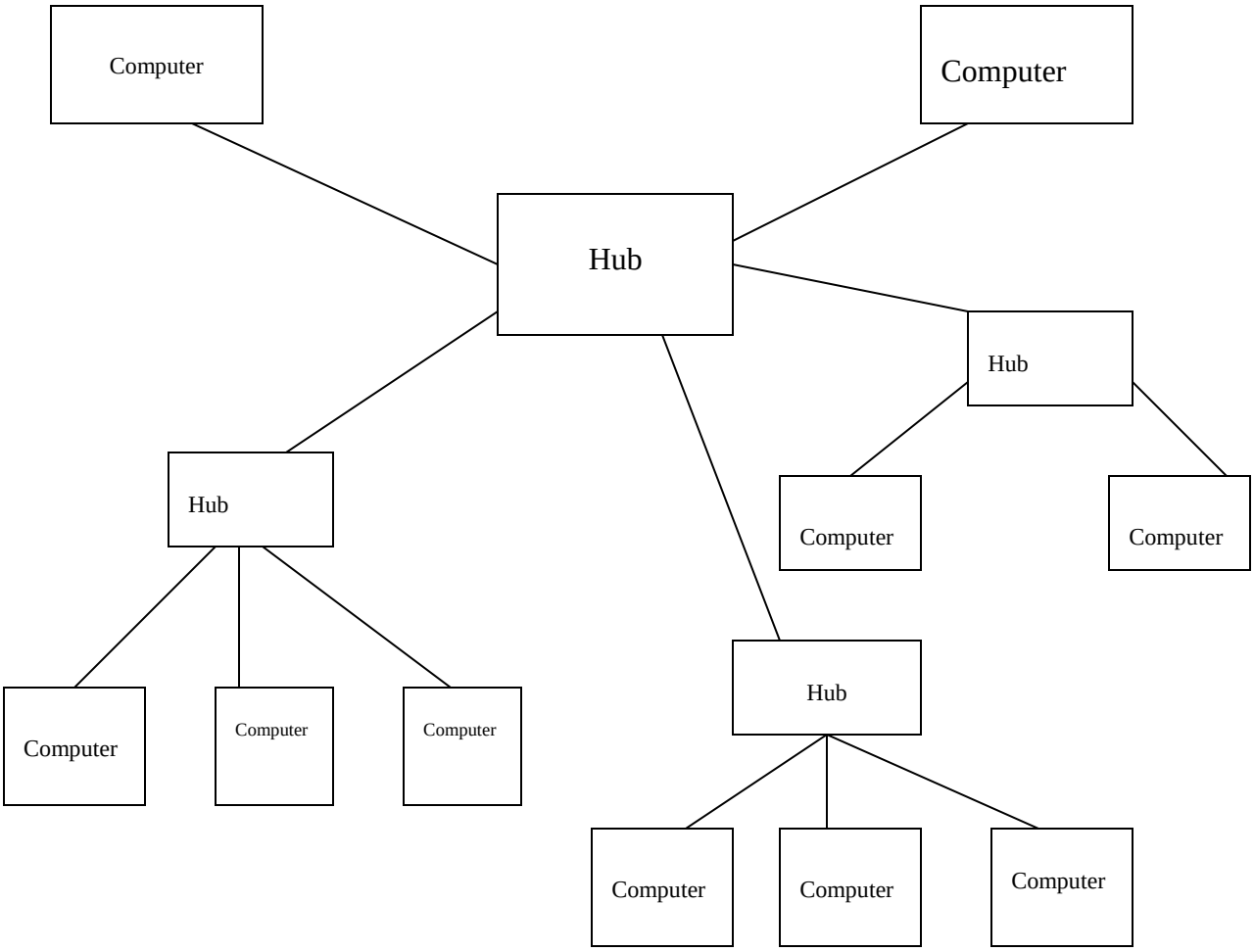


STAR : In a star topology , each device has a dedicated point to point link to the central controller, called HUB. The devices are not directly linked to each other. Unlike the mesh topology , a star topology does not allow direct traffic between devices. The controller acts as the exchanger. For example if the one device want to send data to another, it sends data to the controller. It is less expensive than mesh topology. The advantages are : (i) Each device needs only one link and one I/O port to connect another. (ii) Easy to install and configure, (iii) Require less cable , (iv) Additions, movement, deletions involve only one connection, (v) Robustness, that is if one link fails, only that link is affected, other links are active, (vi) Easy fault identification, (vii) As long as hub is working, it is used to monitor link problems and bypass defective links. The diagram of star topology is as shown below :



TREE : A tree topology is the variation of the star, like star nodes in a tree are linked to central hub that controls the traffic to the network. Here not every device plugs directly into the central hub. The majority of the devices are connect to a secondary jib, which in turn connected to the central Hub. The central hub in the tree is the active hub.

The active hub is acting like repeater, which is to regenerate the received bit patterns. This repeating strengthens transmission and increases the distance the signal can travel. The following diagram shows the structure of Tree topology

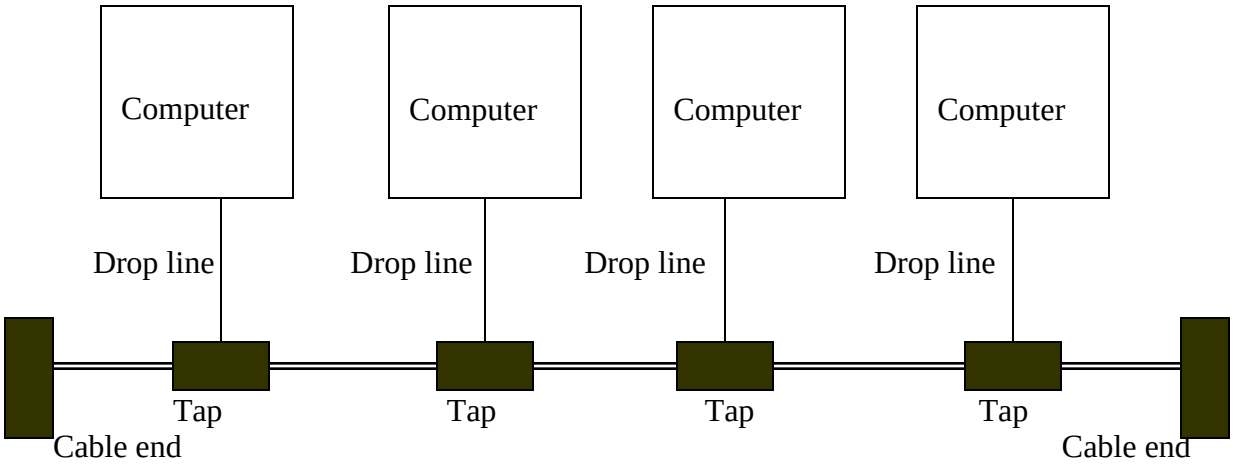


BUS : The above topologies are called as point to point. The Bus topology is a multipoint. Here long cable acts as a backbone to link all devices in the network.

Nodes are connected to the bus cable by drop lines and taps. A drop line is a connection running between the device and main cable. A tap is a connector that splices(join) into main cable or punctures(penetrate) the sheath of the cable to create a contact with a metallic core. The signal travel along the backbone, some of its energy is transmitted into heat. As it travels the signal become weaker and weaker. For this reason there is a number of taps that help to reduce the weaker of signal.

Advantages : (i) Easy installation, (ii) High speed, (iii) Use of backbone cable help the user to extend the bus topology.

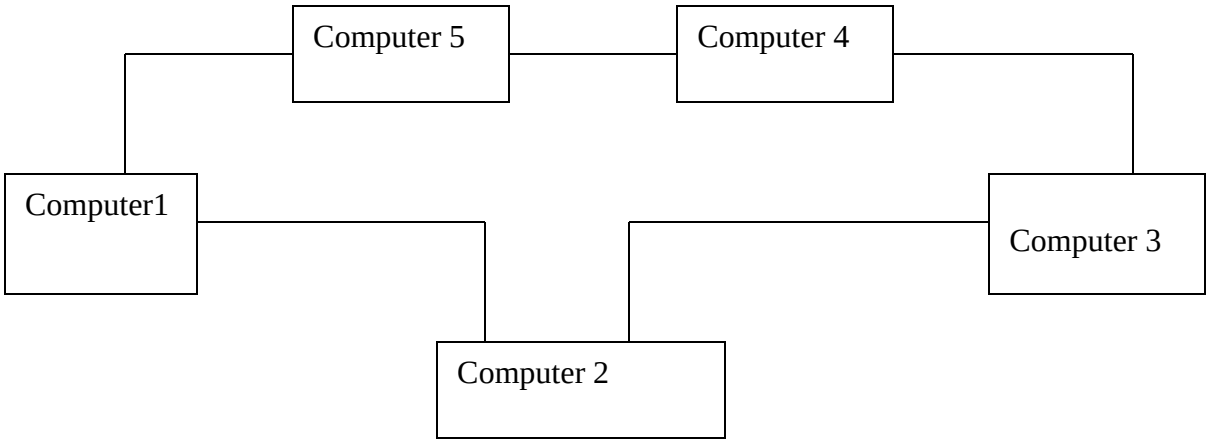
Disadvantages : (i) Difficult to reconfigure, (ii) Fault or break in a bus cable stops all transmission, (iii) A fault in a problem can cause a traffic congestion.



RING : In a ring topology, each device has a dedicated point to point line configuration with two devices or either side of it. A signal is passed along the ring in one direction , from device to device until it reaches the destination. Each device in the ring incorporates as a repeater. When a device receives signal for another device, its repeater regenerates the bits and passes to the other and so on.

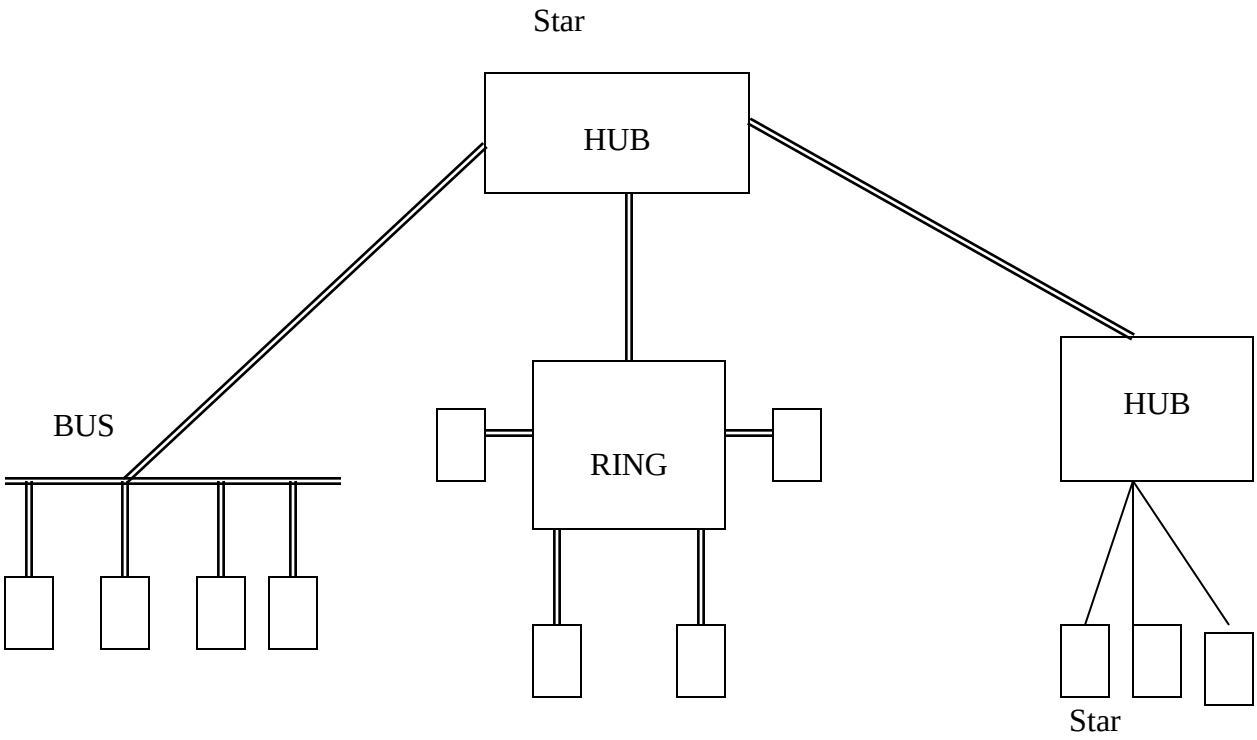
Advantages : (i) Easy to install and configure, (ii) Each device is linked only to its immediate neighbors, (iii) Fault isolation is simple, (iv) If one device does not receive a signal within a specified period, it can issue an alarm, and alerts the network.

Disadvantages : (i) Uniconditional traffic makes it slow process, (ii) Break in a ring can disable the entire network.



Hybrid topologies

Network combines several topologies as subnetworks linked together in a larger topology. For example , one department of a business may have decided to use bus topology while another department has a ring. The two can be connected to each other through central controller like HUB OR SWITCH in a star toplogy.

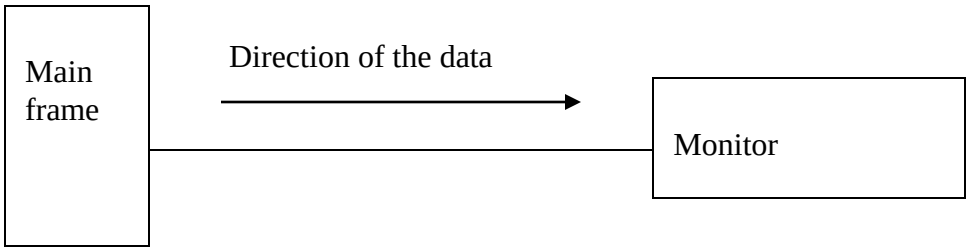


Transmission Mode

Transmission mode is used to define the direction of signal flow between two linked devices. There are three types of transmission modes, they are (i) Simplex, (ii) Half-duplex, (iii) Full-duplex.

Simplex

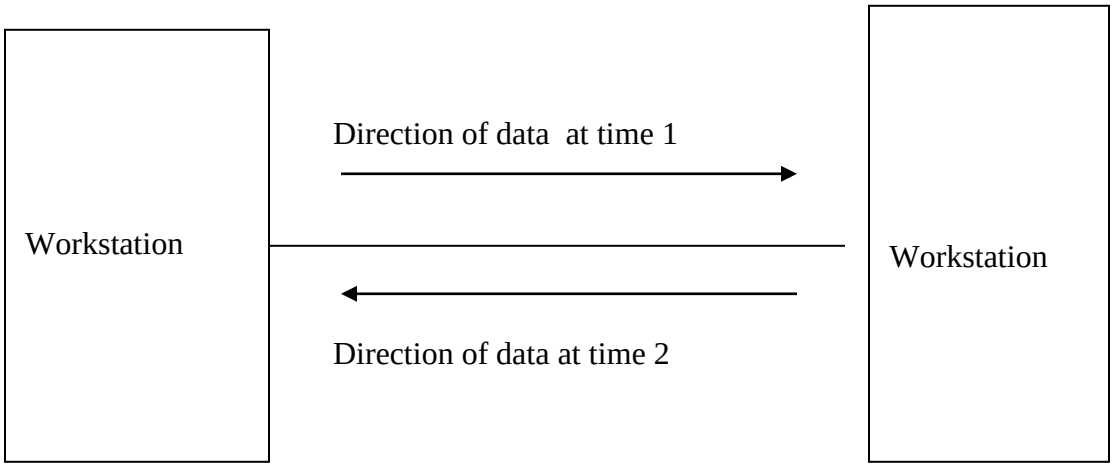
In simplex mode, the communication is unidirectional. It is a one way communication. Only one of the two devices or stations on a link can transmit , other is only receive.



Example of simplex is keyboard and monitor. The keyboard is used to feed the input, and monitor is only to accept the output.

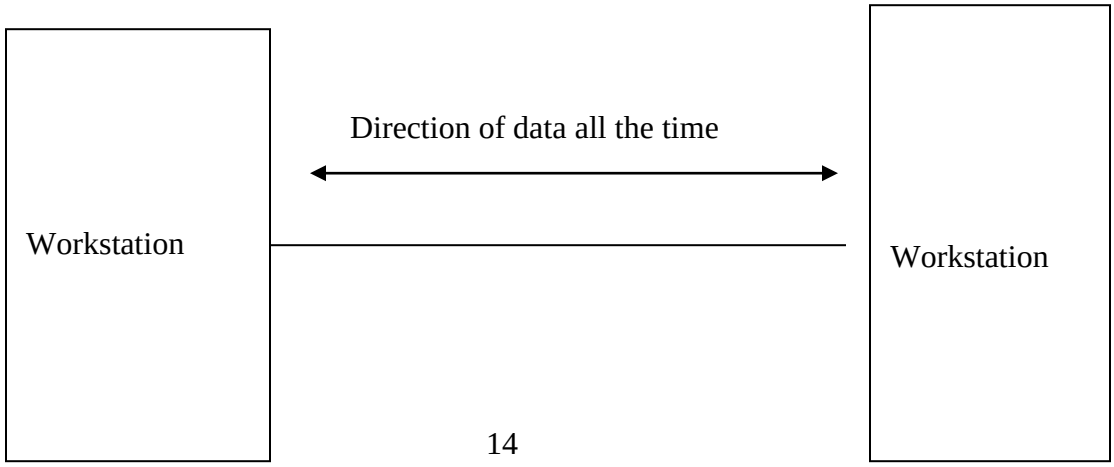
Half-Duplex

Here each station or computer can both transmit and receive , but not at the same time. When one device is sending , the other can only receive.
The example of half-duplex mode is like a one lane road with two directional traffic. When cars are going towards in one direction. The cars from opposite side should wait. Examples of Half-duplex are walkie talkie and citizen band(CB) radio.



Full-Duplex

It is also called duplex, here both systems can transmit and receive simultaneously. The full duplex is a two way street with traffic flowing in both directions at the same time. In a full duplex mode signals can travel in either direction and share the capacity of the link. Example of full duplex mode is a telephone network. When two people are communicating by a telephone line, both can talk and list at the same time. Here is an diagram.



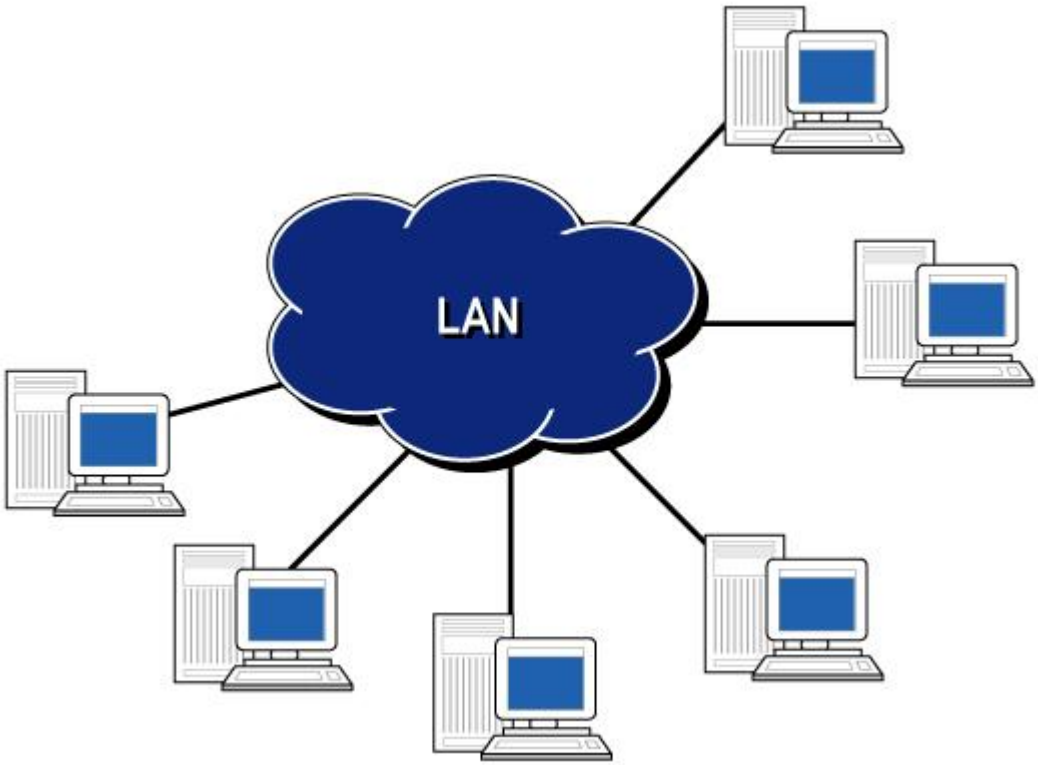
CATEGORIES OF NETWORKS

There are three major categories of networks, they are (i) Local Area Networks, (ii) Metropolitan Area Networks, (iii) Wide Area Networks. These networks can be categorized by its size, ownership, distance and physical architecture.

LOCAL AREA NETWORKS

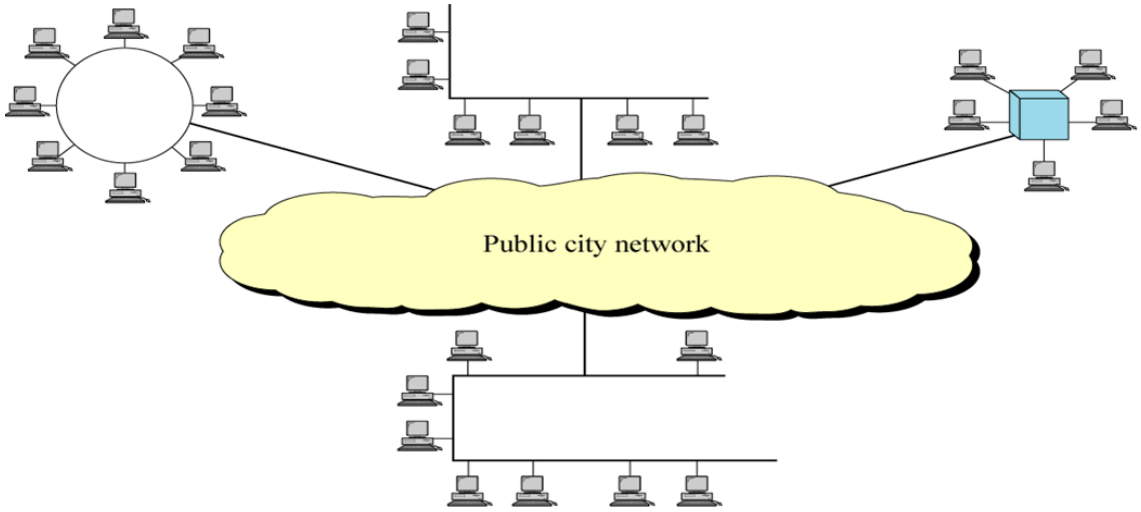
A local area network (LAN) is usually privately owned and links the devices in a single office, building, or campus . Also depend on the needs of an organization and the type of technology used, a LAN can be simple when two PCs and printer is connected in someone office. Nowadays LAN size is limited to few kilometers. LANs are designed to allow the resources to be shared between personal computers or workstations. The resources to be shared can include hardware, software or data. In LAN one of the computer may given a large capacity disk drive and become server to the other clients. Software is stored in this server and used when there is need.

LAN can be distinguished from other networks by its size. LAN uses one type of transmission medium. The most common LAN topologies are Bus, Star, Ring The LAB Speed is about 4 to 16 Mbps. Now it is increased to 100 Mbps



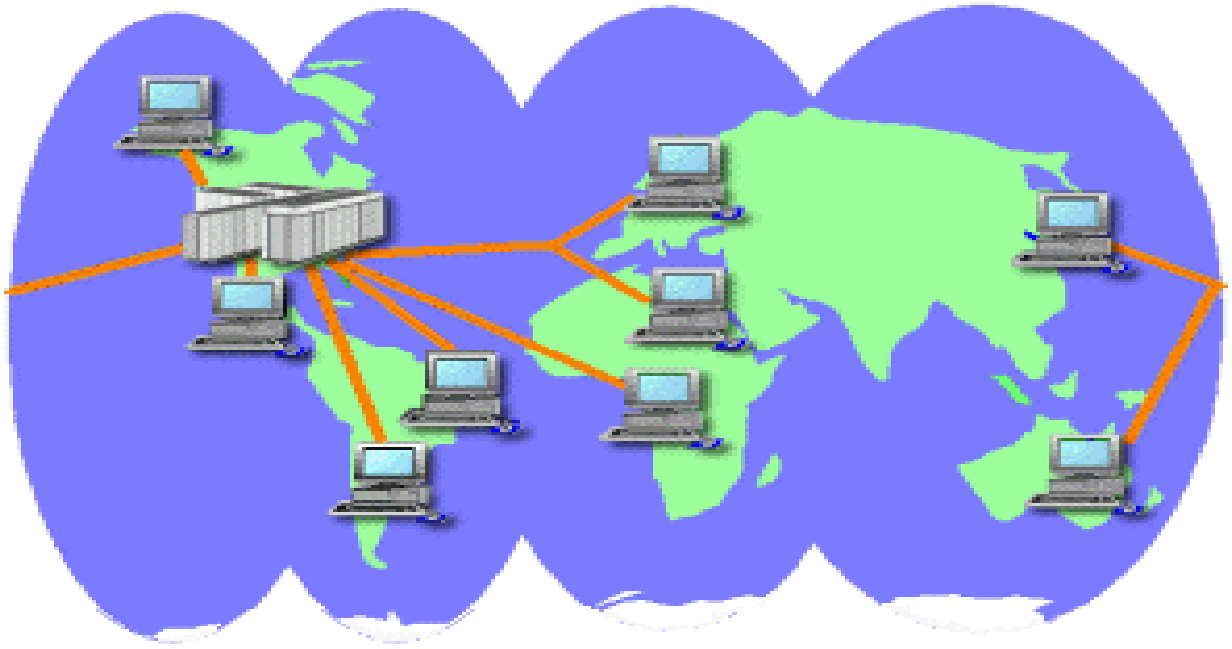
METROPOLITAN AREA NETWORKS(MAN)

A MAN is designed to extend network over the entire city. It may be a single network like cable television network. It is also used to connect number of LANs to form a large network. Example is a company can use a MAN to connect the LANs in all of its offices around the city. MAN can be owned by a private company. Many telephone companies provide a popular MAN service called Switched multi mega bit Data Services called SMDS. The example diagram of MAN is as shown below.



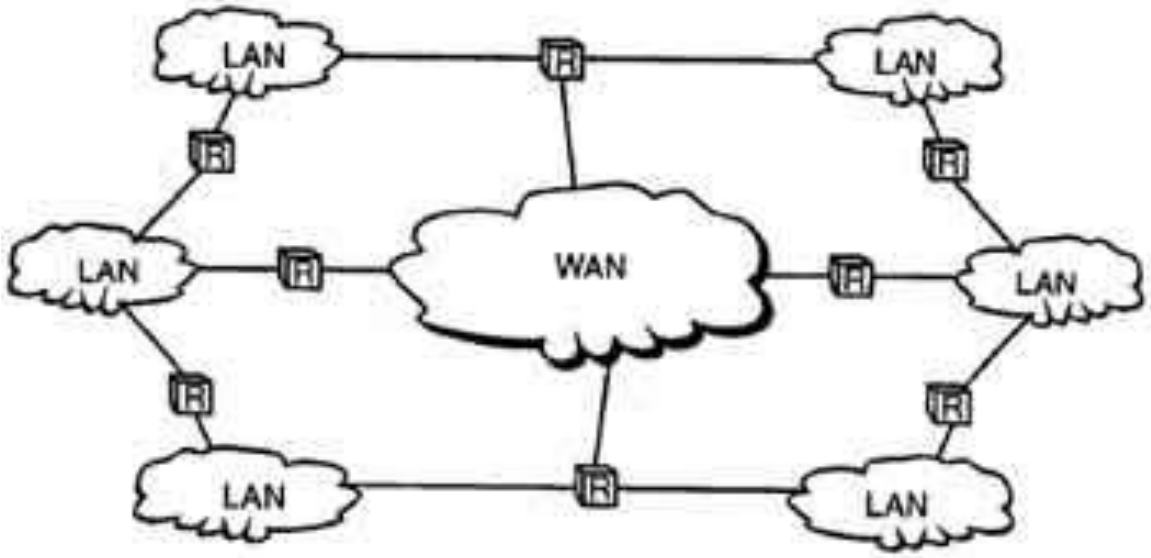
WIDE AREA NETWORKS(WAN)

WAN provides a long distance transmission of data. It is used for data , voice, audio and video information over large geographical areas that comprises a country or around the world. Compare to LAN, WANs may utilize public, leased or private communication devices, or combinations of all the devices. Therefore WAN can span over unlimited number of miles. WAN is maintained by single company and referred as enterprise network. The following diagram shows the example of WAN.



INTERNETWORKS

When two or more networks are connected they become internetwork, or internet. The following diagram is an example of Internetworks. In this diagram R represents routers. Here individual networks are joined into internetworks by the use of internetworking devices. The devices include routers, and gateways. There are two terms used in INTERNETWORKS, they are internet, Internet. The internet is a term which is mean for interconnection of Networks. The Internet is second term which is a world wide network. The following diagram is an example of INTERNETWORKS.



Internetwork

THE OSI MODEL

In 1947 , the International Standards Organization(ISO) is dedicated to worldwide agreement on international standards. The ISO covers all aspects of network communications which is the Open systems Interconnection(OSI) . The open system is a model that allows two different systems to communicate with different architecture. The purpose of OSI model is open communication between different systems without requiring changes to the logic of hardware and software.

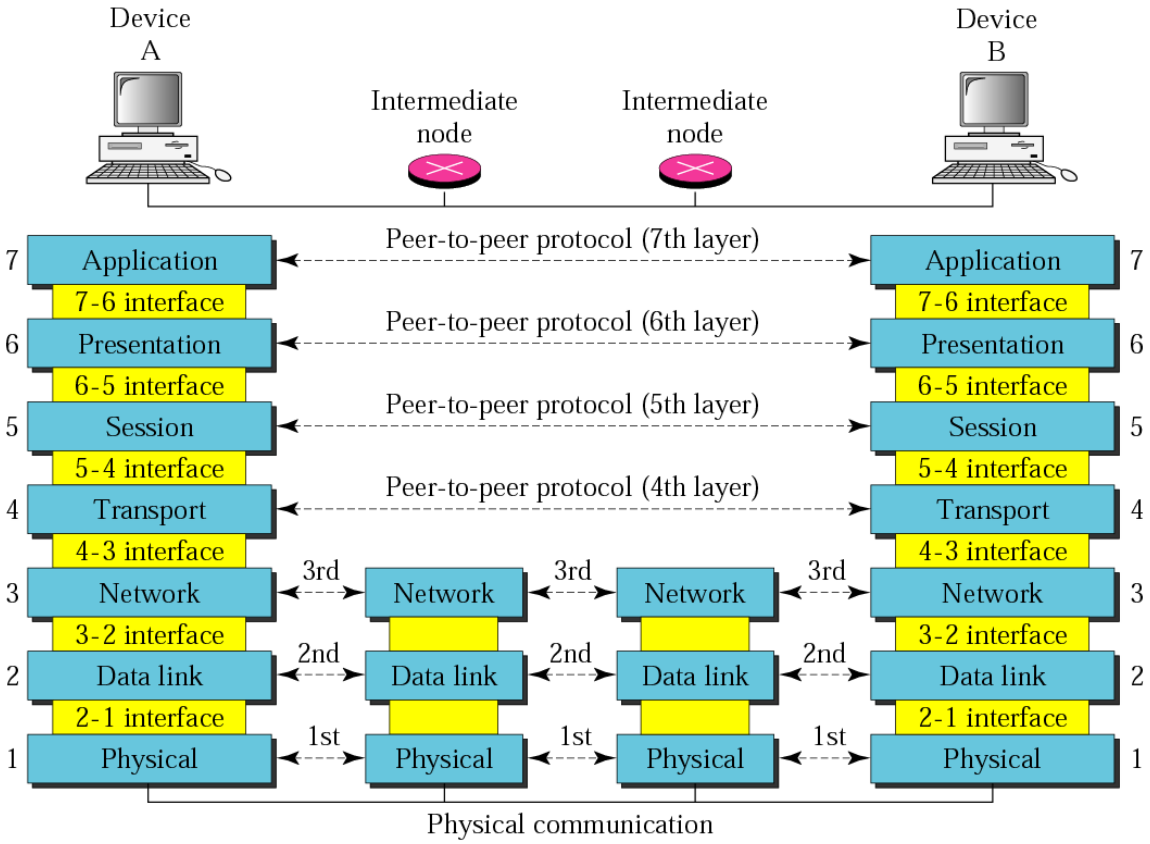
The Open systems Interconnection model is a layered network for the design of network systems that allows for communication across all types of computer systems. It consist seven separate layers , each layer has different functions which helps the data to be moving across the network.

Layered Architecture

The OSI model consists of seven layers, they are (i) Physical layer, (ii) Data link layer, (iii) Network layer, (iv) Transport layer, (v) Session layer, (vi) Presentation layer, (vii) Application layer. The following diagram shows the message is sent from device A to device B.

Peer to Peer process

With in a single machine each layer calls upon the services of the layer just below it. For example Layer 3 uses services provided by the layer 2 and provides services for layer 4. Between machines , the layer x on one machine communicates layer x on another machine. This communication is checked by the agreed upon series of rules called protocols. The process on each machine that communicate at a given layer is called as peer-to-peer processes. Hence communication between machines is a peer to peer process using the protocols.



Functions of the Layers

1. PHYSICAL LAYER : The Physical layer combines the functions required to transmit a bit stream over a physical medium. It deals with electrical and mechanical specifications. It also defines the procedures and functions that physical devices and interfaces have to perform the transmission to occur.

The functions of physical layers are

(i) Physical characteristics of interfaces and media : That is the physical layer defines the characteristics of the interface between the devices and the transmission medium. It defines the types of transmission medium.
(ii) Representation of bits : The physical layer data consist of stream bits without any interpretation. For transmission , the bits are encoded into signals .
(iii) Data rate: The number of bits sent each second is also defined by the physical layer.

(iv) Synchronization of bits : The sender and receiver must be synchronized at the bit level. That is the sender and receiver clocks must be synchronized.

(v) Line configuration : The physical layer deals with the connection of devices with the medium. For example in a point to point configuration , two devices are connected

together through a dedicated link. But in multipoint configuration, a link is shared between several devices.

(vi) Topology : The topology defines how devices are connected to make a network. There are five different topologies used, they are bus, star, ring, mesh, hybrid.

(vii) Transmission Mode : The physical layer defines the direction of transmission between two devices. There are three transmission modes, they are simplex, half duplex and full duplex.

2.Data Link Layer

The data link layer transforms the physical layer a raw transmission facility , reliable link and is responsible for node to node delivery. It makes the physical layer to become error free.

The responsibilities of data link layer are

- **(i)** **Framing : The** data link layer divides the stream of bits received from network layer into manageable data units called frames.
- **(ii)** **Physical Addressing :** The frames are to be distributed to different systems on the network. The data link layer adds a header to the frame to define the physical address of the sender that is source address and the receiver that is destination address of the frame.
- **(iii)** **Flow Control :** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, is done by flow control mechanism.
- **(iv)** **Error control :** The data link layer provides another mechanism called error control , which is used to detect and retransmit damaged or lost frames. It is also used to avoid duplication frames.
- **(v)** **Access Control :** When two or more devices are connected to the same link, the data link layer protocols are used to determine which device has control over the link.

1. Network Layer

The network layer is responsible for source to destination delivery of a packet across the networks. The network layer provides each packet is send to the correct destination. When two computers are connected in a link , there is no need of network layer. But if there are computers which are attached to different networks then there is need of network layer which provides the source to destination delivery. There are two important functions of network layer , they are :

(i) Logical Addressing : The physical addressing implemented by a data link layer handles the addressing problem. Suppose if a packet passes to the network boundary, the ser needs the another addressing system to help to distinguish between source and destination systems. Hence the network layer adds a header to the packet coming from the upper layer . This addition includes the logical address.

(ii) Routing : It is used when independent networks or links are connected together to create an internetwork. It is done by the device like the router.

2. **Transport Layer : The** transport layer is responsible for source to destination and end to end delivery of the message. The network layer sees the packets individually and does not recognize the relationship between these packets. But transport layer on the other hand ensures these packets as combined one by using different techniques like error control , flow control . It is a mid layer which connects upper layers with lower layers. There are various services provided by transport layer.

   (i) Service Point Addressing : Computers run several programs at the same time. For this reason source to destination delivery means delivery not only from one computer to another computer but also from a specific process on one computer to specific process on another computer. The specific process is nothing but a running program on a computer. To achieve this the transport layer provides service point address. That is the network layer gets each packet to the correct computer, but with the help of service packet addressing the transport layer gets the entire message to the correct process on that computer.

   (ii) Segmentation and Reassembly : A message is divided into different segments each segment contains a sequence number. These numbers help the transport layer to reassemble the message correctly upon the arriving at the destination.

   (iii) Connection Control : The transport layer can be considered as connection oriented service or connectionless oriented service. A connectionless transport layer treats each segment as an independent packet and delivers to the destination machine. A connection oriented transport layer makes a connection with transport layer. After the packets are delivered to the destination, the connection is terminated.

   (iv) Flow Control : The flow control is performed at end to end rather than across a single link.

   (v)**Error control :** The error control is responsible for finding the error in the transmission, finding the duplication packet, finding the damage and finding the loss.

5. Session Layer : The services provided by the session layer is the dialog control. It establishes , maintains, and synchronizes the interaction between the communication systems.

The duties of session layer are

(i) Dialog Control : The dialog control allows the communication between two processes to take place either in half duplex or full duplex mode.
(ii) Synchronization : This process allows the check points into a stream of data. For example, the system is sending a file of 2000 pages, it is available to add check points after every 100 pages to ensure that each 100 page unit is received and acknowledge independently . Suppose if there is a crash happens at the 125 page , the synchronization allows to resend the pages from page 101.

6.Presentation Layer

The Presentation layer allows syntax and semantics of the information exchange between two systems. Its duties are
(i) Translation : For example the running programs in two systems are usually exchanging the information in the form of character strings, numbers etcc.. The information should be changed into bit streams before being transmitted . But different computers use different encoding systems, the presentation layer is responsible for interoperability between two systems .
(ii) Encryption: To send the sensitive information, a system is able to assure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting information into the network. Decryption is the reverse process.
(iii) Compression : The data compression reduces the number of bits to be transmitted. It is used when we send information like text, audio and video.

7.Application Layer

The Application layer enables the user , whether human or software to access the network. It provides the user interfaces and support for services , like electronic mail, remote access and transfer, shared database management etc… Its duties are :

(i) Network Virtual Terminal : It is a software that allows a user to login onto the remote host. To do this, the application creates a software emulation of a terminal at the remote host. The user computer talks to the software terminal, which in turn talk to the host.
(ii) File Transfer , Access, and Management(FTAM) : This application allows a user to access files in a remote computer and to retrieve files from a remote computer.
(iii) Mail Services : This provides the E-mail service , forwarding and storage.
(iv) Directory Services : It provides the distributed database sources and access for global information about various objects and services.