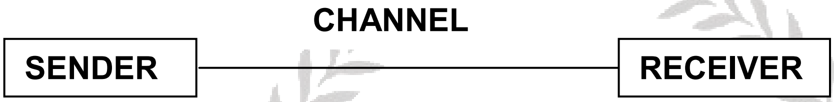
DATA COMMUNICATIONS

The fundamental purpose of data communications is to exchange information between two agents. In other words, we can say that transfer of information or data from one point to another is called data communications. The term data communications can generally be defined as the movement of encoded information by means of electrical transmission systems. It is used to reduce the time required to transmission systems. It is used to reduce the time required to transfer data from a point of origin to the computer and from the computer to point of use.

Elements of data communications

There are three elements of data communications. These are:



SENDER: A device used to send the data or message.

CHANNEL: A medium over which the data is sent.

RECEIVER: A device to receive the data or message.

In other words, it is the physical path between transmitter and receiver in a data transmission system.

When you sending a letter to your friend then you are the sender, your friend is the receiver and the postal service is the medium. Another example is, if you are receiving a telephone call from your friend then your friend is the sender, you are the receiver and the telephone line is the medium.

Types of Data Communications:

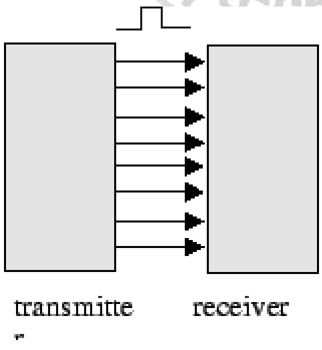
There are two types of data communications, these are:

Serial Communication:

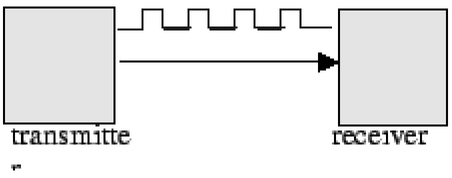
In this type of communication all data is transmitted in a single line in a certain order. This is the slow communication method i.e. one bit at a time, for example, keyboard, mouse.

Parallel Communication:

In this communication data in the form of groups is transmitted i.e. in the form of byte or word at a time. This is the fast method of communication. E.g. Printer, Scanner etc.



Parallel interface transmits all bits in parallel



Serial interface transmits a series of bits

DATA TRANSMISSION MODES

There are 3 modes or ways of or transmitting data.

SIMPLEX TRANSMISSION

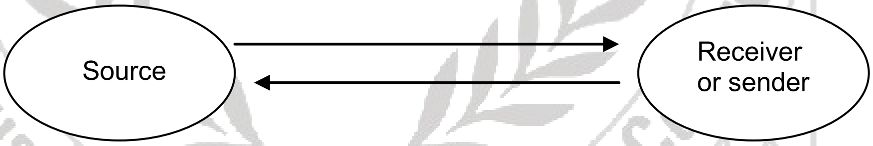
A simplex transmission channel transmits in one direction only. It does not allow an interchange between the message source and the receiver e.g. telegraphs systems.

A terminal connected to such a circuit is either a send only or a receive only device.

The direction may be from the processor to an I/O device, or it may be from a terminal to a processor.
In simplex operation, a network cable or communications channel can only send information in one direction; it's a “one-way street”. This may seem counter-intuitive: what's the point of communications that only travel in one direction? In fact, there are at least two different places where simplex operation is encountered in modern networking. The first is when two distinct channels are used for communication: one transmits from *A* to *B* and the other from *B* to *A*. This is surprisingly common, even though not always obvious. Simplex operation is also used in special types of technologies, especially ones that are asymmetric. For example, one type of satellite Internet access sends data over the satellite only for downloads, while a regular dial-up modem is used for upload to the service provider. In this case, both the satellite link and the dial-up connection are operating in a simplex mode.

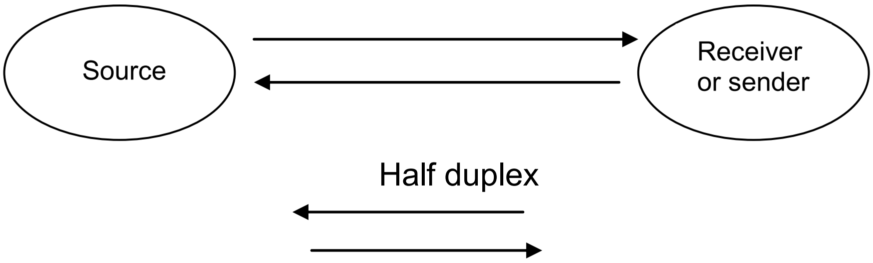
DUPLEX TRANSMISSION:

In this type of communication, the information is transmitted in bi-direction way. Duplex mode is further divided into two types i.e.
Technologies that employ half-duplex operation are capable of sending information in both directions between two nodes, but only one direction or the other can be utilized at a time. This is a fairly common mode of operation when there is only a single network medium (cable, radio frequency and so forth) between devices.
While this term is often used to describe the behavior of a pair of devices, it can more generally refer to any number of connected devices that take turns transmitting. For example, in conventional Ethernet networks, any device can transmit, but only one may do so at a time. For this reason, regular (unswitched) Ethernet networks are often said to be “half-duplex”, even though it may seem strange to describe a LAN that way.



1. HALF DUPLEX TRANSMISSION.

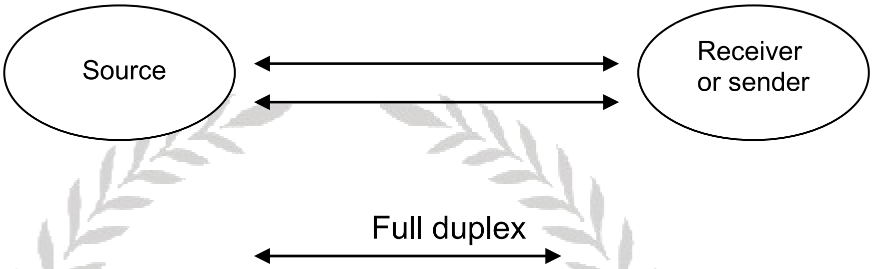
A half duplex channel transmits in either direction, but in one direction at a time.
In full-duplex operation, a connection between two devices is capable of sending data in both directions simultaneously. Full-duplex channels can be constructed either as a pair of simplex links (as described above) or using one channel designed to permit bidirectional simultaneous transmissions. A full-duplex link can only connect two devices, so many such links are required if multiple devices are to be connected together.



(Alternating b/w sent and receive)

2. FULL DUPLEX TRANSMISSION

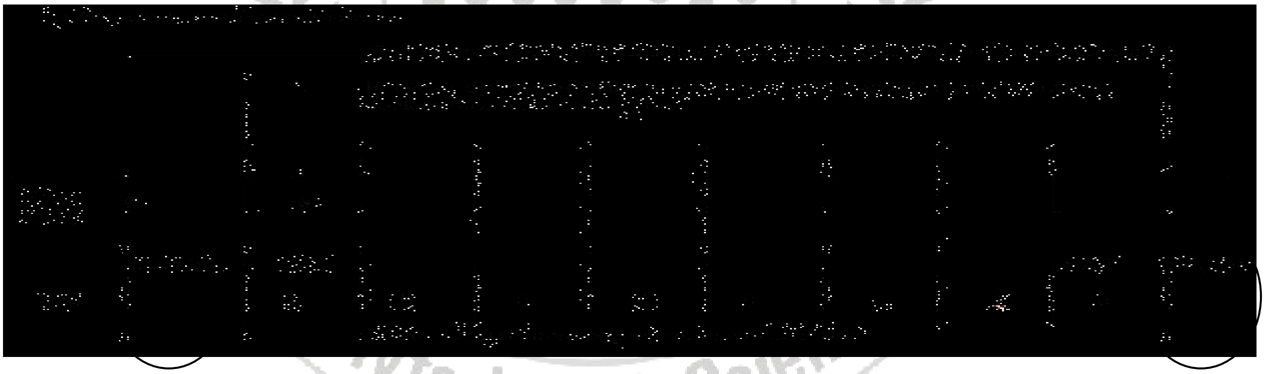
A full duplex system transmits both directions simultaneously. A full duplex line is faster, since it avoids the delay that occurs in a half duplex circuit each time the direction of transmission is changed. In full-duplex operation, a connection between two devices is capable of sending data in both directions simultaneously. Full-duplex channels can be constructed either as a pair of simplex links (as described above) or using one channel designed to permit bidirectional simultaneous transmissions. A full-duplex link can only connect two devices, so many such links are required if multiple devices are to be connected together.



TYPES OF SERIAL TRANSMISSION

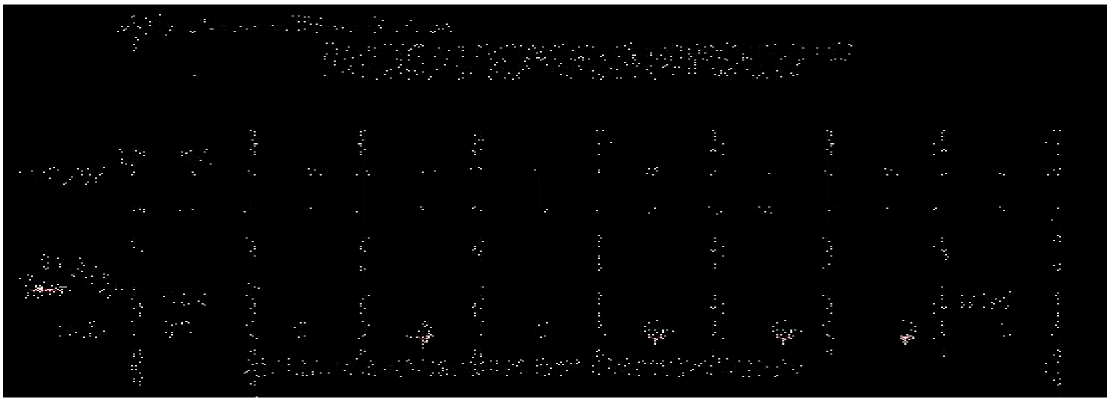
ASYNCHRONOUS

Data are transferred at irregular intervals. Star/stop bits are appended to the beginning and end of the data transmitted. It is used primarily for low speed data transmission. The star/stop bits signal the receiving station about the starting and ending the message. Data can be a single character or a string of characters. Low speed I/O devices and serial printers are the examples..



SYNCHRONOUS

It permits the source and destination to communicate in time synchronization, for high-speed data transmission. Start/stop bits are not used in this mode of transmission. Computers and front-end processors are its examples.

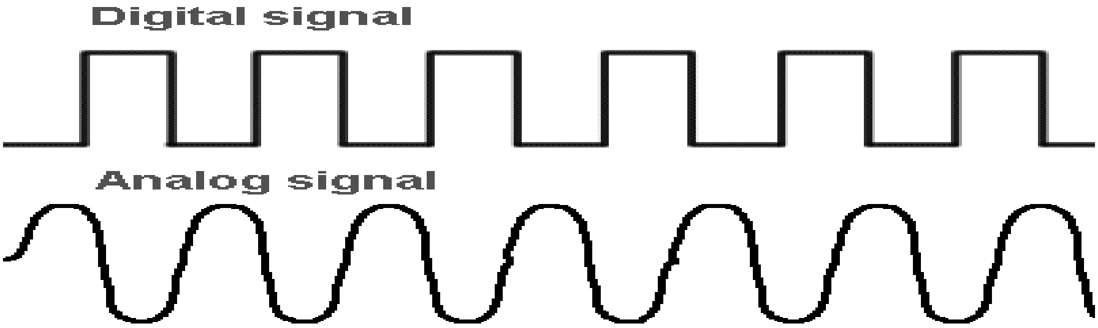


SIGNALS:

All the data or messages are transmitted from one point to another in one of the two forms:

- Analog signals:

These are continuous electrical waves. The telephone line transmits an analog signal rather than a signal. The sound waves are converted into electronic waves that represent the actual data being transmitted.



- Digital Signals:

These are discrete signals of binary form i.e. on or off. Most computers are digital in nature, representing data as patterns of binary numbers. Digital data transmission is better than analog transmission.

Types of Communication according to Bandwidth:

1. Narrow Band:

It transmits data at a low baud rate range of 45-300. Telegraphic systems and low speed terminals are the examples of narrow band communication.

2. Voice Band:

It transmits data at a moderate baud rate of 9600. Fax machine works on voice band systems. It sends a business copy from one location to another in 3-6 minutes. It is also used for transmitting data from card reader to processor and from processor to printer.

3. Broad Band:

It transmits data at a very high baud rate of 1 million. Microwave communications system operate in broad band channels. The speed of transmission is limited by the width of the band and the type of the equipment used.

What is computer network? What are advantages and disadvantages of computer networks?

When two or more than two computers are connected together for the purpose of sharing

- Hardware resources
- Software resources
- Communication

Is called computer network.

A **computer network**, often simply referred to as a network, is a group of computers and devices interconnected by communications channels that facilitate communications among users and allows users to share resources. A network consists of two or more computers that are linked in order to share resources (such as printers and CD-ROMs), exchange files, or allow electronic communications. The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams. Networks may be classified according to a wide variety of characteristics.

ADVANTAGES OF NETWORK

Hardware Sharing

- Hard disk
- Cd rom
- DVD
- Floppy
- Scanner
- Modem
- Flash memory
- Tape drive

Software Sharing:

Expensive soft can be shared over the network, like games, databases and other commercial soft wares which automatically minimizes the cost of soft wares.

Speed. Sharing and transferring files within Networks are very rapid. Thus saving time, while maintaining the integrity of the file.

Cost. Individually licensed copies of many popular software programs can be costly. Network able versions are available at considerable savings. Shared programs, on a network allows for easier upgrading of the program on one single file server, instead of upgrading individual workstations.

Security. Sensitive files and programs on a network are passwords protected (established for specific directories to restrict access to authorized users) or designated as "copy inhibit," so that you do not have to worry about illegal copying of programs.

Centralized Software Management. Software can be loaded on one computer (the file server) eliminating that need to spend time and energy installing updates and tracking files on independent computers throughout the building.

Resource Sharing. Resources such as, printers, fax machines and modems can be shared.

Electronic Mail. E-mail aids in personal and professional communication. Electronic mail on a LAN can enable staff to communicate within the building having tot to leave their desk.

Flexible Access. Access their files from computers throughout the firm.

Workgroup Computing. Workgroup software (such as Microsoft BackOffice) allows many users to work on a document or project concurrently.

Communication: internet, chats, software downloads, uploads and many other activities.

DISADVANTAGES OF NETWORK

- Server faults stop applications being available
- Network faults can cause loss of data.
- Network fault could lead to loss of resources
- User work dependent upon network
- System open to hackers
- Decisions tend to become centralized
- Could become inefficient
- Could degrade in performance
- Resources could be located too far from users
- Network management can become dif

TYPES OF NETWORKS ACCORDING TO SIZE

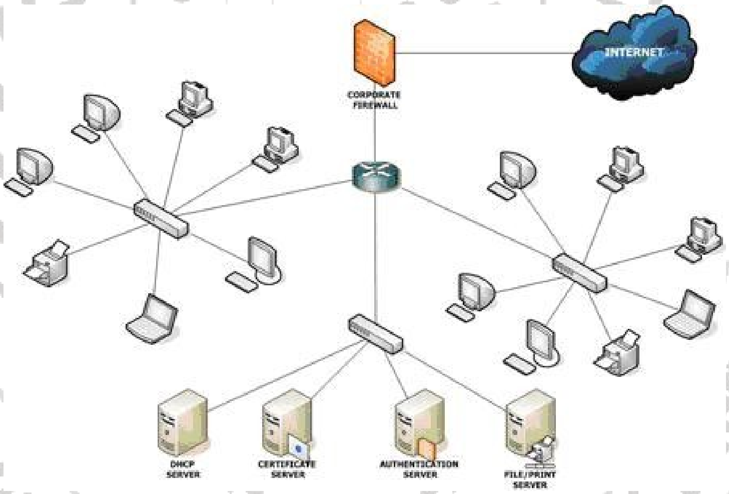
The three basic types of networks include: LAN, MAN and WAN.

LOCAL AREA NETWORK (LAN)

A network is said to be Local Area Network (LAN) if it is confined relatively to a small area. It is generally limited to a building or a geographical area, expanding not more than a mile apart to other computers.

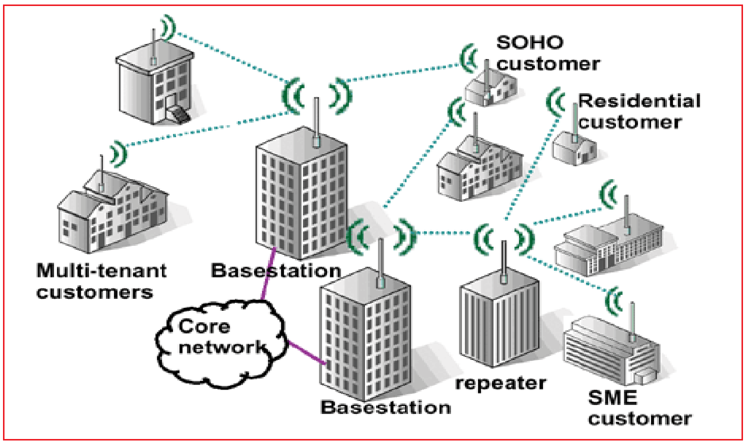
LAN configuration consists of:

- A file server - stores all of the software that controls the network, as well as the software that can be shared by the computers attached to the network.
- A workstation - computers connected to the file server (Mac or PCs). These are less powerful than the file server
- Cables - used to connect the network interface cards in each computer.



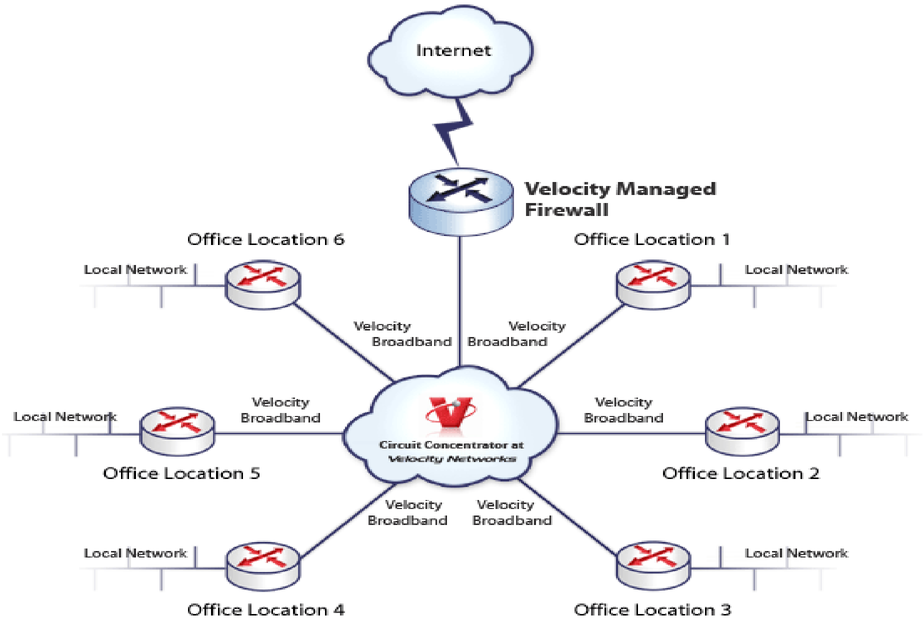
METROPOLITAN AREA NETWORK (MAN)

Metropolitan Area Network (MAN) covers larger geographic areas, such as cities. Often used by local libraries and government agencies often to connect to citizens and private industries.



WIDE AREA NETWORK (WAN)

Wide Area Networks (WANs) connect larger geographic areas, such as London, the UK, or the world. In this type of network dedicated transoceanic cabling or satellite uplinks may be used.



Types of networks according to security:

- Peer to Peer Network
  - Is that type of network which doesn't have central server to control and provide administration to the client computers? It is simple to make, have no security and used in less secure and small organizations.
- Server based network
  - Is that type of network which has a central server called domain controller to manage and provide central administration to the whole network. It is expensive, secure and used in large organizations.

Role of computer in a network:

Server: It is a computer which provides services and administration to the rest of computers in a network called clients.

Client: A computer which use services provided by the server

Peer: A computer which is itself a server as well as client.

The advantages and disadvantages of a peer-to-peer network are as follows:

Advantages:

- It is easy to install.
- Configuration of computers is easy.
- Users can control their shared resources.
- The cost and operation of this network is less.
- It is ideal for small businesses having ten or fewer computers.
- It needs an operating system and a few cables to get connected.
- A full time network administrator is not required.

Disadvantages:

- A computer can be accessed anytime.
- Network security has to be applied to each computer separately.
- Backup has to be performed on each computer separately.
- No centralized server is available to manage and control the access of data.
- Users have to use separate passwords on each computer in the network.

Server Based Network:

Whenever the number of computers in networks becomes more than fifteen you should use a server-based environment because it becomes almost impossible for peer-to-peer networks to handle such computing. In the centralized or server-based system the clients connect to the central computer for one or more services. Almost all processing is done on the server. This helps in the synchronizing the data as every one accesses and manipulates the data that is stored in a centralized location.

Maintaining security in a server based networks much easier than that in a peer-to-peer network as the only system whose security matters is the server. You only need to maintain the security of the data and other resources of the server. In a server-based environment accounts for different users are created and maintained on the server and only those users are granted the access whose details match the details specified in the corresponding account. Different rights are assigned to different users such as whether this particular user has the right to print the data, whether some user has the right to open some particular file etc. The management of such types of rights is easy in centralized networks because the whole administration revolves around the server.

It also reduces the overall cost of the system because most of the cost as you has to spend on one system that needs more resources and also need administration and on the other hand the client systems can be dump terminal or they can have very low processing power. This makes the server based network cost efficient.

Advantages of server based networks.

(1) In sever based networks users can share equipments like laser printers.

(2) Management of users becomes very easy in server based network because you can manage all users from a single computer (server).

(3) All the data stored on central storage device so it becomes easier to backup data.

(4) Security is one of the main issues when we talk about server based networks. In server based network (environment) security is very easy to manage because one server has to make policies and it applies on all the users in network.

(5) Backup of all the data is very easy to perform in server based networks as you just have to make schedule and server automatically makes backup according to the schedule.

(6) A server based network has the power of managing thousands of users. You cannot do this thing in peer to peer networks. Actually if there are ten computers and some of them are clients and some are

servers then it is impossible to manage them in peer to peer network. You have to use server based network.

(7) If you central data storage fails then you can restore by using backup.

Disadvantages of server based network:

- It is expensive
- Needs network administrator
- Whole network goes down if central server is not working
- Difficult to manage and create

Types of Servers:

What is a server?

A server such as an email server is a computer or device on a network that manages network resources, such as printers, database, files, web site, application, and many other resources that users need to access in a common way.

Servers are minicomputers that offer better performance, and larger in size than workstation. However the cost of a server is more than a workstation. Normally servers are designed to support multiple users at a time.

Servers possess larger storage capacities and have a higher processing power than workstation. They support faster peripheral devices, such as high speed printers that can print hundreds of lines per minute.

FILE SERVER: A file server is a dedicated computer in a network that is used to store the files such as word processing documents, spreadsheets, financial data and other useful information. Typically a file server has a large memory and additional hard disks. Server itself and all the client computers stores data on the file server and access it again when required. Additionally, file server software such as Windows 2000 Server, Windows 2003 Server also acts as the logon server and process the logon requests of the client computers.

PRINT SERVER: A print server is a network computer or a specifically designed device to which print devices or printers are attached. A network print server is used to serve the client’s printing requests from all over the network. A Windows 2000 or Windows 2003 computer can serve as a print server. The client computers connect with the print server by using Microsoft Network Printing Protocol.

PROXY SERVER: A network proxy server is an intermediate computer between the client computers in a network and the internet. A proxy server forwards the client’s requests for the specific web pages to the web server. A proxy server when receive the response from the web server (in the form of web pages) it stores a copy of every web page in its cache. So that if next time another client request for the same web page it won’t go to web server for this page, instead it will return the web request from its own cache. A proxy server is software program and when installed on a computer, the computer acts as a proxy server. The most commonly used proxy server programs are WinGate, Win Proxy, and Microsoft ISA Server etc.

WEB SERVER: A web server is a computer that is used to respond the client’s HTTP requests (usually web browsers) and return the response in the form of the web pages, images, voice files, graphics, video clips and others. A single web server is capable to host many websites. Web servers also host shared web based applications and a large number of clients access them simultaneously. Some applications on the web server require some authentication methods such as login name and password. Some dynamics content and applications host on the web server used some related interfaces such as JSP, ASP, PHP, CGI and .NET. HTTPS is used to establish a secure connection between the client and the web server and it is normally used during the credit cards transactions, online shopping where high security is required. A web server is also known as a virtual host when it hosts a large number of the websites on the same IP address.

DATABASE SERVER: There are many database server programs such as Oracle, MySql, and Microsoft Sql 2000. A database server program is used to process the database services. In a client/server networking model, the server component of the database servers (Oracle, MYSQL, and SQL2000) is installed on the server computer and client component of the database program is installed on the client computers in a network. Network distributed applications use database at the backend, which is usually installed on the server computer. In network computing, a database computer should be configured separately and in the enterprise network a large number of the database computers are used, which synchronized with each other.

VIDEO SERVER: A Video server is an online storage computer that is used to provide the video and voice access to the network clients. A video server is used in the broadcast industry, entertainment and in news. A video server also provides online course and lectures to the registered users from all over the world.

STORAGE SERVER: A storage server is high quality and high speed storage device or a computer that is used to store the data of the network applications that are running on the other computers in a network.

TIME SERVER: A time server is a multipurpose, dedicated network computer that is used to compare the time from the atomic clocks and distribute the time among the other network computers. A file server can become a time server by using the NTP (Network time protocol). A NTP is used to synchronizing and distributing the time in a network.

ACCESS SERVER: Access server or Remote Access server is a network device or a computer that is used to access the network by a larger number of the network users. ISP mostly has RAS servers configured and access by a large number of the users.

FAX SERVER: A fax server is software program and when it is installed on a file server, it acts as a Fax server. A fax server is usually a dedicated server attached with a dedicated fax device, fax modem and a telephone line. The fax software receives the fax and converts in the fax form. In the big networks, a fax server can be used as a dedicated computer. There are many only fax services providers like efax.com and upon subscribing to them you can send fax all over the world with a low cost fees

What is Network Topology? What are different network topologies in use? Write their advantages and disadvantages with the help of diagrams.

Network Topology: Topology refers to arrangement of the nodes in the network. Topology is the geometrical representation of linking devices (usually called nodes) to each other in LAN. Possible topologies which are being used are mesh, bus, star, tree and ring. It is the physical layout of computers in a network.

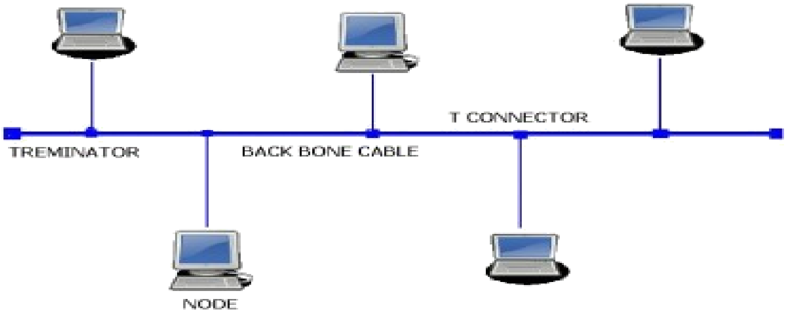
Bus Topology: In such type of topology, long backbone cable is used to link all the devices in the network. Drop lines and taps are used to connect node to this backbone. A drop line is a connection between the node and the Backbone. A tap is the connector.

Advantages:

- Requires less cabling compared to mesh, star and tree topologies.
- Easy to install.

Disadvantages:

- It's Difficult to add new devices.
- Difficult reconfiguration and fault isolation.
- A fault in Backbone stops all transmission, even between devices on the same side of the problem because of noise generated by faulty point.



BUS TOPOLOGY

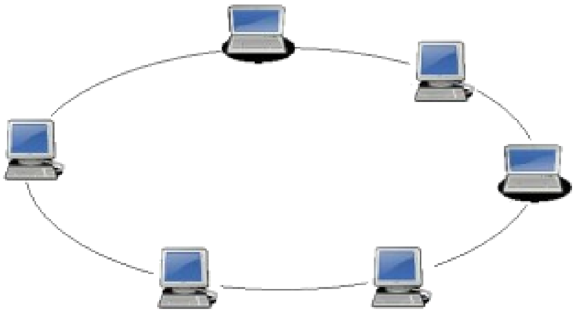
Ring Topology: All nodes are connected in ring structure. Each node contains repeater. A signal passes node to node, until it reaches its destination. If a node receives a signal intended for another node its repeater regenerates the signal and passes it.

Advantages:

- Relatively easy to install and reconfigure.
- Easy to add new node as only two connections need changes.

Disadvantages:

A fault in the ring can disable the entire network. This weakness can be solved by using a dual ring.



RING TOPOLOGY

Mesh topology: In this type of topology, every node has a dedicated point to point link to every other node in the network. This means each link carries traffic only between the two nodes it connects.

- If n is total no of nodes in network
- No. of links to connect these nodes in mesh = N (N-1)/2
- Each node should have (N-1) I/O ports as it require connection to every another node.

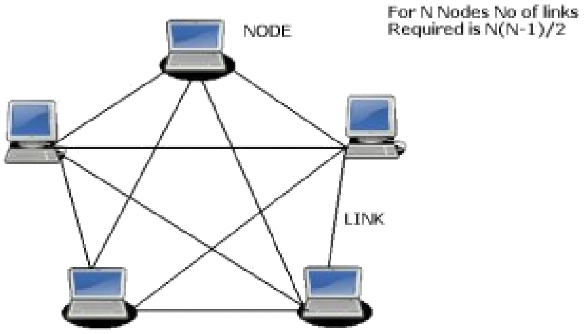
Advantages:

- No traffic problem as there are dedicated links.
- Robust as failure of one link does not affect the entire system.
- Security as data travels along a dedicated line.
- Points to point links make fault identification easy.

Disadvantages:

The hardware is expansive as there is dedicated link for any two nodes and each device should have (n-1) I/O ports.

- There is mesh of wiring which can be difficult to manage.
- Installation is complex as each node is connected to every node.



MESH TOPOLOGY

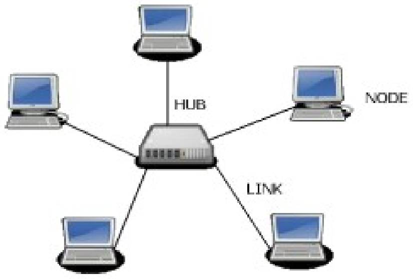
Star Topology: In this type of arrangement, each node has dedicated point to point connection to a central controller hub. As there are no dedicated links between nodes this topology does not allow direct traffic between nodes.

Advantages:

- Star topology is less expensive than a mesh topology as there are no dedicated links between nodes and each device needs only one link and one I/O ports to connect it to any number of nodes.
- Easy to install and make configurations.
- Robust as failure of one link does not affect the entire system. The remaining system will be active.

Disadvantage:

- More cabling is required in a star than in other topologies (except mesh).
- Entire network collapse if central controller fails.
- Other Network related Articles



STAR TOPOLOGY

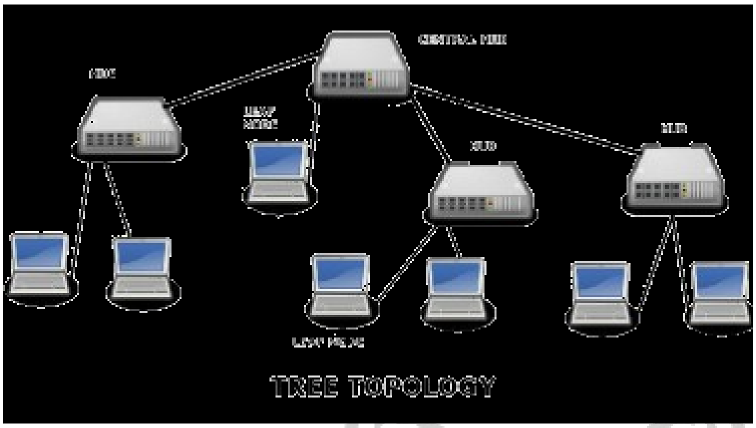
Tree Topology: As its name implies in this topology devices make a Tree structure. This is an advanced version of star topology as central controllers of star topology work as secondary hub. All these Secondary Hubs gets connected to Central hub or Primary Hub that controls the traffic to the network. Most Devices are connected to secondary hubs. The central contains a repeater, which is a hardware device that regenerates the received bit patterns.

Advantages:

- Central hub (repeater) increases the distance a signal can travel between devices.

Disadvantages:

- More cabling is required in a tree than in other topologies (except mesh).
- Entire network collapse if central Hub fails.



What are the factors which should be kept in mind before selection of network media?

1. Attenuation

Attenuation is a general term that refers to any reduction in the strength of a signal. Attenuation occurs with any type of signal, whether digital or analog. Sometimes called *loss*, attenuation is a natural consequence of signal transmission over long distances. The extent of attenuation is usually expressed in units called decibels (dBs).

2. Crosstalk

In electronics, crosstalk (XT) is any phenomenon by which a signal transmitted on one circuit or channel of a transmission system creates an undesired effect in another circuit or channel. Crosstalk is usually caused by undesired capacitive, inductive, or conductive coupling from one circuit, part of a circuit, or channel, to another.

3. EMI

Electromagnetic interference (or **EMI**, also called **radio frequency interference** or **RFI**) is a disturbance that affects an electrical circuit due to either electromagnetic conduction or electromagnetic radiation emitted from an external source. The disturbance may interrupt, obstruct, or otherwise degrade or limit the effective performance of the circuit. The source may be any object, artificial or natural, that carries rapidly changing electrical currents, such as an electrical circuit, the Sun or the Northern Lights.

4. Bandwidth

In computer networking and computer science, **bandwidth, network bandwidth, data bandwidth** or **digital bandwidth**is a bit rate measure of available or consumed data communication resources expressed in bits/second or multiples of it (kilobits/s, megabits/s etc.).

5. Noise

Electronic noise is a random fluctuation in an electrical signal, a characteristic of all electronic circuits. Noise generated by electronic devices varies greatly, as it can be produced by several different effects. Thermal and shot noise are unavoidable and due to the laws of nature, rather than to the device exhibiting them, while other types depend mostly on manufacturing quality and semiconductor defects.

6. Cost

Cost is also the factor involved in choosing network media, cable is a less expensive media as compared to wireless media, and similarly Fiber Optic is one of the most expensive network media in cables.

What is Media and what are the types of Media in Computer Networks?

Media:

1. Bounded

   It is a type of media in which cable are used as a medium of communication.

2. Un bounded

   In unbounded media wireless technologies are used, like

   i. Infrared
   ii. Microwaves
   iii. Radio waves
   iv. Bluetooth
   v. Wi-FI

NETWORK CABLING

There are several types of cable, which are commonly used with LANs. The type of cable chosen for a network is related to the network's topology, protocol, and size. The following are the types of cables used in networks.

- Unshielded Twisted Pair (UTP) Cable
- Shielded Twisted Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable

Unshielded Twisted Pair (UTP) Cable

Twisted pair cable comes in two varieties: shielded and unshielded. Unshielded twisted pair (UTP) is the most popular and is generally the best option for LAN networks .

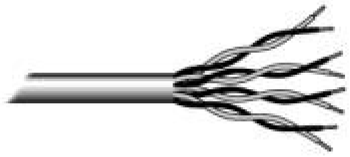


Fig.3. Unshielded twisted pair

The quality of UTP may vary from telephone-grade wire to extremely high-speed cable. The cable has four pairs of wires inside the jacket. Each pair is twisted with a different number of twists per inch to help eliminate interference from adjacent pairs and other electrical devices. The tighter the twisting, the higher the supported transmission rate and the greater the cost per foot. The EIA/TIA (Electronic Industry Association/Telecommunication Industry Association) has established standards of UTP and rated five categories of wire.

Categories of Unshielded Twisted Pair

Type Use

Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)

Category 5 cable will provide more "room to grow" as transmission technologies increase. Both Category 3 and Category 5 UTP have a maximum segment length of 100 meters.

Unshielded Twisted Pair Connector

RJ-45 (Fig 4.) is the standard for unshielded twisted pair cabling connector. This is a plastic connector that looks like a large telephone-style connector. A slot allows the RJ-45 to be inserted only one way. RJ stands for Registered Jack, implying that the connector follows a standard borrowed from the telephone industry. This standard designates which wire goes with each pin inside the connector.

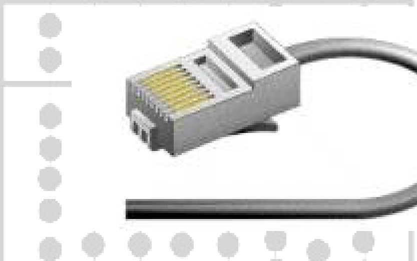


Fig. 4. RJ-45 connector

Shielded Twisted Pair (STP) Cable

A disadvantage of UTP is that it may be susceptible to radio and electrical frequency interference.

Coaxial Cable

Coaxial cabling has a single copper conductor at its center; a plastic layer provides insulation between the centre conductor and a braided metal shield (See fig. 5). The metal shield helps to block any outside interference from fluorescent lights, motors, and other computers.

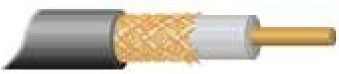


Fig. 5. Coaxial cable

There are two type Tips-thin coaxial and thick coaxial.

Coaxial Cable Connectors

Bayone-Neill-Concelman (BNC) connector is required for coaxial cables. Connectors on the cable are the weakest points in any network. To help avoid problems with your network, always use the BNC connectors that crimp, rather than screw, onto the cable.

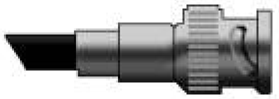


Fig. 6. BNC connector

Fiber Optic Cable

Consists of a centre glass core surrounded by several layers of protective materials, which enables it to transmit light signals at greater speeds over much longer distances eliminating the problem of electrical interference. Ideal for environments that contain a large amount of electrical interference.

Fig.7. Fiber optic cable

Connectors (ST connector) are used for fiber optic cable is an.

Ethernet Cable Summary

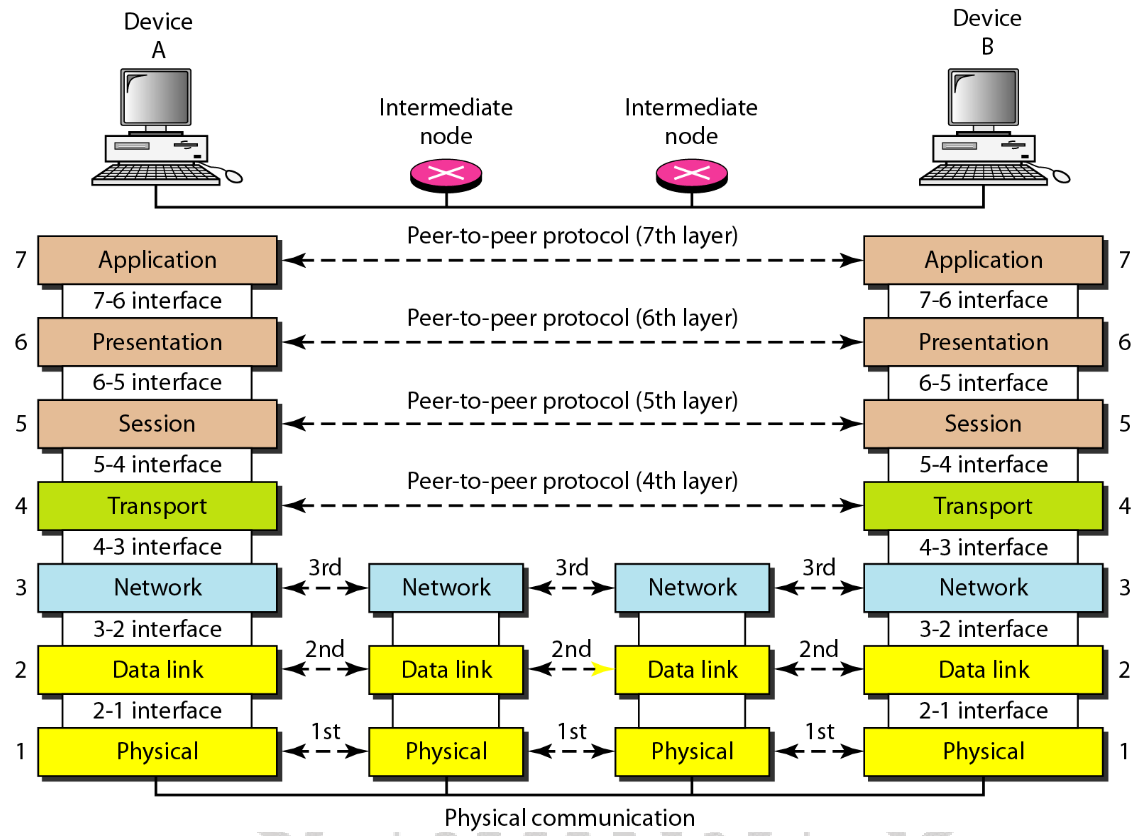
Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100 meters
10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Faber Optic	2000 meters
100BaseT	Unshielded Twisted Pair	100 meters
100BaseTX	Unshielded Twisted Pair	220 meters

What is OSI MODEL? Explain function of each layer with the help of diagram.

The standard model for networking protocols and distributed applications is the International Standard Organization's Open System Interconnect (ISO/OSI) model. It defines seven network layers.

Function of OSI model:

1. Interconnect different network devices
2. Translate protocols
3. Make possible safe and error free communication among devices
4. Synchronization of devices
5. Control flow of data
6. Makes possible when to send data and when not to send data



The Physical Layer

- Defines all electrical and physical specifications for devices.
- Establishment & Termination of Connections
- Connection Resolution & Flow Control of Communication Resources
- Modulation & Conversion between Digital Data
- Example – radio, SCSI (Small Computer System Interface)

The Data Link Layer

- Controls data transfer between network entities
- Performs error detection & correction
- Uses physical/flat Addressing Scheme
- Example - Ethernet

The Network Layer

- Performs network routing, flow control, segmentation, and error control functions
- The router operates at this layer
- Uses local addressing scheme
- Example – IP, token ring

The Transport Layer

- Provide transparent transfer of data between end users
- Controls reliability of a given link
- Some protocols are stateful and connection oriented (cookies)
- Example – TCP / UDP

The Session Layer

- Provides mechanism for managing the dialogue between end-user application processes
- Provides for either duplex or half-duplex operation
- Responsible for setting up and tearing down TCP/IP sessions
- Example – NetBIOS

The Presentation Layer

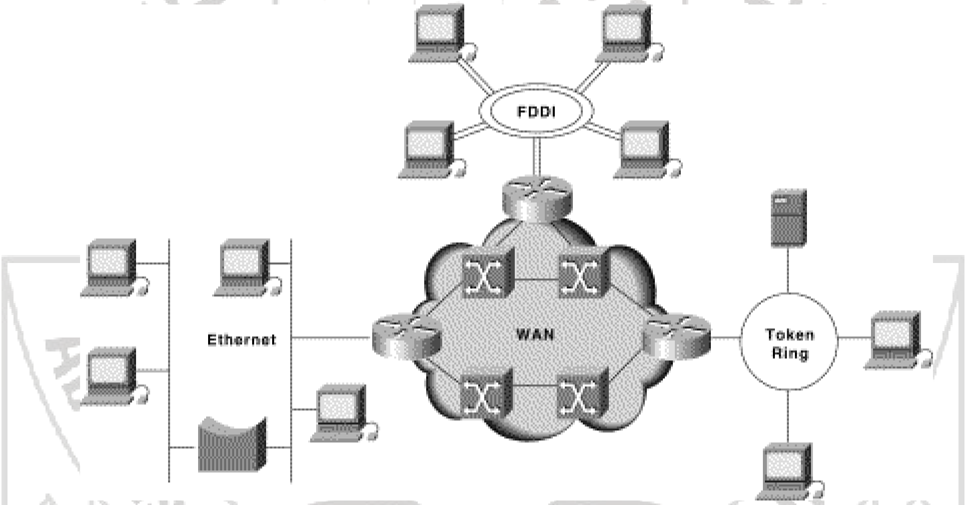
- Little to do with PowerPoint
- Controls syntactical differences in data representation within end-user systems
- MIME encoding is done at this layer
- Example - XML

The Application Layer

- Network software's and applications work at this layer
- Provide semantic conversion between associated application processes
- Interfaces directly to and performs common application services for the application processes
- Example – Telnet, Virtual Terminal

INTERNETWORKING

Internet work is a collection of individual networks, connected by intermediate networking devices, that functions as a single large network.



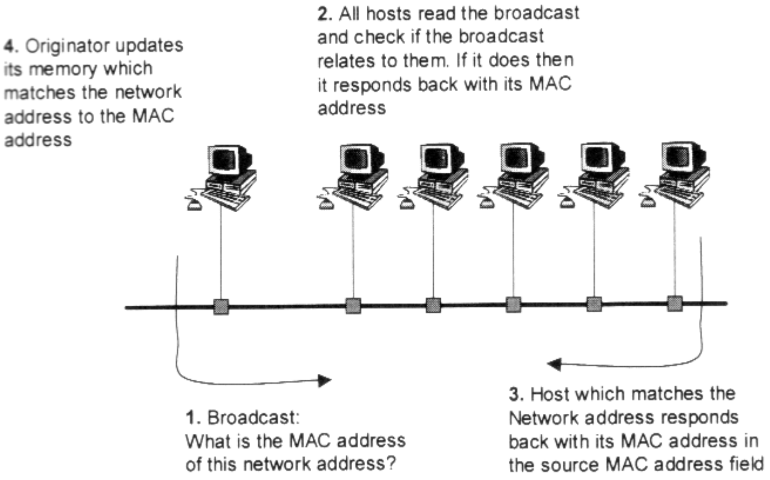
Different Network Technologies Can Be Connected to Create an Internet work

Internetworking devices have many advantages and they are:

- Increases the number of nodes that can connect to the network thus limitations on the number of nodes that connect to a network relate to the cable lengths and traffic constraints.
- Extends the physical distance of the network.
- They localize traffic within a network.
- Merge existing networks.
- Isolate network faults.

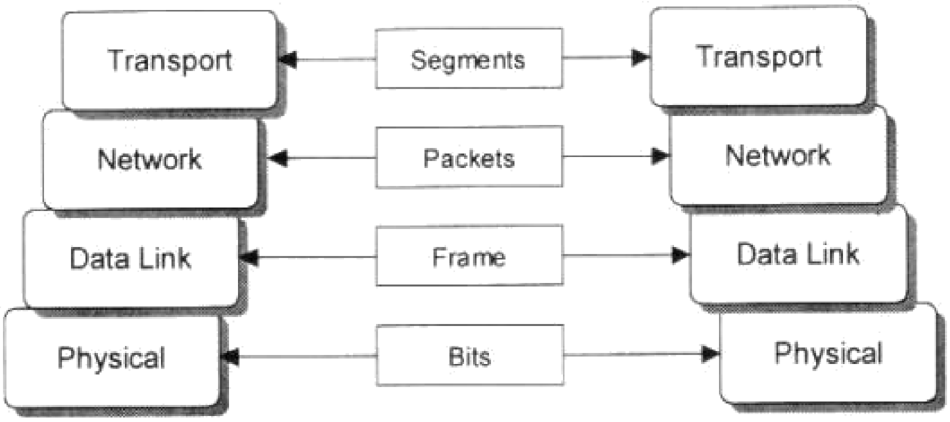
Typical internetworking devices are:

- Repeater. Operate at Layer 1 of the OSI
- Bridges. Passes data frames between net-works using the MAC address (Layer *2* address).
- Hubs. Allow the interconnection of nodes and create a physically attached network.
- Switches. Allow simultaneous communication between two or more nodes, at a time.
- Routers. Passes data packets between connected networks, and operate on network addresses (Layer 3 address).


4. Originator updates its memory which matches the network address to the MAC address
2. All hosts read the broadcast and check if the broadcast relates to them. If it does then it responds back with its MAC address
1. Broadcast: What is the MAC address of this network address?
3. Host which matches the Network address responds back with its MAC address in the source MAC address field

BITS, FRAMES, PACKETS AND SEGMENTS

At each node each of the OSI layers communicates directly with the equivalent layer on the receiving host. The data that is transmitted in each of the lower layers is referred to in a different way. Protocol data units (PDUs) are the data that passes from layer to layer and are referred to in different ways in each of the layers (bits - at the physical, frames - at the data link layer, packets - at the network layer they, and segments - at the transport layer).



Bits, frames, packets and segments

Structure of data packet:

Sender Address	Receiver Address	Data	CRC

PROTOCOL

A protocol is a set of rules that governs the communications between computers on a network. These rules are guidelines that regulate the access method, allowed physical topologies, types of cabling, and speed of data transfer.

Function of Protocol?

Sender side.

7. Covert data into packets
8. Add addressing information to the packets
9. send it to the destination computer

Receiver Side:

1. Receive data from the source computer
2. De-attach addressing information from each packet
3. combine the data packets together

The most common protocols are:

- Ethernet
- TCP/IP
- FTP
- HTTP
- SMTP
- POP
- NETBeui
- IPX/SPX
- Apple Talk
- LocalTalk
- Token Ring
- FDDI
- ATM

ETHERNET

This is the most widely used protocol. This protocol uses an access method called CSMA/CD (Carrier Sense Multiple Access/Collision Detection). In this system each computer listens to the cable for any transmitting node before sending anything through the network. If the network is clear, the computer will transmit. Else wait and try again when the line is clear. Sometimes, two computers attempt to transmit at the same instant (causing a collision). Each computer then backs off and waits a random amount of time before attempting to retransmit. The delay by collisions and retransmitting is very small and does not normally affect the speed of transmission on the network.

TCP/IP

transmission control protocol/internet protocol: a set of protocols (including TCP) developed for the internet in the 1970s to get data from one network device to another. TCP/IP is the most common protocol for transmitting information around a network. Every computer on a TCP/IP network must have its own IP address.

- TCP/IP is a set of protocols developed to allow cooperating computers to share resources across a network. It was developed by a community of researchers centered around the ARPAnet.
- TCP/IP is a family of protocols. A few provide "low-level" functions needed for many applications. These include IP, TCP, and UDP.

- Some example of software/programs and protocols supported by TCP/IP are:
- FTP
- Telnet
- NNTP (Network News Systems)
- 1982: TCP/IP protocol suite is specified fro TCP and IP
- 1983: TCP/IP becomes universal and is used as the protocol to connect to the internet
- Support from vendors:
- TCP/IP receives support from many hardware and software vendors.
- Interoperability
- Can be installed on any platform. A UNIX host can connect to a DOS/WIN95 host
- Flexibility
- Dynamic and automatic assignment of IP addresses.

LOCALTALK

Apple Computer developed LocalTalk for Macintosh computers. The method used by LocalTalk is called CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). It is similar to CSMA/CD except that a computer signals its intent to transmit before it actually does so. LocalTalk adapters and special twisted pair cable can be used to connect a series of computers through the serial port.

LocalTalk protocol allows for linear bus, star, or tree topologies using twisted pair cable.

TOKEN **RING**

This was developed by IBM in the mid 1980s. The method used involves token-passing. Computers are connected so that the signal travels around the network from one computer to another in a logical ring. A single electronic token moves around the ring from one computer to the next. If a computer does not have information to transmit, it simply passes the token on to the next workstation. If a computer wishes to transmit and receives an empty token, it attaches data to the token. The token then proceeds around the ring until it comes to the computer for which the data is meant. At this point, the receiving computer captures the data.

FIBRE DISTRIBUTED DATA INTERFACE (FDDI)

Access method of token-passing via a dual ring physical topology. Transmission on one of the rings; however, if a break occurs, the system keeps information moving by automatically using portions of the second ring to create a new complete ring. Transmission speed is100 Mbps over a fiber optic cable, but expensive.

ASYNCHRONOUS TRANSFER MODE (ATM)

Transmits data in small packets of a fixed size at a speed of 155 Mbps and higher. ATM supports a variety of media such as video, CD-quality audio, and imaging. ATM employs a star topology with fiber optic or twisted pair cabling.

IPX/SPX:

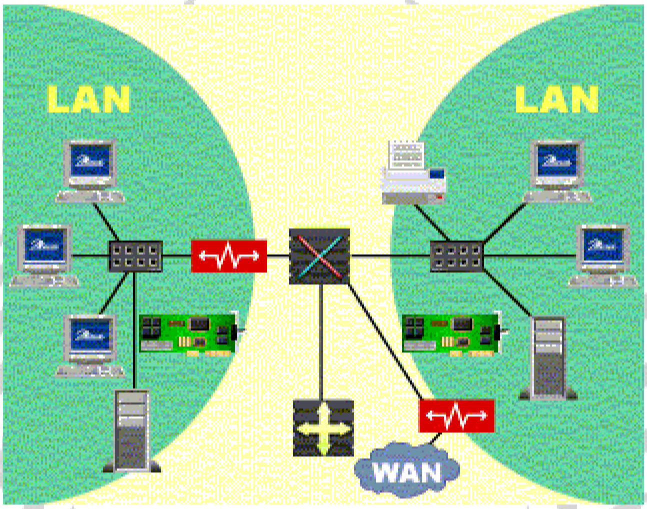
TCP/IP is the most common protocol for transmitting information around a network. Every computer on a TCP/IP network must have its own IP address. Novell is largely responsible for the use of IPX as a popular computer networking protocol due to their dominance in the network operating system software market (with Novell Netware) from the late 1980s through the mid-1990s. IPX and SPX both provide connection services similar to TCP/IP, with the IPX protocol having similarities to IP, and SPX having similarities to TCP. IPX/SPX was primarily designed for local area networks (LANs), and is a very efficient protocol for this purpose (typically its performance exceeds that of TCP/IP on a LAN).

INTERNETWORKING DEVICES

This site is about Internetworking devices which include Repeaters, Hubs, Routers, Switches, and Bridges. We started by defining each device followed by the various types and lastly how they work. Links were also provided for more information about each device.

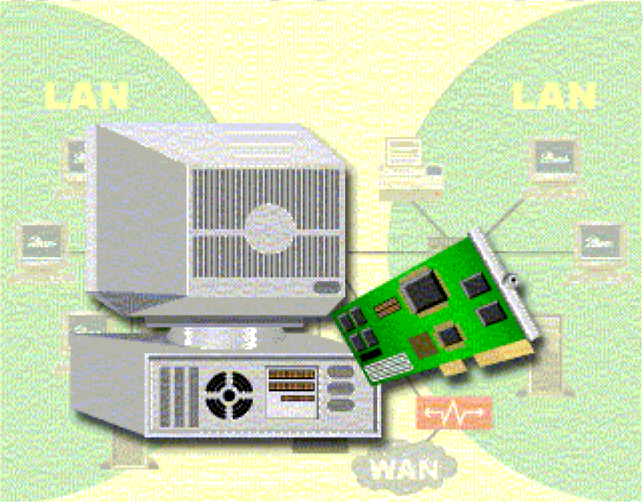
Like any type of technology, LANs have certain limitations. These limitations include the geographical distances that they cover, the number of nodes that can be connected, or the need to run more than one protocol. The devices within a network and the functions they support make a significant impact on the limitations of the network. Various types of hardware devices can be used to extend LAN functionality, each offering a specific function in exchange for added cost and complexity.

LAN Devices



There are a variety of devices used to extend LANs, from a simple Network Interface Card (NIC) that allows you to connect to a network to a sophisticated router that can move information across the Internet. However, each device performs a specific function that, when combined with the functions of others, enables the LAN to transfer information from Point A to Point B.

Network Interface Cards (NICs)



The Network Interface Card (NIC) is a circuit board that is physically installed within an active network node, such as a computer, server, or printer. The NIC is an adapter that controls the exchange of information between the network and the user.

Repeaters/Hubs

A repeater extends the length of a network cabling system by amplifying the signal and then re-transmitting it. Repeaters operate at Physical Layer 1. As a result, they do not look at the data at all. Any information coming into one port is simply repeated out all other ports.

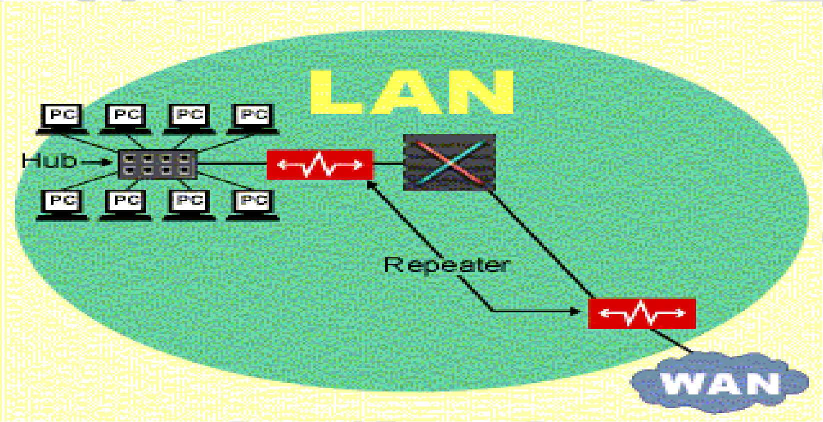
Technically speaking, three different types of hubs exist:

- passive
- active
- intelligent

Passive hubs do not amplify the electrical signal of incoming packets before broadcasting them out to the network. Do not require any power to work, less expensive as compared to passive and intelligent hub.

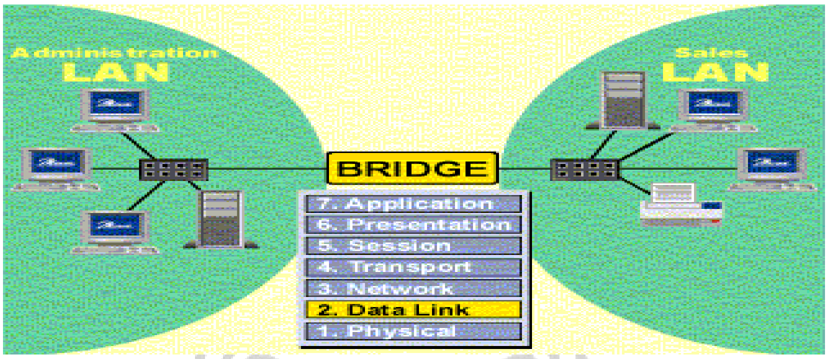
Active hubs, on the other hand, do perform this amplification, as does a different type of dedicated network device called a repeater. Some people use the terms **concentrator** when referring to a passive hub and **multiport repeater** when referring to an active hub.

Intelligent hubs add extra features to an active hub that are of particular importance to businesses. An intelligent hub typically is stackable (built in such a way that multiple units can be placed one on top of the other to conserve space). It also typically includes remote management capabilities via SNMP and virtual LAN (VLAN) support.



A hub is another Layer 1 device that is typically used as a central point for connecting segments in a LAN. While passive hubs simply pass packets from one port to another, the signal may be regenerated in active hubs called multi-port repeaters. Hubs are becoming increasingly intelligent, enabling them to support network management and minimal path selection functions.

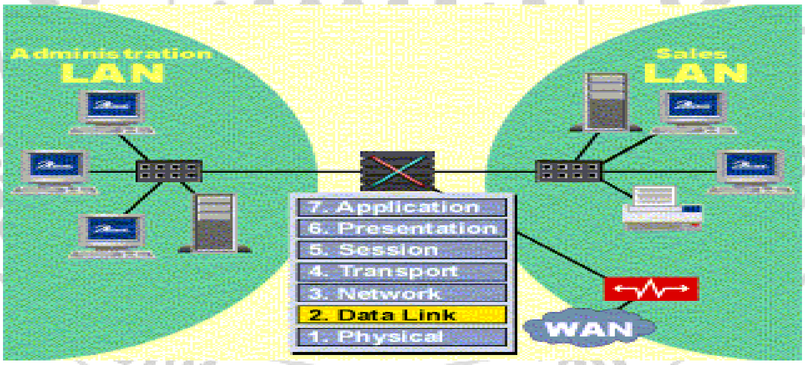
□ Bridges



As networks grow larger, they are often divided into smaller LANs to reduce traffic drain on the network. A bridge is a Data Link Layer 2 device that provides a connection between separate LAN segments. The bridge monitors packets as they move between segments, keeping track of the MAC addresses that are associated with various ports. As they gain more knowledge of the nodes connected to each network, they are better able to manage traffic flow.

A bridge is a combination of software and hardware that connects different network that use similar communication methods. It can also connect different networks with different topologies. Two a more networks using different types of NICS may be interconnected with a process called bridging. A bridge is one fileserver or workstation which has two or more NICS each cabled to different network.

Switches



Switches are becoming a more common way to connect networks together because they are simply faster and more intelligent than bridges. Advances in technology spawned a new generation of networking devices known as LAN switches, which included bridging as one of several functions. Switches have replaced bridges for two reasons: superior performance and lower price per port.

Difference between HUB and switch:

Hubs and switches are different types of network equipment that connect devices. They differ in the way that they pass on the network traffic that they receive.

HUB

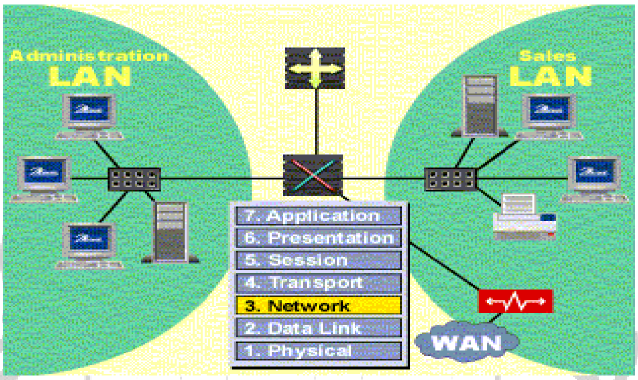
Is sometimes used to refer to any piece of network equipment that connects PCs together, but it actually refers to a multi-port repeater. This type of device simply passes on (repeats) all the information it receives, so that all devices connected to its ports receive that information.

Switches
Switches control the flow of network traffic based on the address information in each packet. A switch learns which devices are connected to its ports (by monitoring the packets it receives), and then

forwards on packets to the appropriate port only. This allows simultaneous communication across the switch, improving bandwidth.

Routers

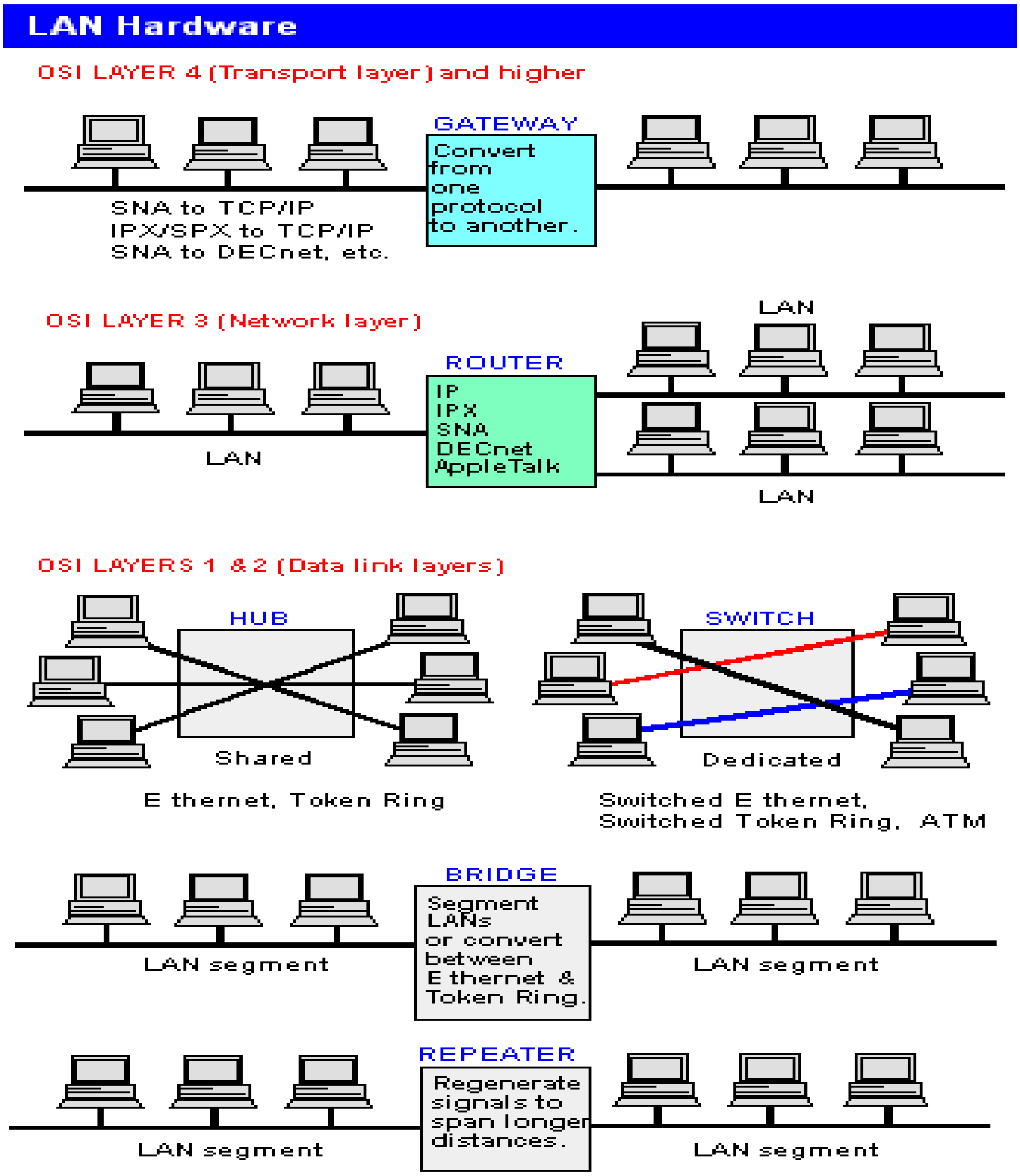
Routers were originally invented to solve some of the problems that weren't addressed by bridges. Like bridges, routers are used to segment a LAN in order to reduce excess broadcast traffic and latency. In addition, routers make internetworking possible by interconnecting both local and wide area networks.



The function of a router is to direct data along the most efficient and economical route to the destination device. Routers operate at Network Layer 3, which means they examine the logical network address (for example, 191.29.21.100) and not the physical hardware address (MAC).

Routers are smarter than bridges because they know about routing protocols, different address schemes, different frame sizes and different data rates in order to make the best decision on which path to choose. The best path is determined by using routing tables and algorithms.

Typical Layout of Internet work



Write a detail note on Bluetooth technology.

What’s in the name?
Bluetooth! The word Bluetooth was borrowed from the 10th century, second King of Denmark, King Harald Bluetooth. He was well known for bringing together Scandinavia. He played a major role in uniting Denmark and Norway and in the introduction of Christianity. To show the significance of bringing together different devices and enabling communication between them, Bluetooth technology got its name after this king.

Bluetooth is a technology, whereby, devices communicate wirelessly to achieve data transfer at the rate of 720kbps within a range of 10 to 100 meters. It operates in the unlicensed ISM (Industrial Scientific and Medical) band at 2.4 gigahertz.

How does Bluetooth work?
Now, about how Bluetooth works … Bluetooth Special Interest Group manages and maintains the Bluetooth Standard. IEEE has accepted it as 802.15la standard. Bluetooth was developed with a purpose of creating a single digital wireless protocol, capable of connecting multiple devices and getting over the synchronization issues. It enables short-range wireless communication thus replacing wires connecting the electronic devices.

The Bluetooth RF transceiver lies at physical layer. There are 79 Bluetooth channels spaced 1MHz apart. A spread spectrum technology is used at the physical layer. Both voice and data transmissions over short distances are possible, creating wireless PANs.

A Bluetooth device consists of an adapter. A Bluetooth adapter can be built into a device or can be in the form of a card that connects to a device. Instructions are embedded into the device, which enable it to communicate with other devices.

When devices come in each other's radio range, their link managers discover each other. Link management protocol (LMP) engages itself in peer-to-peer message exchange. LMP layer performs link setup and negotiation of packet size. Segmentation and reassembly of packets is done, if needed.

Service delivery protocol enables a Bluetooth device to join a piconet. A device inquires what services are available with the piconet. Bluetooth GlobalID is exchanged between the devices. Their profiles are matched and a connection is setup.

Bluetooth uses frequency hopping in timeslots, which means that the Bluetooth signals avoid interference with other signals by hopping to a new frequency after transmission or reception of every packet. One packet can cover up to five time slots.

Bluetooth can support an asynchronous data channel, or up to 3 simultaneous synchronous voice channels, or a channel, which concurrently supports asynchronous data and synchronous voice.

Bluetooth technology makes use of the concept of master and slave. Devices have to wait until the master allows them to talk! One master and up to seven slaves employ a star topology to form a piconet.

Bluetooth Application Models

File Transfer: -This model talks of an object transfer or transfer of files between devices.

Internet Bridge: -In this model, a cordless modem acts as a modem to a PC and provides dialup networking and faxing.

LAN Access: -Multiple data terminals use a LAN access point (LAP) as a wireless connection to an Ethernet LAN.

Synchronization: -Synchronization model provides a device-to-device synchronization of data.

Headset: -It is wirelessly connected and can act as an audio input-output interface of remote devices.

Bluetooth Buzzwords

Piconet: -A group of devices connected by means of Bluetooth technology in an ad hoc manner is known as a piconet. There can be a maximum of 8 devices forming one piconet. For the duration of a piconet connection, one device acts as the master and others act as slaves in order to synchronize.

Scatternet: -A scatternet is composed of two or more independent piconets. This brings about a communication between piconets.

Master unit: -Its clock and hopping frequency are used to synchronize other devices in the piconet. The master device numbers the communication channels.

Slave unit: - The slave units act in co-ordination with the master.

Bluetooth Applications

1. Bluetooth has a wide range of applications. Wireless communication between a mobile phone and a handset is possible by way of Bluetooth.
2. Computers can form a wireless network in a limited space and when bandwidth requirement is less.
3. Unwired communication between the input and output devices of a computer is possible by means of Bluetooth technology.
4. Transfer of files and data between devices with OBEX is achieved. OBEX is a session protocol that provides the functionality of HTTP in a lighter fashion.
5. Some game consoles use Bluetooth for their wireless controllers.
6. Bluetooth-enabled mobile phones and modems can make possible, dial up Internet connections for PCs or PDAs.

Why Headsets?
When on wheels, when driving, you can make and receive calls due the hands free headset. Some recommend headsets to minimize the radiations pumped into your brain. Even if you have several different Bluetooth equipped phones, a headset should work with all of them conveniently. If you replace your phone, the headset will work just fine with the new handset. A Bluetooth headset can be used to connect to your computer and other such devices as well!

Bluetooth GPS…What it is…
Bluetooth GPS can work as your travel escort! You carry some directions or maps in your PDA's memory. Even better is to use Belkin GPS Receiver. This receiver is technologically advanced to receive satellite reception. It supports voice and visual direction. The built-in software can create maps for you. Where does Bluetooth come into picture? It helps make easy the conversion of your PDA to a GPS receiver.

Advantages of Bluetooth
There are numerous advantages of Bluetooth.
Firstly, it eliminates all the cords used in connections. ! Line of sight is not required. The word 'unwired' is in some way synonymous to the word 'uncluttered'!

Secondly, with Bluetooth headsets, you can use your cell phone without the use of your hands. That makes it safe to talk on phone while your hands are engaged in other activities. Due to Bluetooth, you are not required to be physically close to the device you are using.

Thirdly, Bluetooth devices are fairly inexpensive. There is no special cost incurred in using the service.

The next concern is interoperability. Bluetooth is a standardized specification. Bluetooth enabled devices are highly compatible. They understand each other without human intervention. When they enter a range of one another, they start communicating on their own. The process of setup is automatic.

Then comes efficiency! Bluetooth uses low power signals, thus requiring less energy. Due to spread-spectrum frequency hopping, interference with other wireless devices stays away.

Bluetooth Special Interest Group has been working on upgraded versions, which can yet remain backward compatible.

Moreover, Bluetooth is secure. Strict security rules will not allow the devices to communicate unless pre-approved by you. So it is you, who is the controller of communication!

Ericsson was the first to develop the Bluetooth specification. Many companies are now making their products capable to use it. I think Bluetooth technology is a complete package of virtues like feature simplicity, inexpensiveness and the need of least human involvement in its implementation. Bluetooth is here to stay for years to come!

What is Video Conferencing? Discuss the advantages of video conferencing.

A **videoconference** or **video conference** (also known as a *video teleconference*) is a set of interactive telecommunication technologies which allow two or more locations to interact via two-way video and audio transmissions simultaneously. It has also been called 'visual collaboration' and is a type of groupware.

Videoconferencing differs from videophone calls in that it's designed to serve a conference rather than individuals. It is an intermediate form of video telephony, first deployed commercially by AT&T during the early 1970s using their Picture phone technology.

Technologies used in

- Video input : video camera or webcam
- Video output: computer monitor , television or projector
- Audio input: microphones, CD/DVD player, cassette player, or any other source of PreAmp audio outlet.
- Audio output: usually loudspeakers associated with the display device or telephone
- Data transfer: analog or digital telephone network, LAN or Internet
- Computer systems
- Audio and video streams
- Internet or dedicated network connection

Advantages of using Videoconferencing:

Videoconferencing provides students with the opportunity to learn by participating in a 2-way communication platform. Furthermore, teachers and lecturers from all over the world can be brought to classes in remote or otherwise isolated places. Students from diverse communities and backgrounds can come together to learn about one another. Students are able to explore, communicate, analyze and share information and ideas with one another. Through videoconferencing students can visit another part of the world to speak with others, visit a zoo, a museum and so on, to learn. These "virtual field trips" (see history of virtual learning environments) can bring opportunities to children, especially those in geographically isolated locations, or the economically disadvantaged. Small schools can use this technology to pool resources and teach courses (such as foreign languages) which could not otherwise be offered.

Here are a few examples of how videoconferencing can benefit people around campus:

- faculty member keeps in touch with class while away for a week at a conference
- guest lecturer brought into a class from another institution
- researcher collaborates with colleagues at other institutions on a regular basis without loss of time due to travel
- schools with multiple campuses can collaborate and share professors
- faculty member participates in a thesis defense at another institution
- administrators on tight schedules collaborate on a budget preparation from different parts of campus
- faculty committee auditions a scholarship candidate

- researcher answers questions about a grant proposal from an agency or review committee
- student interviews with an employer in another city
- teleseminars

Videoconferencing is a very useful technology for telemedicine and telenursing applications, such as diagnosis, consulting, transmission of medical images,

Videoconferencing can enable individuals in faraway places to have meetings on short notice. Time and money that used to be spent in traveling can be used to have short meetings.

Videoconferencing has allowed testimony to be used for individuals who are not able to attend the physical legal settings

The concept of press videoconferencing (or press videoconference) was developed in October 2007 by the African Press Organization (APO), a Swiss based Non-governmental organization, to allow African journalists to participate in international press conferences on the subject of development and good governance.