KEY ELEMENTS

OF

COMPUTER NETWORK

Authors:

Mr. Chetan N. Rathod [M.C.A., M.Phil.]

VIVEKANAND COLLEGE FOR ADVANCED COMPUTER & INFORMATION SCIENCE, SURAT

Mr. Sagar V.Fegade [M.C.A.]

M.L.PARMAR COLLEGE OF COMPUTER SCIENCE & I.T, SURAT

Ms. Bhumika K. Charnanand [M.C.A., M.Phil.]

PRABHU B.C.A. COLLEGE, UMRA, SURAT

Unit - 1

An Introduction to Networks, Network Topologies and Types

1.1 Data Communication [Analog, Digital]
1.2 Introduction: Networking
1.3 Information Exchange, Sharing, Preserving & Protecting
1.4 Hardware and Software Resource Sharing
1.5 Need Uses and Advantages of Network
1.6 Clients, Servers, Peers based and Hybrid Networks
1.7 Server types
1.8 Network Topologies (Bus, Star, Ring, Star Bus, Star Ring & Physical Mesh)
1.9 Defining Network Protocols (H/W Protocols, S/W Protocols H/W-S/W Interface)
1.10 Introduction to Wireless Network, Ad-hoc Wireless and Sensor Wireless Network

1.1 Data communication:

Data communication refers to the exchange of data between a sender and a receiver via form of transmission media such as a wire cable or by wireless. Data communication is said to be local if communicating devices are in the same building or a similarly restricted geographical area.

The device that transmits the data is known as sender or source and the device that receives the transmitted data is known as destination or receiver. Data communication aims at the transfer of data and maintenance of the data during the process.

Signal: A signal is an electrical or electromagnetic current that is used for carrying data from one device or network to another. A signal can be either analog or digital.

Analog signal:

Analog signal is a continuous signal in which one time-varying quantity represents another time-based variable. These kind of signals works with physical values and natural phenomena such as earthquake, frequency, volcano, speed of wind, weight, lighting, etc.

[1.1 Analog Signals]

Digital signal:

A digital signal is a signal that is used to represent data as a sequence of separate values at any point in time. It can only take on one of a fixed number of values. This type of signal represents a real number within a constant range of values.

[1.2 Digital Signals]

Characteristics of Analog Signal

- These type of electronic signals are time-varying
- Minimum and maximum values which is either positive or negative.
- It can be either periodic or non-periodic.
- Analog Signal works on continuous data.
- The accuracy of the analog signal is not high when compared to the digital signal.
- It helps you to measure natural or physical values.
- Analog signal output form is like Curve, Line, or Graph, so it may not be meaningful to all.

Characteristics of Digital Signals

- Digital signal are continuous signals
- This type of electronic I signals can be processed and transmitted better compared to analog signal.
- Digital signals are versatile, so it is widely used.
- The accuracy of the digital signal is better than that of the analog signal.

Advantages of Analog Signals

- Easier in processing
- Best suited for audio and video transmission.
- It has a low cost and is portable.
- It has a much higher density so that it can present more refined information.
- Not necessary to buy a new graphics board.
- Uses less bandwidth than digital sounds
- Provide more accurate representation of a sound
- It is the natural form of a sound.

Advantages of Digital Signals

- Digital data can be easily compressed.
- Any information in the digital form can be encrypted.
- Equipment that uses digital signals is more common and less expensive.
- Digital signal makes running instruments free from observation errors like parallax and approximation errors.
- A lot of editing tools are available
- You can edit the sound without altering the original copy
- Easy to transmit the data over networks

Disadvantages of Analog Signals

- Analog tends to have a lower quality signal than digital.
- The cables are sensitive to external influences.
- The cost of the Analog wire is high and not easily portable.
- Low availability of models with digital interfaces.
- Recording analog sound on tape is quite expensive if the tape is damaged
- Tape is becoming hard to find
- It is quite difficult to synchronize analog sound
- Quality is easily lost
- Data can become corrupted
- Plenty of recording devices and formats which can become confusing to store a digital signal
- Digital sound's can cut an analog sound wave which means that you can't get a perfect reproduction of a sound
- Offers poor multi-user interfaces

- Sampling may cause loss of information.
- A/D and D/A demands mixed-signal hardware
- Processor speed is limited
- Develop quantization and round-off errors
- It requires greater bandwidth
- Systems and processing is more complex.

Differences of Analog and Digital Signals

ANALOG SIGNAL	DIGITAL SIGNAL
An analog signal is a continuous signal that represents physical measurements.	Digital signals are time separated signals which are generated using digital modulation.
It uses a continuous range of values that help you to represent information.	Digital signal uses discrete 0 and 1 to represent information.
Temperature sensors, FM radio signals, Photocells, Light sensor, Resistive touch screen are examples of Analog signals.	Computers, CDs, DVDs are some examples of Digital signal.
The analog signal bandwidth is low	The digital signal bandwidth is high.
Analog signals are deteriorated by noise throughout transmission as well as write/read cycle.	Relatively a noise-immune system without deterioration during the transmission process and write/read cycle.
Analog hardware never offers flexible implementation.	Digital hardware offers flexibility in implementation.
It is suited for audio and video transmission.	It is suited for Computing and digital electronics.
Analog instruments usually have s scale which is cramped at lower end and gives considerable observational errors.	Digital instruments never cause any kind of observational errors.
Analog signal doesn't offer any fixed range.	Digital signal has a finite number, i.e., 0 and 1.

1.2 Networking /Computer network:

A computer network is defined as the interconnection of two or more computers. It is done to enable the computers to communicate and share the available resources.

A computer network is a group of devices connected with each other through a transmission medium such as wires, cables etc. These devices can be computers, printers, scanners, Fax machines etc. Computer network is used to send and receive data from one device to another devices over the network. These devices are often referred as nodes.

There are **five basic components** of a computer network.

Message: It is the data or information which needs to be transferred from one device to another device over a computer network.

Sender: Sender is the device that has the data and needs to send the data to other device connected to the network.

Receiver: A receiver is the device which is expecting the data from other device on the network.

Transmission media: In order to transfer data from one device to another device we need a transmission media such as wires, cables, radio waves etc.

Protocol: A protocol is a set of rules that are agreed by both sender and receiver, without a protocol two devices can be connected to each other but they cannot communicate. In order to establish a reliable communication or data sharing between two different devices we need set of rules that are called protocol. For example, http and https are the two protocols used by web browsers to get and post the data to internet, similarly smtp protocol is used by email services connected to the internet.

1.3 Information Exchange, Sharing, Preserving & Protecting

Information Exchange

Information exchange has a long history in information technology. Traditional information sharing referred to one-to-one exchanges of data between a sender and receiver. Online information sharing gives useful data to businesses for future strategies based on online sharing.

Sharing

Network sharing is made possible by inter-process communication over the network. Some examples of shareable resources are computer programs, data, storage devices, and printers. E.g. shared file access (also known as disk sharing and folder sharing), shared printer access, shared scanner access, etc.

Preserving

There are a few factors to consider when it comes to **preserving network** integrity: availability, security, bandwidth and control.

The new layered approach to insuring network integrity is composed of the following layers:

1. Perimeter defense.
2. Systems layer.
3. Application gateway layer.
4. Host integrity layer.

Protecting

Networks are the essential system of information technology. All communication between computer systems and terminals takes place in local (LAN) and wide area networks (WAN). Various information and resources are exchanged on a daily basis. The individual nodes in the network are connected to each other via cables, radio connections, dial-up or leased lines. Precisely these need special protection. Network Protection means any activity to protect against manipulation of your network and your data. This includes hardware and software technologies as well as corresponding security strategies. This primarily includes first and foremost preventing intrusion into the network in order to prevent the subsequent spread and further damage to the network. Several types of network protection shall be mentioned here:

1. Antivirus software
2. Application security
3. Behavioral analysis
4. Avoidance of data loss
5. Firewalls (web application firewalls)
6. Mobile Security
7. VPN
8. Browser/Web Security

a computer network:

A computer network is build up from several components. These components together makes it possible to transfer data from one device to another and makes smooth communication between two different devices. In this guide, we will discuss the main components of a computer network.

Server: Servers are computers that runs operating system and hold data that can be shared over a computer network.

Client: A client is a computer that is connected to other computers in the network and can receive data sent by other computers.

Transmission Media: All computers in a computer network are connected with each other through a transmission media such as wires, optical fiber cables, coaxial cables etc.

Network Interface card: Each system or computer in a computer network must have a card called network interface card (NIC). The main purpose of NIC is to format the data, send the data and receive the data at the receiving node.

Hub: Hub acts as a device that connects all the computer in a network to each other. Any request that comes from a client computer first received by Hub and then hub transmit this request over a network so that the correct server receives and respond to it.

Switch: Switch is similar to hub however instead of broadcasting a incoming data request it uses the physical device address in the incoming request to transfer the request to correct server computer.

Router: Router joins multiple computer networks to each other. For example lets say a company runs 100 computers over a local area network(LAN) and another company runs another LAN of 150 computers. These both LANs can be connected with each other through a internet connection which is provided by the router.

LAN cable: A wire that is used to connect more than one computers or other devices such as printers and scanner to each other.

1.5 Need Uses and Advantages of Network

Need of computer network

The computer networks can prove to be useful in the following areas.

1. Sharing the resources such as printers among all the users.
2. Sharing of expensive software and database.
3. Communication from one computer to the other.

4. Exchange of data information amongst the users, via the network.
5. Sharing of information over the geographically wide areas.
6. For connecting the computers between various building of an organization.
7. For educational purposes.

Functions of protocol:

1. Data sequencing: It refers to breaking a long message into smaller packets of fixed size. Data sequencing rules define the method of numbering packets to detect loss or duplication of packets, and to correctly identify packets, which belong to same message.

2. Data routing: Data routing defines the most efficient path between the source and destination.

3. Data formatting: Data formatting rules define which group of bits or characters within packet constitute data, control, addressing, or other information.

4. Flow control: A communication protocol also prevents a fast sender from overwhelming a slow receiver. It ensures resource sharing and protection against traffic congestion by regulating the flow of data on communication lines.

5. Error control: These rules are designed to detect errors in messages and to ensure transmission of correct messages. The most common method is to retransmit erroneous message block. In such a case, a block having error is discarded by the receiver and is retransmitted by the sender.

6. Precedence and order of transmission: These rules ensure that all the nodes get a chance to use the communication lines and other resources of the network based on the priorities assigned to them.

7. Connection establishment and termination: These rules define how connections are established, maintained and terminated when two nodes of a network want to communicate with each other.

8. Data security: Providing data security and privacy is also built into most communication software packages. It prevents access of data by unauthorized users.

9. Log information: Several communication software are designed to develop log information, which consists of all jobs and data communications tasks that have taken place. Such information may be used for charging the users of the network based on their usage of the network resources.

Features of Computer Network:

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

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

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

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

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

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

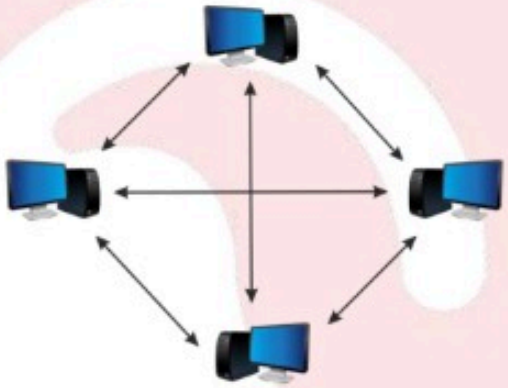
7. Scalability: A computer network should be scalable which means it should always allow to add new computers (or nodes) to the already existing computer network. For example, a company runs 100 computers over a computer network for their 100 employees, lets say they hire another 100 employees and want to add new 100 computers to the already existing LAN then in that case the local area computer network should allow this.

1.6 Clients, Servers, Peers based and Hybrid Networks OR Computer Architecture:

A Computer Architecture is a design in which all computers in a computer network are organized. An architecture defines how the computers should get connected to get the maximum advantages of a computer network such as better response time, security, scalability etc. The two most popular computer architectures are **P2P (Peer to Peer)** and **Client-Server architecture.**

Peer to Peer Architecture:

In peer to peer architecture all the computers in a computer network are connected with every computer in the network. Every computer in the network use the same resources as other computers. There is no central computer that acts as a server rather all computers acts as a server for the data that is stored in them.



1.3 PEER TO PEER ARCHITECTURE

Advantages of a Peer to Peer Architecture

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

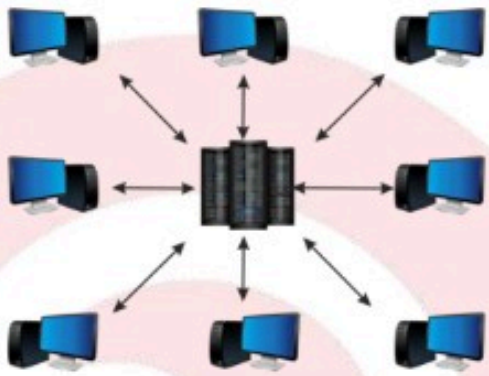
Disadvantages of a Peer to Peer Architecture

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

Client Server Architecture

In Client Server architecture a central computer acts as a hub and serves all the requests from client computers. All the shared data is stored in the server computer which is shared with the client computer when a request is made by the client computer.

All the communication takes place through the server computer, for example if a client computer wants to share the data with other client computer then it has to send the data to server first and then the server will send the data to other client.



1.4 CLIENT SERVER ARCHITECTURE

Advantages of Client Server Architecture:

- Data backup is easy and cost effective as there is no need to manage the backup on each computer.
- Performance is better as the response time is greatly improves because the server is more powerful computer than the other computers in the network.
- Security is better as unauthorized access are denied by server computer and all the data goes through the server.
- Scalability is not an issue in this Architecture as large number of computers can be connected with server.

Disadvantages of Client Server Architecture:

- In case of server failure entire network is down.
- Server maintenance cost is high as the server is the main component in this Architecture
- Cost is high as the server needs more resources to handle that many client requests and to be able to hold large amount of data.

Hybrid Networks :

Hybrid networks have all three types of computers operating on them and generally have active directory domains and workgroups. This means that while most shared resource are located on servers, network users still have access to any resources being shared by peers in workgroup. It also means network users do not have to log on to the domain controller to access workgroup resources being shared by peers.

Advantages of hybrid computing :

Hybrid computing provides these advantages :

- The advantages of server-based networking
- Many of the advantages of peer-based networking
- Ability of users and network administration to control security based on the important of the shared resources

Disadvantages of Hybrid computing:

Hybrid computing shares the disadvantages of server-based networking

1.7 Server types

1. File server
2. Print server
3. Application Server
4. Message Server
5. Database Server

1) File Server :-

File server offers services that allow network users to share files. File service are the network applications that store, retrieve, and move data. This type of services is probably the most important reason companies invest in a network . With network file service, users can exchange, read, write and manage shared files and the data contained in them. The following section consider these types of file services.

- File transfer
- File storage and data migration
- File update synchronization
- File archiving

File transfer :-

Before networking computer become a popular way of sharing files and transfer a file from one computer to another, you would save the file to a floppy disk. If the file is large for a single floppy .for long distance, it was impossible . The most sophisticated option was dial the other computer and transfer your file with the

modem or across a direct serial connection .With all this fie transferring taking place, the need for file security arises. Every network operating system has its own level of file security.

File storage and data migration :-

Three main categories of file storage

1) Online storage 2) Offline storage 3) Near-line storage

Online storage consists, most notable, of hard drive storage. Information stored on a hard drive can called up very quickly. For this reason,hard drives are used to store files that are accessed regularly . However, hard drive space is, as mentioned earlier, relatively expansive. There is also another limitation specific to internal hard drives(but not external hard drives).because they are a fairly permanent part of a computer, they cannot be conveniently removed, placed in storage, and replaced when needed.

Offline Storage device include media such as data tapes and removable optical disks. This type of storage offers a high –capacity, low price alternative to online storage . One disadvantage of this type of storage, however, is that it requires a person to retrieve the disk or tape and mount it on the server.

Near – line storage devices offer fairly low costs and high storage capacities, without requiring the network administrator to wake up, go to the archive shelf, and mount the tape or disk on the server . instead, a machine, such as a tape carousel or jukebox, automatically retrieves and mount the tape or disk. These systems tend to offer faster, more efficient data access than offline systems, but they are still only fast enough for infrequently used data and application.

The process by which data is moved from online to offline or near-line storage is called data migration. Files are selected for migration based on factors such as the last time the file was accessed, the file owner, or the file size.

File update synchronization :-

File update synchronization has the lofty goal of ensuring that each user of a file has the latest version . By using time and date stamping and user tracking, file synchronization works to ensure that changes made to a file organized in the chronological order in which they actually took place and that files are properly updated. File synchronization is usually a thirty party option or an upgrade package for most network operating systems.

File Archiving :- File archiving is the process of backing up files on offline storage devices, such as tapes or optical.

2) Print server : -

Another important factor in the genesis of computer networking was the demand for the ability to share printers. The advent of networking a whole new level of computer printing, because a network can

- Allow users to share printers
- Allow you to place printers where convenient, not just near individual computers
- Achieve better workstation performance by using high-speed network data transfer, print queues, and spooling
- Allow users to share network fax services

Print service manage and control printing on a network, allowing multiple and simultaneous access to printing facilities. The network operating system achieves this by using print queues, which are special storage areas where print job a are stored and then sent to the printer in an organized fashion. When a computer prints to a queue, it actually function as though it were forwarded to the printer when the printer has finished the job scheduled ahead of it.

Printing on a network with queues can be a more efficient way for users to work .the print data is transferred to the queue at network speed . the user can then continue working in an application while the network takes care of the printing.

Network printing also cuts costs by allowing shared access to printing devices. This is especially important when it comes to the more expansive varieties of printers. High-quality color printers, high- speed printers, and large – format printers and plotters tend to cost a lot. It is seldom feasible for an organization to purchase one of these for every individual computer that should have access to one.

3) Application Servers :-

Application services allow client PCs to access and use extra computing power and expensive software application that reside on shared computer. You can add specialized servers to provide specific application on a network. For Example, if your organization needs a powerful database, you can add a server to provide this application.

Application servers can be dedicated computers set up specifically for the purpose of providing application services, or they can serve multiple functions. A single server, for example can provide file, print, communication, and database services.

Message Server : -

Message servers provide message services in a wide variety of communication methods that go far beyond simple file services . With file services, data can pass between users only in file form . With message services, data can take the form of

graphics, digitized video, or audio as well as text and binary data. As hypertext links become more common in messages, message services are becoming an extremely flexible and popular means of transmitting data across a network.

For main type of message services are

- Electronic mail
- Workgroup application
- Object –oriented application
- Directory services

Electronic Mail :-

Electronic mail, or e-mail is an increasingly popular reason for installing a network . With e-mail you can easily send a message to another user on the network or on other networks, including the Internet.

E-mail was text-based it contained only text characters. Now e-mail systems can transfer video, audio and graphics as well . With e-mail, sending this data halfway around the world is usually much easier than by any other method. E-mail is much faster than traditional " snail mail ", much cheaper than courier services, and much simpler than dialing the recipient's computer and transferring the files to it.

Workgroup Application :-

Workgroup application produce more efficient processing of tasks among multiple users on a network. The two main workgroup applications are

- Workflow management application
- Linked – object document

Workflow management application route documents, focus, and notice among network clients. Tasks that require the input of multiple network users are often much easier using this type of application. For example, for supply clerk to complete a requisition at a military base, approval from several higher –ups may be needed. This process could be automated so that each person whose approval is routinely needed would receive the requisition(request) from on the network. The application would send the form around from one person to the next, in the correct order, until all approval had been granted (or refuse).

Linked –object document are documents containing multiple data object. A verity of types of data objects can be linked to construct a document. For example, a single linked object document could contain voice, video, text and graphic linked together . A network message service can then act as an agent for each of these objects, passing message between the object and its originating application or file.

Object – oriented Application :-

Object oriented application are program that can accomplish complex tasks by combining smaller application, called objects. By using a combination of objects, object oriented application gain the ability to handle large tasks.

Message services facilitate communication between these objects by acting as go-between . This way, objects do not need to communicate with other objects on the network. Instead, an object can simply pass data to the agent, which then passes the data to the destination object.

Directory Services :-

Directory services servers help users locate, store, and secure information on the network. Both active directory and novel directory services store information about users and computers. For example, a user can request the postal address of another user from one of these services.

4) Database servers :- Database services can provide a network with powerful database capabilities that are available for use on relatively weak PCs. Most database systems are client – server based .this means that the database applications run on two separate components :

- The client end portion of the application runs on the client, providing an interface and handling less intensive function, such as data requests.
- The server end portion of the application handles the intensive performances of database operations, processing queries, and replying to client.

For Example, Imagine a network with a 100 gigabyte database . This database could be managed by a centralized database application based on the client – server model . Clients could request information from the server, which would then perform a query and report the results to the client . The client could then access the data, process it on the client end, and return it to the server. Database server are becoming increasingly powerful, providing complex services including security, database optimization, and data distribution. Distributed databases, utilizing database management systems, are becoming increasingly popular.

1.8 Network Topology – Mesh, Star, Bus, Ring and Hybrid:

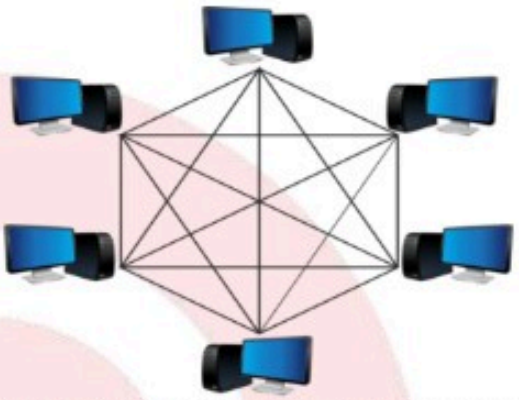
Geometric representation of how the computers are connected to each other is known as topology. There are five types of topology – Mesh, Star, Bus, Ring and Hybrid.

Types of Topology

There are five types of topology in computer networks:

1. Mesh Topology
2. Star Topology
3. Bus Topology
4. Ring Topology
5. Hybrid Topology

Mesh Topology



1.5 MESH TOPOLOGY

In mesh topology each device is connected to every other device on the network through a dedicated point-to-point link. When we say dedicated it means that the link only carries data for the two connected devices only. Let's say we have n devices in the network then each device must be connected with (n-1) devices of the network. Number of links in a mesh topology of n devices would be n(n-1)/2.

Advantages of Mesh topology:

- No data traffic issues as there is a dedicated link between two devices which means the link is only available for those two devices.
- Mesh topology is reliable and robust as failure of one link doesn't affect other links and the communication between other devices on the network.
- Mesh topology is secure because there is a point to point link thus unauthorized access is not possible.
- Fault detection is easy.

Disadvantages of Mesh topology:

- Amount of wires required to connected each system is tedious and headache.

  Since each device needs to be connected with other devices, number of I/O ports required must be huge.
- Scalability issues because a device cannot be connected with large number of devices with a dedicated point to point link.

Star Topology:

1.6 STAR TOPOLOGY

In star topology each device in the network is connected to a central device called hub. Unlike Mesh topology, star topology doesn't allow direct communication between devices, a device must have to communicate through hub. If one device wants to send data to other device, it has to first send the data to hub and then the hub transmit that data to the designated device.

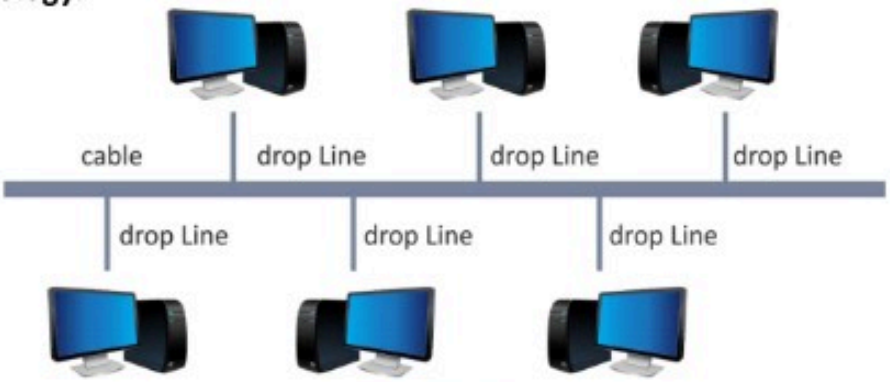
Advantages of Star topology:

- Less expensive because each device only need one I/O port and needs to be connected with hub with one link.
- Easier to install
- Less amount of cables required because each device needs to be connected with the hub only.
- Robust, if one link fails, other links will work just fine.
- Easy fault detection because the link can be easily identified.

Disadvantages of Star topology:

- If hub goes down everything goes down, none of the devices can work without hub.
- Hub requires more resources and regular maintenance because it is the central system of star topology.

Bus Topology:



1.7 BUS TOPOLOGY

In bus topology there is a main cable and all the devices are connected to this main cable through drop lines. There is a device called tap that connects the drop line to the main cable. Since all the data is transmitted over the main cable, there is a limit of drop lines and the distance a main cable can have.

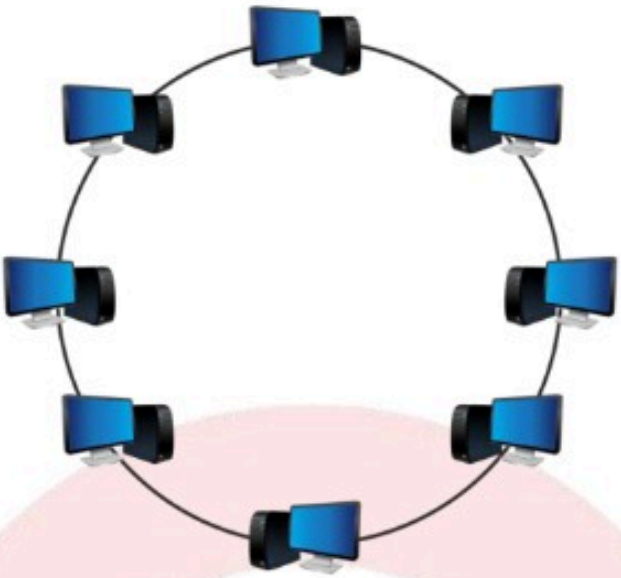
Advantages of bus topology:

- Easy installation, each cable needs to be connected with backbone cable.
- Less cables required than Mesh and star topology

Disadvantages of bus topology:

- Difficultly in fault detection.
- Not scalable as there is a limit of how many nodes you can connect with backbone cable.

Ring Topology:



[1.8 Ring Topology]

In ring topology each device is connected with the two devices on either side of it. There are two dedicated point to point links a device has with the devices on the either side of it. This structure forms a ring thus it is known as ring topology. If a device wants to send data to another device then it sends the data in one direction, each device in ring topology has a repeater, if the received data is intended for other device then repeater forwards this data until the intended device receives it.

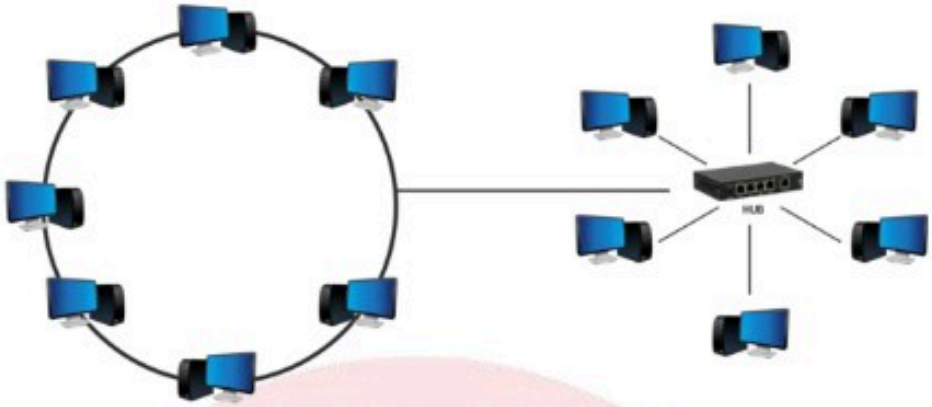
Advantages of Ring Topology:

- Easy to install.
- Managing is easier as to add or remove a device from the topology only two links are required to be changed.

Disadvantages of Ring Topology:

- A link failure can fail the entire network as the signal will not travel forward due to failure.
- Data traffic issues, since all the data is circulating in a ring.

Hybrid topology:



1.9 HYBRID TOPOLOGY

A combination of two or more topology is known as hybrid topology. For example a combination of star and mesh topology is known as hybrid topology.

Advantages of Hybrid topology:

- We can choose the topology based on the requirement for example, scalability is our concern then we can use star topology instead of bus technology.
- Scalable as we can further connect other computer networks with the existing networks with different topologies.

Disadvantages of Hybrid topology:

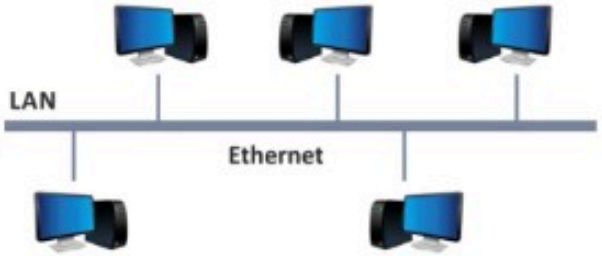
- Fault detection is difficult.
- Installation is difficult.
- Design is complex so maintenance is high thus expensive.

Types of Computer Network: LAN, MAN and WAN:

A computer network is a group of computers connected with each other through a transmission medium such as cable, wire etc. There are mainly three types of computer networks based on their size:

1) Local Area Network (LAN)
2) Metropolitan Area Network (MAN)
3) Wide area network (WAN)

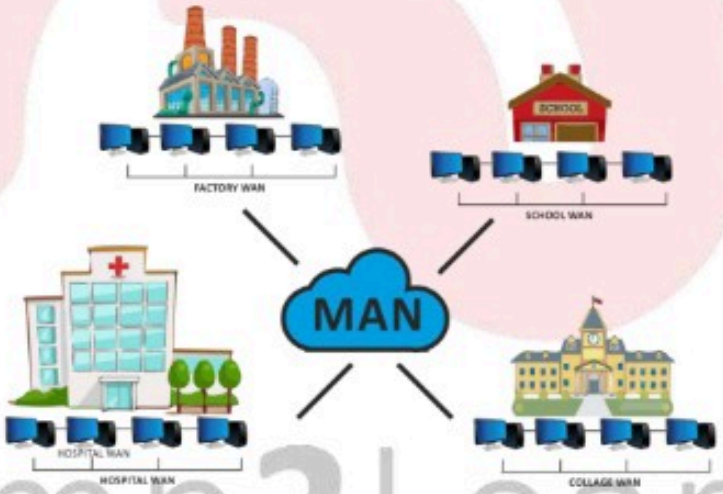
1. Local Area Network (LAN):



1.7 LOCAL AREA NETWORK (LAN)

Local area network is a group of computers connected with each other in a small places such as school, hospital, apartment etc. LAN is secure because there is no outside connection with the local area network thus the data which is shared is safe on the local area network and can't be accessed outside. LAN due to their small size are considerably faster, their speed can range anywhere from 100 to 100Mbps. LANs are not limited to wire connection, there is a new evolution to the LANs that allows local area network to work on a wireless connection.

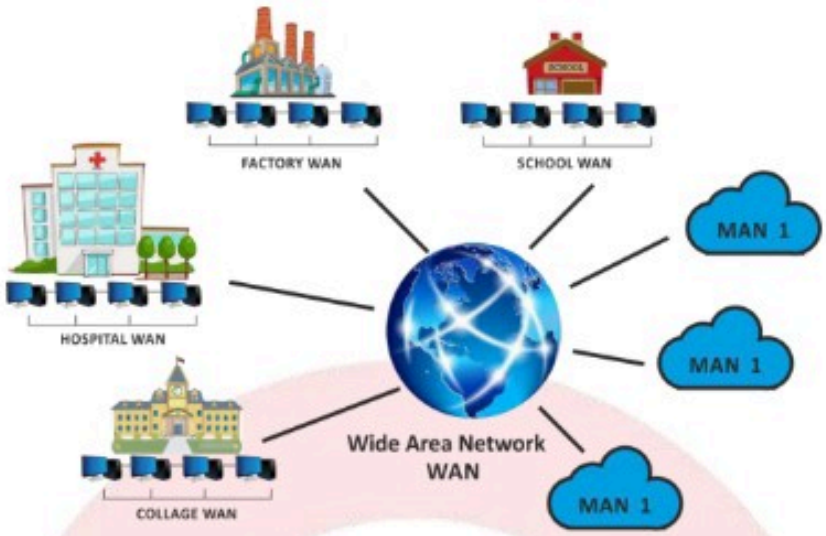
2. Metropolitan Area Network (MAN):



[1.8 Metropolitan Area Network (MAN)]

MAN network covers larger area by connections LANs to a larger network of computers. In Metropolitan area network various Local area networks are connected with each other through telephone lines. The size of the Metropolitan area network is larger than LANs and smaller than WANs(wide area networks), a MANs covers the larger area of a city or town.

2. Wide area network (WAN):



[1.9 Wide Area Network (WAN)]

Wide area network provides long distance transmission of data. The size of the WAN is larger than LAN and MAN. A WAN can cover country, continent or even a whole world. Internet connection is an example of WAN. Other examples of WAN are mobile broadband connections such as 3G, 4G etc.

Interconnection of Networks:

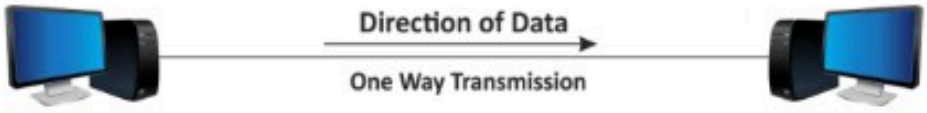
We have read LAN, MAN and WAN above, we also talked about internet. You can say that an internet is a combination of LAN, MAN and WAN.

Transmission Modes:

The data is transmitted from one device to another device through a transmission mode. The transmission mode decides the direction of data in which the data needs to travel to reach the receiver system or node. The transmission mode is divided in three categories:

- Simplex
- Half-Duplex
- Full-Duplex

Simplex Mode:



[1.10 Simplex Mode]

In simplex mode the data transmits in one direction only, from one system to another system. The sender device that sends data can only send data and cannot receive it. On the other hand the receiver device can only receive the data and cannot send it. Television is an example of simplex mode transmission as the broadcast sends signals to our TV but never receives signals back from our TV. This is a unidirectional transmission.

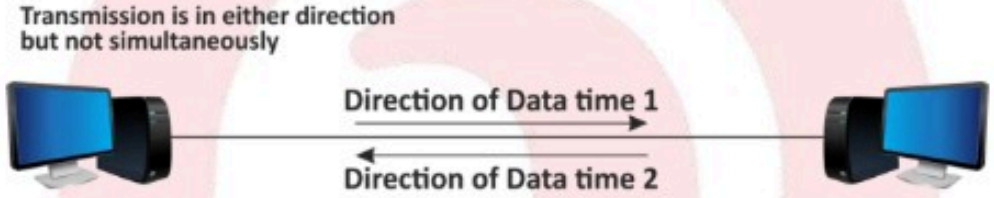
Advantages of Simplex Mode:

The full capacity of the transmission medium is utilized as the transmission is one way and cannot have traffic issues.

Disadvantages of Simplex Mode:

No bidirectional communication is possible. Two devices cannot communicate with each other using simplex mode of transmission.

Half-Duplex Mode:



[1.11 Half Duplex mode]

In half duplex mode transmission can be done both ways which means if two systems are connected with half-duplex mode of transmission, they both can send and receive data but not at the same time. If one device is sending data then other device cannot send data until it receives the data which is already in transmission. You can say that the communication is not simultaneous. The radio communication device that our soldiers use at the battle fields are the examples of half duplex mode transmission as they send message and then say over and then the person on other hand send his message and this way they communicate but not simultaneously like we used to do on mobile.

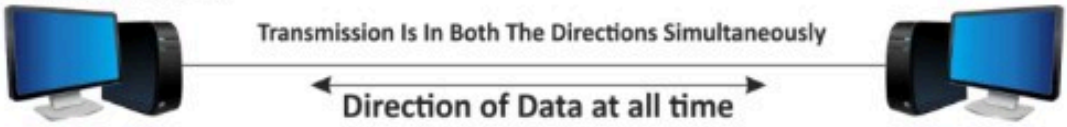
Advantages of Half-Duplex mode:

Both devices can send and receive data. Whole bandwidth can be utilized as at a time only one signal transmits.

Disadvantages of Half-Duplex mode:

The disadvantage in half duplex mode is that the other device cannot send data until it receives the data which is already in transmission, this can cause delays to the communication.

Full Duplex Mode:



[1.12 Full-Duplex mode]

In full duplex mode both the connected devices can send and receive data simultaneously. The mobile phone we use is an example of full duplex mode where we can communicate simultaneously. Both the devices can send and receive the data at the same time.

Advantages of Full Duplex mode:

No delays in communication as both can send and receive data simultaneously.

Disadvantages of Full Duplex mode:

No proper bandwidth utilization as the same line is used for sending and receiving data at the same time.

Network Models:

A computer network consists software and hardware that is used to send and receive data from one device to another. The role of hardware is to prove the physical equipment that are required in order to send and receive data while software defines the set of instructions that uses the hardware equipment for data transmission. A simple transmission of data consists several steps at various layers of computer network. In computer network models we will discuss the models in detail to understand how the data is actually transferred and received at a computer level.

Layers of network models:

1. The main purpose of having several layers in a computer network model is to divide a process of sending and receiving data into small-small tasks.
2. These layers are connected with each other, each layer provide certain data to its immediate higher and immediate lower layer and receives certain data from the same.

3. Dividing a model is layers makes the structure quite simple that makes it easy to identify the issue if it occurs. There are three main components of a computer network model. Sender, receiver and carrier.

At sender Side:

Higher layer: Higher layer serves the middle layer, directs the message (or data) to middle layer

Middle layer: Middle layer picks up the data from higher layer and transfer it to the lower layer

lower layer: The data is transmitted to the lower layer of the receiver side.

At receiver Side:

lower layer: Receives the data from the lower layer of sender side and transfer it to middle layer.

Middle layer: Middle layer picks up the data from lower layer and transfer to higher layer.

Higher layer: Higher layer transfers the data to the receiver.

The most important computer network models are:

1. OSI Model

2. TCP/IP Model

1.9 Defining Network Protocols

Protocol:-

Protocols are the agreed – upon ways that computers exchange information. A computer need to know exactly how message will arrive from the network so it can make sure the message gets to the right place. It needs to know how the network expects the message to formatted .so the network can convey the data to its destination.

Hardware Protocol:-

Hardware protocol define how hardware devices operate and work together. It determines such things as voltage levels and which pairs of wires will be used transmission and reception. There is no program involved, it is all done with circuitry.

Software Protocol:-

Programs communicate with each other via software protocols. Network client computers and network servers both have protocol packages that must be loaded to allow them to talk to other computers. These packages contain the protocols the computer needs to access a certain network device or services

The hardware –software Interface:-

Whenever a program in a computer to access hardware, such as when a message has arrived from the network and is now waiting in the adapter card's memory, ready to be received, the computer program uses a predefined hardware – software protocol. This basically means that the computer program can except the data to always be in the same place; that certain registers are accessed in the proper order, the card will do something logical, such as receive another message or send a message out.

1.10 INTRODUCTION TO WIRELESS NETWORK, AD-HOC WIRELESS AND SENSOR WIRELESS NETWORK

Wireless Networks

Mobile computers such as notebook computers laptops are fastest growing segment of computer industry. Users wants to connect this machine to their office LANs to see the data when they .are out from the office, since the wired connection is not possible we have to use wireless networks.

For e.g. on Aircraft single router will maintain a radio link with some other router on ground, changing routers as it flies along this configuration is just a traditional LAN, except that its connection to the outside world happens to be a radio link instead of a hardwired line

Ad-hoc Wireless

Wireless ad hoc networks are distributed networks that work without fixed infrastructures and in which each network node is willing to forward network packets for other network nodes. The main characteristics of wireless ad hoc networks are as follows:

- Wireless ad hoc networks are distributed networks that do not require fixed infrastructures to work. Network nodes in a wireless ad hoc network can be randomly deployed to form the wireless ad hoc network.
- Network nodes will forward network packets for other network nodes. Network nodes in a wireless ad hoc network directly communicate with other nodes within their ranges. When these networks communicate with network nodes outside their ranges, network packets will be forwarded by the nearby network nodes and other nodes that are on the path from the source nodes to the destination nodes.

- Wireless ad hoc networks are self-organizing. Without fixed infrastructures and central administration, wireless ad hoc networks must be capable of establishing cooperation between nodes on their own. Network nodes must also be able to adapt to changes in the network, such as the network topology.
- Wireless ad hoc networks have dynamic network topologies. Network nodes of a wireless ad hoc network connect to other network nodes through wireless links. The network nodes are mostly mobile. The topology of a wireless ad hoc network can change from time to time, since network nodes move around from within the range to the outside, and new network nodes may join the network, just as existing network nodes may leave the network.

Sensor Wireless Network

A wireless sensor network is an ad hoc network mainly comprising sensor nodes, which are normally used to monitor and observe a phenomenon or a scene. The sensor nodes are physically deployed within or close to the phenomenon or the scene. The collected data will be sent back to a base station from time to time through routes dynamically discovered and formed by sensor nodes.

Sensors in wireless sensor networks are normally small network nodes with very limited computation power, limited communication capacity, and limited power supply. Thus a sensor may perform only simple computation and can communicate with sensors and other nodes within a short range. The life spans of sensors are also limited by the power supply.

Wireless sensor networks can be self-organizing, since sensors can be randomly deployed in some inaccessible areas. The randomly deployed sensors can cooperate with other sensors within their range to implement the task of monitoring or observing the target scene or the target phenomenon and to communicate with the base station that collects data from all sensor nodes. The cooperation might involve finding a route to transmit data to a specific destination, relaying data from one neighbor to another neighbor when the two neighbors are not within reach of each other, and so on.