Chapter: 10

What Is a Network:

A network is defined as an interconnected collection of autonomous computers '. Two computers are said to be interconnected if they are capable of exchanging information. Central to this definition is the fact that the computers are autonomous. This means that no computer on the network can start, stop, or control another.

Network Goals:

Many organizations already have a substantial number of computers, often located far apart. For example, a company with many offices may have computers at each location

to keep track of customer orders, monitor sales, and do the local payroll. Previously, each of these computers may have worked in isolation from others but at some point, management decided to connect them to gather information about entire company. In general, we can refer to it as

(i) **Resource Sharing**. The aim is to make all programs, data, and peripherals available to anyone on the network irrespective of the physical location of the resources and the user.

(ii) **Reliability**. A file can have copies on two or three different machines, so if one of them is unavailable (hardware crash), the other copies could be used. For military, banking, air reservation and many other applications it is of importance.

(iii) **Communication Medium**. Using a network, it is possible for managers, working far apart, to prepare financial report of the company. The changes at one end can be immediately noticed at another and hence it speeds up co-operation among them.

Application of Networks:

- Resource sharing
- Increased reliability
- Reduced overall cost
- Better communication facilities.

Evolution Of Networking:

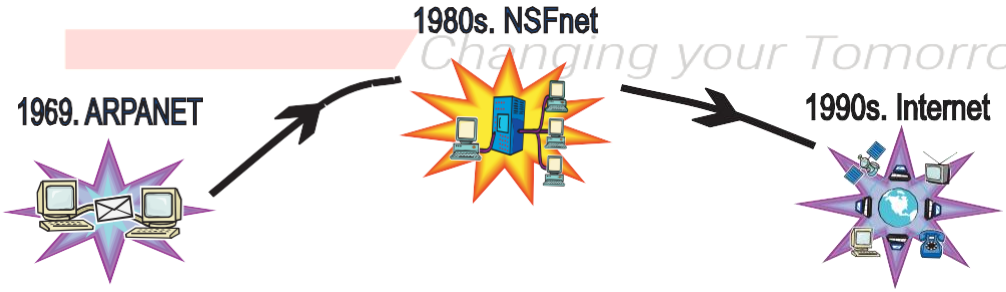
Evolution of networking started way back in 1969 by the development of first network called ARPANET, which led to the development of Internet. Let us learn how first network evolved to today's Internet.

Arpanet:

The seeds of today's Internet were planted in 1969, when U.S. Department of Defence sponsored a project named ARPANET (**Advanced Research Projects Agency NETwork**). The goal of this project was to connect computers at different universities and U.S. defence. Soon the engineers, scientists, students, and researchers who were part of this system, began exchanging data and messages on it. The users of this system were also able to play long

distance games and socialize with people who shared their interests. ARPANET started with a handful of computers, but it expanded rapidly. In mid-80's, another federal agency, the National Science Foundation, created a new, high- capacity network called NSFnet, which was more capable than ARPANET. NSFnet allowed only the academic research on its network and not any kind of private business on it. So many private companies built their own networks, which were later interconnected along with ARPANET and NSFnet to form Internet.

It was the Inter networking i.e., the linking of these two and some other networks (i.e., the ARPANET, NSFnet and some private networks) that was named Internet. The original ARPANET was shut down in 1990, and the government funding for NSFnet discontinued in 1995. But the commercial Internet services came into picture, which are still running the Internet.



The Internet:

The Internet is a worldwide network of computer networks that evolved from the first network ARPAnet. The Internet is made up of many networks each run by a different company and interconnected at peering points. It is an interconnection of large and small networks around the globe. The common use of Internet standards allows users connected to one network to communicate with users on another network.

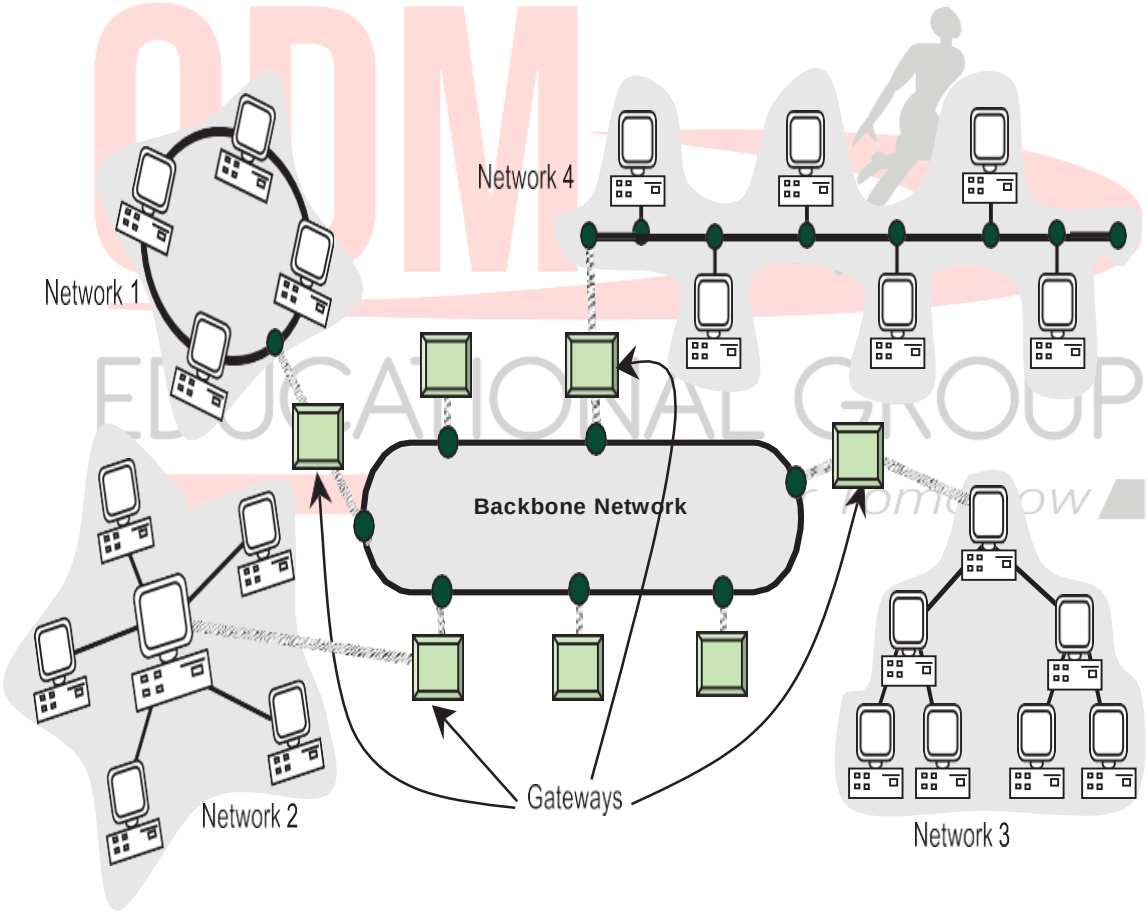
The Internet is a super-network. It connects many smaller networks together and allows all the computers to exchange information with each other. To accomplish this all the computers on the Internet, must use a common set of rules for communication. Those rules are called protocols, and the Internet uses a set of protocols called TCP/IP (Transmission Control Protocol/Internet Protocol).

How Does Internet Work?

In Internet, most computers are not connected directly to the Internet. Rather they are connected to smaller networks, which in turn are connected through gateways to the Internet backbone.

A **Gateway** is a device that connects dissimilar networks.

A **Backbone** is central interconnecting structure that connects one or more networks just like the trunk of a tree or the spine of a human being.



How Internet Functions:

- At the source computer, the message, or the file/document to be sent to another computer is firstly divided into small parts called Packets. A packet generally contains some information.
- Each packet is given a number serial wise e.g., 1, 2, 3.
- All these packets are then sent to the address of destination computer.
- The destination computer receives the packets in random manner. (It may even receive packet 10 before packet 1 arrives). If a packet is garbled or lost, it is demanded again.
- The packets are reassembled in the order of their number and the original message/file/document is obtained.

Internet Functioning:

The reason that the Internet works at all is that every computer connected to it uses the same set of rules for communication. Do you know that set of rules is called protocol ?

The communication protocol used by Internet is TCP/IP.

- The TCP (i.e., Transmission Control Protocol) part is responsible for dividing the file/message into packets on the source computer. It (TCP) is also responsible for reassembling the received packets at the destination or recipient computer.
- The IP (i.e., Internet Protocol) part is responsible for handling the address of destination computer so that each packet is routed (sent) to its proper destination. You shall learn about TCP/IP in details later in the chapter.

The Interspace:

- Interspace is a client/server software program that allows multiple users to communicate online with real-time audio, video, and text chat in dynamic 3D environments.
- The Interspace is a vision of what the Internet will become, where users cross-correlate information in multiple ways from multiple sources.

Elementary Terminology of Networks:

Nodes (Workstations):

The term nodes refer to the computers that are attached to a network and are seeking to share the resources of the network. Of course, if there were no nodes (also called workstations), there would be no network at all.

Server:

On small networks, sometimes, all the shareable stuff (like files, data, software etc.) is stored on the server. A network can have more than one server also. Each server has a unique name on the network and all users of network identify the server by its unique name.

Servers can be of two types: (i) non-dedicated and (ii) dedicated servers.

Non-dedicated Servers:

On small networks, a workstation that can double up as a server, is known as non- dedicated server since it is not completely dedicated to the cause of serving. Such servers can facilitate the resource-sharing among workstations on a proportionately smaller scale. Since one computer works as a workstation as well as a server, it is slower and requires more memory. The (small) networks using such a server are known as PEER-TO-PEER networks.

Dedicated Servers:

On bigger network installations, there is a computer reserved for server's job and its only job is to help workstations access data, software, and hardware resources. It does not double-up as a workstation and such a server is known as dedicated server. The networks using such a server are known as MASTER-SLAVE networks.

Network Interface Unit (NIU):

A standalone computer (a computer that is not attached to a network) lives in its own world and carries out its tasks with its own inbuilt resources. But as soon as it becomes a workstation, it needs an interface to help establish a connection with the network because without this, the workstations will not be able to share network resources.

The network-interface-unit is a device that is attached to each of the workstations and the server, and helps the workstation establish the all-important connection with the network. Each network-interface-unit that is attached to a workstation has a unique number identifying it which is known as the node

address. The NIU is also called Terminal Access Point (TAP). Different manufacturers have different names for the interface. The NIU is also called NIC – The

NIC manufacturer assigns a unique physical address to each NIC card ; this physical address is known as MAC address.

Switching Techniques:

Well, by now you know the significance of networks. One major purpose and use of networks is the sharing or transfer of data and information. Do you know how data are transmitted across networks? Well, for this various switching techniques are used.

Different types of switching techniques are employed to provide communication between two computers. These are: circuit switching, message switching and packet switching.

Circuit Switching:

In this technique, first the complete physical connection between two computers is established and then data are transmitted from the source computer to the destination computer. That is, when a computer places a telephone call, the switching equipment within the telephone system seeks out a physical copper path all the way from sender telephone to the receiver's telephone. The important property of this switching technique is to setup an end-to-end path (connection) between computer before any data can be sent.

Message Switching:

In this technique, the source computer sends data or the message to the switching office first, which stores the data in its buffer. It then looks for a free link to another switching office and then sends the data to this office. This process is continued until the data are delivered to the destination computers. Owing to its working principle, it is also known as store and forward. That is, store first (in switching office), forward later, one jump at a time.

Packet Switching:

With message switching, there is no limit on block size, in contrast, packet switching places a tight upper limit on block size. A fixed size of packet which can be transmitted across the network is specified. Another point of its difference from message switching is that data packets are stored on the disk in message switching whereas in packet switching, all the packets of fixed size are stored in main memory. This improves the performance as the access time (time taken to access a data packet) is reduced, thus, the throughput (measure of performance) of the network is improved.

Data Communication Terminologies:

Let us now talk about some common data communication Terminologies.

Data Channel:

channel is the medium used to carry information or data from one point to another.

Baud:

It is the unit of measurement for the information carrying capacity of a communication channel. The baud is synonymous with bps (bits per second), another unit of measuring data transfer rates.

Bits Per Second (bps):

It refers to the speed at which data transfer is measured. It is generally used to measure the speed of information through a high-speed phone lines or modems.

Bytes per second are denoted as Bps – notice the capital B. Small b i.e., bps stands for

bits per second.

- The rate of a thousand bits per second is known as kbps i.e., kilobits per second. (Small k in kbps).
- A rate of a thousand bytes per second is denoted by Kbps (Kilo bytes per second).

  Notice the capital K.
- A rate of a million bits per second is denoted through mbps – megabits per second. (Small m in mbps).
- A rate of a million bytes per second is denoted as Mbps. (Capital M in Mbps).

Bandwidth:

Technically, the bandwidth refers to the difference between the highest and lowest frequencies of a transmission channel. Or in other words, the bandwidth refers to the width of allocated band of frequencies to a channel.

- In digital systems, bandwidth is data speed in bits per second (bps).
- A kilohertz (kHz) represents a thousand cycles per second

Data Transfer Rates:

The data transfer rate represents the amount of data transferred per second by a communications channel or a computing or storage device.

Data rate is measured in units of bits per second (bps), bytes per second (Bps), or baud.

Transmission Media:

By transmission media or communication channels of network, it is meant that the 'connecting cables' or 'connecting media 'are being talked about. The cables that connect two or more workstations are the communication channels.

Types Of Communication Media:

We can group the communication media in two categories:

- **Guided media**
- **Unguided media**

and being discussed below. also being discussed.

Guided media:

The **guided** media includes cables. The basic types of cables (*i.e.*, guided media) are

- Twisted pair cable
- Coaxial cable
- Optical fiber

Unguided media:

Unguided media includes waves through air, water, or vacuum. The unguided media are

- Microwaves
- Radio waves
- Satellites

Twisted Pair Cable:

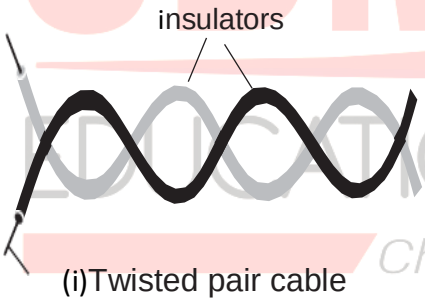
The most common form of wiring in data communication application is the twisted pair cable. As a voice grade medium (VGM), it is the basis for most internal office telephone wiring. It consists of two identical wires wrapped together in a double helix.

Problems can occur due to differences in the electrical characteristics between the pair (e.g., length, resistance, capacitance). For this reason, LAN applications will tend to use a higher quality cable known as data grade medium (DGM).

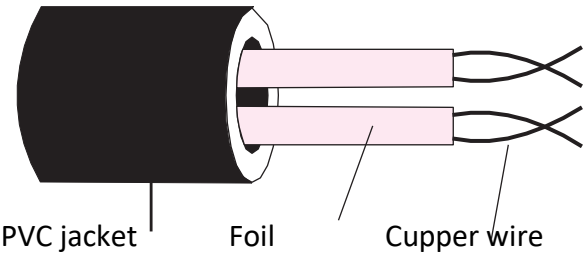
Different types and categories of twisted-pair cable exist, but they all have two things in common:

- The wires come in pairs.
- The pairs of wires are twisted around each other.

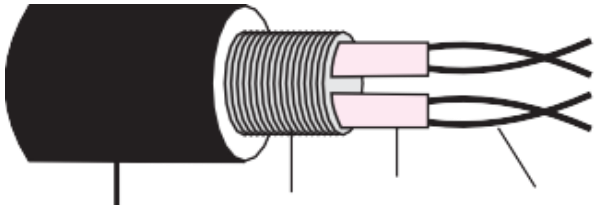
The twisting of wires reduces **crosstalk**, which is the bleeding of a signal from one wire to another and which can corrupt signal and cause network errors. The twisting of the wires not only protects the signal from internal crosstalk, but it also protects it form other external forms of signal interference is called crosstalk.



(i)Twisted pair cable



(ii) Unshielded twisted pair cable



(iii) Shielded twisted pair cable

Advantages:

The main advantages of twisted pair cable are:

(i) It is simple. (ii) It is easy to install and maintain.

(iii) It is physically flexible. (iv) It has a low weight.

(iv) It can be easily connected. (vi) It is very inexpensive

Disadvantages:

(i) Because of high attenuation, it is incapable of carrying a signal over long distances without the use of repeaters (discussed later in the chapter).

(ii) Its low bandwidth capabilities make it unsuitable for broadband applications.

(iii) It supports maximum data rates 1 Mbps without conditioning and 10 Mbps with conditioning.

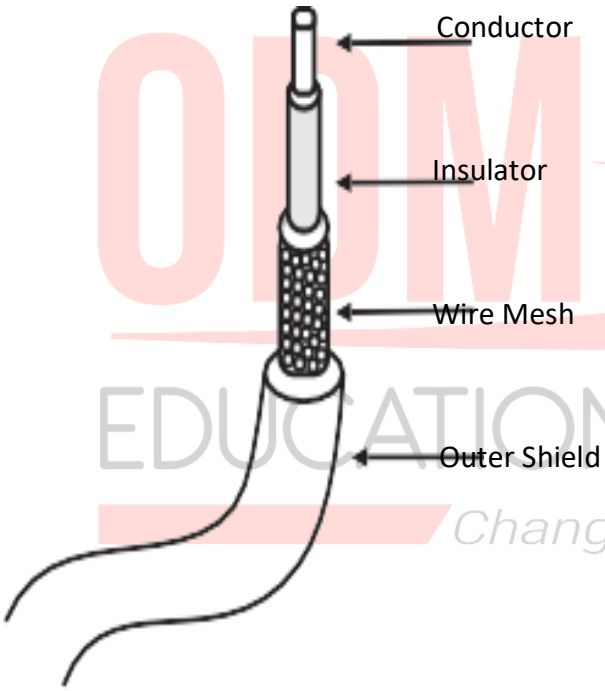
There are two types of twisted pair cables available. These are :

(i) **Unshielded Twisted Pair (UTP) Cable**. UTP cabling is used for variety of electronic communications. The UTP cables can have maximum segment length of 100 metres.

(ii) **Shielded Twisted Pair (STP) Cable**. This type of cables comes with shielding of the individual pairs of wires, which further protects it from external interference. But these also, like UTP, can have maximum segment length of 100 meters. The advantage of STP over UTP is that it offers greater protection from interference and crosstalk due to shielding. But it is heavier and costlier than UTP and requires proper grounding at both ends.

Coaxial Cable:

This type of cable consists of a solid wire core surrounded by one or more foil or wire shields, each separated by plastic insulator. The inner core carries the signal, and the shield provides the ground. The coaxial cable has high electrical properties and is suitable for high speed communication. it is widely used for television signals. In the form of (CATV) cable, it provides a cheap means of transporting multi-channel television signals around metropolitan areas. It is also used by large corporations in building security systems.



Advantages:

(i) The data transmission characteristics of coaxial cables are considerably better than those of twisted-pair cables.

(ii) The coaxial cables can be used as the basis for a shared cable network.

(iii) The coaxial cables can be used for broadband transmission i.e., several channels can be transmitted simultaneously (as with cable TV).

(iv) Offers higher bandwidths-up to 400 MBPS.

Disadvantages:

(i) Expensive compared to twisted pair cables.
(ii) The coaxial cables are not compatible with twisted pair cables.

Types of Coaxial Cables:

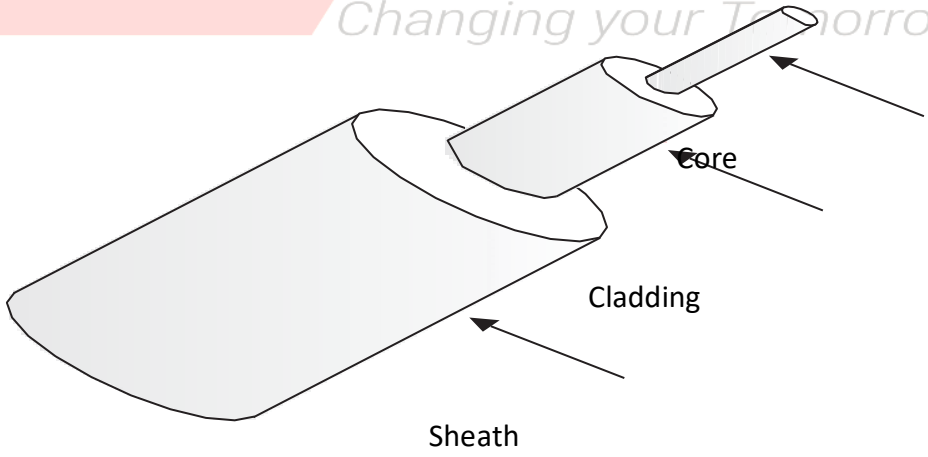
(i) Thicknet. This form of coaxial cable is thicker than thinnet. The thicknet coaxial cable segments (while joining nodes of a network) can be up to 500 meters long.
(ii) Thinnet. This form of coaxial cable is thinner, and it can have maximum segment length of 185 meters i.e., using this cable, nodes having maximum distance of 185 meters can be joined.

Optical Fibers:

Optical fibers consist of thin strands of glass or glass like material which are so constructed that they carry light from a source at one end of the fiber to a detector at the other end. The light sources used are either light emitting diodes (LEDs) or laser diodes (LDs). The data to be transmitted is modulated onto the light beam using frequency modulation techniques. The signals can then be picked up at the receiving end and demodulated.

The fiber cable consists of three pieces :

- The core, i.e., the glass or plastic through which the light travels
- The cladding, which is a covering of the core that reflects light back to the core
- Sheath, a protective coating, which protects the fiber cable from hostile environment



Advantages:

(i) It is immune to electrical and magnetic interference i.e., noise in any form because the information is travelling on a modulated light beam.

(ii) It is highly suitable for harsh industrial environments.
(iii) it guarantees secure transmission and has an extremely high transmission capacity.
(iv) Fiber optic cables can be used for broadband transmission where several channels (i.e., bands of frequency) are handled in parallel and where it is also possible to mix data transmission channels with channels for telescope, graphics, TV, and sound.

Disadvantages:

(i) Installation problem. Fiber optic cables are quite fragile and may need special care to make them sufficiently robust for an office environment.
(ii) Connecting either two fibers together or a light source to a fiber is a difficult process.
(iii) Because of noise immunity, optical fibers are virtually impossible to tap. To incept the signal, the fiber must be cut and a detector inserted.
(iv) Light can reach the receiver out of phase.
(v) Connection losses are common problems.
(vi) Fiber optic cables are more difficult to solder.
(vii) They are the most expensive of all the cables.

Types of Fibre Optic Cables:

Fibre optic cable can be either **single node** that supports a segment length of up to 2 kms and band-width of up to 100 Mbps or **Multi node** with a segment length of 100 kms and bandwidth of 2 Gbps.

Unguided Media:

Microwave (Terrestrial Microwave):

Microwave signals are used to transmit data without the use of cables. The microwave signals are like radio and television signals and are used for long distance communication. The microwave transmission consists of a transmitter, receiver, and the atmosphere.

In microwave communication, parabolic antennas are mounted on towers to send a beam to other antennas tens of kilometres away. The higher the tower, the greater the range. With a 100-meter high tower, distances of 100 km between towers are feasible. The microwave transmission is line-of-sight1 transmission.

Advantages:

(i) It proves cheaper than digging trenches for laying cables and maintaining repeaters and cables if cables get broken by a variety of causes.

(ii) It offers freedom from land acquisition rights that are required for laying, repairing the cables.
(iii) It offers ease of communication over difficult terrain.
(iv) Microwaves can communicate over oceans.

Disadvantages:

(i) Microwave communication is an insecure communication.
(ii) Signals from a single antenna may split up and propagate by slightly different paths to the receiving antenna. When these out-of-phase signals recombine, they interfere, reducing the signal strength.
(iii) Microwave propagation is susceptible to weather effects like rains, thunder storms etc.
(iv) Bandwidth allocation is extremely limited in case of microwaves.
(v) The cost of design, implementation, and maintenance of microwave links is high.

Radio Wave:

The transmission making use of radio frequencies is termed as radio-wave transmission. We all are familiar with radios and their working. When certain radio frequencies are allocated to private businesses for direct voice communication, they can make use of it for private business purposes. In general, private citizens and business users are licensed to operate in the range of about 10 miles.

All radios today, however, use continuous sine waves to transmit information (audio, video, data). Each different radio signal uses a different sine wave frequency, and that is how they are all separated. Any radio setup has two parts :

1. **The transmitter** 2. **The receiver**

The transmitter takes some sort of message (it could be the sound of someone's voice, pictures for a TV set, data for a radio modem or whatever), encodes it onto a sine wave and transmits it with radio waves. The receiver receives the radio waves and decodes the message from the sine wave it receives. Both the transmitter and receiver use antennas to radiate and capture the radio signal.

Advantages:

(i) Radio-wave transmission offers mobility.
(ii) It proves cheaper than digging trenches for laying cables and maintaining repeaters and cables if cables get broken by a variety of causes.

(iii) It offers freedom from land acquisition rights that are required for laying, repairing the cables.

(iv) It offers ease of communication over difficult terrain.

Disadvantages:

(i) Radio-wave communication is an insecure communication.

(ii) Radio-wave propagation is susceptible to weather effects like rains, thunderstorms etc.

Satellite (Satellite Microwave):

Radio wave can be classified by frequency and wavelength. When the frequency is higher than 3 GHz, it is named microwave. Satellite communication is special case of microwave relay system. Satellite communications use the synchronous satellite to relay the radio signal transmitted from ground station. It provides voice, fax, data, and video services as well as email, file transfer, WWW internet applications. When fixed wire terrestrial communication networks are crushed by a disaster, the satellite and microwave system as a emergency backup facility will be stressed.

In satellite communication the earth station consists of a satellite dish that functions as an antenna and communication equipment to transmit and receive data from satellites passing overhead.

Several communication satellites, owned by both governments and private organizations, have been placed in stationary orbits about 22,300 miles above the earth's surface. These satellites act as relay stations for communication signals. The satellites accept data/ signals transmitted from an earth station, amplify them, and retransmit them to another earth station. Using such a setup, data can be transmitted to the other side of the earth in only one step.

Most communication satellites have multiple, independent reception and transmission devices known as **transponders**. In a commercial communication satellite, a single trans- ponder is usually capable of handling a full-colour, commercial television transmission, complete with audio. Transponders for data transmission may be even larger. Some firms that market satellite communications service own a satellite. Others lease a portion of a satellite and provide transmission facilities in smaller units to ultimate users. The security in satellite transmission is usually provided by the coding and decoding equipment.

Advantages:

(i) The area coverage through satellite transmission is quite large.

(ii) The laying and maintenance of intercontinental cable is difficult and expensive, and this is where the satellite proves to be the best alternative.

(iii) The heavy usage of intercontinental traffic makes the satellite commercial attractive.

(iv) Satellites can cover large areas of the Earth. This is particularly useful for sparsely populated areas.

Disadvantages:

(i) Technological limitations preventing the deployment of large, high gain antennas on the satellite platform.
(ii) Over-crowding of available bandwidths due to low antenna gains.
(iii) The high investment cost and insurance cost associated with significant probability of failure.
(iv) High atmospheric losses above 30 GHz limit carrier frequencies.

Infrared:

This type of transmission uses infrared light to send data. You can see the use of this type of transmission in everyday life – TV remotes, automotive garage doors, wireless speakers etc., all make use of infrared as transmission media.

The infrared light transmits data through the air and can propagate throughout a room (bouncing off surfaces) but will not penetrate walls. The infrared transmission has become common in PDAs (Personal digital assistants) e.g., handheld devices like palm pilots etc.

The infrared transmission is a secure one.

Laser:

The laser transmission requires direct line-of-sight. It is unidirectional like microwave but has much higher speed than microwaves. The laser transmission requires the use of a laser transmitter and a photo-sensitive receiver at each end. The laser transmission is point-to-point transmission, typically between buildings.

But lasers have a certain disadvantage, which is : it can be adversely affected by weather.

Types Of Networks:

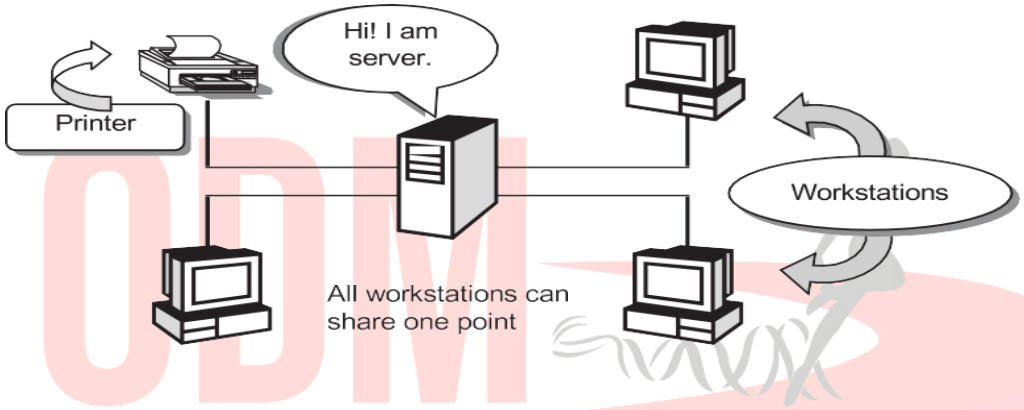
A computer network means a group of computers that are linked by means of a communication system. A network can mean a small group of linked computers to a chain of a few hundred computers of different types (e.g., PCs, minis, mainframes etc.) spread around the world. Thus, networks vary in size, complexity, and geographical spread. Mostly, computers are classified based on geographical spread and on this basis, there can be four types of networks :

- Local Area Networks (LANs)
- Metropolitan Area Networks (MANs)

- Wide Area Networks (WANs)
- Personal Area Network (PAN)

Local Area Network (LAN):

Small computer networks that are confined to a localised area (e.g., an office, a building, or a factory) are known as Local Area Networks (LANs). The key purpose of a LAN is to serve its users in resource sharing. The hardware as well as software resources are shared through LANs. For instance, LAN users can share data, information, programs, printer, hard-disks, modems etc.



In a typical LAN configuration, one computer is designated as the file server2. It stores all the software that controls the network, as well as the software that can be shared by the computers attached to the network. Computers connected to the file server are called workstations. The work- stations can be less powerful than the file server, and they may have additional software on their hard drives. On most LANs, cables are used to connect the network interface cards3 in each computer.

Metropolitan Area Network (MAN):

Metropolitan Area Networks are the networks spread over a city. For example, cable TV networks that are spread over a city, can be termed as metropolitan area networks. The purpose of a MAN is also the sharing of hardware and software resources among its users.

Wide Area Networks (WAN):

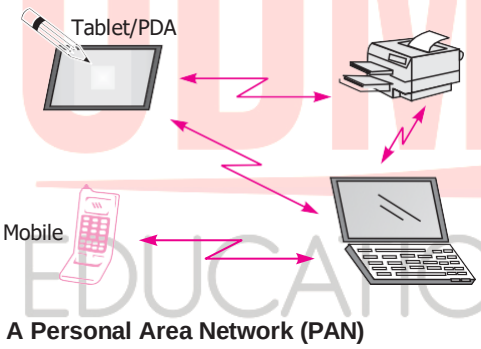
The networks spread across countries are known as WANs. A Wide Area Network (WAN) is a group of computers that are separated by large distances and tied together. It can even be a group of LANs that are spread across several locations and connected to look like one big LAN. The WANs link computers to

facilitate fast and efficient exchange of information at lesser costs. Computers connected to a wide-area network are often connected through public networks, such as the telephone system. Sometimes they can be connected through leased lines4 or satellites. The largest WAN in existence is the Internet.

Personal Area Network (PAN):

A personal area network (PAN) is the interconnection of information technology devices within the range of an individual person, typically within a range of 10 meters.

For **example**, a person traveling with a laptop, a personal digital assistant (PDA), and a portable printer could interconnect them without having to plug anything in, using some form of wireless technology such as Wi-Fi. Typically, this kind of personal area network could also be interconnected without wires to the Internet or other networks. You can use PAN networks to transfer files including email and calendar appointments, digital photos, and music etc from your portable devices such as phones and tablets to PC



A Personal Area Network (PAN)

Difference between a LAN and a WAN:

	LAN	WAN
1.	Diameter of not more than a few kilometers.	Span entire countries.
2.	A total data rate of at least several mbps.	Data rate less than 1 mbps (Megabits per second).
3.	Complete ownership by a single organization.	Owned by multiple organization.
4.	Very low error rates.	Comparatively higher error rates.

NETWORK TOPOLOGIES:

The pattern of interconnection of nodes in a network is called the topology of a network.

factors to consider in making this choice, the most important of which are set out below:

Cost. For a network to be cost effective, one would try to minimize installation cost.

Flexibility. Because the arrangement of furniture, internal walls etc. in offices is often subject to change, the topology should allow for easy reconfiguration of the network. This involves moving existing nodes and adding new ones.

Reliability. Failure in a network can take two forms. Firstly, an individual node can malfunction. This is not nearly as serious as the second type of fault where the network itself fails to operate. The topology chosen for the network can help by allowing the location of the fault to be detected and to provide some means of isolating it.

Point-to-Point Link

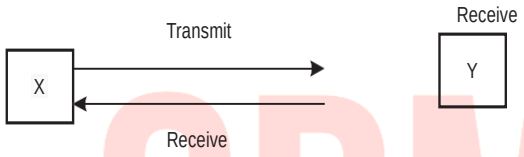


Fig. 14.6 Point-to-Point Network.

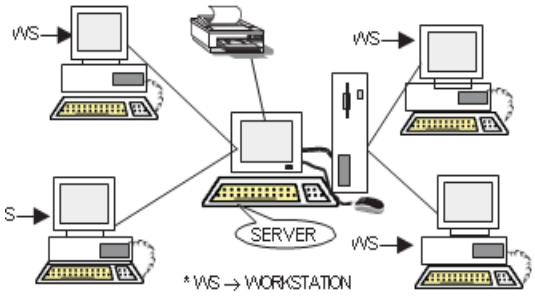
The main characteristic of P-P network is that each station receives exactly from one transmitter, and each transmitter transmits to exactly one receiver.

Many topologies have been developed, but major ones are:

- Star topology
- Bus topology
- Ring topology
- circular topology
- Tree topology
- Graph topology
- Mesh topology

The Star Topology:

This topology consists of a central node to which all other nodes are connected by a single path. It is the topology used in most existing information networks involving data processing or voice communications. The most common example of this is IBM 370 installations. In this case multiple 3270 terminals are connected to either a host system or a terminal controller.



Advantages of the Star Topology:

- Ease of service.
- One device per connection.
- Centralized control/problem diagnosis.
- Simple access protocols.

Disadvantages of the Star Topology:

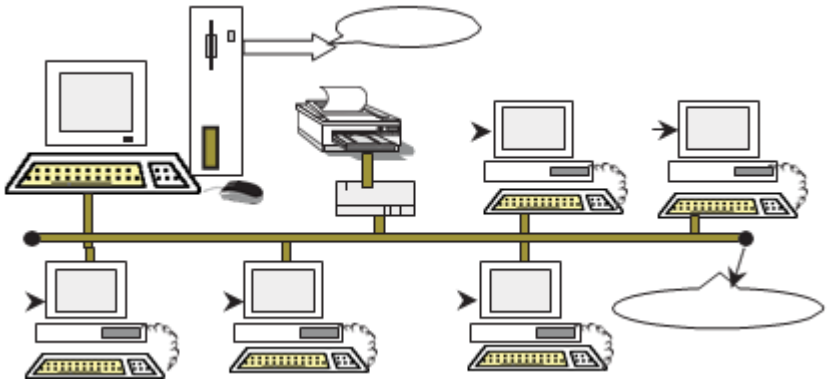
- Long cable length.
- Difficult to expand.
- Central node dependency.

The Bus or Linear Topology:

Another popular topology for data networks is the linear. This consists of a single length of the transmission medium (normally coaxial cable) onto which the various nodes are attached .The topology is used in traditional data communication network where the host at one end of the bus communicates with several terminals attached along its length.

The transmission from any station travels the length of the bus, in both directions, and can be received by all other stations. The bus has terminators at either end which absorb the signal, removing it from the bus.

SERVER



ws

TERMINATOR

Bus Topology.

Data is transmitted in small blocks, known as packets. Each packet has some data bits, plus a header containing its destination address. A station wanting to transmit some data sends it in packets along the bus. The destination device, on identifying the address on the packets, copies the data onto its disk.

Advantages of the Linear Topology:

- Short cable length and simple wiring layout.
- Resilient Architecture.
- Easy to extend.

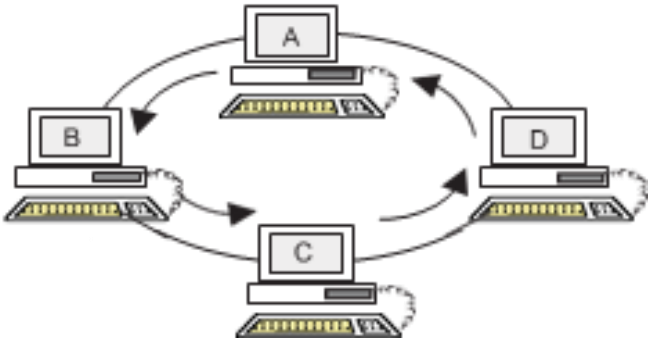
Disadvantages of the Linear Topology:

- Fault diagnosis is difficult.
- Fault isolation is difficult.
- Repeater configuration.
- Nodes must be intelligent.

The Ring or Circular Topology:

The third topology that we will consider is the ring or circular. In this case, each node is connected to two and only two neighbouring nodes. Data is accepted from one of the neighbouring nodes and is transmitted onwards to another. Thus, data travels in one direction only, from node to node around the ring. After passing through each node, it returns to the sending node, which removes it.

It is important to note that data 'passed through' rather than 'travels past' each node. This means that the signal may be

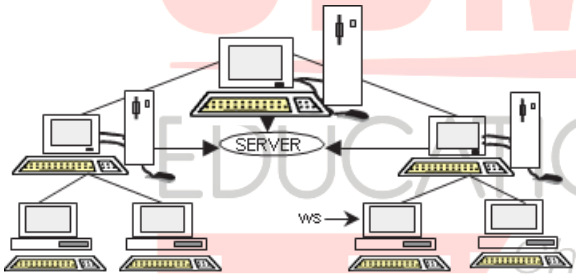


Advantages of the Ring Topology:

- Short cable length.
- No wiring closet space required.
- Suitable for optical fibers.

The Tree Topology:

A variation of bus topology is the *tree topology*. The shape of the network is that of an inverted tree with the central root branching and sub-branching to the extremities of the network .

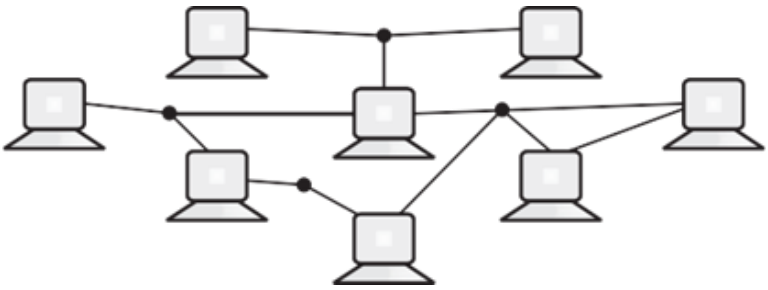


Tree Topology.

Transmission in this topology takes place in the same way as in the bus topology. In both cases, there is no need to remove packets from the medium because when a signal reaches the end of the medium, it is absorbed by the terminators. Tree topology is best suited for applications which have a hierarchical flow of data and control.

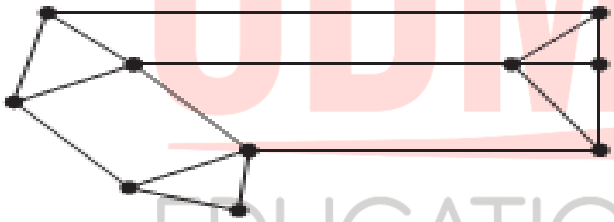
Graph Topology:

In this topology, nodes are connected in an arbitrary fashion. A link may or may not connect two or more nodes. There may be multiple links also. It is not necessary that all the nodes are connected. But if a path can be established in two-nodes via one or more links, it is called a connected graph.



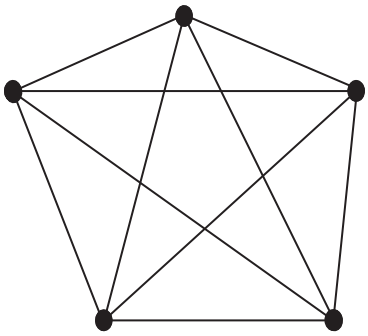
Mesh Topology:

In this topology, each node is connected to more than one node to provide an alternative route in the case the host is either down or too busy. It is an extension to P-P network. The mesh topology is excellent for long distance networking because it provides extensive back-up, rerouting, and pass-through capabilities. Communication is possible between any two nodes on the network either directly or by passing through. This function is needed in the event of a line or node failure elsewhere in the network. The mesh topology is commonly used in large internetworking environments with stars, rings, and buses attached to each node. This is also ideal for distributed networks.



Fully Connected:

When in a network each host is connected to other directly i.e., there is a direct link between each host, then the network is said to be fully connected. This characteristic is termed as full connectivity.



Network Devices:

In the smooth functioning of networks, many devices play important roles. Here, in this section, we are going to discuss a few of them.

Modem:

A Modem is a computer peripheral that allows you to connect and communicate with other computers via telephone lines. Modems allow you to combine the power of your computer with the global reach of the telephone system. modem changes the digital data from your computer into analog data, a format that can be carried by telephone lines. In a similar manner, the modem receiving the call then changes the analog signal back into digital data that the computer can digest Called **modulation/demodulation.** Modems come in two varieties:

Internal modem: the modems that are fixed within the computer.
External modems: the modems that are connected externally to a computer as other peripherals are connected

RJ-45:

RJ-45 is short for Registered Jack-45. RJ-45 is an eight-wire connector, which is commonly used to connect computers on the local area networks i.e., LANs, especially Ethernets. (Ethernet is a LAN architecture developed by Xerox Corp along with DEC and Intel. Ethernet uses either a bus or star topology and supports data transfer rates of up to 10.

Ethernet Card:

As mentioned earlier, Ethernet is a LAN architecture developed by *Xerox Corp* in association with DEC and Intel. Ethernet uses bus or star topologies and can support data transfer rates of up to 10 Mbps. The computers that are part of Ethernet, have to install a special card called **Ethernet Card.**

Hub:

A **hub** is a hardware device used to connect several computers together. A *hub* that contains multiple independent but connected modules of network and inter-networked equipment. A similar term is **concentrator**. A *concentrator* is a device that provides a central connection point for cables from workstations, servers, and peripherals. In a star topology, twisted-pair wire is run from each workstation to a central concentrator.

Basically, hubs are multi-slot concentrators into which several multi-port cards can be plugged to provide additional access as the network grows. Hubs can be either *passive* or *active*.

Active hubs electrically amplify the signal as it moves from one connected device to another. Active concentrators are used like *repeaters*8 to extend the length of a network.

Passive hubs allow the signal to pass from one computer to another without any change.

Switch:

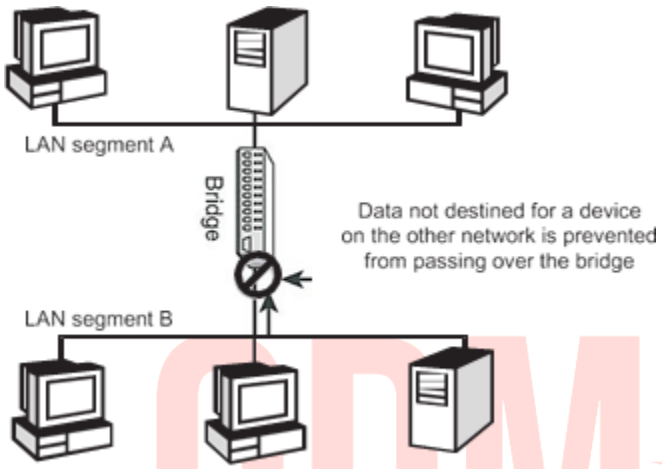
A switch is a device that is used to segment networks into different *subnetworks* called ***subnets*** or ***LAN segments***. Segmenting the network into smaller subnets, prevents traffic overloading in a network. A switch is responsible for *filtering i.e.*, transforming data in a specific way and for forwarding *packets* (a piece of message being transmitted) between LAN segments. Switches support any packet protocol.

Repeater:

A repeater is a device that amplifies a signal being transmitted on the network. Over distance, the cables connecting a network lose the signal transmitted. If the signal degrades too much, it fails to reach the destination. Or if it does arrive, the degradation of the message makes it useless. Repeaters can be installed along the way to ensure that data packets reach their destination. Repeaters are of two kinds : **amplifier and signal repeater**.

Bridge:

A bridge is a device that lets you link two networks together. Bridges are smart enough to know which computers are on which side of the bridge, so they only allow those messages that need to get to the other side to cross the bridge. This improves performance on both sides of the bridge. As a packet arrives at the bridge, the bridge examines the physical destination address of the packet. The bridge then decides whether to let the packet cross.



Gateway

A gateway is a device that connects dissimilar networks. A gateway operates at the highest layer of network abstraction. It expands the functionality of routers by performing data translation and protocol conversion. It is needed to convert Ethernet traffic from the LAN, to SNA10 (Systems Network Architecture) traffic on a legacy system. It then routes the SNA traffic to the mainframe. When the mainframe answers, the reverse process occurs.

Wi-Fi Card:

A Wi-Fi card is either an internal or external Local Area Network adapter with a built-in wireless radio and antenna. The most common Wi-Fi cards used in desktop computers are PCI-Express WiFi cards made to fit the PCI-Express card slots on the motherboard.

PCMCIA WiFi Card Express Card WiFi Card USB WiFi Card

Benefits:

The primary benefit of using a WiFi card in a desktop computer is that it allows you to setup your work-station or home office without considering the proximity or availability of hard-line network access.

Good Network Design: The 80-20 Rule

In a properly designed small to medium- sized network environment, 80 percent of the traffic on a given network segment is local (destined for a target in the same workgroup), and not more than 20 percent of the network traffic should need to move across a backbone (the spine that connects various segments or subnetworks).

COMMUNICATION PROTOCOLS:

A protocol means the rules that are applicable for a network. Protocol defines standardized formats for data packets, techniques for detecting and correcting errors and so on. A protocol is "a formal description of message formats and the rules that two or more machines must follow to exchange those messages.'' We need protocols every time we want to do something on another computer.

HTTP (Hypertext Transfer Protocol):

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring hypertext (i.e., text, graphic, image, sound, video etc.) on WWW (World Wide Web).

The Hypertext Transfer Protocol (HTTP) is an application-level protocol with the lightness and speed necessary for distributed, collaborative, hypermedia information systems. It is a generic, stateless, object-oriented protocol which can be used for many tasks, such as name servers and distributed object management systems, through extension of its request methods (commands).

HTTP is also used as a generic protocol for communication between user agents and proxies/gateways to other Internet protocols, such as SMTP, NNTP, FTP, Gopher and WAIS.

The HTTP protocol consists of two distinct items : the set of requests from browsers to servers and the set of responses going back to the other way.

FTP (File Transfer Protocol):

One of the original services on the internet was designed to allow for transferring files from one system to another. It goes by the name ftp which stands for file transfer protocol.

FTP offers these advantages :

- It is especially useful to transfer files from one network in an organization to another.

- It is an effective way to get a geographically dispersed group to co-operate on a project.
- It is a potent and popular way to share information over the internet.

TCP/IP (Transmission Control Protocol/Internet Protocol):

- The TCP (i.e., Transmission Control Protocol) part is responsible for dividing the file/message into packets on the source computer. It (TCP) is also responsible for reassembling the received packets at the destination or recipient computer.
- The IP (i.e., Internet Protocol) part is responsible for handling the address of destination computer so that each packet is routed (sent) to its proper destination.

Generally, TCP/IP applications use four layers :

- an application protocol such as mail
- a protocol such as TCP that provides services need by many applications
- IP, which provides the basic service of getting datagrams to their destination
- the protocols needed to manage a specific physical medium, such as Ethernet or a point to point line.

Most of the network software deals strictly in terms of the address. TCP/IP is built on "connectionless'' technology. Information is transferred as a sequence of "datagrams''.(A Datagram is a collection of the data that is sent as a single message.)

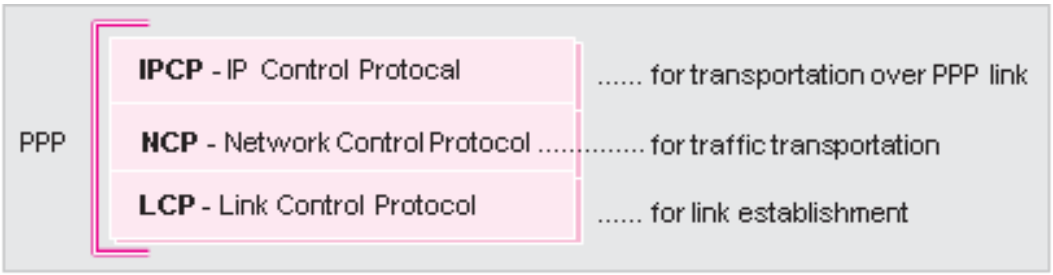
SLIP/PPP

Slip (Serial Line Internet Protocol):

Serial Line IP (SLIP) was the first protocol for relaying IP packets over dial-up lines. It defines an encapsulation mechanism, but little else. There is no support for dynamic address assignment, link testing, or multiplexing different protocols over a single link. SLIP has been largely supplanted by PPP.

PPP (Point to Point Protocols):

PPP is the Internet Standard for transmission of IP packets over serial lines. The Point-to-Point Protocol (PPP), is currently the best solution for dial-up Internet connections, including ISDN. PPP is a layered protocol.



SLIP/PPP provides a form of direct Internet connection in the sense that :

- The home user's computer has a communications link to the Internet even if it is via a service provider (ISP).
- The home user's computer has the networking software that can speak TCP/IP with other computers on the Internet.
- The home user's computer has an identifying address (IP address) at which it can be contacted by other computers on Internet.

WIRELESS/MOBILE COMPUTING:

Wireless Communication:

Wireless communication is simply data communication without the use of landlines. This may involve cellular telephone, two-way radio, fixed wireless, laser, or satellite communications. Here the computing device is continuously connected to the base network. Not all wireless communications technologies are mobile.

Mobile Computing:

Mobile computing means that the computing device is not continuously connected to the base or central network. Mobile simply describes a computing device that is not restricted to a desktop. A mobile device may be a PDA, a "smart'' cell phone or Web phone, a laptop computer, or any one of numerous other devices that allow the user to complete computing tasks without being tethered, or connected, to a network. Mobile computing does not necessarily require wireless communication. In fact, it may not require communication between devices at all.

Wireless/Mobile Computing Technologies:

GSM:

GSM is short for Global System for Mobile communications, which is one of the leading digital cellular systems. The GSM standard for digital cell phones was established in Europe in the mid-1980s. GSM has now become the international standard in Europe, Australia and much of Asia and Africa.

cell-phone users can buy one phone that will work anywhere where the standard is supported. To connect to the specific service providers in these different countries, GSM users simply switch subscriber identification module (SIM) cards. SIM cards are small removable disks that slip in and out of GSM cell phones. They store all the connection data and identification numbers you need to access a particular wireless service provider.

GSM uses narrowband TDMA, which allows eight simultaneous calls on the same radio frequency. TDMA is short for Time Division Multiple Access, a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels.

What is a SIM card?

The SIM – Subscriber Identity Module – is a chip card, the size of a first-class postage stamp. A SIM is a tiny computer chip that gives a cellular device its unique phone number. It has memory (for data and applications), a processor and the ability to interact with the user.

CDMA:

CDMA is short for Code-Division Multiple Access, a digital cellular technology that uses spread-spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence. CDMA is a form of spread spectrum, which simply means that data is sent in small pieces over several the discrete frequencies available for use at any time in the specified range. All the users transmit in the same wide-band chunk of spectrum. Each user's signal is spread over the entire bandwidth by a unique spreading code. At the receiver end, that same unique code is used to recover the signal.

WLL:

Wireless in Local Loop (WLL or WiLL), is meant to serve subscribers at homes or offices. Wireless local loop is analogous with local telephone service, but much more capable. A WLL system serves a local area by deploying a multiplicity of multichannel transmit/receive base stations (transceivers) that are within line-of-site of the intended customers. Each customer is equipped with a mini station of low power, into which the telephone (or PBX) is connected. The WLL unit consists of a radio transceiver and the WLL interface assembled in one metal box.

Advantages of WLL:

- Lacking exterior plant, reliability is greatly enhanced; as well designed WLL facilities do not significantly suffer from weather damage, vandalism, and accidents.
- WLL system offers better bandwidth than traditional telephone systems.

GPRS:

GPRS is the abbreviation for General Packet Radio Service. GPRS is used for wireless communication using a mobile device. With this service you can access the Internet, send emails and large data. We can also watch real time News, download games, and watch movies.

1G, 2G, 3G and 4G Networks:

The "G" in wireless networks refers to the “generation” of the underlying wireless network technology.

Technically generations are defined as follows :

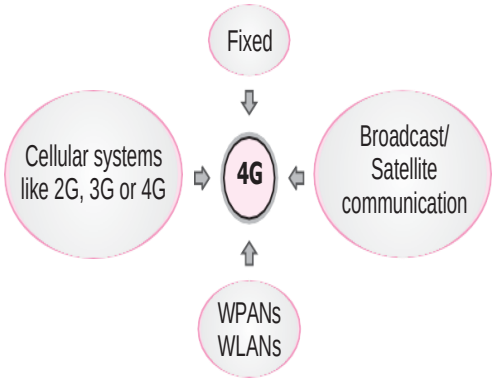
1G networks (NMT, C-Nets, AMPS, TACS) are the first analog cellular systems, which started early 1980s. There were radio telephone systems even before that. 1G networks were designed purely for voice calls with almost no consideration of data services .

2G networks (GSM, CDMAOne, D-AMPS) are the first digital cellular systems launched early 1990s, offering improved sound quality, better security, and higher total capacity. GSM supports circuit-switched data (CSD), allowing users to place dial-up data calls digitally.

2.5G networks (GPRS, CDMA2000 1x) are the enhanced versions of 2G networks with theoretical data rates up to about 144 kbit/s. GPRS offered the first always-on data service.

3G networks (UMTS FDD and TDD, CDMA2000 1x EVDO, CDMA2000 3x,TD-SCDMA, ribWCDMA, EDGE, IMT-2000 DECT) 3G (Third Generation) mobile communications technology is a broadband, packet-based transmission of text, digitized voice, video, and multimedia at data rates up to and possibly higher than 2 megabits per second (Mbps), offering a consistent set of services to mobile computer and phone users no matter where they are located in the world.

4G networks 4G is all about faster Internet speeds. it offers no improvement in making calls or sending texts but very fast web-experience compared to 3G. Fourth generation (4G) technology offers many advancements to the wireless market such as downlink data rates well over 100 Mbps, low latency, very efficient spectrum use and low-cost implementations.



4G wireless technology is also referred to by "MAGIC" which stands for Mobile multimedia, Any-where, Global mobility solutions over, Integrated wireless and Customized services.

Some More Mobile Communication Technologies:

Mobile communication technologies are ever evolving. Some other mobile communication technologies are listed below :

EV-DO:

Shorthand for CDMA2000 1xEV-DO (also known as IS-856), a CDMA based 3G technology developed by Qualcomm and supported by the 3GPP2 that builds on 1X and supports entirely packet based networks. Rev A, the most deployed version of the technology, is capable of peak rates of 3.1 Mbit/s in a 1.25 MHz channel.

HSPA:

High Speed Packet Access is an amalgamation of High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA) that supports increased peak data rates of up to 14 Mbit/s in the downlink and 5.76 Mbit/s in the uplink. Evolved HSPA (also known as HSPA+) is a wireless broadband standard that provides data rates up to 84 Mbit/s in the downlink and 22 Mbit/s in the uplink (per 5 MHz carrier) with MIM) technologies and higher order modulation.

IMS:

IP Multimedia Subsystem is an architectural framework for delivering Internet Protocol (IP) multimedia services, originally designed by the 3GPP as a part of the vision for evolving mobile networks beyond GSM.

LTE (Long Term Evolution):

A OFDMA based 3GPP standard, generally branded as 4G, that uses an all-IP flat network architecture and is capable of peak downlink speeds 100 Mbit/s and uplink speeds of 50 Mbit/s when deployed in a 20 MHz channel, and even higher rates if used with MIMO to deploy LTE in multiple channels.

X LTE-Advanced:

A 3GPP standard that builds off LTE, offering even greater channel flexibility and peak data rates of more than 1 Gbit/s.

WiMax (Worldwide Interoperability for Microwave Access):

WiMax refers to set of implementations of the IEEE's 802.16 wireless network standards supported by the WiMax Forum, which certifies vendor equipment to ensure interoperability. WiMax requires an all-IP, network architecture and makes uses of OFDMA, and generally uses unpaired.

WiMax 2:

The common name for 802.16m, which is truly 4G WiMax technology capable of mobile data speeds up to 120 Mbit/s in a single 20 MHz channel. 802.16m will succeed 802.16e, with which it is backwards compatible.

Mobile Processors:

The popularity of mobile phones of today is because one small machine can serve your various needs like communications, text creation, sending receiving messages, calculator, alarm clock, audio video recording, camera, music player etc. All this and even more are delivered to you in a small compact machine. All this is made possible by one essential and often-overlooked element that is largely responsible for the speed, efficiency, and battery life of your smartphone—the processor.

Let us look at various parts of the processor that work together to enable seamless actions.

- **CPU**, or Central Processing Unit. It receives commands, makes instant calculations, and sends signals throughout your device.
- **GPU**, or Graphics Processing Unit. The GPU assists the CPU by handling the visuals, even for games and other graphically rich applications.
- **Camera ISP** (Image Signal Processor). It provides instant image capture, high-resolution support, image stabilization, and other image enhancements.
- **Audio and Video,** It is a dedicated processing unit for handling audio and video.

- **Radio (RF Transceiver) & 3G/4G Modem**. The RF Transceiver receives and transmits voice connections and the modem enables your phone to send and receive digital signals over high-speed cellular wireless network or Wi-Fi connection.

Smartphones or the mobile phones you use today claim about their performance only because of the capabilities and power of their processors. Some mobile processors of today's age are :

- Qualcomm Snapdragon Snapdragon 835, Snapdragon 820 etc.
- Samsung EXYNOS 8890, 7570, 7420 etc.
- Huawei KIRIN 960, 955, 950 etc.
- Nvidia TEGRA X1, K1 etc.
- MediaTek Helio P10, P20, X20, X30 etc.
- Apple A8, A9, A10 etc.

SMS:

Short Message Service (SMS) is the transmission of short text messages to and from a mobile phone, fax machine and/or IP address. Messages must be no longer than some fixed number of alpha-numeric characters and contain no images or graphics. Once a message is sent, it is received by a Short Message Service Center(SMSC), which must then get it to the appropriate mobile device.

Chat:

Online textual talk, in real time, is called Chatting. In chatting, you type a message on your screen, which is immediately received by the recipient ; then the recipient can type a message in response to your message, which is received by you instantly.

Video Conferencing:

The next dimension in Internet communication is the videophone. People who have a multimedia PC with a camera and video compression handware, access to Internet over an ordinary telephone line, and videophone software can see each other while talking, which is what is called video conferencing.

Protocols for Chat and Video Conferencing:

With the advent of Internet, communication formats such as chat and video- conferencing etc have gained popularity. In this section, we shall talk about some common chat and video conferencing protocols.

- **Most common chat protocol is IRC (Internet Relay Chat)**
- **Most common video-conferencing protocols are: H.323 and SIP (Session Initiation Protocol)**

Chat protocol IRC:

The IRC (Internet Relay Chat) protocol is a simple, text-based conferencing protocol, involving several users spread across several interconnected servers. These users may chat with other individual users or may chat with groups of users on “channels”—what other chat systems refer to as “rooms” or “chat rooms”.

Video-conferencing protocol H.323:

H.323 is a standard that specifies the components, protocols and procedures that provide multimedia communication services - real-time audio, video, and data communications - over packet-based networks (including the Internet). It provides various services and, therefore, can be applied in a wide variety of areas - consumer, business, and entertainment applications. It can be applied in a variety of mechanisms :

- audio only (IP telephony)
- audio and video (video telephony)
- audio and data
- and audio, video, and data.
- H.323 can also be applied to multipoint-multimedia communications.

Video-conferencing protocol SIP:

SIP, short for Session Initiation Protocol is an IP telephony signalling protocol used to establish, modify, and terminate VOIP telephone calls. SIP works with both IPv4 and IPv6. SIP works as follows :

- Callers and callees are identified by SIP addresses.
- When making a SIP call, a caller first locates the appropriate server and then sends a SIP request. The most common SIP operation is the invitation.
- Instead of directly reaching the intended callee, a SIP request may be redirected or may trigger a chain of new SIP requests by proxies.
- Users can register their location(s) with SIP servers. SIP addresses (URL) can be embedded in Web pages and therefore can be integrated as part of powerful implementations such as Click to talk.

Voice over Internet Protocol, VoIP:

VoIP is a technology that enables voice communications over the Internet through the compression of voice into data packets that can be efficiently transmitted over data networks and then converted back into voice at the other end.

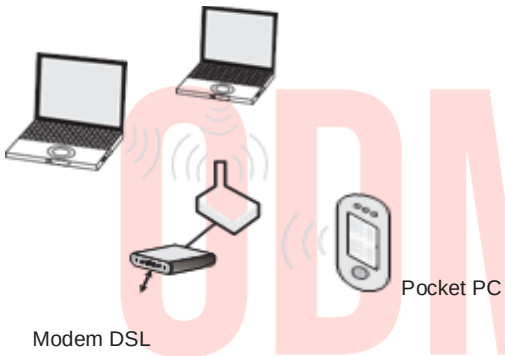
Connecting Wirelessly to Internet:

Two most common ways to connect to Internet wirelessly are:

Wi-Fi:

Wi-Fi refers to Wireless Fidelity, which lets you connect to the Internet without a direct line from your PC to the ISP. For Wi-Fi to work, you need:

- A broadband Internet connection.
- A wireless router, which relays your Internet connection from the "wall" (the ISP) to the PC.
- A laptop or desktop with a wireless internet card or external wireless adapter.



INTERNET - A WI-FI NETWORK

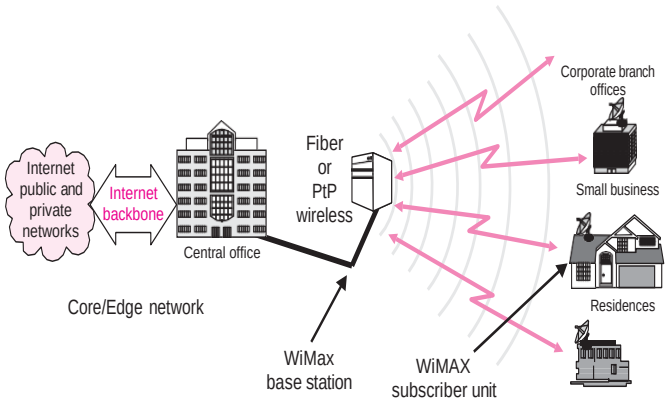
Wi-Fi Hotspots:

A hotspot is a venue that offers Wi-Fi access. The public can use a laptop, WiFi phone, or another suitable portable device to access the Internet through a WiFi Hotspot. Hotspots are public locations (such as libraries, hotels, airports, and local bookstores and restaurants etc.) with free or fee-based wireless Internet access.

WiMax:

WiMAX is a wireless digital communications system. WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3-10 miles (5-15 km) for mobile stations. In contrast, the WiFi wireless local area network standard is limited in most cases to only 100-300 feet (30-100 m).

WiMax requires a tower called WiMax Base Station , like a cell phone tower, which is connected to the Internet using a standard wired high-speed connection. But as opposed to a traditional Internet Service Provider (ISP), which divides that bandwidth among customers via wire.



INTERNETWORKING TERMS AND CONCEPTS:

WWW (World Wide Web):

The world wide web (WWW) is a set of protocols that allows you to access any document on the Net through a naming system based on URLs. WWW also specifies a way—the hypertext Transfer protocol (HTTP)to request and send a WWW in place, one can set up a server and construct hypertext documents with links in them that document over the internet. With these standard protocols of point to the documents on the server.

Before WWW, Internet was mainly used for obtaining textual information. But post-WWW, the Internet popularity grew tremendously because of graphic-intensive nature of WWW.

WWW Attributes:

- User-friendly
- Multimedia Documents
- Hypertext and Hyperlinks
- Interactive
- Frames

Telnet:

Telnet is an older Internet utility that lets you log on to remote computer systems. Basically, a Telnet program gives you a character-based terminal window on another system. You get a login prompt on that system. If you have permitted access, you can work on that system, just as you would if you were sitting next to it.

Web Browser and Web Server:

Web Browser:

A Web Browser is a WWW client that navigates through the World Wide Web and displays web pages

Web Server:

A Web Server is a WWW server that responds to the requests made by web browsers.

The World Wide Web (WWW) is based upon clients and servers. A WWW client is called Web Browser or simply a browser and a WWW server is called a Web Server or just a server. Internet Explorer and Netscape Navigator are two most popular web browsers.

URL and Domain Names:

HTTP uses Internet addresses in a special format called a Uniform Resource Locator or URL, URLs look like this

type://address/path

where **type**: specifies the type of server in which the file is located, **address** is the address of server, and **path** tells the location of file on the server. For example, in the following URL

http://encycle.msn.com/getinfo/styles.asp

http: specifies the type of server,encycle.msn.com is the address of server and getinfo/style.asp is the path of the file styles.asp.

The other examples of URLs are

ftp://ftp.prenhall.com, http://www.yahoo.com, news://alt.tennis etc.

Domain Name:

An Internet address which is character based is called a Domain Name. The naming scheme by which servers are identified is also known as the domain name system. Given table lists some most common domains. Another method of addressing servers is based on numbers e.g. 203.127.54.9. Such addresses are called **IP addresses**.

http://www.microsoft.co.in

here the last in suggests that it is based in India (.in). Similarly, the URL http://www.clearnet.nz suggests that it is based in New Zealand (.nz). Some country abbreviations are being listed below:

au	Australia	ca	Canada
dk	Denmark	fr	France
in	India	jp	Japan
nz	New Zealand	uk	United Kingdom

Table *Internet Servers and What They Provide*

Server	*Protocol*	*Information It Provides*
ftp	File Transfer Protocol	Text and binary files that are organized in a hierarchical structure, much like a family tree.
gopher	Transfer Control Protocol/Internet Protocol (TCP/IP)	Text and binary files that are organized in a menu structure.
http	Hypertext Transfer Protocol	Hypertext/hypermedia files (*i.e.*, multimedia documents that contain links to images, sounds, or other multi-media documents on the World Wide Web).
mail	Post Office Protocol (POP) Version 3 and Simple Mail Transfer Protocol (SMTP)	Messages sent via electronic mail.
news	Network News Transfer Protocol (NNTP)	Newsgroups that are organized in a hierarchical structure.

Table *Some Most Common Domains*

S.No.	*Domain ID*	*Affiliation*	*Remarks*
1.	com	Commercial	for commercial firms
2.	edu	Education	for educational firms
3.	gov	Government	for government organizations / bodies
4.	mil	Military	for Military
5.	net	Network resources	for ISPs/networks
6.	org	Usually non-profit organizations	for NGOs and other no-profit
7.	co	Company	for listed companies
8.	biz	business	for business
9.	tv	television	for television companies and channels

Web Page:

The documents residing on web sites are called web pages. The web pages use HTTP. A location on a net server is called a **Web Site**. A document that uses HTTP is called a **Web Page**.

Home Page:

It is the top-level web page of a web site. When a web-site is opened, its home page is displayed.

Web Portal:

It is a web site, which hosts other web sites. In other words, a web portal has hyperlinks to many other web sites. By clicking upon these links, the corresponding web sites can be opened. www.yahoo.com is an example of a web portal. Other examples are www.indiatimes.com, www.khoj.com, etc.

Web Hosting:

Web Hosting is a means of hosting web-server application on a computer system through which electronic content on the Internet is readily available to any web-browser client. The computer system providing the webhosting is known as **webserver** or the **web host**. Basically, the web hosts allow their customers to place web documents, such as html pages, graphics, and other multimedia files etc. onto a special type of computer called a web server, which maintains constant, high speed connections to the backbone of Internet.

Types of webhosting:

- Free Hosting
- Virtual or Shared Hosting
- Dedicated Hosting
- Co-location Hosting

Web 2.0:

Web 2.0 refers to added features and applications that make the web more interactive, support easy online- information exchange and interoperability. Some noticeable features of Web 2.0 are blogs, wikis, video-sharing websites, social networking websites, RSS etc.
some of the most noticeable are :

- Facebook
- WordPress
- Myspace
- Twitter
- Digg

- YouTube
- Del.icio.us
- Blogger
- Flickr

HTML:

The World Wide Web is an exciting new medium, bringing information, images, advertising and what not to every desktop. Everything that you see on the Web is documents written in a special language called HTML or Hypertext Mark-up Language. This language tells the browsers like Mosaic or Netscape or Internet Explorer how to display text, pictures, and links on the screen.

HTML provides many layout commands, called tags that let you control the presentation of information on a web page. For example, there are tags for various types of headings, lines, image alignment, paragraph alignment, hyperlinking etc. In HTML, both the tag semantics and the tag set are fixed.

XML (eXtensible Markup Language):

XML is a mark-up language for documents containing structured information. Structured information contains both content (words, pictures, etc.) and some indication of what role that content plays (for example, content in a section heading has a different meaning from content in a footnote, which means something different than content in a figure caption or content in a database table, etc.). Almost all documents have some structure. XML specifies neither semantics nor a tag set. In fact, XML is really a meta-language for describing markup languages. In other words, XML provides a facility to define tags and the structural relationships between them. Since there is no predefined tag set, there cannot be any preconceived semantics.

DHTML (Dynamic HTML):

DHTML refers to Web content that changes each time it is viewed. For example, the same URL could result in a different page depending on any number of parameters, such as :

- Geographic location of the reader
- Time of day
- Previous pages viewed by the reader
- Profile of the reader

DHTML refers to new HTML extensions that will enable a Web page to react to user input without sending requests to the Web server.

"Dynamic HTML'' is typically used to describe the combination of HTML, style sheets and scripts that allows documents to be animated. Dynamic HTML allows a web page to change after it is loaded into the browser.

Web Scripting:

The process of creating and embedding scripts in a web page is known as web-scripting. A script or a computer-script is a list of commands that are embedded in a web- page normally and are interpreted and executed by a certain program or scripting engine. Scripts may be written for a variety of purposes such as for automating processes on a local-computer or to generate webpages on the web.

The programming languages in which scripts are written are called **scripting languages**. There are many scripting languages available today. Most common ones are **VBScript, JavaScript, ASP, PHP, PERL, JSP etc.**

Scripts are broadly of following two types :

S.No.	Client Side Scripting	Server Side Scripting
1.	Script code is downloaded and executed at client end.	The script is executed at the server-end and the result is sent to the client-end.
2.	Response to interaction is more immediate once the program code has been down-loaded.	Complex processes are more efficient as the program and associated resources are not downloaded to the browser.
3.	Services are secure as they do not have access to files and databases.	Have access to files and data bases but have security considerations when sending sensitive information.
4.	Browser dependent	Does not depend on browsers
5.	Affected by the processing speed of user's computer	Affected by the processing speed of the host server.

NETWORK SECURITY CONCEPTS:

While ensuring network security, the concerns are to make sure that only legal or authorized users and programs gain access to information resources like databases. Also, certain control mechanisms are

setup to ensure that properly authenticated users get access only to those resources that they are entitled to use.

The problems encountered under network security can be summarised as follows :

- ***Physical Security holes.*** When individuals gain unauthorized physical access to a computer and temper with files. Hackers do it by guessing passwords of various users and then gaining access to the network system.
- ***Software Security holes.*** When badly written programs or 'privileged' software are compromised into doing things that they should not be doing.
- ***Inconsistent Usage holes.*** When a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.

Protection Methods:

To counter or reduce the security threats received under this category, many protection methods are used. These protection methods are being discussed briefly in the coming lines.

- **Authorization.** Authorization determines whether the service provider has granted access to the web service to the requestor. Basically, authorization confirms the service requestor's credentials. It determines if the service requestor is entitled to perform the operation, which can range from invoking the web service to executing a certain part of its functionality.
  Authorization is performed by asking the user a legal login-id. If the user can provide a legal login-id, he/she is considered an authorized user.
- **Authentication.** Authentication ensures that each entity involved in using a web service – the requestor, the provider, and the broker (if there is one) is what it claims to be. Authentication involves accepting credentials from the entity and validating them against an authority.
  Authentication is also termed as password-protection as the authorized user is asked to provide a valid password, and if he/she can do this, he/she is an authentic user.
- **Encrypted Smart Cards.** Passwords in a remote log-in session generally pass over the network in unencrypted form, any hacker (or cracker) can simply record it and can use it later maliciously to corrupt data/files or to harm anyone etc. To counter such threats, newer approaches are suggested such as encrypted smart cards.
  An encrypted smart card is a hand-held smart card that can generate a token that a computer system can recognise. Every time a new and different token is generated, which even-though cracked or hacked, cannot be used later.
- **Biometric Systems.** The biometric systems form the most secure level of authorization. The biometric systems involve some unique aspect of a person's body such as fingerprints, retinal patterns etc. to establish his/her identity.

- **Firewall.** A system designed to prevent unauthorized access to or from a private network is called Firewall. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- **Packet filter**. Looks as each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Application gateway.** Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is highly effective but can impose a performance degradation.
- **Proxy server**. Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.
- **Circuit-level gateway**. Applies security mechanisms when a connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

Related Terms

Cookies:

Cookies are messages that a Web server transmits to a Web browser so that the Web server can keep track of the user's activity on a specific Web site. The browser stores the message in a text file. The message is then sent back to the server each time the browser requests a page from the server.

Cookies have six parameters that can be passed to them:

- The name of the cookie.
- The value of the cookie.
- The expiration date of the cookie - this determines how long the cookie will remain active in your browser.
- The path the cookie is valid for - this sets the URL path the cookie is valid in. Web pages outside of that path cannot use the cookie.
- The domain the cookie is valid for - this takes the path parameter one step further. This makes the cookie accessible to pages on any of the servers when a site uses multiple servers in a domain.

- The need for a secure connection - this indicates that the cookie can only be used under a secure server condition, such as a site using SSL.

Hackers and Crackers:

Hackers:

Hacker is a slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Cracker:

The Crackers are the malicious programmers who break into secure systems

Cyberlaw:

Cyberlaw is a generic term, which refers to all the legal and regulatory aspects of Inter- net and the World Wide Web. Anything concerned with or related to or emanating from any legal aspects or issues concerning any activity of netizens and others, in Cyberspace comes within the ambit of Cyberlaw.

Cyber Crimes:

The Cambridge dictionary defines Cyber Crimes as Crimes committed with the use of computers or relating to computers, especially through the Internet. Universally, Cyber Crime is understood as "an unlawful act where in the computer is either a tool or a target or both".

Classification of Cyber Crimes:

- Tampering with computer source documents
- Hacking
- Publishing of information, which is obscene in electronic form.
- Child Pornography.
- Accessing protected system
- Breach of confidentiality and privacy.

IPR Issues:

The term Intellectual Property (IP) reflects the idea that its subject matter is the product of the mind or the intellect. These could be in the form of Patents; Trademarks; Geographical Indications; Industrial Designs; Layout-Designs (Topographies) of Integrated Circuits; Plant Variety Protection and Copyright.

Intellectual property rights are legal rights, which result from intellectual activity in the industrial, scientific, literary, and artistic fields.

These rights also promote creativity and the dissemination and application of its results and encourage fair-trading, which contributes to economic and social development.

VIRUSES:

Computer virus is a malicious program that requires a host and is designed to make a system sick, just like a real virus. Viruses can spread from computer to computer, and they can replicate themselves. Some viruses are categorized as harmless pranks, while others are far more malicious.

Broadly three types of viruses are:

- File infectors – attach themselves to a program file.
- Boot sector viruses – install themselves on the beginning tracks of a hard drive.
- Macro viruses – infect data files.

The following are characteristics of a computer virus:

- It can replicate.
- It requires a host program as a carrier.
- It is activated by external action.
- Its replication ability is limited to the (virtual) system.

How Computer Viruses Spread?

Computer viruses move from computer to computer by attaching themselves to files or boot records of disks and diskettes. These days it is not uncommon to find them in e-mail attachments and other programs that can be downloaded from the Internet.

Damage that Viruses Cause:

Viruses' main objective is to make your system unstable and cause harm to data.

Mainly these cause damage in many ways:

- can destroy file allocation tables (FAT) and lead to the corruption of an entire file system, resulting in the need to fully reinstall and reload the system.
- can create bad sectors on the disk, destroying parts of programs and files.
- can decrease the space on hard disks by duplicating files.
- can format specific tracks on the disks or format the entire disk.

- can destroy specific executable files and alter data in data files, causing a loss of integrity in the data.
- can cause the system to hang so that it does not respond to any keyboard or mouse movements.

Trojan Horses:

A Trojan horse is code hidden in a program such as a game or spreadsheet that looks safe to run but has hidden side effects. When the program is run, it seems to function as the user expects, but it is destroying, damaging, or altering information in the background. It is a program on its own and does not require a host program in which to embed itself. An example of a Trojan horse would be a Christmas executable that, when executed, pops up with an animated figure of Santa Claus and a caption saying, "Merry Christmas." In the background, extra code could be deleting files or performing other malicious actions.

How Trojan Horses Spread:

Trojan horses generally are spread through e-mail and exchange of disks and information between computers. Worms could also spread Trojan horses.

Damage Caused by Trojan Horses:

The damage that Trojan horses cause is much the same as what a virus causes. Most of the time the users are unaware of the damage it is causing because of the Trojan horse's masking effect.

Worms:

A worm is a program designed to replicate. The program may perform any variety of additional tasks as well. The following are characteristics of a worm:

- It can replicate.
- It is self-contained and does not require a host.
- It is activated by creating process (it needs a multitasking system).
- If it is a network worm, it can replicate across communication links.

Worms are programs that run independently and travel from computer to computer across network connections. Worms may have portions of themselves running on many different computers. Worms do not change other programs, although they may carry other code that does.

How Worms Spread?

Worms are autonomous agents capable of propagating themselves without the use of another program or intervention or action by a user. Worms are found primarily on computers that are capable of multitasking and are connected by a network.

Damage that Worms Can Cause:

Most worms disrupt services and create system management problems. Some worms scan for passwords and other loopholes and then send the information back to the attacker. In some cases, worms can install Trojan horses or viruses that cause damage to the systems.

Spam:

Spam refers to electronic junk mail or junk newsgroup postings. Some people define spam even more generally as any unsolicited e-mail. Merriam-Webster dictionary defines spam as unsolicited usually commercial e-mail sent to many addresses.

Avoiding Spam:

- One way to help avoid Spam or junk mail is to create a filter that finds and does something to e-mail that you suspect is Spam.
- Another tip is not to register yourself with true id to sign up for things on the Internet. These places often share that e-mail address with other companies that then send you spam.

Virus Prevention:

Virus prevention is not a difficult task. All you need to be is extra careful and ensure to follow the following guidelines to lead virus free computing life.

- Never use a “foreign” disk or CD without scanning it for viruses.
- Always scan files downloaded from the internet or other sources.
- Never boot your PC from a floppy unless you are certain that it is virus free.
- Write protect your disks.
- Use licensed software.
- Passwords protect your PC to prevent unattended modification.
- Make regular backups.
- Install and use antivirus software.
- Keep antivirus software up to date.

PAYMENT TRANSACTIONS USING ONLINE BANKING:

Online banking allows a user to execute financial transactions via the Internet. Online banking is also known as "internet banking" or "web banking". An online bank offers customers just about every service traditionally available through a local branch, including deposits, which is done online or through the mail, and online bill payment.

Advantages:

- Convenience is a major advantage of online banking
- In effect, consumers can perform banking transactions 24 hours-a-day, seven-days a week.
- Online banking is fast and efficient.
- Funds can be transferred between accounts almost instantly, especially if the two accounts are held at the same banking institution.

Disadvantages of Online Banking:

- For a novice online banking customer, using systems for the first time may present challenges that prevent transactions from being processed.
- Although online banking security is continually improving, such accounts are still vulnerable when it comes to hacking.
- Consumers are advised to use their data plans, rather than public Wi-Fi networks when using online banking, to prevent unauthorized access.
- Additionally, online banking is dependent on a reliable internet connection. Connectivity issues from time-to-time may make it difficult to determine if banking transactions have been successfully processed.
- On occasion, consumers may prefer face-to-face interactions for more complex banking issues.

Mobile Banking:

When you perform or use the banking services via a mobile, it is called mobile banking. Difference between online banking and mobile banking is that Mobile banking is done via a mobile banking app while the online baking is done via secure website of the bank. Some popular mobile apps used today are:

- State Bank Freedom (State Bank of India App). This is the official State Bank of India mobile banking application.
- iMobile Android App (ICICI Bank App). This is the official ICICI Bank mobile banking application.
- Connect (BOB App). This is the official Bank of Baroda mobile banking application.

- Citibank IN (Citibank App). You can manage your Citibank Accounts and Credit Cards with official Citi Mobile application.
- NGpay Application (HDFC BANK). NGpay is also the official mobile banking application for Axis Bank and HDFC Bank.

e-Wallet:

E-wallet is a similar electronic service used for payments. E-wallet as the name suggests is your own wallet available to you electronically where you can use your own money (in electronic form) for payments. Some most popular e-wallets of today are: Paytm, Freecharge, Mobikwik, Citrus Pay, Airtel Money, Oxigen Wallet, OlaMoney, HDFC PayZapp, Chillr, Pockets By ICICI Bank, JioMoney, SBI Buddy, mRupee, ItzCash etc.

Govt of India announced a new digital payments app named BHIM – Bharat Interface for Money – after Babasaheb Dr Bhimrao Ambedkar. BHIM is a digital payments solution app based on the Unified Payments Interface (UPI) from the National Payments Corporation of India (NPCI), the umbrella organisation for all retail payments systems in India.

****