2020
EDITION

Textbook for CBSE Class XII

Computer Science

With

Python

PREETI ARORA

Web Support
at
sultan-chand.com/ws/python12

- Presentations • Projects & Program Codes
- Sample Papers • Model Test Papers
- Practical File • Viva Voce

- ❖ Advanced Python Concepts
- ❖ Modules
- ❖ Recursion
- ❖ Data Structures
- ❖ Computer Networks
- ❖ MySQL
- ❖ Society, Law & Ethics
- ❖ Project Work

SCS
sultan chand

8 Computer Networks

8.1 INTRODUCTION

The greatest breakthrough in technology and communication over the past 20 years has been the development and advancement of the computer network. From emailing a friend, to online bill payment, to downloading data from the internet, to e-commerce, networking has made our world much smaller and forever changed the way we communicate.

Network provides salient features which have made our life easy and comfortable, be it sending an email, withdrawing money from an ATM machine, online railway or airline reservation, or sharing audio and video files. Apart from these, the most extensively-used feature is the Print command sent from a computer to get a printout from a printer attached to some other computer. All this involves a network.

It is the network that connects various computers to each other and handles a large volume of data.

Fig. 8.1: A Computer Network

8.2 COMPUTER NETWORK—A BRIEF OVERVIEW

Several devices connected to each other for reliable communication/transfer of data constitute a network. A network can consist of a computer, a fax machine, a printer, a camera, a cell phone, *etc.* A collection of interconnected computers is called a **Computer Network**. Two computers or devices are said to be interconnected if they are capable of sharing and exchanging information with each other by following a protocol (set of rules).

CTM: A computer network is a collection of interconnected computers and other devices to share data and other resources (hardware and software resources).

8.2.1 Advantages of Computer Networks

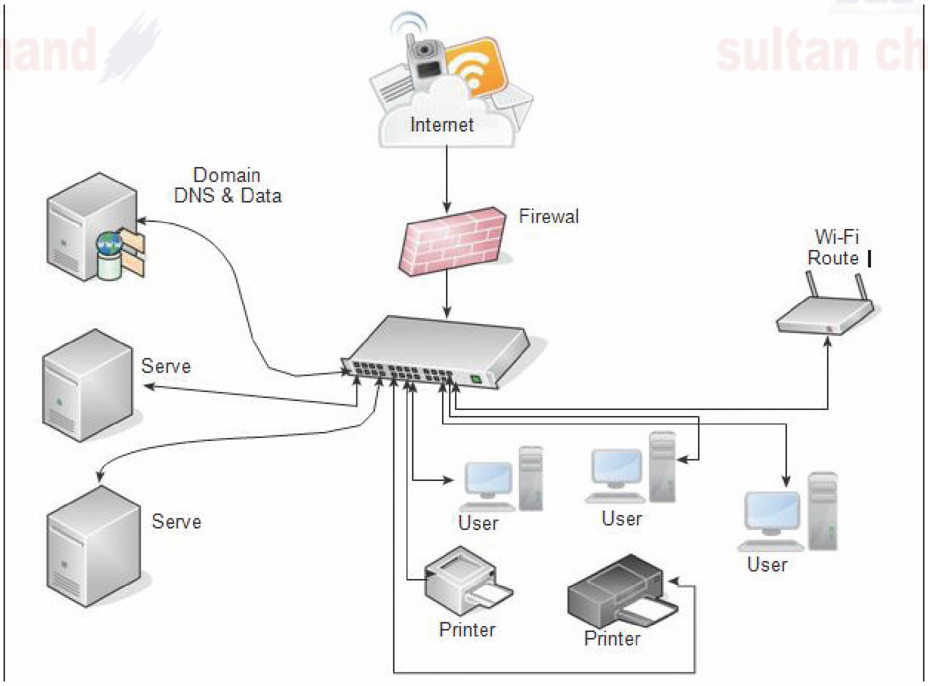


Fig. 8.2: The Network Diagram

Let us now discuss why networks are essential. Are there any advantages of networked computers over stand-alone machines? Yes, networked systems are far better. A network uses a distributed processing system in which a task is divided among several devices which are interconnected with each other. Therefore, instead of a single computer being responsible for completing the entire task, all the interconnected computers are responsible for completing the task assigned to them. This leads to better performance with high processing speed.

Networks have several advantages which are described below:

(a) **Resource Sharing:** The primary use of a network is to share among users programs/applications, data and peripheral devices connected to the network, irrespective of their physical location. You must have noticed in your networked computer labs that when a print command is given on one computer, the document is printed by a printer attached to some other system. This allows printing of documents by several users and, hence, the printer is shared by multiple users on the network. Other resources like hard disk, DVD drive, scanner, *etc.*, can also be shared on a computer network. *For example*, sharing database, audio and video files, antivirus software, application software, printers and scanners, *etc.*

(b) **Improved Communication:** A computer network enables fast, reliable and secure communication between users. It saves time and offers easy communication methods. *For example*, in an organization, managers work at different locations to make financial reports. While working on a network, any change made by one manager on his/her computer can easily be seen by other managers and employees. Thus, a network allows managers to easily update information. This increases their efficiency and allows them to complete their work quickly.

(c) **Reduced Communication Cost:** Sharing resources also reduces communication cost. Using public networks, we can send a large quantity of data at a low cost. Internet anmjd mobile networks are playing a very important role in sending and receiving text, image, audio and video data at a low cost.

(d) **Reliability of Data:** Reliability means backing up of data, *i.e.*, data can be copied and stored on multiple computers. In a network system, all computers are connected to each other. Thus, the information or message which is shared by each device is stored on their respective workstations (computers). If, due to some reason (hardware crash, *etc.*), the data gets corrupted and, thus, becomes unavailable on one computer, a copy of the same data can be accessed from another workstation for future use. This leads to smooth functioning and further processing without disruption.

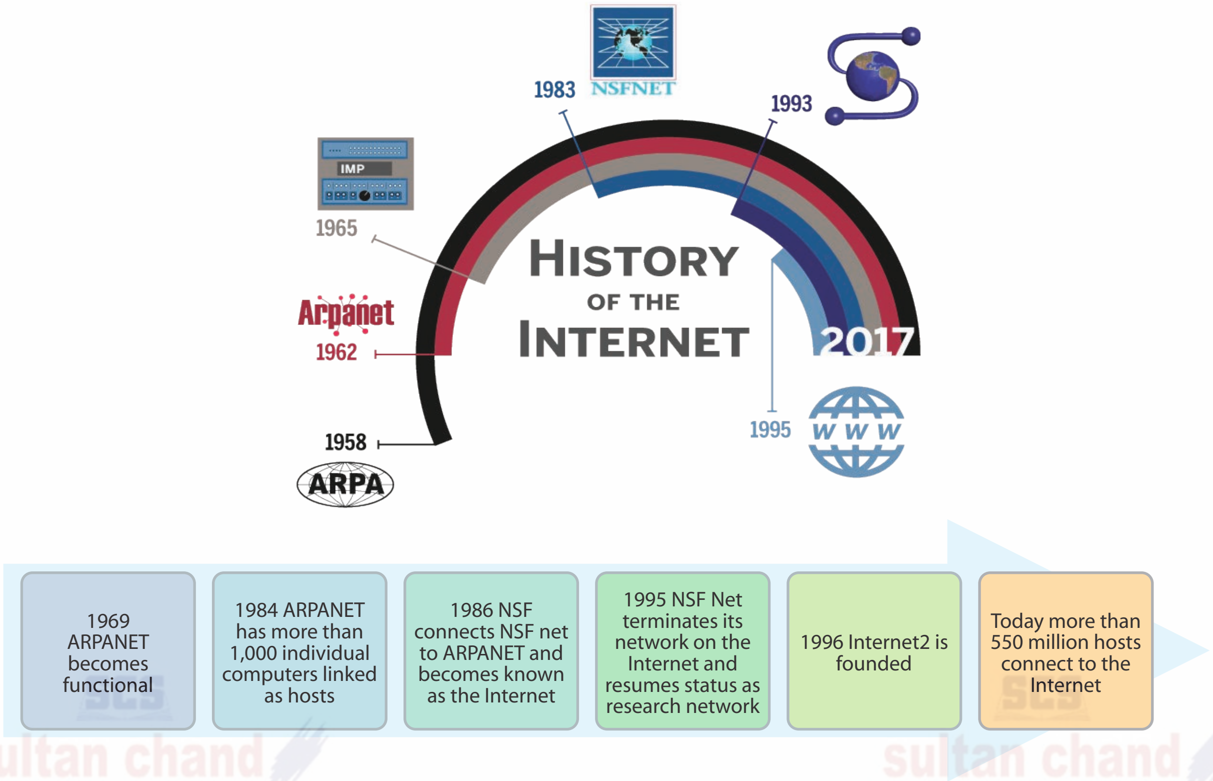
(e) **Central Storage of Data:** Files can be stored on a central node (the file server) that can be shared and made available to each and every user in an organization. With centralized processing, data is stored and retrieved from a single central location. Thus, there is no duplication of data and almost no data redundancy.

8.3 EVOLUTION OF NETWORK

The network did not evolve in a single day; rather, it took decades to become more powerful, efficient and reliable. The network has passed through several stages which are described below:

- **ARPANET (Advanced Research Project Agency Network):** ARPANET, which was jointly designed and named by the Advanced Research Projects Agency (ARPA) and US Department of Defence (DoD), was the first network and came into existence in 1969. It was a project that connected a handful of computers at different universities and US DoD for sharing of data and messages and playing long-distance games, and socializing with people to share their views.
- **NSFNET (National Science Federation Network):** In the mid-80's, another federal agency, NSFNET (National Science Federation Network), created a new network which was more capable than ARPANET. Its main aim was to use network only for academic research and not for any private business activity. Later, many private companies combined their own private networks with ARPANET and NSFNET to make a more capable and broad network—the Internet. It is the internet that links two or more networks to make a large network for sharing of information and messages.

ARPANET + NSFNET + PRIVATE NETWORKS = INTERNET



1969 ARPANET becomes functional

1984 ARPANET has more than 1,000 individual computers linked as hosts

1986 NSF connects NSF net to ARPANET and becomes known as the Internet

1995 NSF Net terminates its network on the Internet and resumes status as research network

1996 Internet2 is founded

Today more than 550 million hosts connect to the Internet

Fig. 8.3: Evolution of Internet

- **Internet:** In the 1990's, internet, which is a network of networks, came into existence.The internet has evolved from ARPANET. The computers are connected through World Wide Web that comprises a large network and shares a common communication protocol (Transmission Control Protocol-Internet Protocol, TCP/IP). It allows computers of different types to exchange information and is known as internet. Millions of domestic, business and government networks are connected with each other for the purpose of sharing files, data, email, *etc.* Most of the computers are not connected directly to the internet. Instead, they are connected to smaller networks which are further connected to a backbone network through gateways.

CTM: Network of networks makes the internet.

- **Interspace:** Interspace is a software that allows multiple users in a client-server environment to communicate with each other by sending and receiving data of various types such as data files, video, audio and textual data in a 3-D environment. It facilitates online real-time exchange of data. Interspace is the most advanced term of communication available on the internet today.

8.4 HOW DOES INTERNET WORK

One of the greatest things about the internet is that nobody really owns it. It is a global collection of networks, both big and small. These networks connect together in many different ways to form the single entity that we know as internet. In fact, the very name comes from this idea of interconnected networks.

Since its beginning in 1969, the internet has grown from four host computer systems to tens of millions. However, just because nobody owns the internet does not mean that it is not monitored and maintained in different ways. The Internet Society, a non-profit group established in 1992, oversees the formation of the policies and protocols that define how we use and interact with the internet.

Google
India
Google Search
I'm Feeling Lucky
Make Google my homepage
Google.co.in offered in: हिन्दी বাংলা తెలుగు मराठी தமிழ் ગુજરાતી ಕನ್ನಡ മലയാളം ਪੰਜਾਬੀ

Fig. 8.4(a): Working of the Internet

Before we learn about the basic underlying structure of the internet, e.g., domain name servers, network access points and backbones, we first need to understand how our computer connects to others.

Every computer that is connected to the internet is part of a network, even the one in our home. *For example*, we may use a modem and dial a local number to connect to an **Internet Service Provider** (ISP). At work, a computer may be part of a **Local Area Network** (LAN), but it most likely still connects to the internet using an ISP that the company has contracted with. When it connects to the ISP, it becomes part of their network. The ISP may then connect to a larger network and become part of their network. The internet is simply a network of networks.

Most large communication companies have their own dedicated backbones connecting various regions. In each region, the company has a **Point of Presence** (POP). The POP is a place for local users to access the company's network, often through a local phone number or dedicated line. The amazing thing here is that there is no overall controlling network. Instead, there are several high-level networks connecting to each other through **Network Access Points** or NAPs.

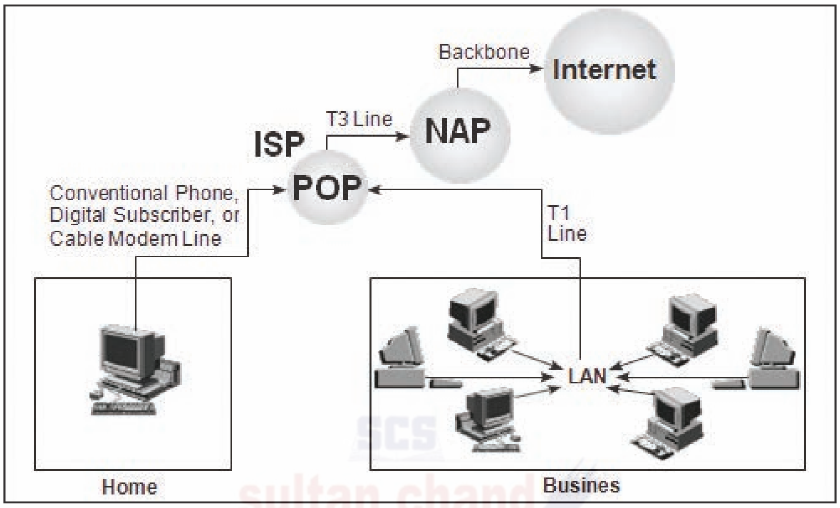


Fig. 8.4(b): POP and NAP

Gateway: Gateway is a device that connects dissimilar networks. A backbone is a central interconnecting structure that connects one or more networks just like the trunk of a tree.

At the source computer the message to be sent is broken down into small parts called packets. Each packet is given a serial number, e.g., 1, 2, 3. All these packets are sent to the destination computer. The destination computer receives the packets in random order (10 may come before 1). The packets are reassembled in the order of their number and message is restored.

How it functions smoothly: Every computer connected to the internet uses the same set of rules for communication. A set of rules is called protocol. Communication protocol used by internet is TCP/IP. The TCP (Transmission Control Protocol) part is responsible for dividing the message into packets on the source computer and reassembling them at the destination computer. The IP (Internet Protocol) is responsible for handling the address of the destination computer so that the packet is sent to its proper destination.

8.4.1 Elementary Terminology of Networks

1. **Nodes (Workstations):** The term node refers to computers that are attached to a network and are seeking to share resources.
2. **Server:** A computer that facilitates the sharing of data, software and hardware resources on the network.
3. **Network Interface Unit (NIU) (MAC Address):** A network interface unit is an interpreter that helps in establishing communication between the server and the client.

4. **IP Address:** Every machine on a TCP bar/IP Network has a unique identifying number called an IP Address.

5. **Domain Name:** It is a way to identify and locate the computers connected to the internet. It must be unique.

8.5 COMPONENTS OF DATA COMMUNICATION

A network comprises several components along with their functionalities that contribute to its smooth functioning. To form a network, a lot of hardware devices are required which are described as follows:

- **Sender:** A device or a computer that sends the data.
- **Receiver:** A device or a computer that receives the data.
- **Message:** Message is the information to be communicated. It may be text, image, audio or video.
- **Transmission Medium:** A transmission medium is a physical path through which the data flows from sender to receiver. A cable or wire or r adio waves can be the medium.
- **Protocol:** A set of rules that governs data transmission. It represents the communication methods which are to be followed by the sending and receiving devices.

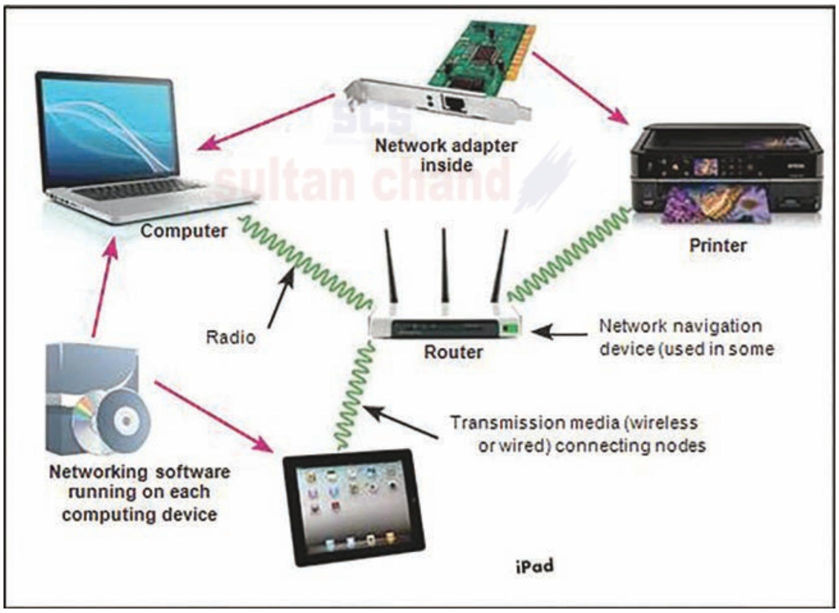

Network adapter inside
Computer
Printer
Radio
Router
Network navigation device (used in some
Transmission media (wireless or wired) connecting nodes
Networking software running on each computing device
iPad

Fig. 8.5: Components of a Network

8.6 MODES OF DATA TRANSMISSION

(a) Analog or Broadband Transmission

- The signal is a radio frequency signal or analog, *i.e.*, it can consist of continuous electrical waves that are of varying amplitudes.
- Telephone networks use this type of transmission.
- Requires modem for transmitting data over baseband medium.

(b) Digital or Baseband Transmission

- No special device for conversion of signal to be transmitted over baseband medium.
- The signal is a group of discrete electrical units which is transmitted in rapid succession.

(c) Parallel Communication

- When data is transmitted through multiple wires with each wire carrying each bit, it is called parallel communication.

(d) Serial Communication

- When bits are sent one after another in a series along a wire, it is called serial communication.

10001----------------10001

(e) Synchronous or Asynchronous Transmission

- When sender and receiver synchronize their checks before transmission, *i.e.*, the sender first sends control characters to the receiver and then sends the actual data, it is called synchronous transmission.

  Advantage—Faster than asynchronous mode.

  Disadvantage—Costly and complex set-up required.

- In asynchronous transmission, data is preceded and succeeded by a start bit and stop bit respectively. No synchronization is required.

  Advantage—Hardware required is simple and cheap.

  Disadvantage—Slower than synchronous mode.

8.7 DIFFERENT WAYS OF SENDING DATA ACROSS NETWORK

There are several ways of sending data from one node to another through network. It can be in the form of calls, messages, *etc.* By using various types of switching techniques, we can establish the connection/communication.

8.7.1 Network Switching

A network is made up of several interconnected nodes. There can be a point-to-point connection or star topology between pairs of devices, but both are not relevant for a large network. Hence, various switching techniques are used to transfer packets of data from one port of a node to another. A switched network is made up of a series of interconnected nodes called switches.

8.7.2 Switching Techniques

The main goal of networking is the reliable exchange of data or information among several interconnected nodes. For the delivery of data with accuracy, various types of switching techniques are used, namely:

1. Circuit Switching
2. Packet Switching
3. Message Switching

CTM: The technique of sending data across the network is known as Switching technique. The three types of techniques used are circuit switching, packet switching and message switching.

Circuit Switching

This provides end-to-end connection between two computers. Circuit switching is established usually in a telephone network where one person is making a call and another is receiving a call. In telephone system, the communication must be established between the two participants, *i.e.*, the sender and the receiver. The circuit is established between these two participants before the transfer of data takes place.

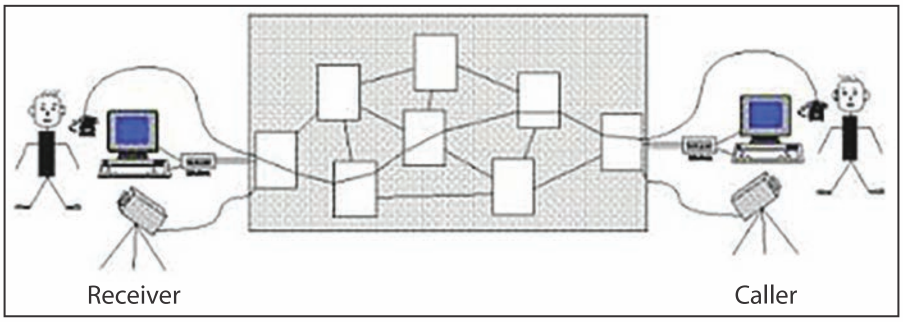


Fig. 8.6: Circuit Switching

In this technique, the entire link remains dedicated and no other user can use it even if the path remains idle. The following actions take place during circuit switching:

1. A request signal is sent by the sender to set up the connection with the receiver. It establishes a physical connection between the two participants.
2. All intermediate nodes are identified. These nodes are also called switching nodes.
3. If the destination node is available, it sends back the acknowledgement of receiving a signal. Hence, data transmission begins.
4. When the data transmission is complete, the call can be terminated.

CTM: Circuit switching is a connection-oriented service. In this technique, there is a dedicated link between the sender and the receiver and no other call can be made during this link, even if the link remains idle.

Packet Switching

In packet switching technique, the entire data is divided into small fragments called packets. Each packet is of a fixed size, usually 128 bytes or 512 bytes. Packet switching is similar to post office operation. Each packet has a source address as well as destination address (IP address) for being transmitted, in the same way as a postman delivers a letter to a specific destination address.

As there is no direct connection established between the sender and the receiver, each packet follows different routes and, therefore, the packets are delivered in a random order at the destination address. It is the TCP protocol which then arranges all received packets in a sequential order. During the transfer of packets, each packet has to pass through several intermediate nodes, so each intermediate node checks for destination IP address. If the packet matches with the node address, it is received; otherwise it is passed on to the next node until it reaches the destination IP address.

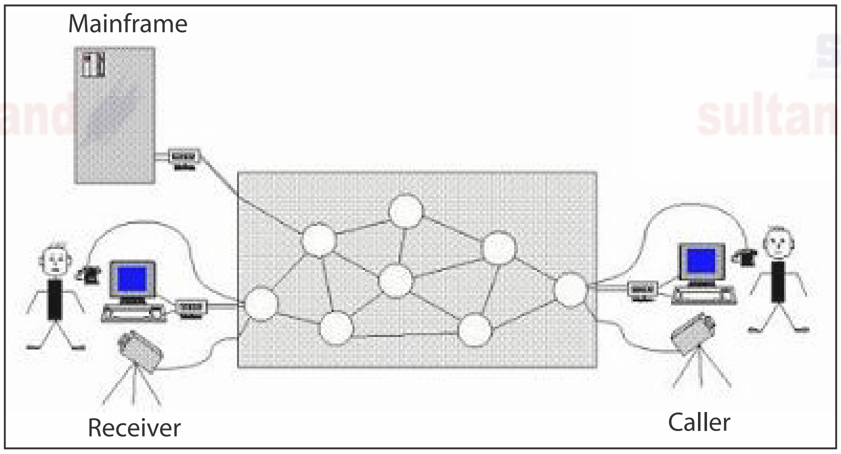


Fig. 8.7: Packet Switching

CTM: Packet switching offers a connectionless service. Data is fragmented into small packets and each packet is of fixed size in packet switching technology.

Message Switching

In message switching, the sender sends the data to a switching office first, which is then stored in its buffer. It then checks the available link and if it is free, the data is relayed to another switching office. This process goes on until the data is sent to the destination (receiver). As the data is first stored in a buffer and then sent to the next switching office, it is also called store and forward switching technique.

CTM: Message switching is a store and forward switching technique where there is no direct connection between the sender and the receiver.

8.7.3 Difference between Circuit Switching and Packet Switching

1. The circuit switching reserves the required bandwidth in advance, whereas packet switching uses bandwidth as and when required by the packets to be transmitted.
2. Circuit switching is a fast technology as compared to packet switching which is a slow mechanism of transferring packets from sender to receiver.
3. Circuit switching requires a dedicated path. Once the connection is established, the communication path is entirely dedicated to it until the data is completely transferred from sender to receiver, whereas in packet switching, packets can use any dynamic path.
4. In circuit switching, if the path is overloaded, the call is blocked and communication is delayed. But in packet switching, packets are allocated to different paths.
5. Circuit-switched networks are used for phone calls and packet-switched networks handle data.
6. Packet switching is more efficient because the cost of the link is shared by many users.
7. In circuit switching, the telephone message is sent unbroken. The message is received in the same order as it is originally sent. In packet switching, the message is broken into small packets which are randomly sent from source and received in random order at destination, which is then sequentially arranged.

8.8 DATA COMMUNICATION TERMINOLOGIES

1. **Channel:** A channel is a communication path through which the data is transmitted from the sender device to the receiver device.
2. **Baud:** The number of changes in a signal per second is known as baud. It is the measuring unit of the data transfer rate. Technically, baud refers to a number of discrete signal elements transmitted per second. 1 baud represents only 1 signal change per second and is equivalent to 1 bit per second.
3. **Bandwidth:** The amount of data that can be passed along a communication channel in a given period of time (1 second) is termed as bandwidth. The measuring unit is hertz (Hz), where 103 Hz = 1 Kilo Hertz (KHz), 103 KHz = 1 Mega Hertz (MHz).
4. **Data and Signals:** Information that is stored within computer systems and transferred over a computer network can be divided into two categories—data and signals. Data are entities that are stored in the form of 0's and 1's, which convey some special meaning to the computer system. When this data is transmitted from one place to another, it is converted into signal. Signals are the electric or electromagnetic encoding of data and are used to transmit data.
5. **Communication/Transmission Media:** It is a means of communication or access (lines of communication) set up between two organizations to exchange data/information. Communication media is the way of transmitting the signal from one place to another. Communication media is also known as transmission media. It plays an important role in sending and receiving of data to and from the sender and receiver.
6. **Data Transfer Rate:** It is the amount of data transferred in one direction over a link divided by the time taken to transfer it in bits per second (bps). The various measuring units are Both bits per second and bytes second have been abbreviated as (bps). or baud, kilobits per second (kBps), megabits per second (mBps), gigabits per second (gBps), terabits per second (tBps.)

8.9 NETWORK DEVICES

1. **Modem:** A MODEM (Modulator DEModulator) is an electronic device that enables a computer to transmit data over telephone lines. It is a device used to convert digital signals into analog signals and vice versa. There are two types of modems, namely internal modem and external modem.
2. **RJ-45 Connector:** RJ-45 is a standard type of connector for network cables. The RJ-45 (Registered Jack) connectors are the plug-in devices used in networking and telecommunications applications. They are used primarily for connecting LANs, particularly Ethernet.

CTM: RJ-45 is a short term for Registered Jack-45. It is an eight-wire connector used to connect computers on LANs, especially Ethernets.

3. **Ethernet Card:** It is a hardware device that helps in the connection of nodes within a network. Ethernet card is also known as a network card, network adapter or NIC (network interface card). It is a card that allows computers to communicate over a computer network. On Ethernet card, a physical address of each communicating computer is mentioned. Physical address is known as MAC address.

4. **Hub:** It is multi-port and unintelligent network device which simply transfers data from one port of the network to another. A hub is a hardware device used to connect several computers together with different ports. When the packet reaches one port, it is copied to all other ports of the hub without changing the destination address in the frame. Rather, it simply copies the data to all of the nodes connected to the hub.

   Hubs can be either active or passive. Hubs can usually support 8, 12 or 24 RJ-45 ports.

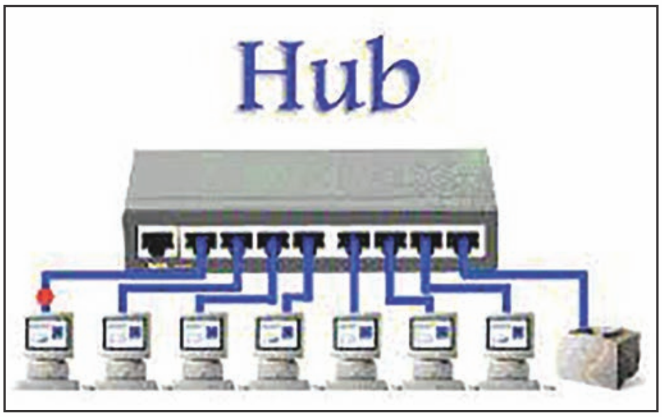


Fig. 8.8: Hub

   But the problem with hub is that it is not an intelligent device. It shares bandwidth with all the attached devices and broadcasts the data, *i.e.*, sends the data frames to all the connected nodes, as it does not remember devices/computers connected to it. Also, it cannot filter the data and causes unnecessary traffic jams.

   A hub can both send as well as receive information, but only one task at a time. However, a hub is an inexpensive way to connect multiple nodes/devices to network.

CTM: Hub is a device used to connect several computers with each other.

5. **Switch:** A switch (switching hub) is a network device which is used to interconnect computers or devices on a network. It filters and forwards data packets across a network. It is also a multi-port device but with some intelligence and so the data packets received from one port of network are refreshed and delivered to the other port of the network. The main difference between hub and switch is that hub replicates what it receives on one port onto all the other ports, while switch keeps a record of the MAC addresses of the devices attached to it.

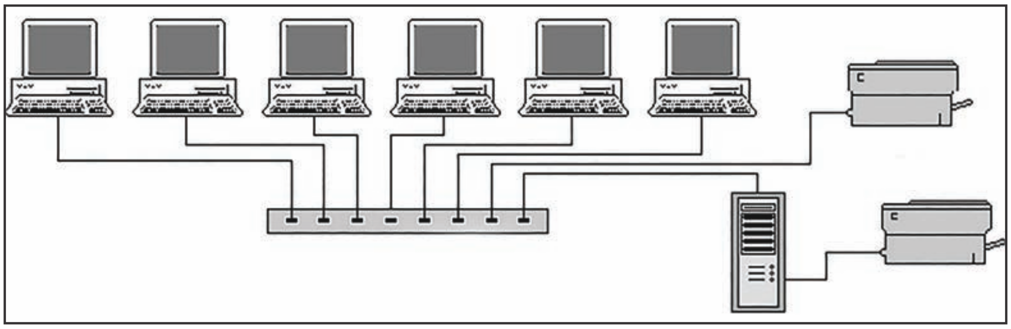


Fig. 8.9: Switch

CTM: A switch is a device that transmits data to the computers in a LAN.

6. **Bridge:** A bridge is a device that works on the physical layer as well as on data link layer. A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges relay frames between two originally separate segments. When a frame enters a bridge, the bridge not only regenerates the signal but also checks the physical address of the destination and forwards the new copy only to that port.

   An important advantage of using a bridge is that it is a smarter hub as it can filter network traffic on the basis of the MAC addresses.

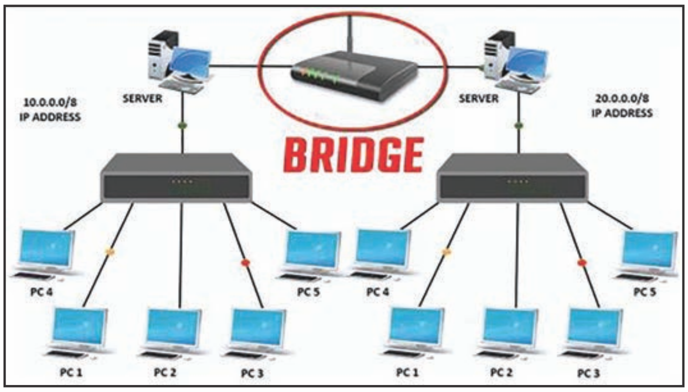


Fig. 8.10: Ethernet Bridge

CTM: A bridge is a device that links two segments together of the original network.

7. **Gateway:** A gateway is a device that connects dissimilar networks. In internet, several networks are communicating with each other and each network has a different configuration. In order to make reliable communication, there must be a device that helps in communicating.

   Gateway is a device which establishes an intelligent connection between a local area network and external networks with completely different structures.

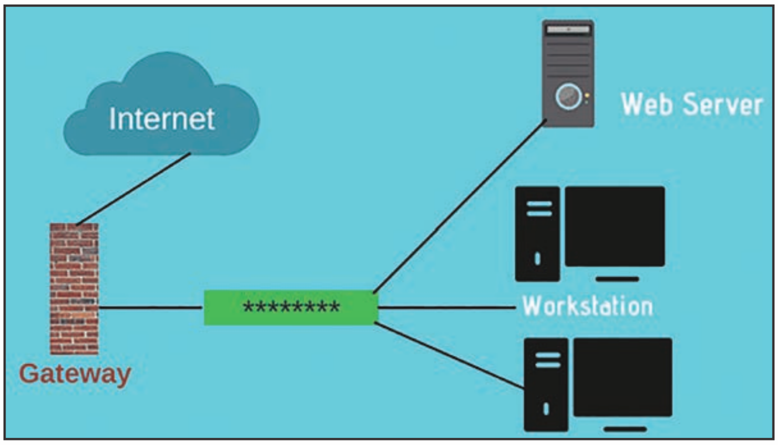


Fig. 8.11: Gateway

CTM: A gateway is a device that connects dissimilar networks.

8. **Repeater:** A repeater is a device that operates only on the physical layer of the OSI model. As a signal travels a fixed distance, before attenuation of the signal, a repeater is used which amplifies and restores signals for long-distance transmission. A repeater is an electronic device that receives a signal before it becomes too weak and regenerates the original signal. Also, it is a two-port network device that strengthens the signal intensity and connects two

identical networks. In most twisted pair Ethernet configurations, repeaters are required for cable runs longer than 100 metres. A repeater does not change the functionality of the network; instead, it makes the signal strong before it degrades.

Repeaters are also extensively used in broadcasting where they are termed as translators or boosters.

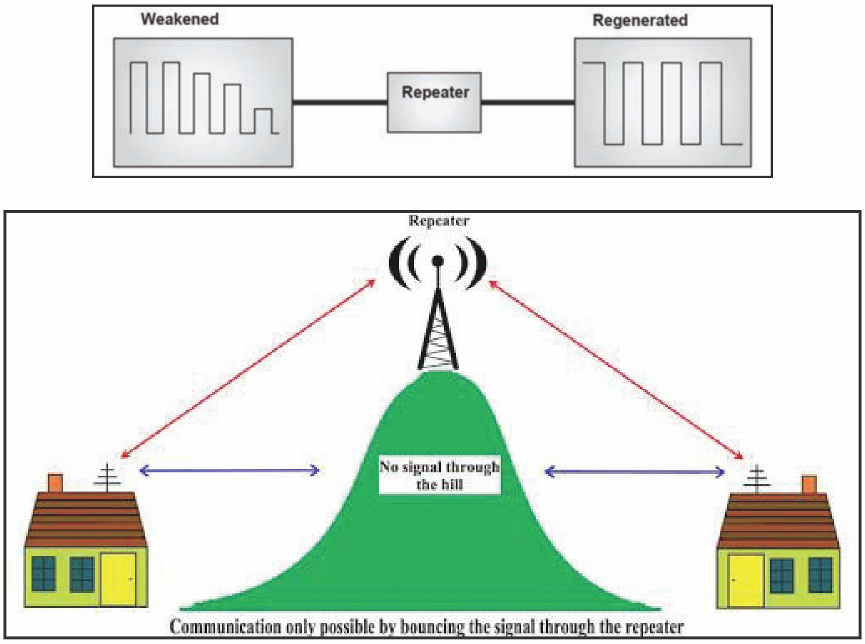

Weakened
Regenerated
Repeater
Repeater
No signal through the hill
Communication only possible by bouncing the signal through the repeater

Fig. 8.12: Working of a Repeater

CTM: Repeater is a device that amplifies a signal that is transmitted across the network so that the signal is received in the same way as it is sent.

9. **Router:** A routers is a networking device that forwards data packets from the source machine to the destination machine by using the shortest path. Routers are used at the network layer, which is the third layer of the OSI model.

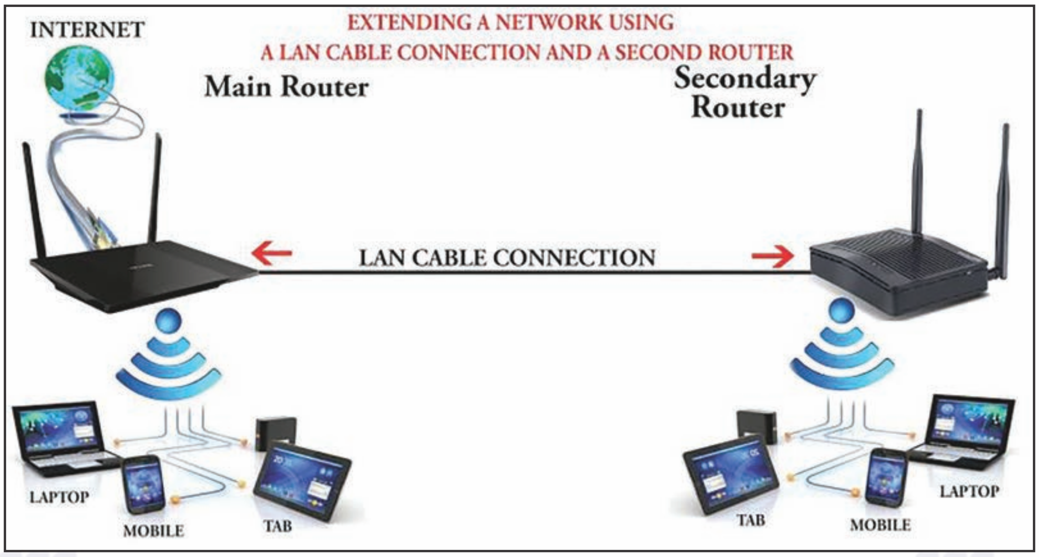


Fig. 8.13: Router

CTM: A router is a networking device that helps in forwarding packets from one machine to another.

10. **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. A Wi-Fi card is used in a desktop computer that enables a user to establish an internet connection. Wi-Fi cards are known as wireless fidelity cards as they allow the user to set up connection without any wire. Wireless Fidelity (Wi-Fi) cards are widely used in notebook computers due to their highly portable nature. The most common Wi-Fi cards used in desktop computers are PCI-Express Wi-Fi cards made to fit the PCI- Express card slots on the motherboard.

8.10 TYPES OF NETWORKS

A computer network may be small or big depending upon the number of computers and other network devices linked together. Thus, networks vary in size, complexity and geographical spread. A computer network can be on a table, in a room, building, city, country, across continents or around the world.

On the basis of geographical spread, networks may be classified as:

1. PAN
2. LAN
3. MAN
4. WAN

8.10.1 Personal Area Network (PAN)

PANs are small networks used to establish communication between a computer and other handheld devices in the proximity of up to 10 metres using wired USB connectivity or wireless systems like Bluetooth or Infrared. PANs are used to connect computers, laptops, mobiles and other IT-enabled devices to transfer files including emails, digital photos, audio and video, *etc.* The Bluetooth technology implements PAN. PAN may include wireless computer keyboard and mouse, Bluetooth-enabled headphones, wireless printers and TV remotes.

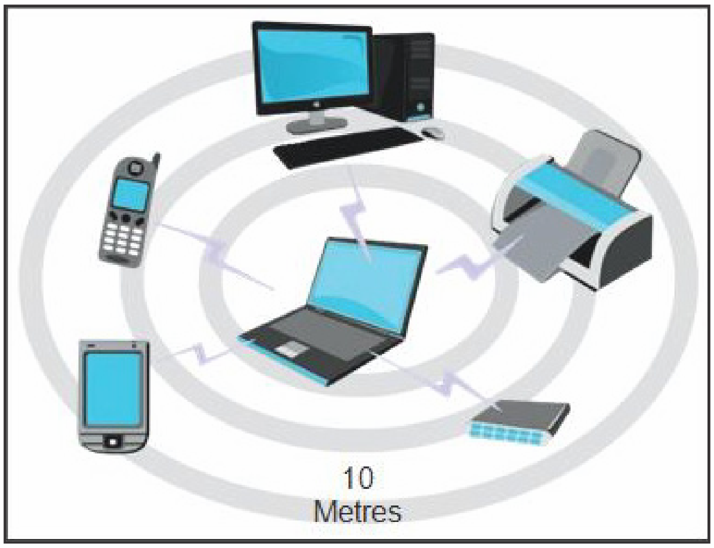


Fig. 8.14: Personal Area Network (PAN)

CTM: The network that belongs to a single person or user is known as PAN.

8.10.2 Local Area Network (LAN)

LAN is a privately owned computer network covering a small geographical area (small physical area), like a home, office or a building such as a school. It can cover an area spread over a few metres to a radius of a few kilometres.

Occasionally, a LAN can span a group of nearby buildings. In addition to operating in a limited space, a LAN is owned, controlled and managed by a single person or organization. A LAN can be set up using wired media (UTP cables, coaxial cables, etc.) or wireless media (Infrared, Radio waves). If a LAN is set up using unguided media, it is known as WLAN (wireless LAN). The key purpose of a LAN is to share resources. LAN users can share data, programs, printer, disk, modem, etc.

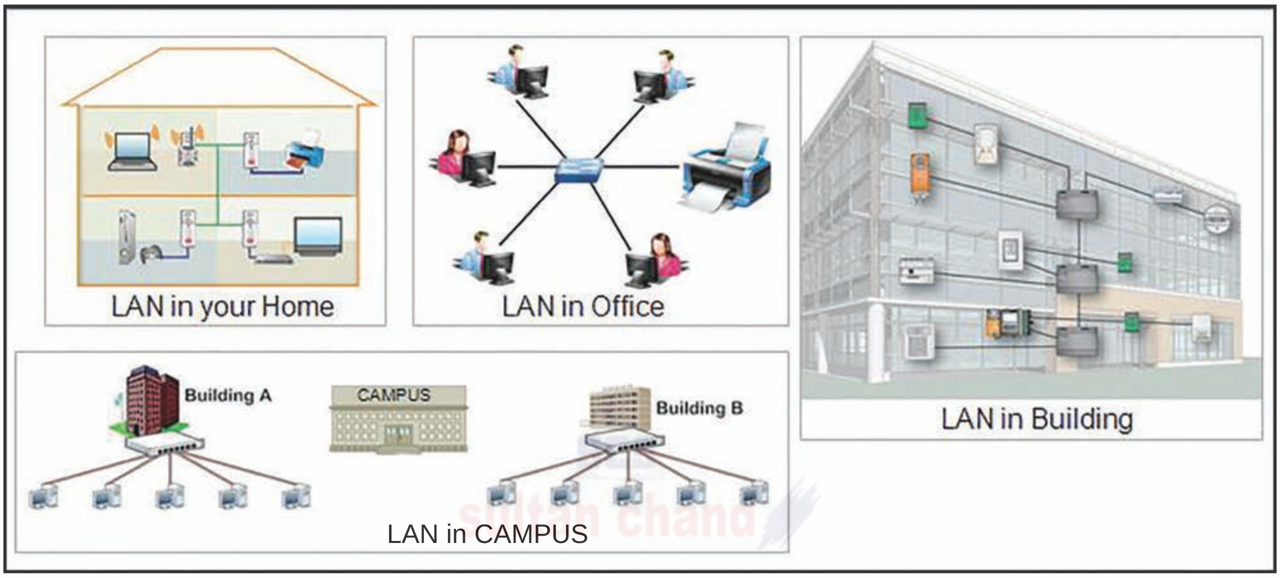


Fig. 8.15: Local Area Network (LAN)

Data transfer rate speed over a Local Area Network can vary from 10 mbps to 1 gbps.

8.10.3 Metropolitan Area Network (MAN)

MAN is larger than a LAN and can cover a city and its surrounding areas. A MAN usually interconnects a number of LANs and individual computers. It also shares the computing resources among users. All types of communication media (guided and unguided) are used to set up a MAN. A MAN is typically owned and operated by a single entity such as a government body or a large corporation. A good example of MAN is the interconnected offices of a Multinational Corporation (MNC) or cable television networks available in the whole city.

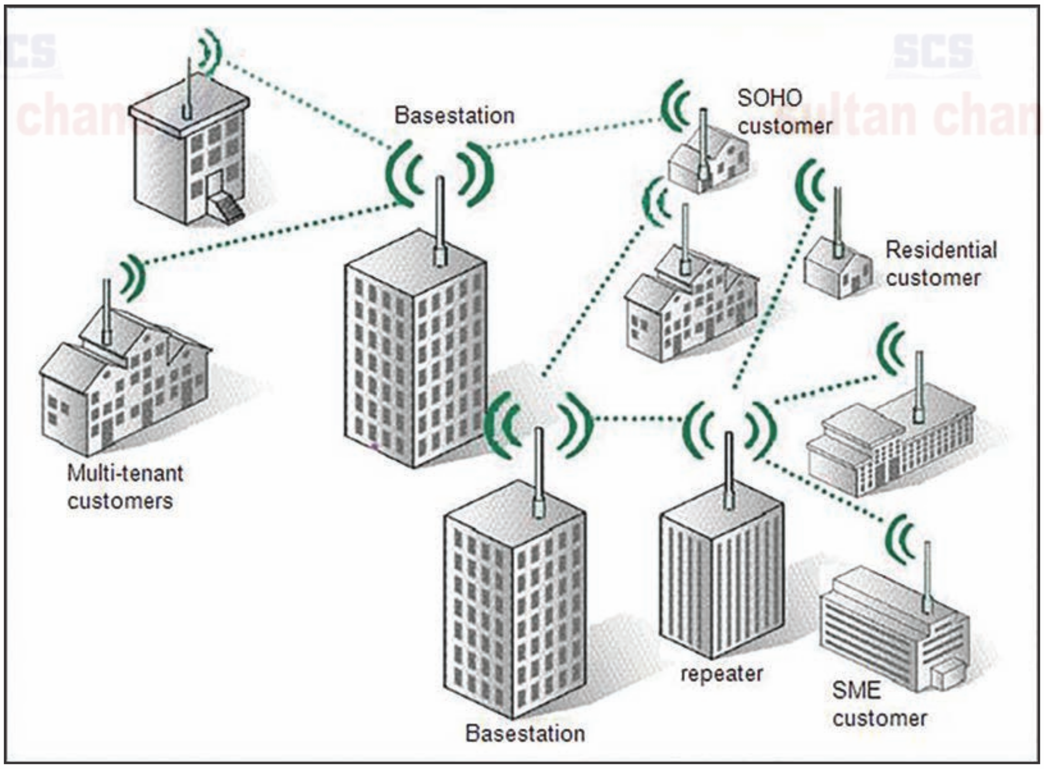


Fig. 8.16: Metropolitan Area Network (MAN)

8.10.4 Wide Area Network (WAN)

WAN is a telecommunication network. This type of network spreads over a large geographical area across countries and continents. WANs are generally used to interconnect several other types of networks such as LANs, MANs, *etc.* They facilitate fast and efficient exchange of information at a high speed and low cost. A WAN uses common carriers like satellite systems, telephone lines, *etc.*

WAN can cover an area with a radius spanning hundreds of kilometres. A network of ATMs, banks, government offices, international organizations' offices, *etc.*, spread over a country, continent or covering many continents are examples of WAN.

All types of communication media (guided and unguided) are used to set up a WAN. The best known example of a WAN is the internet. The internet is the largest WAN spanning the entire planet.

CTM: A WAN interconnects all the computers across the world.

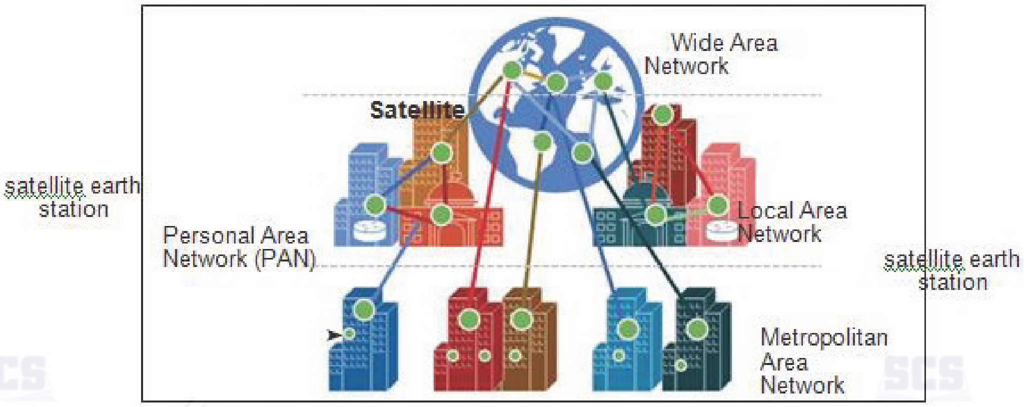


Fig. 8.17: Wide Area Network (WAN)

The following table summarizes the characteristics of PANs, LANs, MANs and WANs.

Parameter	PAN	LAN	MAN	WAN
Area covered	Small area (up to 10 m radius)	A building or campus (up to 10 km)	A city (up to 100 km radius)	Entire country, continent or globe
Networking cost	Negligible	Inexpensive	Expensive	Very expensive
Transmission speed	High speed	High speed	Moderate speed	Low speed
Error rate	Lowest	Lowest	Moderate	Highest
Network devices used	WLAN, USB Dongle	LAN/WLAN, Hub/ Switch, Repeater, Modem	Router, Gateway	Router, Gateway
Technology/ media used	Infrared, Bluetooth	Ethernet, Wi-Fi	Optical fibre, Radio-wave, Microwave	Microwave Satellite

CTM: LAN and WAN are the two primary and best-known categories of area networks; the others have emerged with technological advances.

Comparing LAN and WAN

As we have seen, computer networks can be classified into LAN, MAN and WAN categories on the basis of their geographical domains. A WAN extends over a large geographical area, such as states or countries. A LAN is confined to relatively smaller areas, such as an office, a building, *etc.* A MAN usually covers an entire city. It uses the LAN technology. The most common example of MAN is the cable television network. Thus, the basic points of difference between LAN and WAN are as follows:

1. The distance between the nodes in a LAN connection is limited to a specific range. The upper limit is approximately 10 kilometres and the lower limit is one metre. On the other hand, WANs are spread across thousands of kilometres in different countries or regions.
2. LANs operate between speeds of 1 mega bit per second (mbps) and 10 mbps while WANs operate at speeds of less than 1 mbps. To achieve speeds of several hundred mbps, it is advisable to use the optical fibre technology.
3. The error rate in LANs is lower than that in WANs because of the short distances involved in LANs. The error rate in LANs is approximately one thousand times less than that in WANs.
4. As LANs are limited by distance, an entire LAN is usually under the control of a single entity, such as an organization. On the other hand, WANs are usually operated and controlled by multiple organizations.

Thus, we can say that in comparison to WANs, LANs cover a limited area but they operate with high speed and low error rates.

8.11 NETWORK TOPOLOGIES

Topology is a way of connecting devices with each other either physically or logically. Two or more devices make a link and two or more links form a topology. It is basically a geometrical representation of how a network is laid out.

CTM: Topology is a way of connecting several devices with each other on a network.

Types of Topologies

Basically, there are five types of topologies and each topology has some advantages and disadvantages.

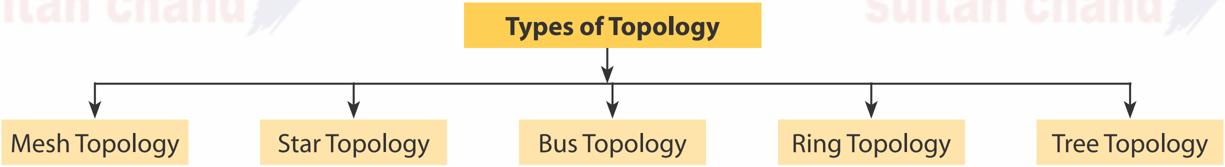


Fig. 8.18: Classification of Network Topologies

8.11.1 Mesh Topology

In mesh topology, each computer is connected with the other computer. There is a point-to-point link between each dedicated node (workstation). In this type of topology, the link carries traffic only between the two connected devices. A fully connected mesh network has **n(n–1)/2** links, where n is the total number of connecting nodes.

For example, if there are five computers and each is connected with the other one, then there will be 5(5–1)/2=10 links.

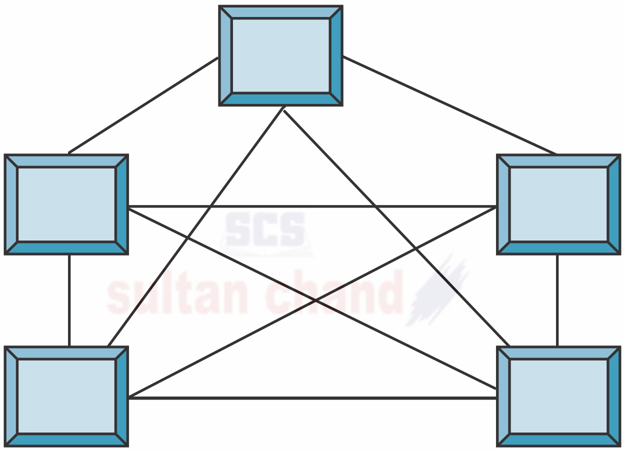


Fig. 8.19: Mesh Topology

Advantages of Mesh Topology

(a) Each communicating device carries its own data through its own dedicated link, hence eliminating traffic problems.

(b) A mesh topology is robust. If one link becomes unusable, it does not affect the entire system.

(c) Expansion and modification in topology can be done without disrupting other nodes.

(d) There is the advantage of privacy or security of data. When every message travels along a dedicated line, only the intended recipient sees it. Physical boundaries prevent other users from gaining access to messages.

(e) Point-to-point links make fault identification and fault isolation easy. Traffic can be routed to avoid links with suspected problems. This facility enables the network manager to discover the precise location of the fault and aids in finding its cause and solution.

Disadvantages of Mesh Topology

(a) Mesh topology is highly expensive to set up and involves high maintenance costs because of the amount of cabling and the number of I/O ports required.

(b) The hardware required to connect each link (I/O ports and cable) can be prohibitively expensive.

(c) Set-up and maintenance of this topology is very difficult. Even administration of the network is tough.

CTM: When there is a point-to-point link between each computer in a network, it forms mesh topology.

8.11.2 Star Topology

In star topology, each communicating device is connected to a central controller called **hub.** ***(A hub is a hardware device used to connect several computers together.)*** Unlike mesh topology, the devices in star topology send and receive data indirectly; the data passes to and from the hub. If the data is required to be sent from one computer and received by another computer, then this can be accomplished only by the central controller as each data is first sent to the hub, which then relays that data to the destination computer.

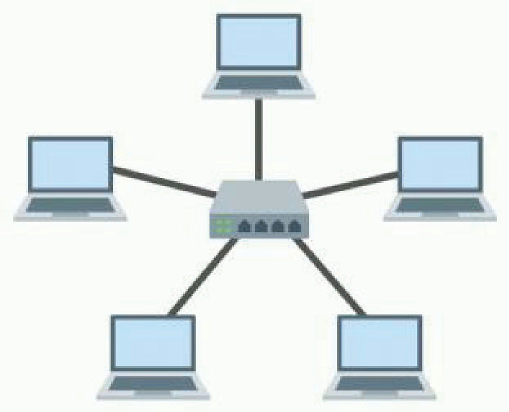


Fig. 8.20: Star Topology

Most popular and widely used **LAN** technology, **Ethernet**, currently operates in Star Topology.

Advantages of Star Topology

(a) Fewer wires are required as compared to mesh topology which, thus, reduces the number of input/output ports.

(b) Installation and maintenance of network is easy and takes less time.

(c) It is easy to detect faults in this network as all computers are dependent on the central hub.

This means that any problem which makes the network non-functioning can b e traced to the central hub.

(d) The rate of data transfer is fast as all the data packets or messages are transferred through central hub.

(e) As the nodes are not connected to each other, any problem in one node does not hamper the performance of other nodes in the network.

(f) Removal or addition of any node in star topology can take place easily without affecting the entire performance of t h e network.

Disadvantages of Star Topology

(a) Extra hardware is required for installation of central controller known as hub.

(b) All nodes of star topology are dependent on central hub and, therefore, any problem in the hub makes the entire network shut down.

(c) The performance of the entire network is directly dependent on the performance of the hub. If the server is slow, it will cause the entire network to slow down.

(d) More cabling is required in star topology as compared to any other topology (ring, bus, tree) as all nodes are directly connected to a central hub.

8.11.3 Bus Topology

Bus topology is a multipoint configuration, *i.e.*, several devices are connected to a main long cable which acts as a backbone. Nodes are connected by drop lines and taps. A drop line is a connection between the long cable and devices and taps are the connectors that are punctured inside the main cable. The data flows from one end of the cable to the other.

However, as the signal travels a long distance, it becomes weaker and weaker.

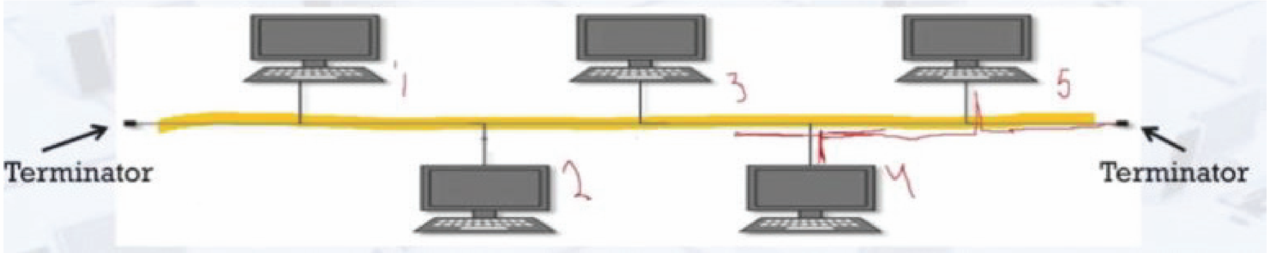


Fig. 8.21: Bus Topology

Therefore, there should be a limited number of nodes connected to a line. Ethernet is a common example of bus topology.

Advantages of Bus Topology

(a) Nodes can be connected or removed easily from bus network.

(b) It requires less cable length than a star topology.

(c) Bus network is easy to implement and can be extended up to a certain limit.

(d) It works well for small networks.

Disadvantages of Bus Topology

(a) If there is a fault or break in the main cable, the entire network shuts down.

(b) Terminators are required at both ends of the backbone cable.

(c) Fault isolation is difficult to detect if the entire network shuts down.

(d) When the network is required in more than one building, bus network cannot be used.

(e) The signal becomes weaker if number of nodes becomes large.

(f) Performance degradation occurs with the increased number of nodes.

(g) Collision of data can take place because several nodes can transmit data to each other at one time.

CTM: There is a main cable which is connected to several workstations through taps. Collision of data can take place in bus topology.

8.11.4. Ring Topology

In ring topology, each node is connected to two other nodes on either side of it, forming a ring network. It shows the line configuration in which each node is connected to one predecessor node and one successor node. Signal is transmitted only in one direction along the entire ring in a circular fashion. In ring topology, each device is incorporated with a repeater to strengthen the signal as a signal passes through all nodes in the entire network. When the data is transmitted from one node to its recipient node, then the intermediate node regenerates the signal and passes the signal to the destined node.

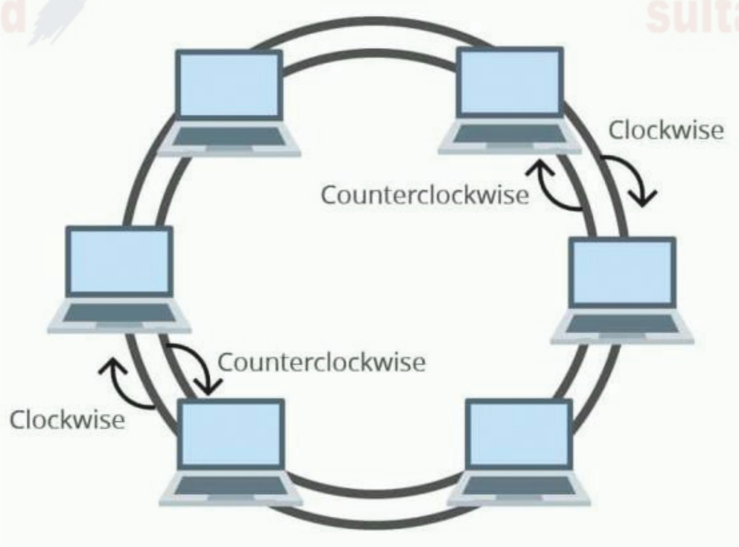


Fig. 8.22: Ring Topology

Token Ring is an example of ring topology.

Advantages of Ring Topology

(a) A central server is not required in ring topology as the data is passed between two nodes which then pass through the entire network.

(b) The data is transmitted in one direction only and, hence, the transmission rate increases.

(c) The adding or removing of network nodes is easy as the process requires changing only two connections.

(d) The configuration makes it easy to identify faults in network nodes.

(e) In this topology, each node transmits the data to its next node in a ring.

(f) It is relatively cheaper as compared to star topology.

Disadvantages of Ring Topology

(a) If there is a fault in a single node, it can cause the entire network to fail.

(b) The movement or changes made to network nodes affect the entire network's performance.

(c) Transmission speed becomes slower with an increase in the number of nodes.

(d) If there is a fault or break in a cable to which all other nodes are connected, the entire network shuts down.

(e) For proper communication between each node, it is required that each computer must be turned on.

CTM: In ring topology, each workstation is connected with the predecessor node as well as with the successor node and, thus, forms a ring. Data is transmitted only in one direction.

8.11.5 Tree Topology

In tree topology, all or some of the devices are connected to the central hub, called an active hub, and some of the devices are connected to the secondary hub, which may be an active hub or passive hub. An active hub contains the repeater that regenerates the signal when it becomes weaker with longer distances. A passive hub simply provides a connection between all other connecting nodes.

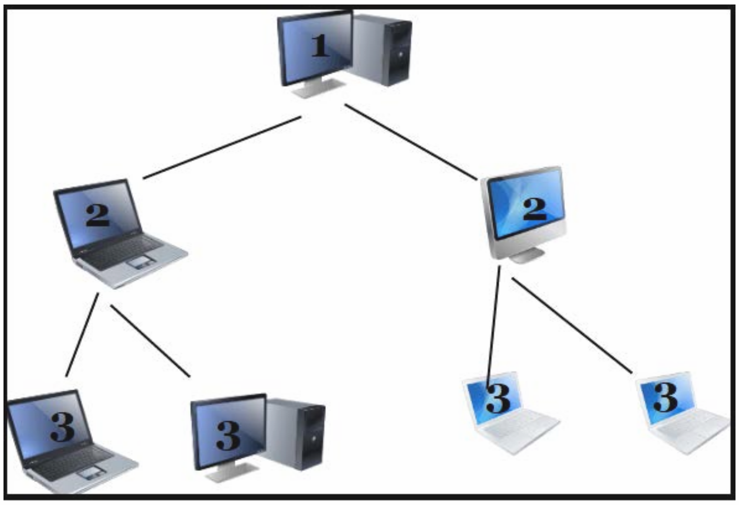


Fig. 8.23: Tree Topology

Advantages of Tree Topology

(a) The tree topology is useful in cases where a star or bus cannot be implemented individually.

(b) It is most suited in networking multiple departments of a university or corporation, where each unit (star segment) functions separately, and is also connected with the main node (root node).

(c) The advantages of centralization that are achieved in a star topology are inherited by the individual star segments in a tree network.

(d) Each star segment gets a dedicated link from the central bus. Thus, failing of one segment does not affect the rest of the network.

(e) Fault identification is easy.

(f) The network can be expanded by the addition of secondary nodes. Thus, scalability is achieved.

Disadvantages of Tree Topology

(a) As multiple segments are connected to a central bus, the network depends heavily on the bus. Its failure affects the entire network.

(b) Owing to its size and complexity, maintenance is not easy and costs are high. Also, configuration is difficult in comparison to other topologies.

(c) Though it is scalable, the number of nodes that can be added depends on the capacity of the central bus and on the cable type.

CTM: In tree topology, the main central hub is connected to the secondary hub through which all devices are connected with each other. Tree topology is just like a parent-child relationship.

The decision to select a particular topology for a network does not take place in isolation as the topology determines the type of media and access methods that would be used on the network. Therefore, several factors are taken into consideration before selecting a topology which are as follows:

- **Cost:** Cost signifies that the network should be cost-effective. For this, it is required to minimize the installation cost. This can be done by selecting an economical transmission medium (that is, wires) for data exchange between the network nodes. The network cost can also be minimized by reducing the distances between the nodes.
- **Flexibility:** Flexibility signifies that the network must be flexible enough, *i.e.*, it should be easy to reconfigure. Reconfiguring a network means to rearrange the existing nodes or add new ones on the network.
- **Reliability:** It refers to the degree of trust that can be placed on a network. Like any other system, a network can also encounter failure. A network failure can occur due to the following causes:
  1. When an individual node stops working.
  2. When the entire network fails. This is caused by a more serious fault that stops the working of an individual node.

What is Point-to-Point (P-P) Link

A P-P link, also known as a dedicated link, is used to connect two nodes in a network. The function of P-P link is to send and receive data over a network. In a P-P network, each workstation receives data from only one transmitter and each transmitter transmits data only to one receiver. Fig. 8.23 shows a P-P link in a network.

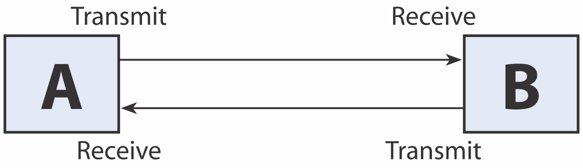


Fig. 8.24: A Point-to-Point Link

For better performance, the transmit and receive operations can occur over separate cables or wires, or they can occur in turns over the same wire by using different transmission techniques. A P-P link can be established in several ways. The simplest way is to install a P-P link between each pair of computers over a network.

8.12 COMMUNICATION MEDIA

Communication media is also known as transmission media through which data or signal is transferred between two communicating devices, *i.e.*, from one system to another system, through wires or without wires. If the data is sent across network through wires, it is called guided media and if the data is sent without wires, it is called unguided media.

CTM: Communication media is a transmission media used for sending data or signal across the network.

Types of Communication/Transmission Media

All communication/transmission media can be divided into two categories:

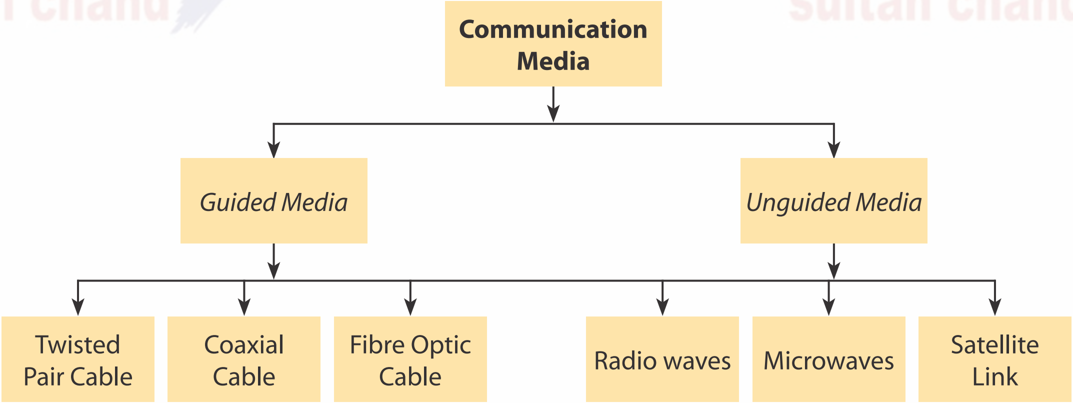


Fig. 8.25: Types of Communication Media

A. **Guided Media (Wired Media):** Guided media is also known as physical or conducted media. These media use wires for transmitting data. Various wired connections are twisted pair wire, coaxial cable and fibre optic cable.

B. **Unguided Media (Wireless Media):** A transmission media that does not require the use of cables for transmission of data is known as unguided media. Wireless transmission is also known as unguided media or non-physical media as the transmission takes place through various types of electromagnetic waves, such as radio waves, terrestrial microwave transmissions, satellite transmissions, cellular radio systems, infrared transmissions, *etc.*

8.12.1 Guided Media or Wired Networking Technologies

1. Twisted Pair Cable

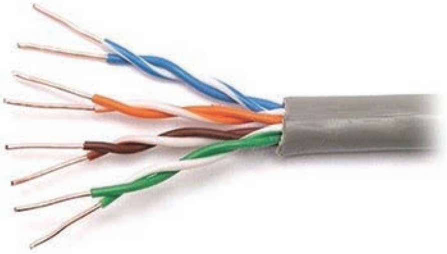


Fig. 8.26: Twisted Pair Cable

A twisted pair cable is the oldest, simplest and the most common type of conducted media. It is made of two plastic insulated copper wires which are twisted together to form a single wire. Each wire is 1 mm thick. Out of these two wires, only one carries the actual signal while the other is used for ground reference. The wires so twisted are helpful in avoiding interference from the nearby similar pairs, which is known as crosstalk. Twisted pair can be specified as Category 1–5 and is abbreviated as Cat 1–5. Category 6 twisted pair can support data transmission as high as 200 mbps for 100 metres while Category 7 twisted pair can support still higher data rates.

Twisted pair comes in two varieties:

(a) **Shielded twisted pair (STP): STP cables** are covered in metal foil. This makes them indifferent to noise and crosstalk.

(b) **Unshielded twisted pair (UTP): UTP** has seven categories, each suitable for a specific use. In computer networks, mostly Cat-5, Cat-5E and Cat-6 cables are used. UTP cables are connected by RJ-45 connectors.

Advantages of Twisted Pair Cable

(a) It is simple to use.

(b) It is inexpensive and does not require skilled personnel.

(c) It is less susceptible to electrical interference caused by nearby equipment or wires in a telephone system. Signals can travel several kilometres without amplification when twisted pair wires are used.

(d) These media can be used for both analog and digital data transmission. The bandwidth depends on the thickness of the wire and the distance travelled, but several megabits per second can be achieved for a few kilometres in many cases.

(e) If a portion of a twisted pair cable is damaged, the entire network is not shut.

Disadvantages of Twisted Pair Cable

(a) STP wire is physically larger and more expensive than twisted pair wire.

(b) STP is more difficult to connect to a terminating block.

(c) It easily picks up noise signals which results in higher error rates when the line length exceeds 100 metres.

(d) Being thin in size, it is likely to break easily.

(e) It can support 19,200 bps up to 50 feet on RS-232 port.

2. Coaxial Cable

A coaxial cable is generally called a coax wire. It consists of insulated copper wires surrounded by a braided metal shield and covered in a plastic jacket. Coax cables are capable of carrying higher frequency signals than that of twisted pair cables. The wrapped structure provides it a good shield against noise and crosstalk. Coaxial cables provide high bandwidth rates of up to 450 mbps. Coaxial cable also comes in two primary physical types: **thin coaxial cable** and **thick coaxial cable**. There are three categories of Coax cables, namely RG-59 (Cable TV), RG-58 (Thin Ethernet) and RG-11 (Thick Ethernet). RG stands for Radio Guide. Coax cables are widely used for internet connections and cable televisions.

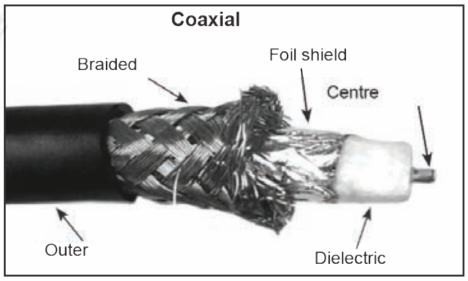


Fig. 8.27: Twisted Pair Cable

Advantages of Coaxial Cable

(a) Coaxial cable can support greater cable lengths between network devices than twisted pair cable.

(b) It is useful for transmitting analog as well as digital data across the network. For analog data transmission, 75 ohm broadband coaxial is used and for digital transmission, 50 ohm baseband cable is used.

(c) It is widely used for cable television and internet connections.

(d) Coax are used for transmitting several channels simultaneously, *i.e.*, they are helpful in broadband transmission.

(e) Coaxial cable has excellent noise immunity because of thick covering outside the insulated wires.

(f) Thick coaxial cable has an extra protective plastic cover that helps keep moisture away.

(g) It is relatively inexpensive as compared to fibre optic cable.

Disadvantages of Coaxial Cable

(a) Thick coaxial cables do not bend easily and thus are difficult to install.

(b) It is expensive as compared to twisted pair cable.

3. Fibre Optic Cable

Fibre optic transmits light signals rather than electrical signals. It is the newest form of guided media. Several glass fibres are bundled together and are encased in an insulated covering. Light signals travel into the fibre optic cable at one end and are received at the other end. When the light enters the fibre optic, the light pulse inside the cable hits the outer walls of the wire at a similar angle, which helps in moving the light wave forward. The outer surface of the glass wire provides just the right angle reflection to keep the light bouncing back and forth along the length of cable. The light source used in this process is light emitting diode (LED).

Optical fibres may be single mode or multimode. Single mode optic fibre transmits only single light width but multimode fibre uses multiple light paths.

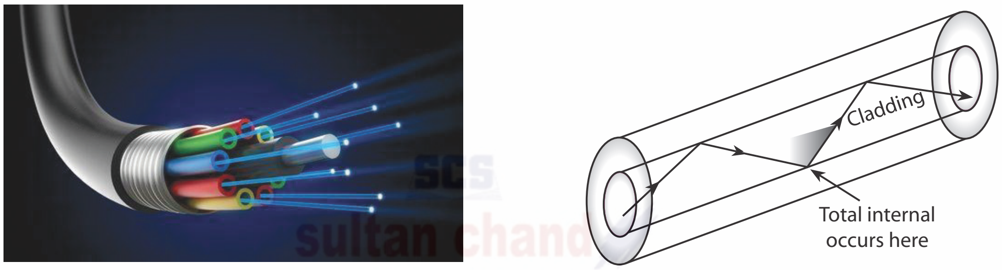


Fig. 8.28: Fibre Optic Cable

Advantages of Fibre Optic

(a) Fibre optic typically offers better bandwidth and can carry more information at once.

(b) As the signal travels in the form of light, there is less attenuation and signal degradation.

(c) Optical fibre wires are made of glass, so there is little risk of fire because of absence of spark hazards.

(d) Fibre optic cables are much thinner and lighter than metal wires.

(e) Lighter weight makes fibre easier to install.

(f) It does not leak signals, so it is immune to eavesdropping.

(g) A signal can run for 50 km without requiring regeneration.

(h) Fibre optic cables are also used in research and development.

Disadvantages of Fibre Optic

(a) A highly skilled labour is required for its installation and maintenance.

(b) It is relatively expensive as compared to other guided media.

(c) As fibre optic is made of glass, they can be easily broken.

(d) As light travels in a straight line, two fibres are needed if we need bidirectional communication.

8.12.2 Unguided Media or Wireless Networking Technologies

Features of Unguided Media:

1. Transmission and reception are achieved by means of an antenna.
2. Transmission can be either directional or omnidirectional.
   (a) Directional
   - transmitting antenna puts out focused beam
   - transmitter and receiver must be aligned

   (b) Omnidirectional
   - signal spreads out in all directions
   - can be received by many antennas

1. Microwave

Microwave signals are used to transmit data without the use of cable. It is a line-of-sight transmission as signal travels in a straight line. In microwave communication, two directional parabolic antennas are mounted on towers, buildings or hills to send and receive signals through air. However, they must be properly aligned with each other, otherwise the signal will not be focused well at the receiving antenna.

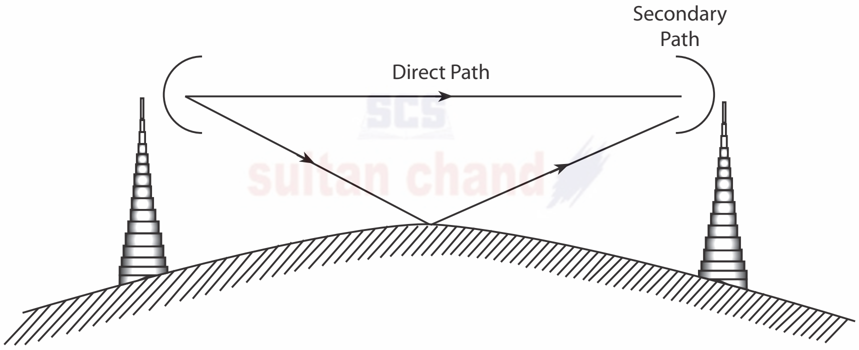


Fig. 8.29: Microwave

Advantages of Microwave Transmission

(a) It is a cheaper source of communication as it avoids using cables and maintaining repeaters.

(b) Communication through microwave is much easier over difficult terrain.

(c) Microwave system permits data transmission rate of about 16 gigabits per second.

Disadvantages of Microwave Transmission

(a) It is an insecure mode of communication.

(b) Signals can be split and propagated in different directions in air and received by the receiver antenna with a reduced strength.

(c) Microwave propagation is affected by weather conditions such as rain, thunderstorm, etc.

(d) The cost of implementing towers, antennas is relatively high.

2. Radio Waves

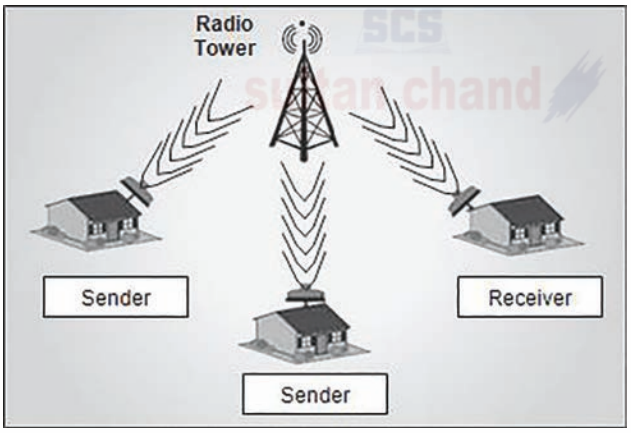


Fig. 8.30: Radio Waves

Radio waves use radio frequencies which are allocated to private businesses for direct voice communication. A radio set-up uses transmitter and receiver. A transmitter sends radio waves and encodes them into sine waves which, when received by a receiver, are decoded and the message is received. Both the transmitter and receiver use antennas to radiate and fetch radio signals. They are not line-of-sight transmission and, hence, can penetrate buildings easily.

Advantages of Radio Waves

(a) They can be used indoors or outdoors.

(b) They are omnidirectional and can travel in any direction.

(c) Transmitter and receiver antenna do not need to be physically aligned.

(d) Radio wave transmission offers mobility.

(e) It is cheaper than laying cables and fibres.

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

Disadvantages of Radio Waves

(a) Radio wave communication is an insecure mode of communication.

(b) Radio wave propagation is susceptible to weather effects like rain, thunderstorm, etc.

3. Satellite Link

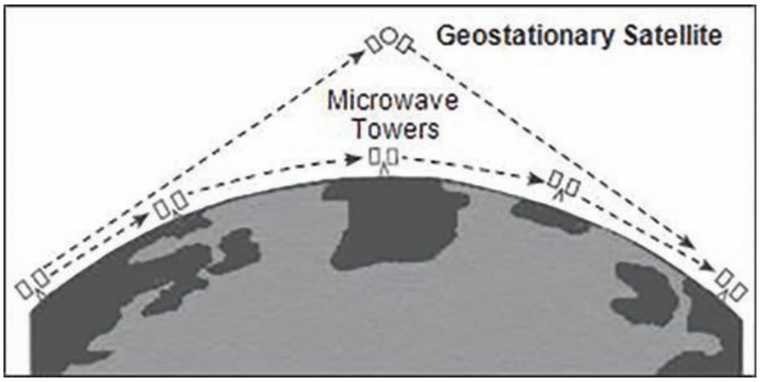


Fig. 8.31: Satellite Link

Satellite transmission is also a kind of line-of-sight transmission that is used to transmit signals throughout the world. When the frequency is greater than 3 GHz, the transmission is known as microwave. Satellite is a special type of microwave transmission medium.

It provides various types of services such as transmitting fax, voice data, video, email and other internet applications. In satellite communication, an earth station has a satellite dish, which functions as an antenna to transmit and receive data from satellites.

When data is transmitted from an earth station to a satellite, it is known as uplink and when transmission takes place from a satellite to an earth station, it is known as downlink. In satellite, there are transponders that send and receive signals from/to the earth station.

Advantages of Satellite Link

(a) The area covered is quite large.

(b) No line-of-sight restrictions such as natural mountains, tall buildings, towers, etc.

(c) Earth station which receives the signals can be at a fixed position or can be relatively mobile.

Disadvantages of Satellite Link

(a) It is very expensive as compared to other transmission mediums.

(b) Installation is extremely complex.

(c) Signals sent to the stations can be interrupted by external interference.

(d) Low antenna gains result in overcrowding of available bandwidth.

4. Infrared

The type of transmission that uses infrared light to send data is known as infrared transmission. The data is transmitted through air and can propagate in the open space; however, it cannot penetrate the walls of the room. It is an example of short range wireless network. Infrared speed varies from 2.4 kbps to 16 mbps. A very good example of infrared transmission is a handheld remote control such as remote control of a TV or AC, etc.

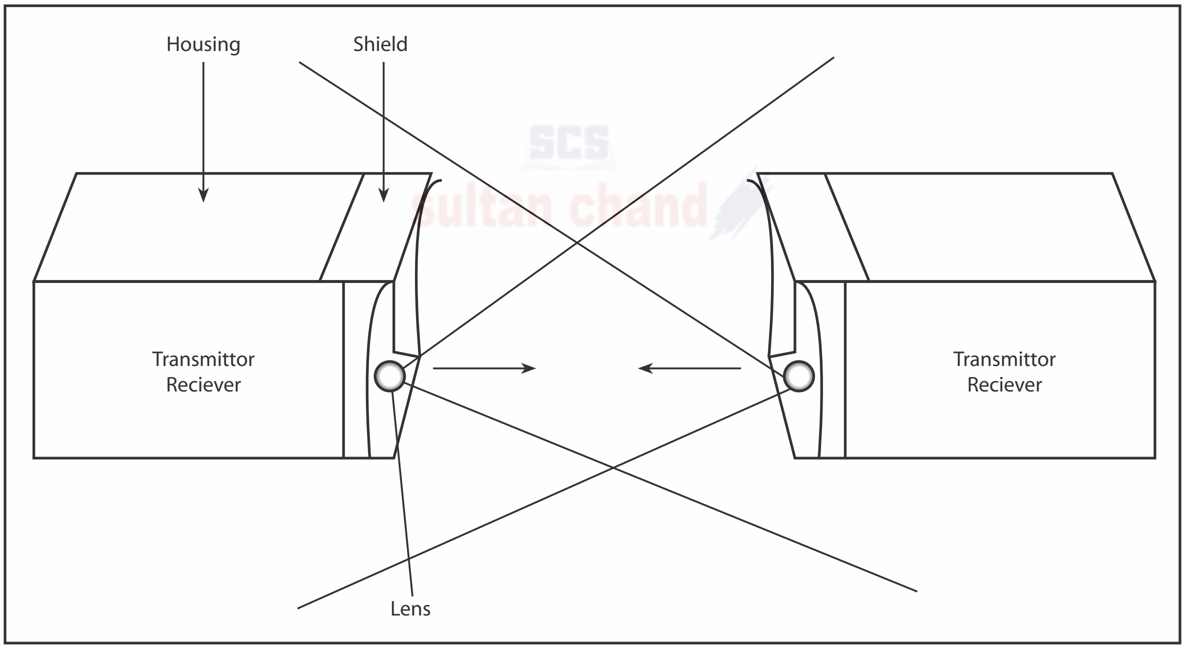


Fig. 8.32: Infrared Transmission System

Advantages of Infrared Transmission

(a) It is a secure medium of transmitting data.

(b) It is a cheap mode of transmission.

Disadvantages of Infrared Transmission

(a) It can work only for short distances.

(b) It cannot penetrate walls and is affected by distance, noise and heat.

5. Wireless Technology

Wireless technology is the process of sending information through invisible waves in the air. Information such as data, voice and video are carried through the radio frequency of the electromagnetic spectrum. Thus, wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor. The various wireless technologies available are described as follows:

(a) **Wi-Fi (Wireless Fidelity):** Wi-Fi is wireless fidelity where communication takes place without wires. The users share the data with each other by connecting to the broadband internet service without using cables. As it is not a secured media of transmitting data, the user must use privacy methods such as using passwords and make the connection security enabled so that it does not become susceptible to hackers. For transmission of data through Wi-Fi, a user must have a broadband connection, a wireless router and a laptop or desktop.

(b) **Wi-Max (Worldwide Interoperability for Microwave Access):** Wi-Max is a wireless communication system that provides broadband internet accessibility up to 30 miles. The data transmission takes place without wires. It provides data rates up to 30 to 40 megabit-per-second and up to 1 Gbit/s for fixed stations. Wi-Max is based on standard IEEE 802.16 technology that provides users with access to high-speed voice, data and internet connectivity. Wi-Max uses broadband internet connection and requires a tower known as base station to communicate with the user. Instead of wires, it uses a microwave link to establish a connection. Internet connectivity to end-user is provided by a microwave link between the tower and the end-user.

6. Other Unguided/Wireless Media

In this section, we will discuss two other important and extensively used wireless media— laser waves and Bluetooth.

(a) **Laser Technology:** Laser refers to a transmission medium that requires direct line of sight. It provides point-to-point transmission between points located at short distances, such as buildings. Similar to microwave, a laser is unidirectional but much faster. Lasers require transmitters and photosensitive receivers for transmission. A disadvantage associated with laser transmission is that it is badly affected by weather conditions.

Fig. 8.33: Bluetooth Technology

(b) **Bluetooth Technology:** Bluetooth refers to a telecommunication industry specification that defines how different devices can be connected virtually and transfer information among each other. Bluetooth technology is commonly used in various portable devices such as laptops and PDAs to establish a wireless connection in the form of Wireless LAN (WLAN).

Transmission of information using Blue- tooth requires a low-cost transceiver chip in each of the devices that need to be connected. Data is transferred at the frequency of 2.45 GHz, which is available globally. The rate of data transfer in this type of transmission is 1 mbps. Each device has a 48-bit address as per the IEEE 802 standard. The connection between the devices can be either point-to-point or multipoint. Bluetooth is equipped with various features such as encryption and verification to provide security.

8.13 NETWORK TERMINOLOGIES

1. **Data Channel:** A channel is a communication medium through which data or message is transferred from the sender to the receiver.
2. **Baud:** The number of changes in a signal per second is called a baud. It is the unit of measurement for the information-carrying capacity of a communication channel.
3. **Bits per second:** It is the measuring unit of speed at which data transfer takes place.
4. **Bandwidth:** The bandwidth measures the information-carrying capacity of a line or a network. It is the difference between the highest and lowest frequencies allowed on a transmission media.

   $$B = fh - fl$$

   where fh and fl are the highest and lowest frequencies.

   For example, If the highest frequency is 80 Hz and lowest frequency is 50 Hz, what is the bandwidth of a signal?

   Sol. B = fh – fl

   B = 80 – 50

   B = 30 Hz.
5. **Protocol:** A protocol is an agreement between the communicating parties on how communication is to proceed. Protocol means a set of rules that governs a network. A protocol is a formal description of message formats and the rules that two or more machines must follow to exchange those messages.

   For example, using library books.

CTM: Protocol is a set of rules that governs the network.

Types of Protocols

Protocol specifies what is communicated and how. Let us take an example to explain this concept. In India, different people speak different languages. Now, a person from Tamil Nadu and a person from Punjab may not be able to communicate with each other because of the language difference. However, they can exchange their ideas and communicate with each other using English as their common language. Similarly, in case of computers, the hardware, software or even a combination of the two might be required to implement and carry out the protocol. Thus, the protocol will help in setting up a channel of communication or a connection between two computers; in other words, a hardware connection between two computers.

There are multiple protocols defined for computer networks, which are as follows:

(a) TCP (Transmission Control Protocol)

(b) IP (Internet Protocol)

(c) FTP (File Transfer Protocol)

(d) PPP (Point-to-Point Protocol)

(e) SMTP (Simple Mail Transfer Protocol)

(f) POP3 (Post Office Protocol)

(g) TELNET (Remote Login)

(a) **TCP/IP (Transmission Control Protocol/Internet Protocol)**

TCP is one of the main protocols in TCP/IP networks. The IP protocol deals only with packets but TCP enables two hosts to establish a connection and exchange streams of data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other. The packets are delivered not in a sequential order; instead, they are delivered randomly. Now, TCP at the receiver side collects all packets and arranges them in a sequential order. TCP is a reliable stream delivery service that guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packets are transferred over many networks and, thus, not reliable, a technique known as positive acknowledgement with retransmission is used to guarantee reliability of packet transfers.

(b) **IP (Internet Protocol)**

IP is the primary protocol present in the internet layer of the internet protocol suite. It is responsible for delivering packets from the source host to the destination host based on the IP addresses mentioned in the packet headers. IP forwards each packet based on a four byte destination address (the IP number). The packets are moved randomly from source to destination, which are then assembled in a sequential order at the destination computer. IP stores destination addresses in the form of IP addresses so that the packets will move to the destined address only by following the shortest route.

(c) **FTP (File Transfer Protocol)**

FTP is the simplest and most secure way to exchange files over the internet. The main objectives of FTP are:

- Transmitting and sharing of files (computer programs and/or data).
- Indirect or implicit use of remote computers.
- To shield a user from variations in file storage systems among different hosts.
- To transfer data reliably and efficiently.
- FTP uses the internet's TCP/IP protocols to enable data transfer.

FTP is most commonly used to download a file from a server using the internet or to upload a file to a server (e.g., uploading a web page file to a server).

While sharing files from one system to another, we may encounter several problems—two systems may have different directory structures, two systems may have different file-naming conventions, or two systems may have different ways to represent text and data. All these problems are solved by FTP.

CTM: File transfer protocol is used to transfer files from server system to requesting node, primarily for information sharing.

(d) **PPP (Point-to-Point Protocol)**

PPP is the most commonly used data link protocol. It is a protocol used to establish a direct connection between two nodes. It can provide connection authentication, transmission encryption and compression. It is used to connect the Home PC to the server of ISP. The communication takes place through high speed modem. PPP is used to connect telephone dial-up lines to the internet. Internet service provider may provide you with a PPP connection so that when you send any request, the provider's server can respond to your requests, forward it to the internet server, and then forward responses back to you. For communicating through PPP, the user needs to install PPP drivers assigned by the internet to the computer.

The following steps are required to connect to the internet:

- Double click on the dial-up icon.
- Dial the number provided to you by the ISP.
- Enter the login and password.
- Open a browser like Internet Explorer or Netscape Navigator.

The various features of PPP are:

- Establishing the link between two devices.
- Maintaining this established link.
- Configuring this link.
- Terminating this link after the transfer.
- PPP provides error detection.
- PPP supports multiple protocols.
- It also defines how two devices can authenticate each other.

(e) SMTP (Simple Mail Transfer Protocol)

As the name suggests, SMTP is used for sending email messages to other networks or computers. It handles only outgoing messages and not incoming messages. SMTP does not create messages: rather, it helps in forwarding messages between client servers. It uses TCP to send messages to another host. For receiving messages, another protocol POP (post office protocol) is used. Thus, email clients require addresses of both SMTP server and another server that processes incoming messages (usually POP or IMAP). SMTP uses TCP port number 25 for standard communication.

(f) POP3 (Post Office Protocol 3)

The POP (Post Office Protocol 3) is a simple and standard method to access mailbox and download messages to the local computers. The user can receive messages with the help of POP protocol. The advantage is that once the messages are downloaded, an internet connection is no longer needed to read the mail. A user can read all emails offline as these are saved on the computer's hard disk.

Just like with the SMTP protocol, the POP protocol (POP2 and POP3) sends text commands to the POP server. There are two main versions of this protocol—POP2 and POP3—to which ports 109 and 110 respectively are allocated and which operate using radically different text commands. To get a mail from POP server, a user must enter a valid username and password for their email account. The POP3 protocol thus manages authentication using the user name and password; however, it is not secure because the passwords, like the email, circulate in plain text over the network. POP3 protocol blocks inbox during its access which means that simultaneous access to the same inbox by two users is impossible

(g) **TELNET (Remote Login)**

Telnet is a remote login that helps a user to log on to another user's terminal without being its original user. A user who is logging in to their own system can also get access to log on to another user system and perform various functions such as accessing files or sharing files to/from the remote system. With TELNET, a user logs in as a regular user with whatever privileges they may have been granted to the specific application and data on that computer.

Working of Telnet

(i) A user is logged in to the local system and invokes a TELNET program (the TELNET client) by typing **telnet<host address> or telnet <IP address>**

(ii) The TELNET client is started on the local machine (if it isn't already running). The client then establishes a TCP connection with the TELNET server on the destination system.

(iii) Once the connection has been established, the client program accepts characters from the keyboard feed by the user and passes one character at a time, to the TELNET server.

(iv) The server on the destination machine accepts the characters sent to it by the client and passes them to a terminal server.

(v) The terminal server gives outputs back to the TELNET server and displays them on the user's screen.

The user can terminate the telnet session by typing LOGOFF or LOGOUT on the system prompt.

8.14 WIRELESS/MOBILE COMMUNICATION

8.14.1 GSM (Global System for Mobile Communication)

GSM stands for Global System for Mobile communication. It provides its subscribers with roaming facility so that they can use their mobile phones all over the world to communicate with each other. GSM provides digital signalling as well as digital call facility and is so considered as a second generation (2G) mobile phone system. It provides consumers with better voice quality and low-cost alternatives to making calls such as short message service (SMS). It has an ability to carry 64 kbps to 120 mbps of data rates. The key feature of GSM is the Subscriber Identity Module (SIM), generally known as SIM card. It is a detachable smart card that contains the subscriber's information along the phone book. This allows the user to use the phone book and other information even after changing the handset.

CTM: GSM is a wireless communication medium that provides the user with roaming facility, good voice quality, SMS, etc., through digital signals.

8.14.2 CDMA (Code Division Multiple Access)

CDMA stands for Code Division Multiple Access. CDMA is an example of multiple access, where several transmitters can send information simultaneously over a single communication channel. It is a channel access method used by various radio communication technologies. It allows the division of transmission medium into different channels so that transmission from different stations is separated from each other. It employs spread spectrum digital technology where the data is fragmented into small chunks over a number of different frequencies available for use. Analog to digital conversion takes place where audio input is first digitized into binary elements. The CDMA system works directly on 64 kbit/sec digital signals.

CTM: CDMA is a digital cellular technology that uses spread spectrum technique where the entire bandwidth is divided among several users for transmission of data.

8.14.3 GPRS (General Packet Radio Services)

GPRS or General Packet Radio Services provides various features over 2G phones with respect to high speed data transfer. A user can send and receive data at the same time and thus uses the same bandwidth for both purposes. Using GPRS technology, a user can make a call and at the same time receive a message without disconnecting the call. However, GPRS usage is charged for the amount of data sent or received. GPRS can provide data rates up to 32kbps to 48kbps. With this data rate, email messages, video streaming, audio files, etc., can be downloaded and, therefore, can be called 2.5G technology as it lies between the second (2G) and third (3G) generations of mobile telephony.

Services Provided By GPRS

(a) Sending and receiving text messages.

(b) Internet access.

(c) Multimedia Messaging Service (MMS).

(d) Internet applications for smart devices through Wireless Application Protocol (WAP).

(e) Networking facility with one person or with several persons in a group, *i.e.*, videoconferencing.

CTM: GPRS provides high speed data transfer. A user is allowed to download video streaming, audio files, email messages, etc.

8.14.4 Wireless in Local Loop (WLL)

WLL provides the subscribers with wireless phone facility to communicate with each other in order to get better voice quality. It employs the use of electromagnetic radiation to connect subscribers to the local exchange without the use of wires. The user can use wireless phone, speaker phone and parallel phones for communication with each other. In traditional telephone networks, phone would be connected to the nearest exchange through a pair of copper wires. But in Wireless Local Loop (wireless in local loop) technology, the subscriber is connected to the nearest exchange through a radio link instead of copper wires. Wireless in local loop is cheaper and quicker than copper wire connectivity. As the cost of copper along with the cost of digging increases over time, this method proves cheaper than using copper wires. It is used in remote areas where digging for copper wires is not possible.

There are various technologies like Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) and Code Division Multiple Access (CDMA) used for wireless in local loop. In crowded urban localities where permission to dig may be almost impossible to get, wireless technology is advised. However, there are also some disadvantages of using wireless in local loop. First, as the distance between a receiver and transmitter increases in a wireless system, the strength of the signal at the receiving end decreases even if there are no obstacles in the way. Second, as the electromagnetic waves are propagated through air, a signal travelling from a transmitter may take alternative paths on its way to the receiver. These paths may cause delays in the received signal due to the extra distance travelled.

CTM: Wireless in local loop is a system that is similar to telephone system which provides wireless telecommunication by deploying a multiplicity of multichannel transceivers.

8.15 MOBILE TELECOMMUNICATION TECHNOLOGIES—1G, 2G, 3G & 4G

➢ 1G Technology

1G technology was used in the first mobile phones. 1G was introduced in the 1980's. Transmission of voice data took place through analog radio signals. 1G network was used for voice calls and not for transmitting text messages. *For example*, NMT, C-Nets, AMPS, TACS.

Salient features of 1G technology:

- It provides data rates up to 2.4 kbps.
- It uses analog signals.
- Voice quality is not very good.
- It does not support transmission of text messages.
- It does not provide security.

➢ 2G Technology

2G technology is the first digital cellular system that was launched in the early 1990's that provides high data transmission rate in digital format. 2G also introduced data services for mobiles, starting with SMS. *For example*, D-AMPS, GSM/GPRS, CDMAOne.

Salient features of 2G technology:

- Good quality of sound.
- Higher data rates up to 64 kbps.
- Improved security mechanism.
- Transmission of data such as text messages in digital format.
- Support transfer of picture messages and MMS.
- It does not support transfer of complex data such as videos.
- It allows multiple users per radio channel with each user talking one at a time.
- Digital transmissions enable compressed voice and multiplexing multiple users per channel.

➢ 3G Technology

3G technology was introduced in the year 2000 and provides much higher data rates with speed from 144kbps to 2mbps.

3G technology has introduced more efficient ways of carrying data, making it possible to have faster web services, live chat, fast downloading, videoconferencing, etc., over mobile phones. *For example*, CDMA2000/EV-DO,WCDMA/HSPA+,TD-SCDMA.

Salient features of 3G technology:

- It has introduced more efficient ways of carrying data with faster web services.
- Live chat, fast downloading, videoconferencing, etc., are also possible over mobile phones.
- It allows the user to play 3D games.
- A user can see live streaming on smartphones.
- It provides broadband internet services.
- It allows the user to send and receive large email messages.
- High bandwidth is required.
- Splits channel into time intervals enabling a single user to get all the resources at once.

➢ **4G Technology**

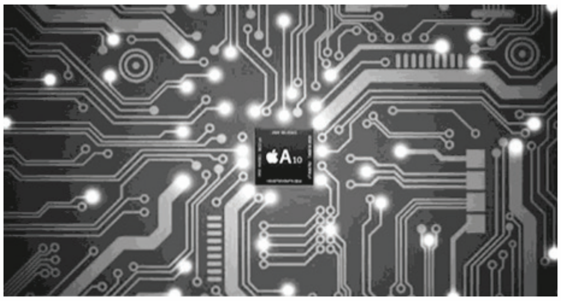
Unlike previous generations of mobile technology, 4G mobile technology uses ultra-high broadband internet services with much faster data speed, typically between 100 mbps–1gbps. Now, 4G rules the mobile market. Unlike previous generations of mobile technology, 4G mobile technology is used for internet access on computers also, and it is totally wireless. 4G provides internet access, high quality streaming video and "anytime, anywhere" voice and data transmission at a much faster speed than 3G. The "anytime, anywhere" feature of 4G is also referred to as "MAGIC" (Mobile multimedia; Anytime/anywhere; Global mobility support; Integrated wireless solution; Customized personal services).

Salient features of 4G technology:

- It is used for internet access on computers also and is totally wireless.
- 4G provides internet access, high quality streaming video and "anytime, anywhere" voice and data transmission at a much faster speed than 3G.
- It delivers faster and better mobile broadband experiences.
- It provides more data capacity for richer content and more connections.

  The "anytime, anywhere" feature of 4G is also referred to as "MAGIC" (Mobile multimedia) anytime/anywhere.

8.16 MOBILE PROCESSORS



Processors are required to run an operating system, be it a desktop, laptop or a mobile. Processors provide the necessary resources to start an operating system, run applications and do certain tasks. Today's smartphones and mobile processors are very powerful, so much so that they can compete with desktop computers.

Processors are now available in many cores. First it was single core, then came the dual core, and we now have quad core, hexa core and even octa core processors. Most processors available today are 64-bit as against 32-bit earlier. The processing speed has also touched 3.0–3.5 GHz now. The ability to equip mobile processors with GPU (Graphics Processing Unit) has enabled the devices to churn out best graphic pictures, have 3-D capability, Virtual Reality and 4K recording capability. The improved processor technology has also made modern mobile devices more power-efficient.

Today, there are many processors available in the market. QUALCOMM, Apple mobile processors, Intel mobile processors and some other giants are ruling the market. Let us discuss these mobile processors.

8.16.1 Qualcomm Snapdragon

Qualcomm Technologies is a US-based company. Qualcomm first became a known brand when they introduced the CDMA technology. Qualcomm is actively involved in technology related to semiconductor designing for mobile devices, tracking devices, satellite phones, virtual reality, wireless charging, communications, etc. Qualcomm is now known for its Snapdragon brand which is responsible for marketing mobile processors and LTE modems (4G).

Snapdragon became a big name in the processors market after it introduced the first 1 GHz processor when the average speed of most smartphones was only 512 MHz.

Since 2005, Snapdragon has come out with a number ofseries—S1, S2, S3, S4, S200, S400, S600, and S800. S800 series has already released S800, S801, S805, S808, S810, S820 and S821. The most common Qualcomm processor in the medium-to high-end phone market is either S820 or S821, which is the latest version.

8.16.2 Apple Mobile Processors

Apple does not manufacture microprocessors. Instead, it enters into contracts with processor-manufacturing companies, mainly Samsung and TSMC, for making custom-built processors that suit its design and performance expectations. For instance, A9 14nm processor was built by Samsung, while the A9 16nm version was built by TSMC.

Apple A series is designed for processors to be used in iPhone, iPad, iPad Touch and Apple TV.

Some of the processors in the series are A4, A5, A5X, A6, A6X, A7, A8, A8X, A9, A9X and A10.

- **Apple A10 Fusion** is the latest processor which is used in iPhone 7 and iPhone 7 Plus. A10 is a quad core built on 16 nm FinFET processor capable of running at 2.4GHz speed and a hexa core PowerVR GPU. A10 is twice as fast as its predecessor A9 and improves graphic processing by 50%. This processor is manufactured by TSMC.
- **Apple S series** is designed for processors to be used in Apple Watch. Some of the processors in the series are Apple S1, Apple S1P and Apple S2.

  The current version, Apple S2, is a dual core processor with built-in GPS used in Apple Watch Series 2. The processor is manufactured by Samsung under a contract with Apple.
- **Apple W series** is used in headphones for wireless audio connectivity. The current series, Apple W1, is used in wireless headphones and AirPods.
- **Apple T series** is designed to be used in TouchID sensors in MacBook Pro. The only version released till date is Apple T1.

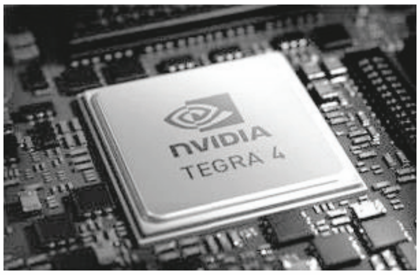
8.16.3 Intel Atom and Core M Processors

Intel is an American multinational company synonymous with PC and microprocessors. Atom is the brand name given for the low power-consuming and low-cost 32-bit and 64-bit chips manufactured for smartphones and tablets.

Intel processors are based on X86 architecture which is more powerful than ARM but consumes more power compared to ARM architecture. The latest versions of Intel processors have reduced the power consumption, bringing it down to less than 5 watts, which is ideal for all mobile devices. Though Atom processors in the beginning supported only Windows, they now support all major mobile operating systems.

Intel Atom processors are currently used in Atom X5 and X7 series. These chips are 64-bit quad core processors in 14 nm size with speeds of up to 1.6 GHz that can be scaled up to 2.4 Ghz. Intel also released **Intel Core M** ultra low-voltage microprocessors designed for ultra-thin notebooks, mobile devices and 2-in-1 convertibles. The processor consumes 4.5 watts or less power, making it ideal for long battery life. These are dual core processors with a speed of about 1.5 GHz which can be scaled up to 3.2 GHz. Intel Core M processors offer 40% boost in CPU and graphics performance as compared to the earlier versions.

8.16.4 Nvidia Tegra



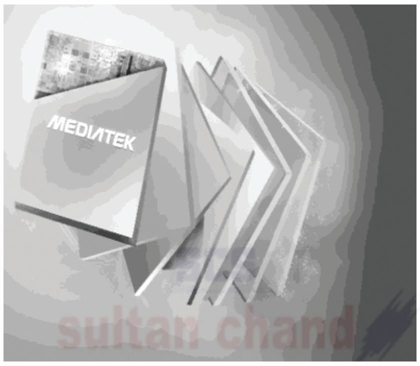
Nvidia Corporation is a US-based technology company which specializes in making processing units for graphics, gaming units and mobile devices. Nvidia develops chips for smartphones, such as transmitting fax, voice data, tablets and mobile devices under the brand Tegra.

Tegra processors are built on 64-bit ARM architecture. Tegra has already marketed Tegra 1, Tegra 3, Tegra 4, Tegra 4i, Tegra K1, Tegra X1.

Tegra X1 is currently the most advanced Tegra chip in the market. The processor is Quad Core with 256 GPU cores and 4K video capabilities. The chips are built on 20 nm technology. The processor is currently used in Nvidia SHIELD Android TV.

The Tegra processors mainly used in smartphones and tablets are Tegra 4, Tegra 4i and Tegra K1.

8.16.5 MediaTek



MediaTek is a Taiwanese semiconductor company providing chips for mobile devices, HDTVs and other electronic devices.

MediaTek processors are built on 64-bit ARM architecture. The latest MediaTek processor supports up to 3 GHz speed. They come in a variety of cores such as dual core (2 core), quad core (4 core), hexa core (6 core) and deca core (10 core).

The latest processors from MediaTek, **Helio X20** and **Helio X25**, are used in smartphones and tablets. MediaTek processors are mostly popular with Chinese manufacturers. Xiaomi, Meizu, LeEco Le, Yu, etc., use them in smartphones. Acer, Asus, Lenovo, Amazon Fire HD, QMobile are some of the other manufacturers that use MediaTek processors in their tablets.

Helio X30 and Helio X27, the latest from the company's stable, use 10 nm and 20 nm processors respectively. Both are deca core with 2 dual core and a single dual core built inside the processor.

8.16.6 HiSilicon

HiSilicon is a Chinese company specializing in semiconductor technology. The company, owned by Huawei, creates chips based on ARM architecture. It is the largest domestic integrated circuit designer in China.

Some of the processors released by HiSilicon are K3V1, K3V2, K3V2E, Kirin 620, Kirin 650, Kirin 910, Kirin 920, Kirin 930, Kirin 950 and Kirin 960. Some of the devices with Kirin 950 are Honor 8, Huawei mate 8 and Huawei MediaPad M3.

Kirin 960 is the latest model to be released in the series. It is built on 64-bit ARM architecture on 16 nm FinFET technology. The processor is quad core capable of attaining a speed of 2.4GHz.

8.16.7 Samsung Exynos

Exynos is a brand of Samsung Electronics which makes processors based on ARM architecture. Some of the processors in the series are Exynos 7 Dual, Exynos 7420, Exynos 7 Octa 7580, Exynos 7 Octa 7870.

Exynos 8 Octa 8890 is the latest processor from Exynos. The processor is equipped with Octa Core on 64-bit ARM architecture with Mali GPU. The processor is capable of running at a speed of 2.3 GHz with support for 3D gaming and 4K UHD resolution. The chips are built on 14 nm technology. **Exynos 8 Octa 8890** is used in Samsung Galaxy S6 and S6 edge.

8.17 ELECTRONIC MAIL (EMAIL)

Email is a method of exchanging digital messages from a sender to one or more recipients. Some common email protocols are:

- **Internet Message Access Protocol (IMAP):** A protocol for receiving email messages on the internet.
- **Post Office Protocol Version 3 (POP3):** A protocol used by email clients to retrieve messages from remote servers.
- **Simple Mail Transfer Protocol (SMTP):** A protocol used for sending email messages on the internet.
- **GOPHER:** Another tool of the internet is Gopher, a menu-based program that enables us to browse for information without knowing where the material is located. It lets us search a list of resources and then sends the material to us.

Some other networking-related terms are:

1. **Domain Name System (DNS):** It translates network address (such as IP addresses) into terms understood by humans (such as domain names) and vice versa.
2. **Domain Host Configuration Protocol (DHCP):** It automatically assigns internet addresses to computers and users.

8.18 VIDEOCONFERENCING

Videoconferencing is a communications technology that integrates video and audio to connect users anywhere in the world as if they were in the same room. This term usually refers to communication between three or more users who are in at least two locations, rather than one-on-one communication and it often includes multiple people at each location. Each user or group of users who is participating in a videoconference typically must have a computer, a camera, a microphone, a video screen and a sound system.

Basically, this is a system that allows us to conduct meetings or trainings in different places simultaneously. So, this technology is especially popular in the field of business because it allows meetings or conferences to be held without the need for all the participants to travel to a single location, so it saves time and money.

The most popular software used for videoconferencing is:

(a) TCP Cam

(b) Ekiga

(c) Skype

8.19 PROTOCOLS FOR CHAT AND VIDEOCONFERENCING

With the arrival of internet, communication formats such as chat and videoconferencing, etc., have gained popularity. In this section, we shall talk about some common chat and videoconferencing protocols. The most common chat protocol is IRC (Internet Relay Chat) while the most common videoconferencing protocols are H.323 and SIP (Session Initiation Protocol).

8.19.1 IRC (Internet Relay Chat)

IRC is an application layer protocol that allows users to share text messages. It uses client server model where the clients install IRC client program on their system so that they can communicate with IRC chat server to transfer messages to other clients. In fact, the IRC client sends request to IRC client server and the server forwards this request to another client to enable them to communicate with each other. It provides one-to-one communication as well as group communication for chatting and file sharing, such as Talk City. IRC networks such as the Undernet provide servers and help us download an IRC client on our PC.

The IRC protocol was developed over four years since it was first implemented as a means for users on a BBS to chat amongst themselves.

CTM: IRC is used for chatting by sending and receiving text messages. The sender sends request to IRC server, which then forwards this request to another client to communicate with each other.

8.20 PROTOCOL FOR VoIP

VoIP stands for Voice over Internet Protocol. For transferring of voice, voice over internet protocol is used. The voice calls are first digitized, compressed and then fragmented into small packets, which are then relayed by Internet Protocol (IP) cross network. Voice-over-IP (VoIP) implementation enables users to carry voice traffic (*For example*, telephone calls and faxes) over an IP network. So, VoIP can be achieved on any data network that uses IP, like the internet, intranets and Local Area Networks (LAN). As the data is transmitted in the form of packets, VoIP uses packet switching technology where each packet follows best route to reach its destination. VoIP allows both voice and data communications to be run over a single network, which can significantly reduce infrastructure costs.

There are 3 main causes for the evolution of the voice-over IP market:

1. Low-cost phone calls
2. Add-on services and unified messaging
3. Merging of data/voice infrastructures

Services provided by VoIP are:

Phone to phone, PC to phone, phone to PC, fax to email, email to fax, fax to fax, voice to email, IP Phone, transparent CCS (TCCS), toll free number (1-800), class services, call centre applications, VPN, Unified Messaging, Wireless Connectivity, IN Applications using SS7, IP PABX and soft switch implementation.

The various protocols used for VoIP are:

1. H.323
2. Session Initiation Protocol (SIP)

CTM: VoIP is a protocol that is used for transmitting voice data and multimedia data over internet protocol. It uses high speed broadband internet connection.

1. H.323 Protocol for VoIP

H.323 is a protocol that provides communication for multimedia services such as audio, video and data communication over packet-based network. It specifies the standards and protocols for all these services. As H.323 provides various communication facilities, it can be applied in a wide variety of areas—consumer, business and entertainment applications. H.323 supports call set-up, teardown and forwarding/transfer. A key feature of H.323 is Quality of Service (QoS). QoS technology allows real-time prioritization and traffic management constraints to be placed on “best-effort” packet delivery systems like TCP/IP over Ethernet. It can be applied in a variety of mechanisms:

- Audio only
- Audio and data
- Audio and video
- Audio, video and data

2. SIP Protocol for VoIP

The expanded form of SIP is Session Initiation Protocol. SIP is a communication protocol (more specifically, a signalling protocol) originally developed in 1996. It uses IP protocol that establishes, modifies and terminates VoIP telephone calls. It provides videoconferencing service to the users, so that a user can communicate with more than one person at a time. Other SIP applications include streaming multimedia distribution, instant messaging and information, file transfer, fax over IP and online games. SIP transparently supports name mapping and redirection services which support personal mobility.

8.21 NETWORK SECURITY CONCEPTS

Network is used for sharing, messaging and collaboration of data. However, more and more network is used for this purpose, the lesser is the security of data, either in terms of viruses or hacking and other cyberattacks. To prevent the network from these malicious and/or unethical practices, various strategies and choices are available that work as building blocks of network security. These include password authentication, digital signature, challenge handshake authentication protocol, etc.

8.22 Types of Threats and Prevention

1. Viruses

Viruses are small programs that are written intentionally to damage the data and files on a system. These programs are spread from one computer system to another which interrupts the normal functioning of a computer. Viruses can attack any part of a computer's software such as boot block, operating system, system areas, files and application program macros. Viruses are most easily spread with email attachments.

Viruses are broadly classified into three types:

(a) **File Infector Viruses:** Viruses that attach themselves to a program file.

(b) **Boot Sector Viruses:** Viruses that install themselves in boot sectors of hard drive.

(c) **Macro Viruses:** They infect data files and corrupt the data.

Characteristics of Viruses:

(a) Speed of a computer system becomes slower than normal.

(b) Computer system frequently hangs up.

(c) Computer restarts automatically after every few minutes.

(d) Various applications of computer do not function properly.

(e) Dialog boxes, menus and other error message windows are distorted.

Damage caused by Viruses:

(a) They corrupt file allocation table which results in corrupting the entire file system.

(b) Replication of files occurs that decreases space in hard disk.

(c) They can destroy system programs and files.

(d) They can cause destruction of specific executable files and alteration in data files resulting in reinstallation of a system.

(e) They can format specific tracks on the disks or format the entire disks.

Prevention from Viruses:

(a) Use antivirus software to permanently remove viruses.

(b) Always scan pen drives and other secondary storage media in order to detect viruses and safeguard your system.

(c) Frequent update your computer system.

CTM: A virus is a malicious program that damages data and files of a system and can also corrupt the file allocation table.

2. Worms

A worm is a self-replicating program that runs independently and travels across network connections. The characteristics of viruses and worms are more or less same, but a worm causes more damage.

CTM: A worm is a computer program which can self-replicate and propagate over the network, with or without human intervention, and has malicious content.

Characteristics of Worm:

(a) It replicates itself.

(b) Unlike virus, worm does not require host and it is self-contained.

(c) It spreads across networks through email, instant messaging or junk mails.

(d) Worms run independently.

The various types of Worms are:

(a) **Email Worms:** Worms spread through any email which contains any file attachment or link to any infected website.

(b) **Instant Messaging Worms:** Worms spread through instant messaging across the network by sending mails to infected website.

(c) **Internet Worms:** The infected worm will use the contact list of the user's chat-room profile or instant-message program to send links to infected websites. These are not as effective as email worms as the recipient needs to accept the message and click the link. The users of the particular program are affected by it.

(d) **File Sharing Network Worms:** These types of worms are downloaded along with the required files downloaded by the user. A user is not aware about this worm and, therefore, when the user downloads any file, the worm will copy itself into a shared folder with an unassuming name. When another user on the network downloads files from the shared folder, the worm gets downloaded on their system also. In this way, the worm copies itself and repeats the process. In 2004, a worm called "Phatbot" infected millions of computers in this way and had the ability to steal personal information, including credit card details, and send spam on a large scale.

Damage caused by Worms:

(a) A worm may corrupt the files on the host computer.

(b) It may affect communication between the host and other systems.

(c) It may disable the antivirus software on the host, which will enable it to cause more damage.

(d) Bulk email chaining can be created with an intention to guess email passwords.

(e) A worm consumes too much system memory (or network bandwidth), causing web servers, network servers and individual computers to stop responding.

3. Trojan Horse

A Trojan horse is a kind of virus that looks safe but has hidden effects. It is a hidden code in a program such as a game or a spreadsheet that can damage the system when running these applications. It can destroy or alter information on a computer system in the background. Unlike viruses, Trojans do not replicate themselves but they are destructive. Trojans are executable programs, which means that when a user runs any application or plays games, they work behind that application and can damage the system completely.

There are several types of Trojan Horse:

(a) Remote access Trojan horse

(b) Data sending Trojans

(c) Destructive Trojans

(d) Proxy Trojans

(e) FTP Trojans

(f) Denial-of-service attack Trojans

Trojans are generally spread through email attachments and exchange of disks and information between computers. Worms can also spread Trojans. The damage caused by Trojans is similar to that caused by viruses. Sometimes the user is unaware about a Trojan because of its masking effect as it runs as a hidden code.

CTM: Trojan horse is a hidden code that looks safe but it has some hidden effects while running applications.

4. Spams

Spam is an unwanted bulk mail which is sent by an unauthorized or unidentified person in order to eat the entire disk space. In non-malicious form, it floods the internet with many copies of the same message to be sent to a user which he may not otherwise receive. Generally, it is in the form of pampering the user with various discount schemes, or commercial advertising, often for dubious products, get rich quick schemes, etc. Mobile phone spam is a form of spamming that uses text message service of mobile phone.

Spams can be avoided by using email filtering, spam traps, etc.

CTM: Spam refers to electronic junk mail that eats up the entire computer's space.

8.23 COOKIES

A cookie is also known as an HTTP cookie, web cookie, internet cookie or browser cookie. When the user browses any website, a cookie identifies users and prepares web pages for them which are then sent to the web server for later use. Cookie is basically a piece of data that is stored by the website on the user's hard disk. The information is stored in the form of name value pair. Generally, the cookies folder is stored in c:\windows\cookies.

Working of Cookies

1. The user enters the name of the website on the browser.
2. The browser contacts the DNS server to convert the domain name into IP address. The browser looks for the cookies on the hard disk.
3. The IP address is used to contact the corresponding server along with cookies data.
4. If no cookies data is supplied, then the website comes to know that the user is visiting the website for the first time.
5. The server creates an ID of a person which is then stored by cookies on the hard disk.

The information which is stored by a website is known as state information. The information can be of the following types:

1. How many visitors have visited the site?
2. How many are new visitors?
3. How many are repeat visitors?
4. What is the frequency of a particular visitor?

> **CTM:** Cookies are the messages which are stored by the website on a user's hard disk whenever they visit any website.

8.24 FIREWALL

A firewall is a software that protects the private network from unauthorized user access. The firewall filters the information coming from the internet to the network or a computer to protect the system. Firewall exists both as a software solution and as a hardware application. In the form of hardware firewall such as router, it protects the network, and in terms of software firewall, it helps in preventing the spread of virus from one computer to another. A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. Various examples of firewalls are CISCO firewall, NetGear firewall, Netscreen 25, etc.

A firewall can use various methods for filtering the information such as:

1. **Packet filtering:** In packet filtering, the data, which is outgoing or incoming in the form of packets, is filtered. Packet filter looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
2. **Proxy service:** The information which is requested is not directly sent to the person who makes the request; rather, the information is first received in firewall and then sent to the proxy server. The proxy server intercepts all messages entering and leaving the network and effectively hides the true network addresses.
3. **IP address blocking:** If the data is coming from a network or website that contains some unwanted data, then the data from that particular IP address or domain name is blocked by firewall.

4. **Protocol blocking:** The firewall can be set to disallow a particular protocol service to a particular user or group of users.
5. **Application Gateway:** It applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective but can impose performance degradation.
6. **Circuit-level Gateway:** It applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
7. **Port blocking:** The firewall can be used to block a particular block. Generally, HTTP and FTP services use port80 and port21.

Firewall protects the user from the following:

1. Remote login by others who are not authorized to gain access to the system
2. Application backdoors
3. SMTP session hijacking
4. Email bombs
5. Viruses and macros
6. Spam or junk mails

CTM: Firewall is a system that is designed to protect the network from illegal use by an unauthorized person.

8.25 INDIA'S IT ACT

The **Information Technology Act 2000** (also known as **ITA-2000** or the **IT Act**) is an Act of the Indian Parliament (No. 21 of 2000) notified on October 17, 2000.

IT Act 2000 has been defined as:

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

8.26 CYBER LAW

The law that governs the cyber space is known as cyber law. It is the law which deals with various computer-related activities. In essence, cyber law is an attempt to apply laws designed for the physical world to human activity on the internet. In India, the IT Act, 2000, as amended by the IT (Amendment) Act, 2008, is known as the cyber law. It has a separate Chapter XI entitled "Offences" in which various cyber crimes have been declared as penal offences punishable with imprisonment and fine. A large number of cyber-criminal activities such as hacking passwords or accessing files by an unauthorized person or getting private information, etc., have been prevented by implementing cyber laws.

As the usage of internet has been growing at an exponential rate, it has become very important to protect individual users and organizations from unauthorized intruders into the system.

8.27 CYBER CRIMES

When any crime is committed over the internet, it is referred to as cyber crime. There are many types of cyber crimes and the most common ones are explained below:

1. **Hacking:** Gaining knowledge about someone's private and sensitive information by getting access to their computer system illegally is known as hacking. This is different from ethical hacking, which many organizations use to check their internet security protection. In hacking, a criminal uses a variety of software so as to enter a person's computer and that person may not be aware of his computer being accessed from a remote location.
2. **Theft:** Theft occurs when a person downloads music, movies, games and software by violating copyright. There are even peer-sharing websites which encourage software piracy and many of these websites are now being targeted by the Federal Bureau of Investigation (FBI).
3. **Cyber Stalking:** Cyber stalking is a kind of online harassment where the victim gets unwanted abusive online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the internet to stalk. If they notice that cyber stalking is not having the desired effect, they begin offline stalking along with cyber stalking to make their victim's life miserable.
4. **Identity Theft:** This has become a major problem with people using the internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit card, social security card, debit card and other sensitive information to gain money or to buy things online in the victim's name that can result in major financial loss for the victim and even spoil the victim's credit history.
5. **Malicious Software:** These are internet-based software or programs known as pirated software that are used to disrupt proper functioning of the network. The software is used to steal sensitive information or data that can cause damage to existing software in a computer system.
6. **Child Pornography:** In this cyber crime, defaulters create, distribute or access materials that sexually exploit underage children. The criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hope of reducing and preventing child abuse and soliciting.
7. **Sales and Investment Fraud:** With the increase in e-commerce, the application of digital technology to fraudulent endeavours has become that much greater. The use of telephone for fraudulent sales pitches, deceptive charitable solicitations or bogus investment overtures is becoming increasingly common. There are some fraudulent sites that sell poor quality products at cheaper rates. They also promise the customers heavy discounts and freebies.
8. **Electronic Funds Transfer Fraud:** A cyber crime occurs when there is a transfer of funds which may be intercepted and diverted. Valid credit card numbers can be hacked electronically and then misused by a fraudulent person or organization.

9. **Defamation:** It involves a cyber crime with the intent of lowering the dignity of someone by hacking into their email account and sending mails using vulgar language to an unknown person's account.

CTM: Cyber law defines all the legal and regulatory aspects of internet and the World Wide Web.

10. **Assault by Threat:** It refers to threatening a person or his family members with dire consequences through the use of a computer network, *i.e.*, email, videos or phones.

11. **Denial of Service (DoS) Attacks:** A DoS attack is an attack by which legitimate users of a computer are denied access or use of the resources of that computer. Generally, DoS attacks do not allow the attacker to modify or access information on the computer. A DoS attack can be of the following types:

    - **Denial of Access to Information:** Refers to an attack in which information sought by a legitimate user is either destroyed or changed to some unsubtle form.
    - **Denial of Access to Applications:** Refers to an attack that denies a user from accessing an application by making it either unusable or unavailable. This is usually done to prevent the user (or organization) from using applications to perform any task.
    - **Denial of Access to Systems:** Refers to the unavailability of the system, including all the applications installed on the system or any data stored on the system.
    - **Denial of Access to Communications:** Refers to a common type of attack that can range from cutting wires and jamming radio communications to flooding networks with excessive traffic. An example of this type of attack is flooding a computer with junk mail.

8.28 IPR ISSUES

IPR stands for intellectual property rights which is the right to intangible property such as music, literature and artistic work created by a person. **Intellectual property (IP)** is a legal term that refers to creations of the mind. Intellectual property rights may be protected by patents, copyrights, industrial design rights, trademarks, trade dress and, in some jurisdictions, trade secrets. The owner of intellectual property is the person who has developed the product or the organization which has funded it. Safeguarding intellectual property from illegal use can be done by giving some exclusive rights to the owner of that property. These rights also promote creativity and dissemination and application of its result and encourage fair trading which helps in developing social and economic areas of a country.

IPR-related issues in India like patents, trademarks, copyrights, designs and geographical indications are governed by the Patents Act, 1970 and Patent Rules, 2003, Trademarks Act, 1999 and the Trademarks Rules, 2002, Indian Copyrights Act, 1957, Design Act, 2000 and Design Rules, 2001, and the Geographical Indications of Goods (Registration & Protection) Act, 1999 and the Geographical Indications of Goods (Registration & Protection) Rules, 2002, respectively.

Prevention from Security Threats

There are various methods to protect network threats. These protection methods are as follows:

1. **Authorization:** Authorization means Intrusion Detection. Authorization means to grant a person access to a network for legal use. It is an act of giving authority or legal identity to a user to become an authorized user of the system. Authorization checks can also be

implemented to a program or process to make data free of risk, such as entering of viruses, worms or Trojan horse.

2. **Authentication:** To determine the identity of a person before granting access to private or sensitive data or information is known as authentication. Verifying the identity of an intruder or a person is difficult and needs complex protocols based on cryptography.

3. **Privacy:** The data which is accessible only to an authorized person is known as private data.

4. **Secrecy:** Hiding some relevant information from an unauthorized person is called secrecy.

5. **Biometric System:** Biometric system forms the most secure level of authorization. It involves digital signature, finger prints, retinal patterns, etc., to establish identity.

6. **Password Protection:** To protect the system or network from an unauthorized person, a system must be password protected. A password protected system allows access to resources based upon a secret word entered by the user.

7. **File Permission:** A user can give access to a person to read a file, write to a file, open a file, modify a file, etc. Different types of permissions can be given to a specific person according to their authorization. Each file has an access control list attribute that describes which user or group accounts have what type of access to the file.

   Three types of file access permissions that are granted to a user:

   (a) *Read:* Allows a user to view and read a file.

   (b) *Write:* Allows a user to edit and write on a file.

   (c) *Execute:* Allows a user to execute a file.

   File access permission is granted to three types of users:

   (a) *Owner:* Refers to the user who has created the file.

   (b) *Group:* Refers to the group of users which is working with the file owner.

   (c) *Others:* Refers to all other users.

8. **Firewall:** A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communication. It is a programmer software or device or set of devices configured to permit, deny, encrypt, decrypt, or proxy wall (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

9. **Proper Security Policy:** An organization's security policy is a formal statement consisting of the rules that its employees need to follow to access information about the organization. The policy should clearly communicate the security goals to all the users, administrators and managers of the organization. A good security policy must be:

   ➢ enforced with adequate security tools.

   ➢ able to define the areas of responsibility for a user, an administrator or a manager.

   ➢ able to adjust itself according to the changing configurations of computer networks.

8.29 HACKING

Hacking is the practice of modifying the features of a system in order to accomplish a goal outside the creator's original purpose. A person who consistently engages in hacking activities and has accepted hacking as a lifestyle and philosophy of their choice is called a hacker.

Computer hacking is the most popular form of hacking nowadays, especially in the field of computer security. However hacking exists in many other forms also, such as phone hacking, brain hacking, etc., and it is not limited to either of them.

Due to the mass attention given to black hat hackers by the media, the whole hacking term is often mistaken for any security-related cyber crime.

8.30 INTRODUCTION TO WEB SERVICES

Internet offers several important and extensively used features or services which are described as follows:

8.30.1 WWW (World Wide Web)

WWW is an information service that can be used for sending and receiving information over the internet through interlinked hypertext documents. Web pages may contain text, images, videos and other multimedia components as well as web navigation features consisting of hyperlinks. The documents are formatted in a markup language called HTML (Hyper Text Markup Language) that provides links to other documents as well as graphics, audio and video files. The World Wide Web is based upon client-server architecture where a client sends a request and the server processes that request and sends responses. A WWW client is called a web browser and a WWW server is called a web server.

CTM: WWW is a set of programs and protocols that allows the user to create and display multimedia web pages and is linked to the internet.

8.30.2 Hyper Text Markup Language (HTML)

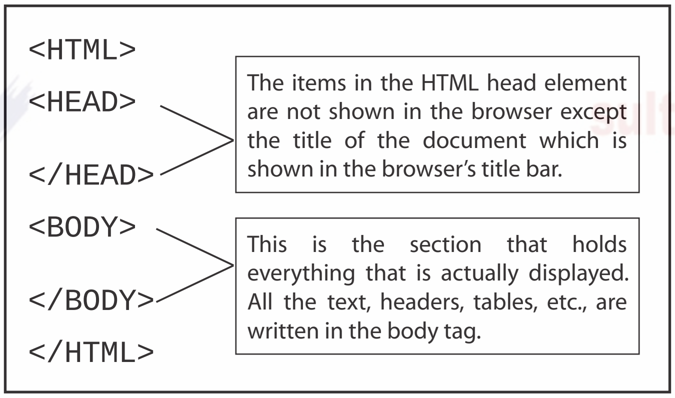
HTML is a language that is used to create web pages which are then displayed by web browsers. This language tells the browser how to display text, pictures and links on the screen. HTML is a language that supports multimedia documents and consists of audio, video, graphics, pictures, etc. It also helps in creating hyperlinks so that various documents can be linked together. When a person clicks on a specified link, the document related to that link displays. HTML is a document layout and hyperlink specification language, *i.e.*, a language that uses various coded elements known as tags for formatting the document and to specify the hyperlinks.

HTML document can be written using any text editor such as NOTEPAD or NOTEPAD2 and save a file with extension either **.HTM** or **.HTML**

Any HTML document, in general, contains at least three elements—HTML, HEAD, and BODY.

These elements are specified by the following respective tags:

1. `<HTML> . . .</HTML>`
2. `<HEAD> . . .</HEAD>`
3. `<BODY> . . .</BODY>`



```
<HTML>
<HEAD>

</HEAD>
<BODY>

</BODY>
</HTML>
```

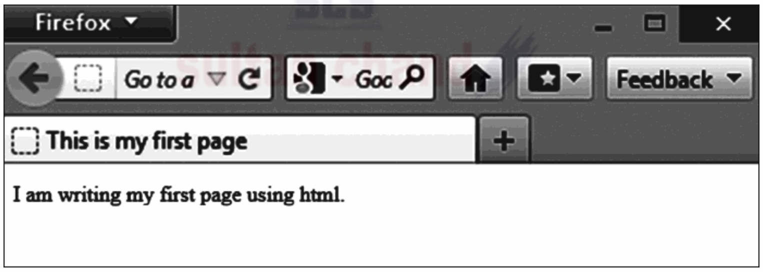
The items in the HTML head element are not shown in the browser except the title of the document which is shown in the browser's title bar.

This is the section that holds everything that is actually displayed. All the text, headers, tables, etc., are written in the body tag.

The structure of HTML document is as follows:

```
    <HTML>
        <HEAD>
            <TITLE> This is my first page</TITLE>
            </HEAD>
        <BODY> I am writing my first page using html.
        </BODY>
        </HTML>
```

Now, execute this file using any web browser and it will display a page as below:



This is my first page

I am writing my first page using html.

CTM: HTML is a Markup language that enables users to create web pages and format them using predefined tags. Tags are called coded elements.

8.30.3 Extensible Markup Language (XML)

Extensible Markup Language is a text-based Markup Language that allows the user to create their own tags to store data in a structured format. However, these structured formats can be represented in different ways. In XML, the tags are not predefined; rather, they are created by the user for their own purpose. Unlike HTML, in XML, tags are case-sensitive and each tag must have a corresponding closing tag. It is a general-purpose specification that allows users to create custom Markup language. XML was designed to carry data and not to display data. For formatting data, a separate style sheet known as cascading style sheet is used.

XML is recommended by the World Wide Web Consortium (W3C). It is a free open standard. The W3C recommendation specifies both the lexical grammar and the requirements for parsing.

Structure of XML document:

```
<?xml version="1.0">
<Client>
<Clientid>C100</Clientid>
<Clientname>Johnson</Clientname>
<Company>APPLE</Company>
</Client>
<Client>
<Clientid>C101</Clientid>
<Clientname>McGraw</Clientname>
<Company>HCL</Company>
</Client>
</xml>
```

CTM: XML is a Markup Language for creating documents in a structured format. Users can create their own tags along with predefined tags already defined by HTML.

8.30.4 Hyper Text Transfer Protocol (HTTP)

HTTP is used to transfer all files and other data (collectively called resources) from one computer to another on the World Wide Web. This protocol is used to transfer hypertext documents over the internet. HTTP defines how the data is formatted and transmitted over the network. When an HTTP client (a browser) sends a request to an HTTP server (web server), the server sends responses back to the client. This transfer of requests and responses is done following HTTP protocol.

The main features of an HTTP document are:

1. It is a stateless protocol; this means that several commands are executed simultaneously without knowing the command which is already executing before another command.
2. It is an object-oriented protocol that uses client server model.
3. The browser (client) sends request to the server, the server processes it and sends responses to the client.
4. It is used for displaying web pages on the screen.

8.30.5 Domain Names

To communicate over the internet, we can use IP addresses. But it is not possible to remember the IP address of a particular website or computer every time. Domain names make it easier to resolve IP addresses into names, *for example*, cbse.nic.in, google.com, meritnation.com, etc. It is the system which assigns names to some computers (web servers) and maintains a database of these names and corresponding IP addresses. Domain names are used in URLs to identify particular web servers, *for example*, in the URL https://www.cbse.nic.in/welcome.htm, the domain name is cbse.nic.in.

A domain name consists of the following parts.

1. Top-level domain name or primary domain name, and
2. Sub-domain name(s).

For example,

In the domain name cbse.nic.in:
in is the primary domain name
nic is the sub-domain of in
cbse is the sub-domain of nic.
The top-level domains are categorized into following domain names:

Generic Domain Names

·com - commercial business
·edu - Educational institutions
·gov - Government agencies
·mil - Military
·net - Network organizations
·org - Organizations (non-profit)

Country Specific Domain Names

.in - India
·au - Australia
·ca- Canada
.ch- China
.nz- New Zealand
.pk- Pakistan
.jp- Japan
.us - United States of America

8.30.6 URL

URL stands for uniform resource locator that helps in locating a particular website or a web page, *for example*, http://www.cbse.nic.in/academics.html is a URL for a specific website. In this URL, 'http' stands for hypertext transfer protocol, and 'www.cbse.nic.in' indicates the IP address or the domain name where the source is located. 'academics.html' specifies the name of the specified html document on the website of CBSE.

CTM: URL stands for uniform resource locator that stores the address of a web page.

8.30.7 IP Address

The computers connected to a network also need to follow some rules to communicate with each other. These sets of rules are known as protocols. Several types of protocols are used for communication over networks. However, the most common one is the Transmission Control Protocol/Internet Protocol or TCP/IP. A network using TCP/IP is known as a TCP/IP network. The internet is an example of the TCP/IP network. Therefore, it becomes important that each device should have a unique address to identify it on a TCP/IP network. This unique address is known as IP address. IP address is short for Internet Protocol (IP) address. An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can be 0 to 255. Some examples of IP addresses are: 192.168.1.2, 10.324.1.3 and 109.134.2.2.

As seen in the above examples, the numbers in an IP address are in the decimal form. When an IP address is processed, the computer converts these numbers into binary form internally. The following is an example of IP address in the decimal form: 192.168.1.10

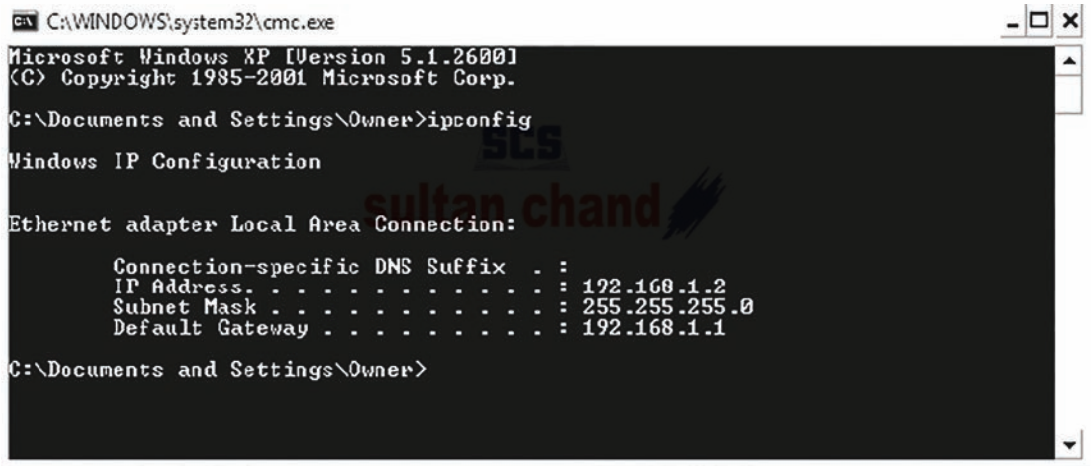
The preceding IP address in its binary form is: 11000000.10101000.00000001.00001010

The IP address of a computer is assigned by the Internet Service Provider (ISP) whose internet connection is used on that computer.

You can find out the IP address of your computer by performing the following steps:

1. Click the **Start** button. A pop-up menu containing various options appears.
2. Open the **Run** dialog box.

   Type cmd in the **Run** dialog box and press Enter. The command prompt (cmd) window opens.
3. Type **ipconfig** and press Enter. The output appears, displaying the IP address of your computer (as shown in the output window given below).



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Owner>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.2
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\Documents and Settings\Owner>
```

8.30.8 Website

A website is a collection of various web pages, images, videos, audios or other kinds of digital assets that are hosted on one or several web servers. The first page of a website is known as home page where all the links related to other documents are displayed. The web pages of a website are written using HTML and the information is transferred over the internet through HTTP protocol. The HTML documents consist of several hyperlinks that are accessed through HTTP protocol. Examples of various websites are: cbse.nic.in, google.com, amazon.in, etc.

CTM: A website is a collection of several web pages which are related to each other through hyperlinks.

8.30.9 Web Page

A web page is an electronic document/page designed using HTML. It displays information in textual or graphical form. Traversal from one web page to another web page is possible through hyperlinks.

A web page can be classified into two types:

- **Static web page:** A web page which displays same kind of information whenever a user visits it is known as a static web page. A static web page generally has .htm or .html as extension.
- **Dynamic web page:** An interactive web page is a dynamic web page. A dynamic web page uses scripting languages to display changing content on the web page. Such a page generally has .php, .asp, or .jsp as extension.

8.30.10 Web Browser

It is a software that helps in accessing web pages and, thus, is also called web client. It helps the user to navigate through the World Wide Web and display web pages. Some popular web browsers are: Mozilla Firefox, Opera, AOL, Webkit, Iceweasel, etc.

CTM: A web browser is a WWW client that navigates through the WWW and displays web pages.

8.30.11 Web Server

A web server is a server that stores web pages and when a web client is sending any request to a server, a server responds to the request and displays the requested web pages. A web server is a program that runs on a computer connected to the internet. Web server waits for a request, finds the documents and generates information, if required, and sends back to the browser that requested for it. A single web server may support multiple websites, or a single website may be hosted on several linked or mirrored web servers.

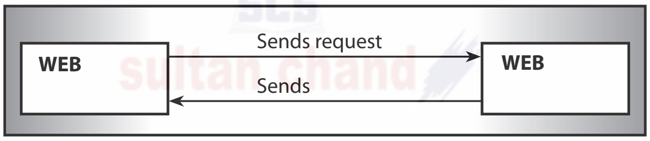


Fig. 8.34: Sending and Receiving Request

Some popular web servers are: Apache web server, Netscape enterprise web server, Microsoft internet information server, etc.

CTM: A web server stores web documents and responds to the requests made by web browsers.

8.30.12 Web Hosting

Web hosting is a service which is provided by companies to its clients to allow them to construct their own websites which are accessible to the internet users via World Wide Web. Such companies are known as web host. These companies provide space on a web server they own for use by their clients as well as provide internet connectivity. The websites which are constructed display information for their organization in the form of web pages. The host may also provide an interface or control panel for managing the web server so as to add news and events related to their organization or for uploading some information which may be valuable for the internet users. A client can also use control panel for installing scripts as well as other modules and service applications like email. webhostingsitesindia.co.in is one of the top domain name registration and web hosting companies in India. It is the only hosting company which provides support in regional languages.

CTM: Web hosting is a service that is provided by the company to users to create web-based applications.

8.30.13 Domain Name Resolution (DNR)

You already know that communication between computers on a network takes place with the help of IP addresses. However, to access a particular website, you use its URL because it is much easier to remember than the IP address. When you use the URL to access a website, your computer needs to find its matching IP address. How does it find this address? The answer is: by using the Domain Name Resolution (DNR). DNR is the name given to the process by which your computer finds the IP addresses of domain names.

The DNR process takes place in the background, and can be explained in the following steps:

1. Enter the domain name of the website that you want to access in the Web browser.
2. The Web browser issues a command to the operating system of your computer to generate the IP address of the given domain name.

The domain name is resolved according to the configuration of the operating system you are using. Different operating systems, such as Windows, XP, Windows 7, Linux, and Unix have different configurations.

This is done in the following manner:

- Generally, the operating system maintains a HOSTS file, which contains a list of the IP addresses of some domain names. Therefore, the operating system first checks this file to find the IP address of the given domain name.
- If the IP address is not found in the HOSTS file, the operating system connects to the DNS server on a network. The DNS server maintains a directory containing a list of all the domain names and IP addresses that are registered on the internet. The DNS server finds the IP address of the given domain name and returns it to the operating system.

3. After obtaining the IP address, the operating system sends it to the Web browser that has requested it.

CTM: A web browser is a WWW client that navigates through the WWW and displays web pages.

8.30.14 Web Scripting

Website Scripting is used for creating web pages to publish them on the web interactively. The communication between web browser and web server happens through small programs called web scripts. Script is a programming language which, when executed, displays the web page. The written codes for a script may be used by the server side or may be used by the client side as per the requirement. The tasks which are executed by a web server are interpreted and automated through the web scripts written in Web Scripting Language.

CTM: A script is a list of commands embedded in a web page which are executed by a certain program or scripting engine.

(a) Client-Side Web Scripting Languages

Client-side scripting enables the user to interact with web pages. The client-side scripts are downloaded at the client end and then interpreted and executed by the web browser. The client-side scripting is browser dependent and, therefore, the browser must be scripting-enabled that can interpret the script code. Examples of client-side scripting where it is used are online games, downloading data from the server, etc.

Some Popular Client-Side Scripting Languages are:

1. JavaScript
2. VBScript
3. PHP

1. **JavaScript**

   JavaScript was the first web scripting language to be introduced and it is still by far the most popular. The original name of JavaScript was "LiveScript" and it was first introduced in Netscape Navigator 2.0 in 1995 and was renamed JavaScript so as to correlate with Java Language. JavaScript is primarily used for client-side processing. It is a scripting language and not a programming language. It can easily be embedded in HTML tag and executes immediately as the page is displayed. JavaScript, along with languages like XML, can call in only the required data from the server without receiving a full web page.

   Example of Java Script is as follows:

```
<HTML>
<HEAD>
<TITLE>My first java script</TITLE>
</HEAD>
<BODY>
<SCRIPT LANGUAGE="JAVASCRIPT">
document.write("Welcome")
</SCRIPT>
</BODY>
</HTML>
```

   JavaScript allows the user to perform several functions such as:

   (i) Add scrolling or changing messages to the browser's status line.

   (ii) Update the contents of a form by using validation checks and make calculations. (*For example*, on entering the marks of 5 subjects of a student, it will calculate total marks and percentage.)

   (iii) Display messages to the user, either in a new web page, which is a sub-part of the main web page, or in alert boxes.

   (iv) Create and animate images that change when the user hovers the mouse over them.

   (v) Detect the browser in use and display different contents for different browsers.

   (vi) Detect installed plug-ins and notify the user if a plug-in is required.

2. **VBScript (Visual Basic Script)**

   VBScript is a light weight programming language developed by Microsoft Corporation. VBScript is the default scripting language for ASP (Active Server Pages). VBScript is a server-side scripting language. However, it may also be used for client-side scripting (although it is currently only supported by Internet Explorer).

Some of the useful features of visual basic are not supported by VBScript such as strong typing, extended error trapping and the ability to pass a varied number of parameters to a sub-routine. However, its use is relatively widespread because it is easy to learn. VBScript can be effectively used for automating day-to-day office tasks as well as monitoring in Windows- based environment. When used for client-side web development in Microsoft Internet Explorer, VBScript is similar in function to JavaScript. It is used to write executable functions that are embedded in or included from HTML pages and interact with the Document Object Model (DOM) of the page, to perform tasks not possible in HTML alone. VBScript is simple to create and can be written using text editor like Notepad. A simple VBScript document is saved with ".vbs" extension.

Example of VBScript is as follows:

```
<HTML>
<HEAD>
<TITLE>My first VBScript</TITLE>
</HEAD>
<BODY>
<SCRIPT TYPE="text/vbscript">
document.write("Welcome")
</SCRIPT>
</BODY>
</HTML>
```

3. **PHP (Hypertext Pre-Processor)**

PHP stands for Hypertext Pre-processor. It is a server-side scripting language that is used to enhance web pages. With PHP, a user can do things like create username and password login pages, check details from a form, create forums, picture galleries, etc. It was created in 1994 by Rasmus Lerdorf to add dynamic content to an HTML page. PHP initially stood for 'Personal Home Page', but now it is translated as 'PHP Hypertext Pre-processor'. The PHP code is embedded within the HTML code between special tags. When the page is accessed, the server processes the PHP code and then sends the output from the script as HTML code to the client.

The salient features of PHP are as follows:

(i) A user can create dynamic web pages with the PHP scripting language.

(ii) It is a server-side scripting language and, therefore, the PHP scripts are executed on the server.

(iii) PHP is free and an open source software product.

(iv) PHP provides connectivity with many databases (MySQL, Sybase, Oracle and many others).

(v) PHP runs on different platforms (UNIX, Linux, Windows).

(vi) PHP is compatible with almost all web-servers used today (Apache, IIS, etc.).

(vii) PHP commands are embedded within a standard HTML page.

(viii) Its syntax is similar to that of C and Perl languages which makes it easy to use.

(ix) PHP files can have one of the following extensions: PHP, PHP3 or PHTML.

The structure of PHP Script is as follows:

```
<HTML>
<HEAD>
<TITLE>PHP Test</TITLE>
</HEAD>
<BODY>
<?php echo'<p>Hello World</p>'?>
</BODY>
</HTML>
```

(b) Server-Side Script

Server-side scripting gets executed on the server before displaying the information requested.

1. **ASP (Active Server Pages)**

It is a technology that is used to create dynamic web pages so that the user can see these pages without any specific web browser. The user does not require any specific web browser to view these pages. To create active server pages, a default scripting language is used, viz. VBScript and sometimes JSCRIPT. ASP pages are saved with the extension .ASP and not by .html. Any web page that contains ASP code cannot be run simply by executing it through web browser; instead, the page must be requested through a web server that supports ASP. When a browser requests an ASP, the web server generates a page with HTML code and sends it back to the browser. ASP is also the short term used for Application Service Provider.

Various services offered by ASP are:

(i) It helps in creating interactive and dynamic web pages.

(ii) It allows access to any data or databases and returns the result to web browser.

(iii) It allows the user to dynamically edit, change or add any content of a web page.

(iv) It provides security to a page as it is not executed by a web browser.

2. **JSP (Java Server Pages)**

Java Server Pages (JSP) is a technology that helps software developers to create dynamic web pages based on HTML, XML or other document types. It was released in 1999 by Sun Microsystems. JSP is similar to PHP, but it uses the Java programming language. JSPs have dynamic scripting capability that is embedded in an HTML code. Java server pages can be run by a compatible web server with a servlet container, such as Apache Tomcat or Jetty. To process a JSP file, developers need a JSP engine, which is connected to a Web server. The JSP page is then compiled into a servlet, which is handled by the servlet engine. This phase is known as translation. The servlet engine then loads the servlet class and executes it to create dynamic HTML, which is then sent to the browser. A Java Server Pages compiler is a program that parses JSPs and converts them into executable Java Servlets.

The various features of JSP are as follows:

(i) **Platform Independent:** JSP can be deployed across many platforms. All these components can be run across web servers.

(ii) **Configured for reusability:** JSP components can be reused across servlets, JavaBeans and Enterprise JavaBeans (EJB).

(iii) **Simple and easy to use:** JSP is simple in the process of development and maintenance.

CTM: Scripting languages are also often used by applications as control or configure languages. An example: Firefox is written in C/C++ and can be controlled with JavaScript.

Table: 14.1: Difference between Client-Side Scripting and Server-Side Scripting

S.No.	Client-Side Scripting	Server-Side Scripting
1.	Scripting runs through web browser.	Scripting runs through web server.
2.	The processing takes place on the end-user's computer.	The processing takes place on the server side.
3.	The browser receives the page sent by the server and executes the client-side scripts.	Server executes server-side scripts to send out a page but it does not execute client-side scripts.
4.	Client-side scripting cannot be used to connect to the databases on the web server.	Server-side scripting is used to connect to the databases that reside on the web server.
5.	Client-side scripting can be blocked by the user.	Server-side scripting cannot be blocked by the user.
6.	Response from a client-side script is faster as compared to a server-side script because the scripts are processed on the local computer.	Response from a server-side script is slower as compared to a client-side script because the scripts are processed on the remote computer.
7.	Examples of client-side scripting languages are Javascript, VBScript, etc.	Examples of server-side scripting languages are PHP, JSP, ASP, ASP.Net, Ruby, Perl, etc.

8.31 WEB 2.0

Web 2.0 is often known as World Wide Web for second generation where people collaborate with each other through social networking sites, blogs, wikis, folksonomies, video-sharing sites, hosted services, web applications and mashups. Web 2.0 offers more dynamic pages instead of static pages that allows users to create online applications. Web 2.0 also allows groups of people to work on multiple applications. *For example*, a user can work on a document or spreadsheet simultaneously, while in the background a computer keeps track of who made what changes, where and when.

Web 2.0 tools are also less expensive than traditional software—many are even free. Because they are web-based, the need is only to update the browser.

The various features of Web 2.0 are:

- Web-based applications can be accessed from anywhere.
- It provides multitasking.
- It is less expensive and provides dynamic pages.
- Specific problems can be solved by using simple applications.
- Value lies in content, not in the software used to display content.
- Transfer of data is readily shared.
- Employees and customers can create their own newsgroup.
- Social tools encourage people to create, collaborate, edit, categorize, exchange and promote information.

Web 2.0 website uses a new programming language called AJAX (Asynchronous JavaScript and XML).

Applications supported by Web 2.0 are as follows:

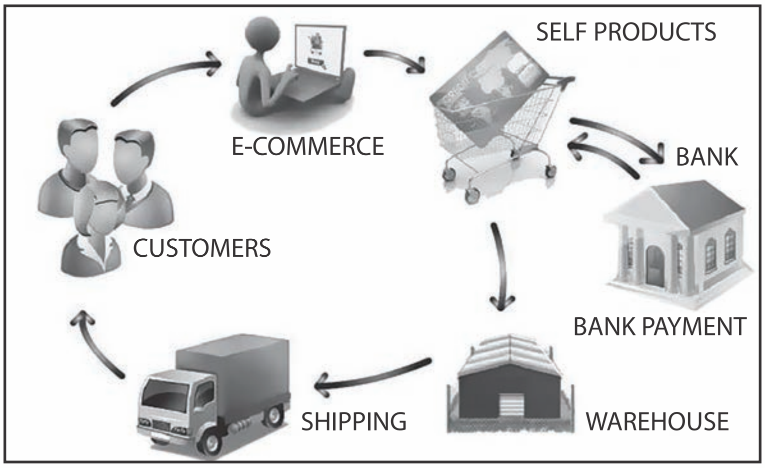
- Blogging
- Social bookmarking
- RSS
- Wikis and other collaborative applications
- Interactive encyclopaedias and dictionaries
- Advanced Gaming

CTM: Web 2.0 refers to added features and applications that make the web more interactive and easy to provide information using newsgroups, social networking sites, RSS, etc.

8.32 E-COMMERCE

E-commerce (electronic commerce or EC) is the buying and selling of goods and services, or the transmitting of funds or data over an electronic network, primarily the internet. These business transactions occur either as business-to-business, business-to-consumer, consumer-to-consumer or consumer-to-business. The terms e-commerce and e-business are often used interchangeably.

E-commerce is conducted using a variety of applications, such as email, online catalogues and shopping carts, EDI, File Transfer Protocol and web services. This includes business-to-business activities and outreach such as using email for unsolicited ads (usually viewed as spam) to consumers and other business prospects, as well as to send out e-newsletters to subscribers. More companies now try to entice consumers directly online, using tools such as digital coupons, social media marketing and targeted advertisements.



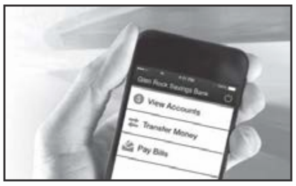
The advantages of e-commerce include its round-the-clock availability, speed of access, wide availability of goods and services to the consumer, easy accessibility and international reach.

8.32.1 Payment Transactions through E-Commerce

1. **Online Banking**

Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or a financial institution to conduct a range of financial transactions through the financial institution's website.

2. **Mobile Banking**



Mobile banking is a service provided by a bank or a financial institution that allows its customers to conduct a range of financial transactions remotely using a mobile device such as a **mobile phone** or **tablet**, and using software, usually called an app, provided by the financial institution for the purpose.

8.32.2 Payment Apps and Services

Payment apps are also referred to as Mobile Wallets. There are many payment apps available in the market which are very efficient to use and convenient to handle.

The following are some of the wallets which are frequently used in the market.

1. Google Wallet
2. Apple Passbook
3. Paytm Wallet
4. Freecharge Wallet
5. MobiKwik Wallet
6. PayU
7. Square Wallet
8. PayPal
9. Dwolla
10. Venmo
11. Bharat Interface for Money (BHIM) App

The online mode of payment has brought about a drastic change to marketing. There are many start-ups which are doing very well thanks to the online mode of payment. This revolution has taken the world by storm.

8.33 CLOUD COMPUTING

Cloud computing provides computing and storage capacity services to the heterogeneous community of end-recipients. The name comes from the use of clouds as an abstraction for the complex infrastructure.

Cloud Computing = Software as a Service + Platform as a Service + Infrastructure as a Service + Data as a Service

Therefore, cloud computing:

- Provides a shared pool of configurable computing resources
- Provides on-demand network access
- Is provisioned by the Service Provider

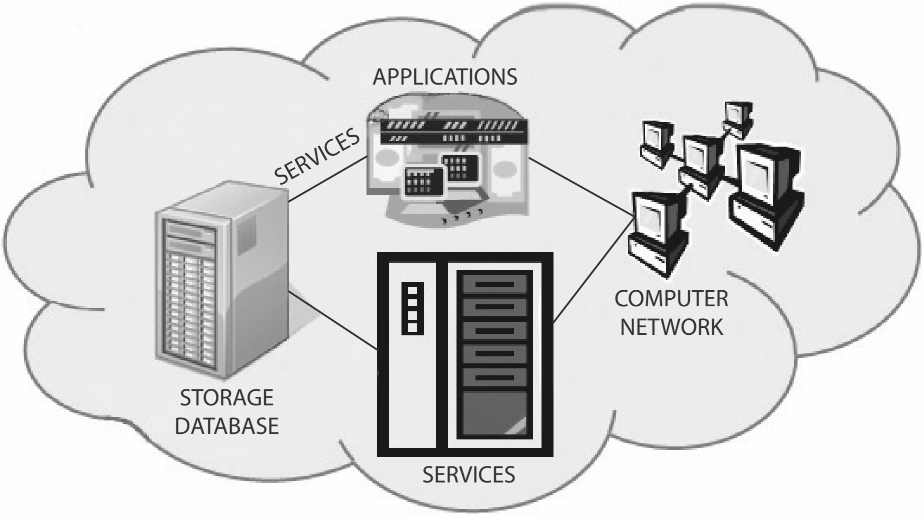


Fig. 8.35: Components of Cloud Computing

It entrusts services with a user's data, software and computation over a network. It has considerable overlap with Software as a Service (SaaS).

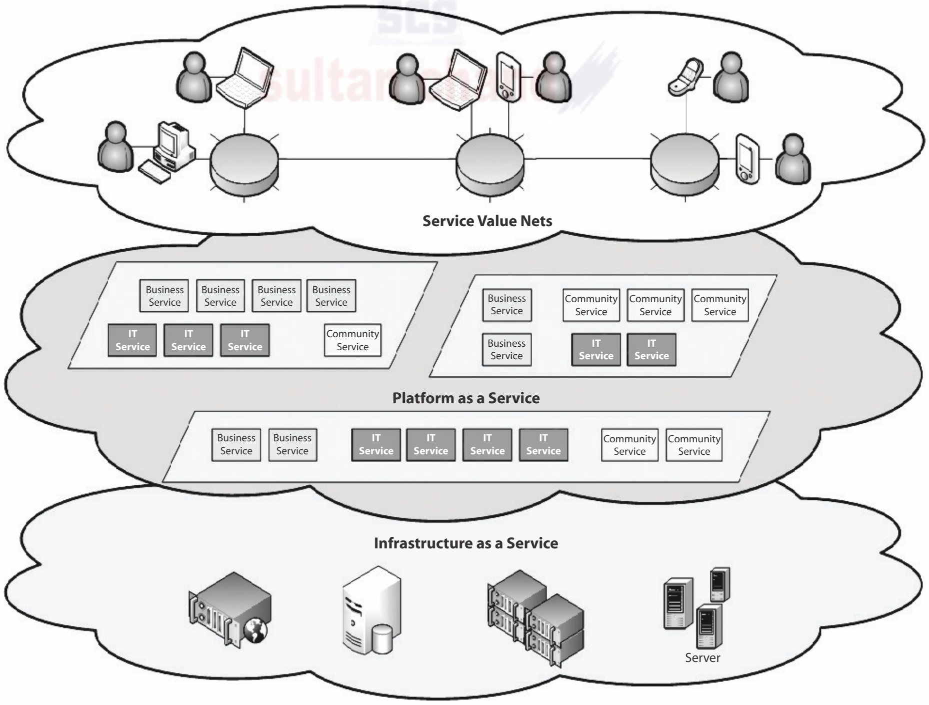


Fig. 8.36: Cloud Architecture

➢ **Software as a Service (SaaS)**

- From the end-user's point of view
- Apps are located in the cloud
- Software experiences are delivered through the internet

- Platform as a Service (PaaS)
  - From the developer's point of view (*i.e.*, cloud users)
  - Cloud providers offer an internet-based platform to developers who want to create services but do not want to build their own cloud.
- **Infrastructure as a Service (IaaS)**
  - Cloud providers build datacentres
  - Power, scale, hardware, networking, storage, distributed systems, etc.
    - Datacentre as a service
  - Cloud users rent storage, computation and maintenance from cloud providers (pay- as-you-go-like utility)
- **Data as a Service (DaaS)**

  Data → Information → Knowledge → Intelligence
  - Infrastructure for web-scale data mining and knowledge discovery
  - Empower people with knowledge
  - Empower applications and services with intelligence

Benefits of cloud computing: There are several benefits of cloud computing because of which it has become essential and popular these days.

- **Reduces capital and operational costs**
  - No longer required to make large upfront capital investment on datacentres
  - Eliminates the need to plan ahead for provisioning
  - Allows companies to start small and increase their resource investment as needed (pay-as-you-go)
- **Simplifies app deployment & management**
  - Common programming model across mobile, browser, client, server, cloud
  - Access to strong ecosystem of widely deployed applications
  - Integration with existing IT assets (Software + Services)

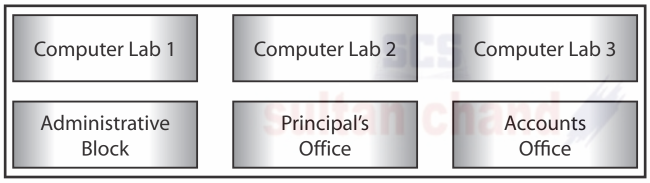
8.34 SETTING UP A COMPUTER NETWORK—AN EXAMPLE

The network functioning is based on Client-Server architecture which requires effective and efficient network design. It defines how clients are connected to server machine(s) on a network. The most important rule or methodology for network (LAN) design is the 80:20 rule.

The 80:20 Thumb Rule

This thumb rule states that in a well-organized and designed network, 80 percent of the traffic on a given network segment is local (*i.e.*, destined for a destination system in the same workgroup), and not more than 20 per cent of the network traffic should move across a backbone. The backbone in a network which violates this 80:20 rule leads to network congestion and traffic jams.

Keeping the above significant rule in mind, let us take an example to understand how to go about LAN design.



An educational society (say XYZ Educational Society), with its head office in Chennai (Tamil Nadu) and schools in various parts of the globe, is setting up a new senior secondary school, 'SF School', in Bahadurgarh (Haryana). The 'SF School' will have 3 computer labs with 30 computers in each lab, one Accounts office with three computers, one Administrative block with five computers, and a Principal's office with one computer.

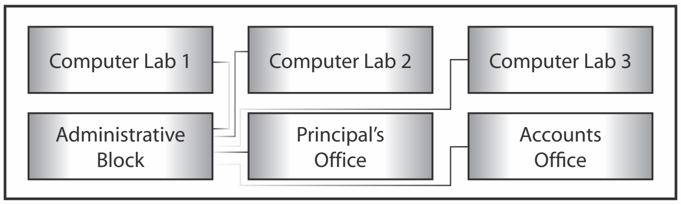
Let us see how a computer network can be set up in the school. First of all, we can draw a rough sketch of the school with computers at various locations as follows:

1. Independent LANs can be set up in each of the following buildings: Computer Lab1, Computer Lab2, Computer Lab3, Administrative Block, and Accounts Office.
2. These LANs can be set up in STAR topology using UTP cable (economical, reliable and easily available).
3. For this, one switch (with suitable number of ports) will be required in each of these buildings. More than one switch can be used in computer labs if a switch with more than 30 ports is not available.
4. Two internet connections (broadband for high speed) can be procured in Administrative Office.

   Two connections should be procured from two different ISPs so that:

   (a) Internet connection in Administrative office can be kept separate from the other Computer labs where students may do a lot of experimentation.

   (b) If one internet connection is not working, the other can be used in case of urgent requirements.
5. These buildings can then be connected as follows:



6. This interconnection will ensure that each building is directly connected to Administrative block.
7. This way, internet connection will be available in each building irrespective of the status of the other building.
8. Server (if any) of the school may be placed in the Administrative block so that it remains safe (physically) and a firewall can be set up so that the whole network remains safe from any kind of virus or intrusion attacks.

   There is no need to put in any extra efforts or expenses to link the school to its head office. This can be taken care of using the internet connections

Tips to solve technical questions based on Networking

Where Server should be placed: Server should be placed in the building where the number of computers is maximum.

1. **Suggest a suitable cable layout of connection:** A suitable cable layout can be suggested in the following two ways:

(a) **On the basis of Server:** First, the location of the Server is found out. Server should be placed in that building where the number of computers is maximum (according to the 80:20 rule). After finding the server position, each building distance is compared with the Server building directly or indirectly (taking other building(s) in between). The shortest distance is counted, whether it is directly or indirectly calculated.

(b) **On the basis of distance from each building:** The distance between each building is compared to all other buildings, either directly or indirectly. The shortest distance is calculated, whether it is direct or through some other building.

2. **Where the following devices should be placed:**

Server	:	Large number of computers in the building
HUB/Switch	:	Each building
Modem	:	In the server room
Repeater	:	It is used if the distances are higher than 70m. It regenerates data and voice signals.
Router	:	When one LAN is required to be connected to the other LAN
Best Layout	:	Star (from Server), BUS topology
Best Cable	:	Twisted Pair, Ethernet Cable, coaxial cable (when distance is in metres); For large distances—Fibre optics cable.
Best connecting technique	:	In hilly regions, radio waves should be used and city-to-city, state-to-state satellite should be used.

MEMORY BYTES

- Internet is a network of networks that spreads all over the world.
- ARPANET was the first internet followed by NSFNET and other small networks.
- A gateway is a device that connects dissimilar networks.
- A backbone is a central interconnecting device that connects two or more computers.
- Topology is a way of connecting computers physically or logically.
- Star topology uses a central hub where each computer indirectly connects with the other computer on the network.
- A set of rules that governs internet is called protocol.
- TCP protocol is responsible for sequential arrangement of packets.
- IP protocol is responsible for fragmentation of data into packets and sends those packets in random order.
- FTP protocol is used to share files across networks.
- TELNET is a remote login where a user can login on another user's system.
- HTTP is used for displaying web pages.
- Web browser is an application program that helps in opening web pages.
- The first page of any website is known as home page.
- Communication media is a transmission media for transmitting data across the network.
- Guided media is also known as wired media while unguided media is also known as wireless media.
- LAN, MAN, WAN and PAN are the four types of networks.
- Viruses are malicious programs that can damage files, disks, file allocation table, etc.
- Spams are unsolicited mails that eat up the disk space.

- Hub refers to a networking component which acts as a convergence point of a network allowing the transfer of data packets.
- Switch refers to a device which filters and forwards data packets across the network.
- Web hosting service is a type of internet hosting service that allows individuals and organizations to host their own website and users with online systems to store information such as images, videos, etc.
- A data channel is the medium used to carry information or data from one point to another.

OBJECTIVE TYPE QUESTIONS

1. Fill in the blanks.

(a) Through .... you can establish contact with anyone in the world.

(b) The main function of .... is to divide the message or data into packets of a definite size on the source computer.

(c) .... refers to wireless fidelity which enables us to connect to the ISP without any cable.

(d) .... is a software that enables us to access the internet and explore websites.

(e) Web page constitutes the ....

(f) A .... is someone with a strong interest in how things work, who likes to create and modify things for their own enjoyment.

(g) A computer .... is a small software program that spreads from one computer to another and interferes with the normal functioning of computer.

(h) Electronic junk mail or junk newsgroup postings are known as ....

(i) Digital signature meets the need for .... and integrity.

(j) The first network that planted the seed of internet was ....

(k) The protocol used for internet is ....

(l) A device used to connect dissimilar networks is called ....

(m) .... is responsible for handling the address of the destination computer so that each packet is delivered to its proper destination.

(n) Tricking people through authentic-looking emails or websites is called ....

(o) A program designed to replicate and eat up a computer's storage is called ....

(p) A digital document issued to a site by a certification authority of the internet is called a ....

(q) To connect computers located in a specific building or campus is known as ....

(r) Wi-Fi, infrared and Bluetooth are examples of ....

(s) Interspace is a ....

(t) A server that provides its services to other workstations on a network is a ....

(u) The techniques of switching in which data is fragmented into smaller techniques is called ....

(v) .... is a dedicated line between the caller and the sender.

(w) .... is the measuring unit of speed at which the data transfer takes place.

(x) All the computers are connected with each other in an unorganized manner in topology ....

(y) In ...., all computers share equivalent responsibility for processing data..

Answers: (a) Internet (b) TCP (c) Wi-Fi
(d) Browser (e) World Wide Web (f) Hacker
(g) Virus (h) SPAM (i) Authentication
(j) ARPANET (k) TCP/IP (l) Gateway
(m) IP (n) Hacking (o) WORM
(p) Digital certificate (q) LAN
(r) Communication Mediums (s) Network (t) Dedicated server
(u) Packet switching (v) Circuit switching (w) Bits/Second
(x) Mesh (y) Peer-to-peer network

2. State whether the following statements are True or False.

(a) A set of rules that governs internet is called protocol.

(b) A repeater handles different protocols.

(c) A hub is known as an intelligent device on the network.

(d) A location on a net server is called a website.

(e) A document that uses HTTP is called a web page.

(f) A switch is a device used to segment networks into sub-networks or subnets.

(g) Email is sending and receiving messages through videoconferencing.

(h) The degeneration of a signal over a distance on a network is called attenuation.

(i) Coaxial cable possesses higher tensile strength than optical fibre.

(j) When two entities are communicating and do not want a third party to listen, this situation is defined as secure communication.

Answers: (a) True (b) False (c) False (d) True (e) True (f) True
(g) False (h) True (i) False (j) True

3. Multiple Choice Questions (MCQs)

(a) A computer network:
- (i) Is a collection of hardware components and computers
- (ii) Is interconnected by communication channels
- (iii) Allows sharing of resources and information
- (iv) All of the above

(b) What is a firewall in computer network?
- (i) The physical boundary of network
- (ii) An operating system of computer network
- (iii) A system designed to prevent unauthorized access
- (iv) A web browsing software

(c) What is the use of Bridge in the network?
(i) To connect LANs (ii) To separate LANs
(iii) To control network speed (iv) All of the above

(d) Each IP packet must contain:
(i) Only Source address (ii) Only Destination address
(iii) Source and Destination address (iv) Source or Destination address

(e) Which of these is not a communication channel?
(i) Satellite (ii) Microwave (iii) Radio wave (iv) Wi-Fi

(f) MAN Stands for ....
(i) Metropolitan Area Network (ii) Main Area Network
(iii) Metropolitan Access Network (iv) Metro Access Network

(g) Which of these is not an example of unguided media?
(i) Optical Fibre Cable (ii) Radio wave
(iii) Bluetooth (iv) Satellite

(h) In which topology are all the nodes connected through a single Coaxial cable?
(i) Star (ii) Tree (iii) Bus (iv) Ring

(i) Which of the following is the smallest network?
(i) WAN (ii) MAN (iii) LAN (iv) Wi-Fi

(j) Which protocol is used for the transfer of hypertext content over the web?
(i) HTML (ii) HTTP (iii) TCP/IP (iv) FTP

Answers: (a) (iv) (b) (iii) (c) (i) (d) (iii) (e) (iv) (f) (i)
(g) (i) (h) (iii) (i) (iii) (j) (ii)

SOLVED QUESTIONS

1. Define a network. What is its need?

Ans. A network is an interconnected collection of autonomous computers that can share and exchange information.

Need for networking:

(a) *Resource sharing:* Resources are shared by all computers over the network for effective utilization.

(b) *File sharing:* A file in a network can be accessed from anywhere.

2. Write **two** advantages and **two** disadvantages of network.

Ans. *Advantages of network:*

(a) We can share resources such as printers and scanners.

(b) We can share data and access files from any computer.

Disadvantages of network:

(a) If there is any problem in the server, then no communication can take place.

(b) Network faults can cause loss of data.

(c) If there is no privacy mechanism used then the entire network can be accessed by an unauthorized person.

3. What is ARPANET? What is NSFNET?

Ans. ARPANET (Advanced Research Project Agency Network) is a project sponsored by US Department of Defence.

NSFNET was developed by the National Science Foundation which was a high capacity network and strictly used for academic and engineering research.

4. What are the various types of networks?

Ans. A network is an interconnection of several nodes through some communication media with the goal of sharing data, files and resources. There are three types of networks:

(a) Local Area Network (LAN)

(b) Metropolitan Area Network (MAN)

(c) Wide Area Networks (WAN)

5. Name the various layers of coaxial cable.

Ans. Coaxial cable consists of the following layers:

(a) A metallic rod-shaped inner conductor.

(b) An insulator covering the rod.

(c) A metallic outer conductor called shield.

(d) An insulator covering the shield.

(e) A plastic cover.

6. What is a spam mail? [CBSE D 2015]

Ans. Spam is the abuse of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately.

7. Differentiate between FTP and HTTP. [CBSE D 2015]

Ans. FTP is a protocol to transfer files over the internet. HTTP is a protocol which allows the use of HTML to browse web pages in the World Wide Web.

8. Out of the following, which is the fastest (a) Wired, and (b) Wireless medium of communication? Infrared, Coaxial Cable, Ethernet Cable, Microwave, Optical Fibre. [CBSE D 2015]

Ans. (a) *Wired:* Optical Fibre

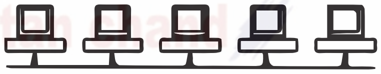
(b) *Wireless:* Infrared or Microwave

9. What is a worm? How is it removed? [CBSE D 2015]

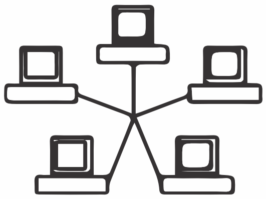
Ans. A worm is a self-replicating computer program. It uses a network to send copies of itself to other computers on the network and it may do so without any user intervention. Most of the common antivirus (anti-worm) software remove worm.

10. Illustrate the layout for connecting five computers in a Bus and a Star topology of Networks.

Ans. Bus topology



Star topology



11. In networking, what is WAN? How is it different from LAN? [CBSE D 2011]

Ans. Internet is an example of WAN (Wide Area Network). Most WANs exist to connect LANs that are not in the same geographical area. WAN is different from LAN due to its network range. WAN is for connecting computers anywhere in the world without any geographical limitation whereas LAN is confined within a range of 100m to 500m.

12. What is meant by topology? Name some popular topologies.

Ans. Topology is the arrangement by which computers are connected with each other, either physically or logically.

The popular topologies are:

(a) Bus or Linear Topology

(b) Ring Topology

(c) Star Topology

(d) Tree Topology

13. Why are fibre optic cables becoming popular?

Ans. Fibre optic transmission is becoming increasingly popular due to its noise resistance, low attenuation and high bandwidth capabilities.

14. What factors should be taken into consideration while opting for a particular topology?

Ans. There are a number of factors which are to be considered:

(a) Cost

(b) Flexibility

(c) Reliability

15. What is a modem? What are the two types of modems?

Ans. Modem stands for modulator demodulator that converts analog signals to digital signals at the sender's end. It converts digital signals back to analog signals at the receiver's end.

The two types of modems are: internal modem and external modem.

16. What is remote login? What is Telnet?

Ans. Remote login is the process of accessing a network from a remote place without actually being present at the place of working. Telnet is an internet utility that lets us log on to a remote computer system. A user is able to log in the system for sharing of files without being the actual user of that system.

17. Briefly explain FTP.

Ans. FTP stands for File Transfer Protocol. It is the standard mechanism provided by TCP/IP for copying a file from one host to another. While sharing files from one system to another, we may encounter several problems—two systems may have different directory structures, two systems may have different file-naming conventions, or two systems may have different ways to represent text and data. All these problems are solved by FTP.

18. What is protocol? Name some commonly used protocols.

Ans. A protocol means the rules that are applicable for a network, or we can say the common set of rules used for communication in network.

Different types of protocols are:

(a) **HTTP:** Hyper Text Transfer Protocol

(b) **FTP:** File Transfer Protocol

(c) **SLIP:** Serial Line Internet Protocol

(d) **PPP:** Point-to-Point Protocol

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

(f) **SMTP:** Simple Mail Transfer Protocol

(g) **POP:** Post Office Protocol

(h) **IMAP:** Internet Mail Access Protocol

19. What is TCP/IP?

Ans. TCP/IP (Transmission Control Protocol/Internet Protocol) is a protocol for communication between computers used as a standard for transmitting data over networks and is the basis for standard Internet protocols. It is also responsible for assembling packets at the receiver's side.

20. How is FTP different from HTTP?

Ans. FTP is a protocol used to upload files from a workstation to an FTP server or download files from an FTP server to a workstation, whereas HTTP is a protocol used to transfer files from a Web server on to a browser in order to view a web page that is on the internet.

21. Define Mobile Communication and Wireless Communication.

Ans. Mobile Communication essentially refers to a computing device that is not continuously connected to the base or central network. This may include laptops, newly-created smartphones and also PDAs. Wireless Communication is simply data communication without the use of a landline. This may involve a cellular telephone, a two-way radio, a fixed wireless connection, a laser or satellite communication.

22. What is Mobile Processor?

Ans. Mobile Processors are required to run an operating system, be it desktop, laptop or mobile. They provide necessary resources to start an operating system, run applications and do tasks.

23. Name any four popular mobile processors in the market.

Ans. Four popular mobile processors are Qualcomm Snapdragon, Apple's Mobile Processors, HiSilicon and Samsung Exynos.

24. What are the advantages of e-commerce applications?

Ans. The advantages of e-commerce applications include their round-the-clock availability, the speed of access, the wide availability of goods and services for the consumer, easy accessibility, and international reach.

25. Define web browser and web server.

Ans. **Web Browser:** A web browser is a software which is used for displaying the content on web page(s). It is used by the client to view websites. Examples of web browser—Google Chrome, Firefox, Internet Explorer, Safari, Opera, etc.

Web Server: A web server is a software which entertains the request(s) made by a web browser. A web server has different ports to handle different requests from web browser, like generally FTP request is handled at Port 110 and HTTP request is handled at Port 80. Example of web server is Apache.

26. Differentiate between XML and HTML.

Ans. In HTML (Hyper Text Markup Language), both tag semantics and the tag set are fixed, whereas XML (Extensible Markup Language) is a meta-language for describing markup languages. XML provides the facility to define tags and the structural relationships between them. All the semantics of an XML document will either be defined by the applications that process them or by style sheets.

27. What is web hosting?

Ans. Web hosting is a means of hosting web server applications on a computer system through which electronic content on the internet is readily available to any web-browser client.

28. What is hacking?

Ans. Hacking is a process of accessing a computer system or network without knowing the access authorization credential of that system. Hacking can be illegal or ethical depending on the intention of the hacker.

29. What are cookies?

Ans. 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 website. Cookies are saved in the form of text files in the client computer.

30. Differentiate between cracking and hacking.

Ans. Cracking is defined as an attempt to remove the copy protections inserted into software programs. A program successfully stripped of protections is then known as having been "Cracked". Hacking can be ethical/legal but cracking is a totally illegal method and is also called piracy.

31. What is web scripting?

Ans. A script is a small bit of code that enables web browsers to do something rather than just displaying static results. Scripts are used in web design to create dynamic pages. There are two categories of web scripts: Client-Side Script which can be written by using JavaScript, VBScript, and Server-Side Script, which can be written in PHP (used for client-side scripting also) and JSP.

32. Name some web scripting languages.

Ans. There are many scripting languages available today. Most common are VBScript, JavaScript, ASP, PHP, PERL and JSP.

33. What is Cyber Crime?

Ans. When any crime is committed over the internet, it is referred to as Cyber Crime.

34. What is Web 2.0?

Ans. Web 2.0 is a concept that takes the network as a platform for information sharing, interoperability, user-centred design, and collaboration on the internet or World Wide Web. A Web 2.0 site allows users to interact and collaborate with each other. Examples of Web 2.0 include social networking sites, facebook, google+, twitter, etc.

35. Give one advantage of bus topology of network. Also state how four computers can be connected with each other using star topology of network.

Ans. In bus topology, the workstations can easily be extended or removed. In star topology, four computers can be connected with each other through a server.

36. Write two advantages of using an optical fibre cable over an Ethernet cable to connect two service stations which are 200m away from each other. [CBSE D 2013]

Ans. Optical fibre cable guarantees secure transmission and a very high transmission capacity. Optical fibre cable is immune to electrical and magnetic interference.

37. Write two characteristics of Wi-Fi. [CBSE D 2014]

Ans. (a) It allows an electronic device to exchange data or connect to the internet wirelessly using microwaves.

(b) Network range of Wi-Fi is much less than other network technologies like wired LAN.

38. What is the difference between Email and Chat? [CBSE D 2014]

Ans. (a) Chat is a type of software while Email is a protocol.

(b) Chat requires the permission of both parties while Email does not.

(c) Chat is typically software dependent while Email is not.

(d) Chat needs accounts on the same provider while Email does not.

39. What are VoIP?

Ans. VoIP are communication protocols and transmission technologies for delivery of voice communication and multimedia sessions over Internet Protocol (IP) networks, such as the internet. Also, we can say that VoIP are IP technology, internet telephony and broadband telephony.

40. Expand the following terms:

(a) XML (b) GSM

(c) SMS (d) MAN

Ans. (a) XML– Extensible Markup Language

(b) GSM– Global System for Mobile communication

(c) SMS– Short Messaging Service

(d) MAN– Metropolitan Area Network

41. How many switching techniques are there? Explain any one.

Ans. There are three switching techniques:

(a) Circuit Switching

(b) Packet Switching

(c) Message Switching

Circuit Switching: In this technique, first the complete physical connection between two computers is established and then data is transmitted from the source computer to the destination computer. The entire dedicated line is used by the caller and the receiver and no other user can use it even if the line becomes idle. When the data transmission is over, the line is disconnected and is available for the next communication.

42. How are Trojan horses different from Worms? Mention any one difference. [Sample Paper]

Ans. A Trojan horse is a term used to describe malware that appears to the user to perform a desirable function but which, in fact, facilitates unauthorized access to the user's computer system.

A computer Worm is a self-replicating program. It uses a network to send copies of itself to other nodes and that too without human intervention.

43. What is a communication channel? Name the basic types of communication channels available.

Ans. A communication channel is also known as communication media or transmission media. Communication media can be wireless or wired. Wireless media is also known as unguided media while wired media is also known as guided media.

Following are three basic types of communication channels available:

(a) Twisted Pair Cables

(b) Coaxial Cables

(c) Fibre-optic Cables

44. Define baud, bps and Bps. How are these interlinked?

Ans. **Baud** is a unit of measurement for the information-carrying capacity of a communication channel.

bps (bits per second) refers to a thousand bits transmitted per second.

Bps (Bytes per second) refers to a thousand bytes transmitted per second.

All these terms are measurement units used to refer to the amount of information travelling through a single channel at any one point of time.

45. Differentiate between star topology and bus topology.

Ans. The main points of difference between star and bus topology are:

Star topology	Bus topology
A central hub is required to connect all computers with each other.	A long cable known as backbone is used to connect all computers with each other.
The data is transmitted from the sender to the receiver by passing through the hub.	The data is transmitted through a long cable from the sender to the receiver.
No collision takes place through transmission of data.	Collision can take place as the data can be transmitted from both ends at the same time.
If the central hub fails, the entire network shuts down.	If there is a break in a cable, no transmission takes place.

46. Define the following terms:

(a) RJ-45 (b) Ethernet

(c) Ethernet card (d) Hub

(e) Switch

Ans. (a) **RJ-45:** RJ-45 is a standard type of connector for network cables and networks. It is an 8-pin connector usually used with Ethernet cables.

(b) **Ethernet:** Ethernet is a LAN architecture developed by Xerox Corp. along with DEC and Intel. It uses a bus or star topology and supports data transfer rates of up to 10 mbps.

(c) **Ethernet card:** The computer parts of Ethernet are connected through a special card called Ethernet card. It contains connections for either coaxial or twisted pair cables

(d) **Hub:** In computer networking, a hub is a small, simple, low-cost device that joins multiple computers together.

(e) **Switch:** A switch is a small hardware device that joins multiple computers together within one local area network (LAN).

47. Define the following data communicating devices:

(a) Repeater (b) Bridge

(c) Router (d) Gateway

Ans. (a) **Repeater:** It is a device that amplifies and restores the signal before it gets degraded and transmits the original signal back to the destination. A repeater is a regenerator and not an amplifier.

(b) **Bridge:** A bridge is a device designed to connect two LAN segments. The purpose of a bridge is to filter traffic on a LAN. Bridge relays frames between two originally separate segments. When a frame enters a bridge, the bridge not only regenerates the signal but also checks the physical address of the destination and forwards the new copy only to that port.

(c) **Router:** Routers operate in the physical, data link and network layers of the OSI model. They decide the path a packet should take. A router is a networking device whose software and hardware are usually tailored to the tasks of routing and forwarding data packets across network.

(d) **Gateway:** A gateway operates on all the seven layers of OSI model. A network gateway is a computer which has internet-working capability of joining together two networks that use different base protocols. Gateway converts one protocol to another and can, therefore, connect two dissimilar networks.

48. What is HTML? Where is it used?

Ans. HTML (Hyper Text Markup Language) is used to create Hypertext documents (web pages) for websites.

HTML is the static mark-up language which is used for the following purposes:

- It is used to create web pages.
- It tells the browser how to display text, pictures and other support media.
- It supports multimedia and new page layout features.
- It provides many tags for controlling the presentation of information on the web pages, such as: <BODY>, <LI>, <HR>, etc.

49. Define GSM, CDMA and WLL.

Ans. **GSM:** Global system for mobile communication (GSM) is a wide area wireless communications system that uses digital radio transmission to provide voice data and multimedia communication services. A GSM system coordinates the communication between mobile telephones, base stations and switching systems.

CDMA: Code Division Multiple Access (CDMA) is a digital wireless telephony transmission technique which allows multiple frequencies to be used simultaneously—Spread Spectrum.

WLL: Wireless in Local Loop (WLL) is a system that connects the subscriber to the public switched telephone network (PSTN) using radio signals as alternative to other connecting media.

UNSOLVED QUESTIONS

1. What is internet?
2. What is network?
3. What are the various types of topologies?
4. Describe bus topology and star topology.
5. Define the following terms:
   (a) Baud (b) Communication channel
   (c) Hubs (d) Repeaters
6. Define GSM and GPRS wireless communication system.
7. What is modem? Define the functioning of internal modem and external modem.
8. Expand and explain the following terms:
   (a) PPP (b) POP3
   (c) VoIP (d) IRC
9. What is the significance of cyber law?
10. Describe the following networking devices:
    (a) Hubs (b) Repeaters (c) Routers
    (d) Bridges (e) Gateways
11. What are Wi-Fi cards? Explain.
12. What is the significance of using firewalls and authentication?
13. What is a communication protocol? What is its role in networking?
14. What is https? How does it work?
15. What is Ethernet? What is Ethernet Card?
16. What are hubs? How are active hubs different from passive hubs?
17. What are the facilities provided by the Server in a network environment?
18. Which communication medium is to be suggested for very effective and fast communication in guided medium?
19. In a harsh industrial environment, which cable would you like to use?
20. Which media have the ability to communicate over oceans?
21. What is the difference between microwave and radio wave transmission?
22. Which transmission medium is useful for sparsely populated areas?
23. Which network is easy to expand?
24. Which device filters the data and which device can handle different protocol?
25. What is a network? What are its goals and applications?
26. Write some advantages and disadvantages of the following:
    (a) Optical fibres (b) Coaxial cables (c) Twisted pair cables
    (d) Radio waves (e) Microwaves (f) Satellites
27. Explain the role of HTTP protocol.
28. Define email.
29. What do you understand by data transfer rates?
30. What are hubs? What are its types?
31. What is the role of a switch in a network?
32. Briefly discuss the role of the following devices in the context of networking:
    (a) Repeater (b) Router
    (c) Bridge (d) Gateway
33. Briefly
    (a) HTTP (b) TCP/IP (c) FTP
34. What is computing? How is it different from mobile computing?
35. When would you prefer (i) hubs over repeaters, (ii) bridges over hubs, and (iii) switches over other networking devices?