7 Computer Networks

7.1 INTRODUCTION

The greatest breakthrough in technology and communication over the past 30 years has been the development and advancement of 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, 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.

Some of the examples of network in our everyday life include:

- Social network
- Mobile network
- Network of computers
- Airlines, railways, banks, hospital networks

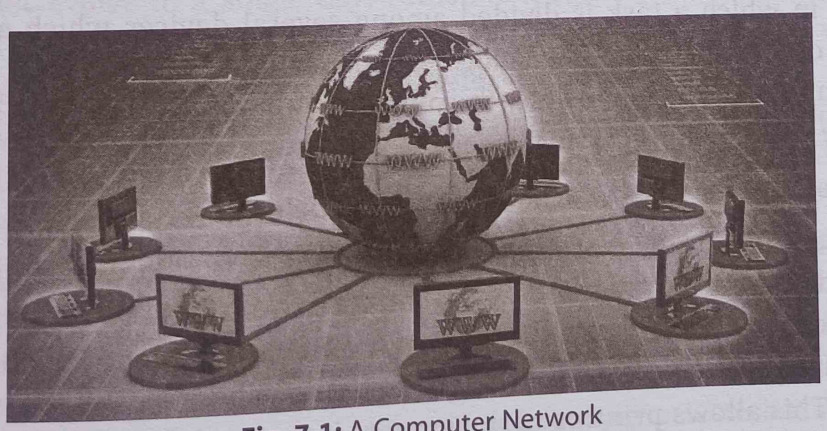


Fig. 7.1: A Computer Network

7.2 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, fax machine, printer, camera, 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 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).

A basic network may connect a few computers placed in a room. The network size may vary from small to large, depending on the number of computers it connects. A computer network can include different types of hosts (also called nodes) like server, desktop, laptop, cellular phones.

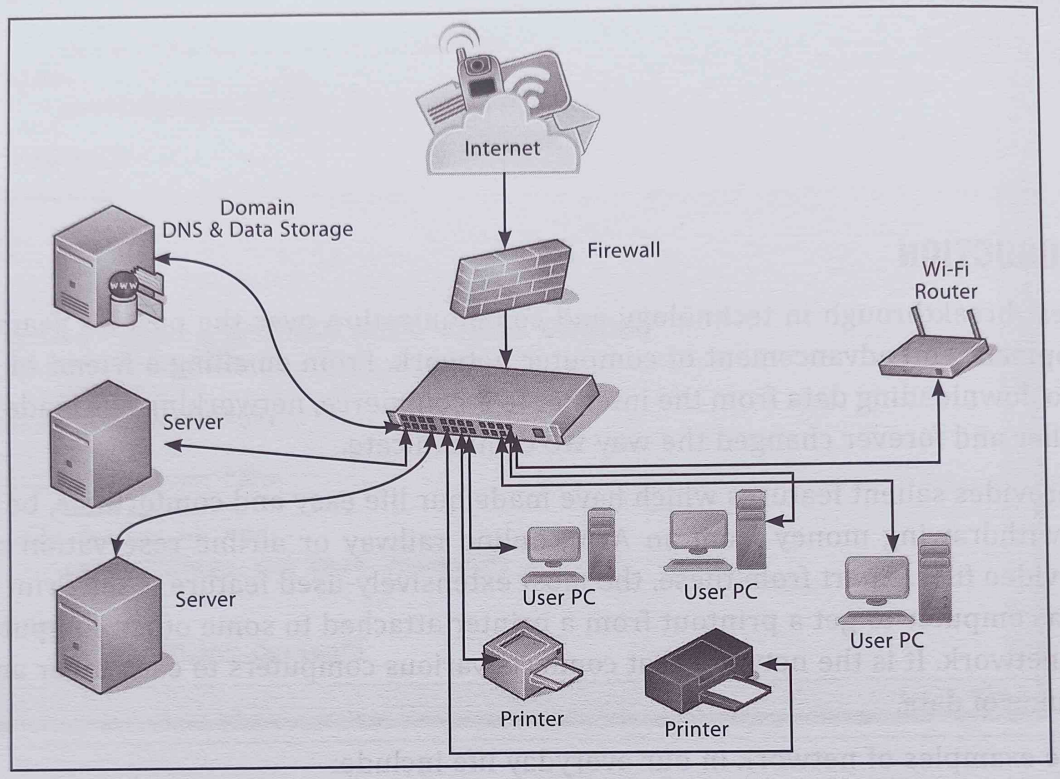


Fig. 7.2: The Network Diagram

7.2.1 Advantages of Computer Networks

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. 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 and 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.

7.2.2 Disadvantages of Computer Networks

These are the main disadvantages of computer networks:

(a) **Cost of set-up and maintenance:** It is difficult to set up larger networks as the systems on a network are sophisticated and complex to run. Even cabling and equipment cost can be expensive. In addition to this, maintenance cost may be very high for large networks.

(b) **Threat to data security:** Unauthorized access to data leading to data theft or data corruption, computer viruses, worms, malware, phishing, etc., are some of the threats to network security.

7.3 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. The development of ARPANET led to the development of today's internet.
- **NSFNET (National Science Federation Network):** In the mid-80's, another federal agency, NSFNET, 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 information and messages.

ARPANET + NSFNET + PRIVATE NETWORKS = INTERNET

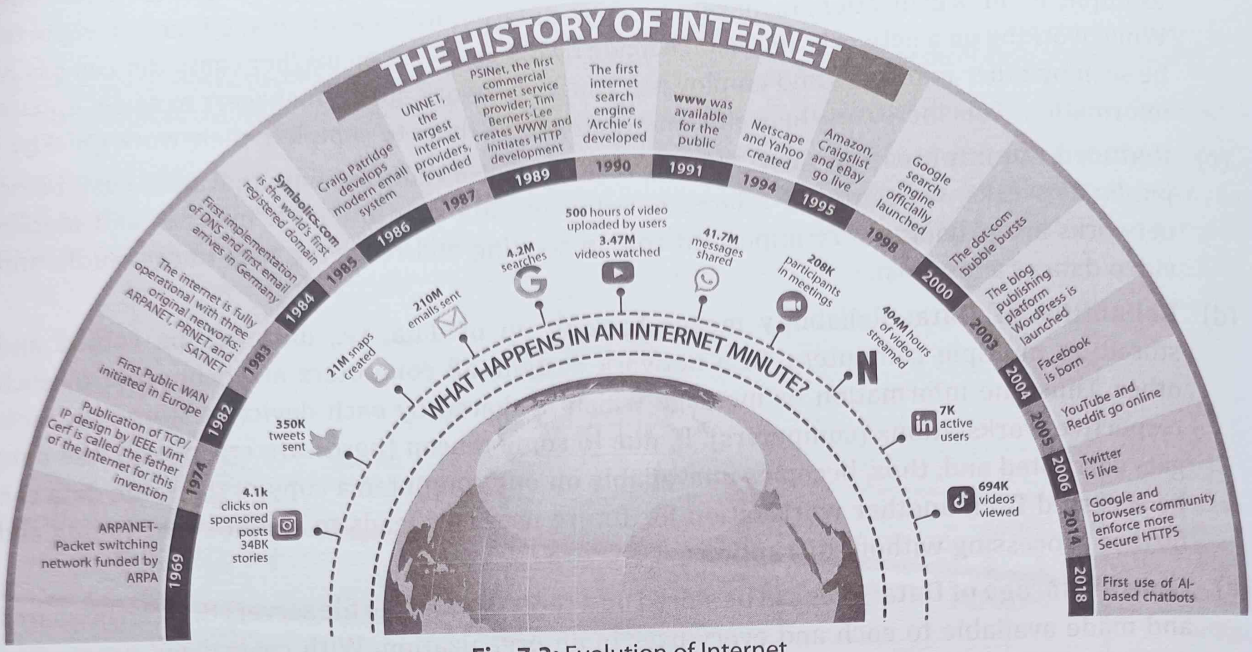


Fig. 7.3: Evolution of Internet

- **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.

7.4 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.

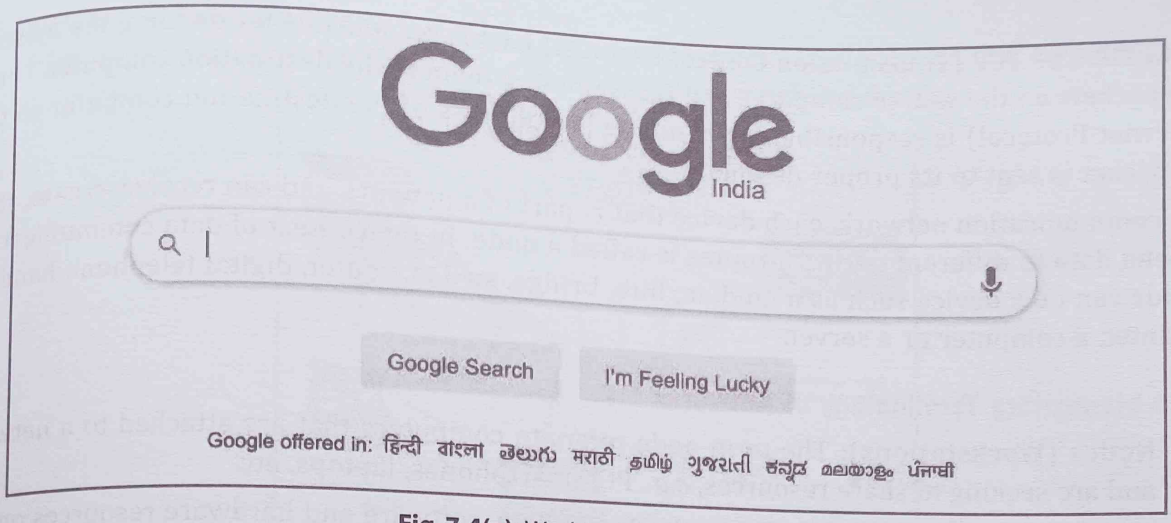


Fig. 7.4(a): Working of the Internet

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.

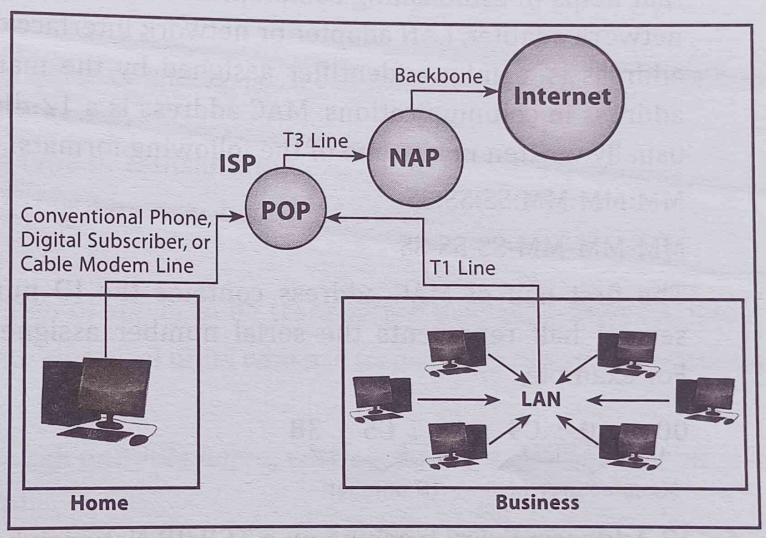


Fig. 7.4(b): POP and NAP

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.

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.

In a communication network, each device that is part of a network and can receive, create, store or send data to different network routes is called a node. In the context of data communication, a node can be a device such as a modem, hub, bridge, switch, router, digital telephone handset, a printer, a computer or a server.

7.4.1 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, *e.g.*, PC, smartphones, laptops, etc.
2. **Server:** A computer that facilitates sharing of data, software and hardware resources on the network. Servers tend to have more memory, processing power and storage than a normal workstation.
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. It is also called network adapter, LAN adapter or network interface controller. A Media Access Control (MAC) address is a unique identifier assigned by the manufacturer to NIC for use as a network address in communications. MAC address is a 12-digit hexadecimal number. MAC address is usually written in any one of the following formats:

   MM:MM:MM:SS:SS:SS

   MM-MM-MM-SS-SS-SS

   The first half of MAC address contains the ID number of the adapter manufacturer and second half represents the serial number assigned to the adapter by the manufacturer. For example,

   $$\underbrace{00 : A0 : C9}_{\text{Manufacturer Id}} : \underbrace{18 : C5 : 38}_{\text{ID number}}$$

4. **IP Address:** Every machine on a TCP/IP Network has a unique identifying number called an IP Address. It is provided by ISP.
5. **Domain Name:** It is a way to identify and locate the computers connected to the internet. It must be unique.

7.5 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 radio 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.

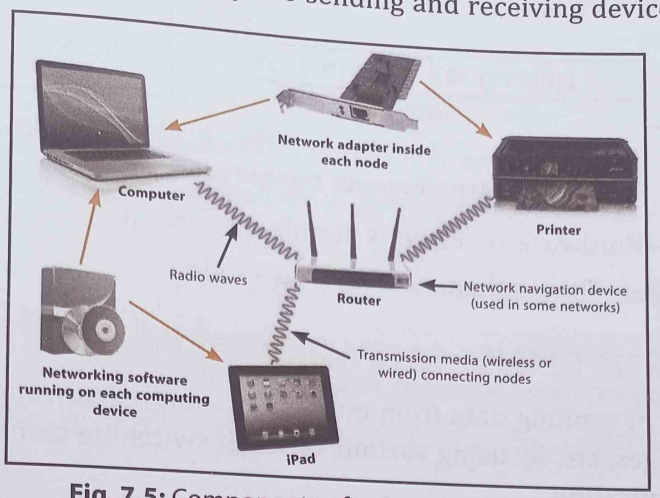


Fig. 7.5: Components of a Computer Network

7.6 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.

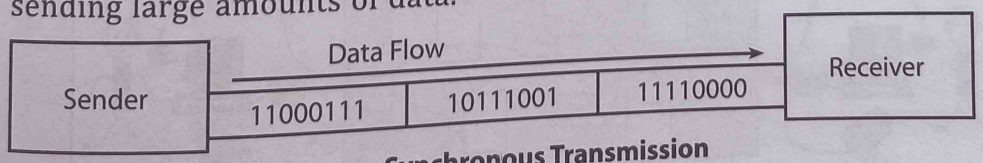
(d) Serial Communication

- 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. There is no space between data, hence it is efficient for sending large amounts of data.

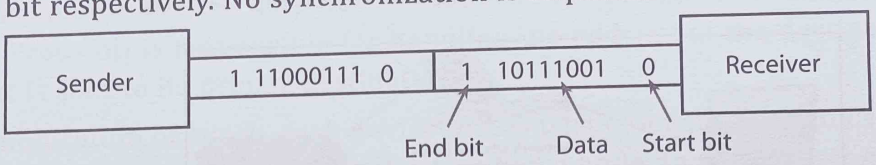


Synchronous Transmission

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.



Asynchronous Transmission

Advantage—Hardware required is simple and cheap.

Disadvantage—Slower than synchronous mode.

7.7 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.

7.7.1 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 till they reach the destination. A switched network is made up of a series of interconnected nodes called switches.

7.7.2 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.

1. Circuit Switching

Circuit switching provides end-to-end connection between two computers. It is established usually in a telephone network where one person is making a call and another is receiving a call. In a 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.

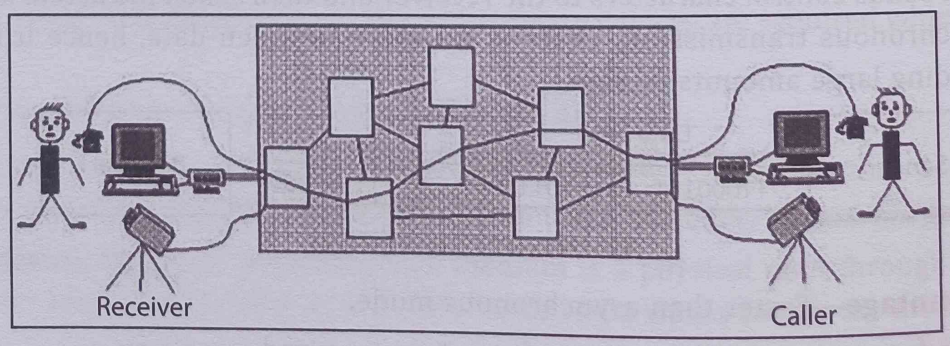


Fig. 7.6: Circuit Switching

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

(a) 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.

(b) All intermediate nodes are identified. These nodes are also called switching nodes.

(c) If the destination node is available, it sends back the acknowledgement of receiving a signal. Hence, data transmission begins.

(d) 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.

2. 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.

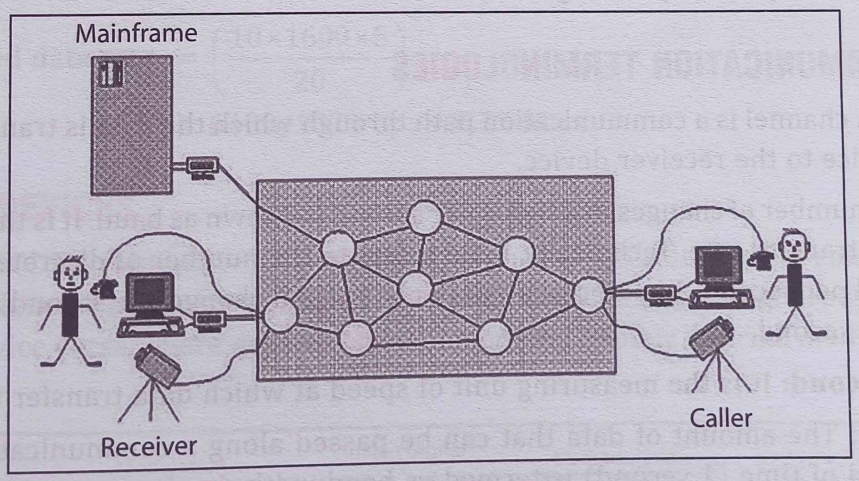


Fig. 7.7: Packet Switching

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

3. 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.

7.7.3 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.

7.8 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 the 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. **Bits per second:** It is the measuring unit of speed at which data transfer takes place.
4. **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, *i.e.*, it 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. The measuring unit is hertz (Hz), where 10^3 Hz = 1 Kilo Hertz (KHz), 10^3 KHz = 1 Mega Hertz (MHz).

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. **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.

6. **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.

7. **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 bits per second (bps) and bytes per second (Bps) or baud, kilobits per second (kbps), megabits per second (mbps), gigabits per second (gbps), terabits per second (tbps.)

$$1 \text{ Kbps} = 2^{10} \text{ bps} = 1024 \text{ bps}$$

$$1 \text{ Mbps} = 2^{20} \text{ bps} = 1024 \text{ Kbps}$$

$$1 \text{ Gbps} = 2^{30} \text{ bps} = 1024 \text{ Mbps}$$

$$1 \text{ Tbps} = 2^{40} \text{ bps} = 1024 \text{ Gbps}$$

Example: A user wants to upload a text document at the rate of 10 pages per 20 seconds. What will be the required data rate of the channel? (Assume that 1 page contains 1600 characters and each character is of 8 bits).

Sol. Required data rate $= \left(\frac{10 \times 1600 \times 8}{20}\right)$

$= 6400/1024$ bps $= 6.25$ Kbps

7.9 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.

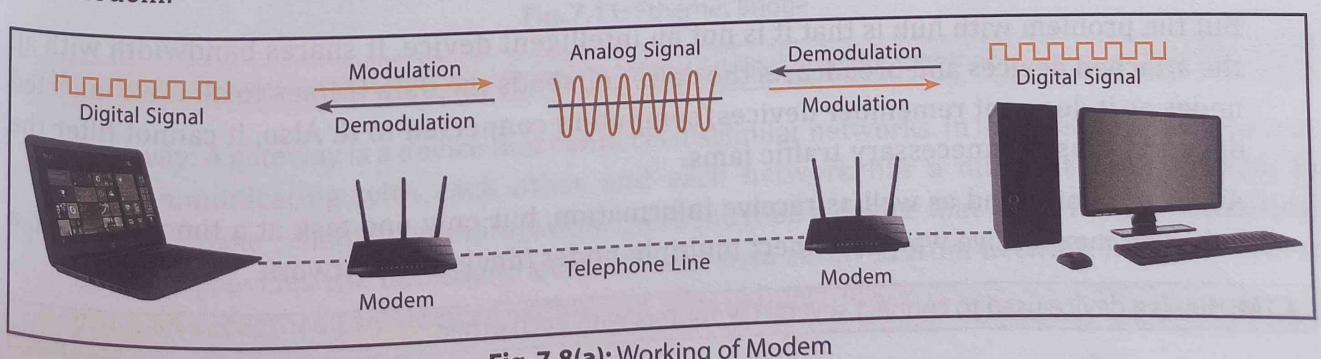


Fig. 7.8(a): Working of Modem

We know computers store and process data in terms of 0s and 1s. However, to transmit data from a sender to a receiver, or while browsing the internet, digital data is converted to an analog signal and the medium (be it free-space or a physical media) carries the signal to the receiver. There are modems connected to both the source and destination nodes. The modem at the sender's end acts as a **Modulator** that converts the digital data into analog signals while the modem at the receiver's end acts as a **Demodulator** that converts the analog signals into digital data for the destination node to understand.

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.

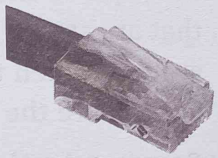


Fig. 7.8(b): RJ-45 Connector

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.

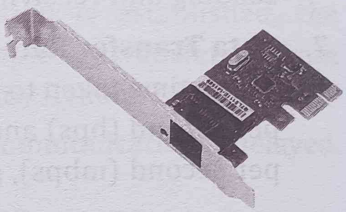


Fig. 7.8(c): Ethernet Card

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.

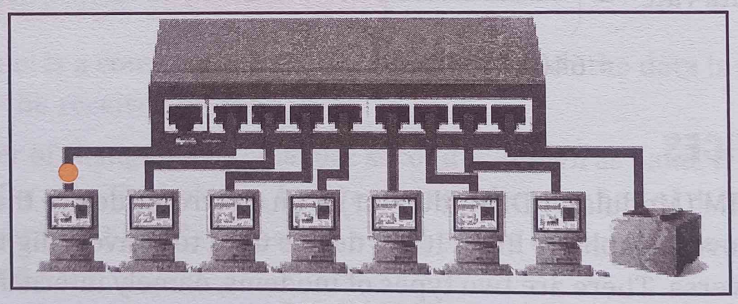


Fig. 7.9: Hub

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 only to one or more devices for which the packet is intended 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.

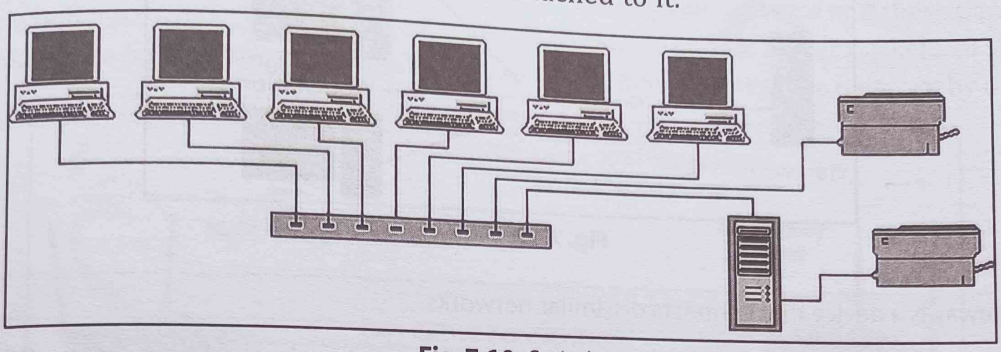


Fig. 7.10: Switch

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 (LANs) at the data link layer (layer 2) of the OSI model. Bridges relay frames between two originally separate segments that follow same protocols. 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.

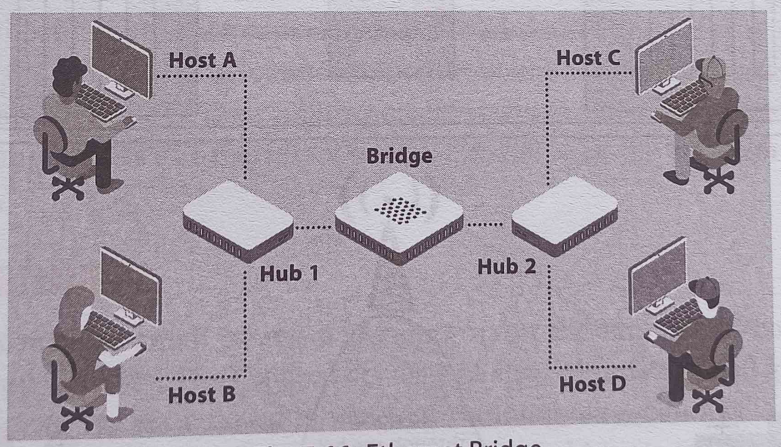


Fig. 7.11: Ethernet Bridge

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

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 provides the necessary translation of data received from network into a format or protocol recognized by devices within the internal network.

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

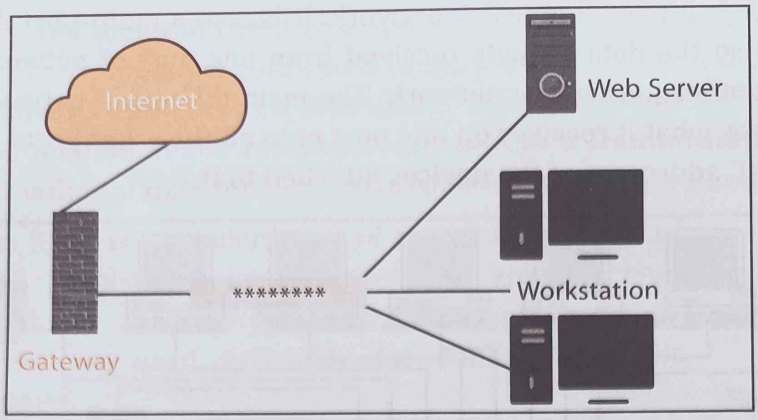


Fig. 7.12: Gateway

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.

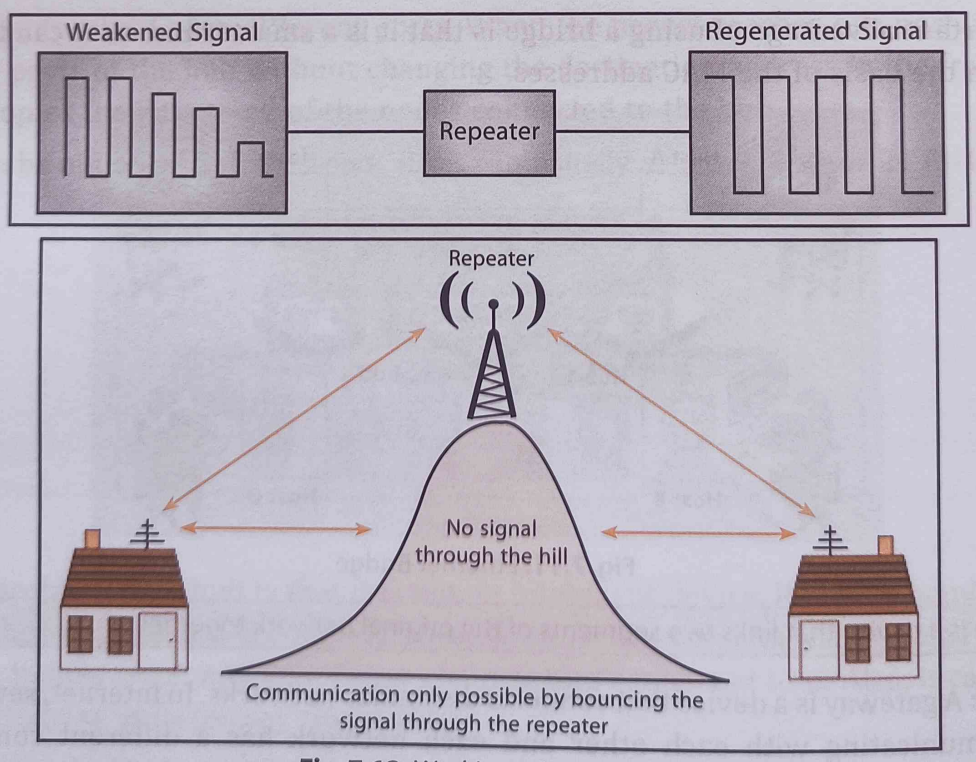


Fig. 7.13: Working of a Repeater

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 router is a networking device that forwards data packets from the source machine to the destination machine over a network by using the shortest path. Routers are used at the network layer, which is the third layer of the OSI model.

   A router uses IP address to connect a local area network to the internet. Compared to a hub or a switch, a router has advanced capabilities as it can analyze the data being carried over a network, decide/alter how it is packaged, and send it to another network of a different type. For example, suppose data has been divided into packets of a certain size and these packets are to be carried over a different type of network which cannot handle bigger packets. In such a case, the data is to be repackaged as smaller packets and then sent over the network by a router.

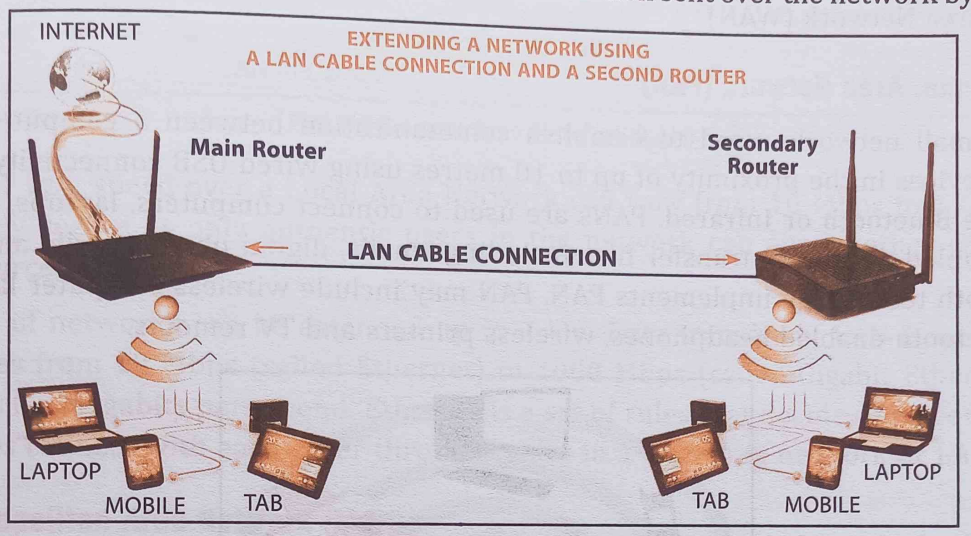


Fig. 7.14: Router

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. Wi-Fi cards are widely used in notebook computers due to their highly portable nature. The most common Wi-Fi card used in desktop computers is PCI-Express Wi-Fi card made to fit the PCI-Express card slot on the motherboard.

7.10 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. Computer networks can logically be divided into two types:

1. Client-Server network
2. Peer-to-Peer network

Client-Server network: In Client-Server network, multiple clients or workstations are connected to at least one central server. A server is a powerful computer with all applications and hardware installed in it and a client is a computer which seeks any resource from another computer. When clients need access to these resources, they access them from the server. This network is used for larger networks.

Peer-to-Peer network: In Peer-to-Peer network, all nodes in the network have equivalent capability and function as both client and server. In this network, all workstations are connected together for sharing devices, information or data. This network is ideal for small networks where there is no need of dedicated servers.

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

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)

7.10.1 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.

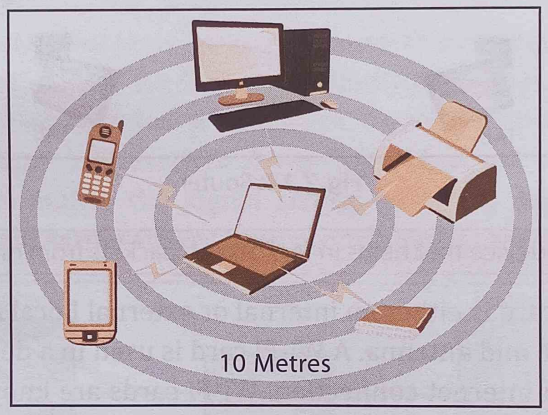


Fig. 7.15: Personal Area Network (PAN)

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

7.10.2 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. The geographical area covered by a LAN can range from a single room, a floor, an office having one or more buildings in the same premise, a laboratory, school, college or a university campus. The connectivity is done by means of wires, Ethernet cables, fibre optics or Wi-Fi.

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.

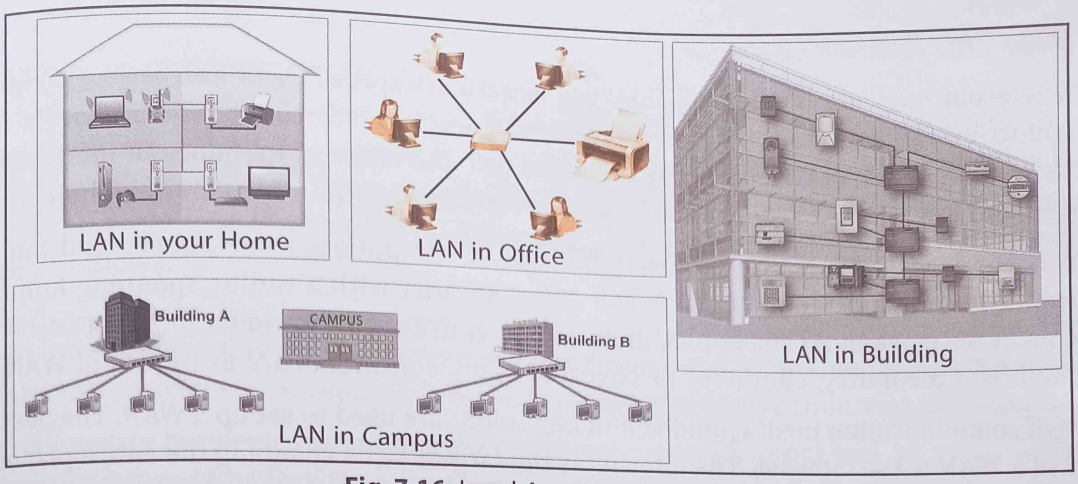


Fig. 7.16: Local Area Network (LAN)

Data transfer rate speed over a Local Area Network can vary from 10 Mbps to 1 Gbps. LAN is comparatively secure as only authentic users in the network can access other computers or shared resources.

These types of networks can be extended up to 1 km. Data transfer in LAN is quite high and usually varies from 10 Mbps (called Ethernet) to 1000 Mbps (called Gigabit Ethernet), where Mbps stands for Megabits per second. Ethernet is a set of rules that decides how computers and other devices connect with each other through cables in a local area network or LAN.

7.10.3 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.

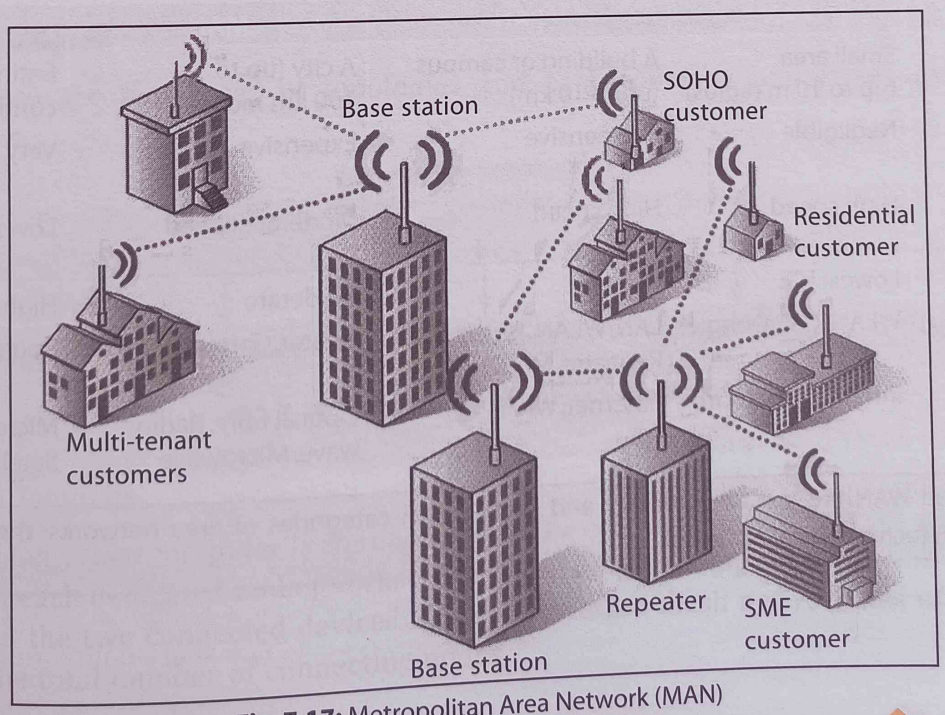


Fig. 7.17: Metropolitan Area Network (MAN)

7.10.4 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.

Internet is the largest WAN that connects billions of computers, smartphones and millions of LANs from different continents. A 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.

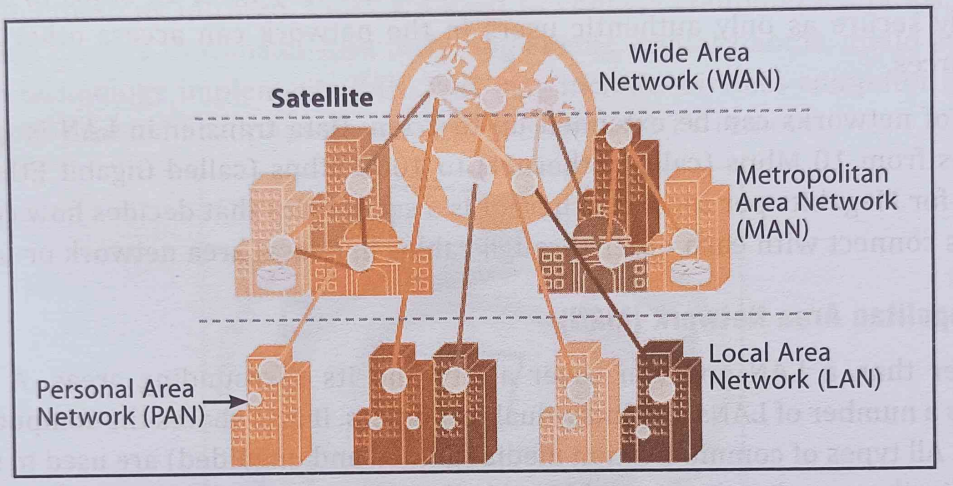


Fig. 7.18: Wide Area Network (WAN)

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.

7.11 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.

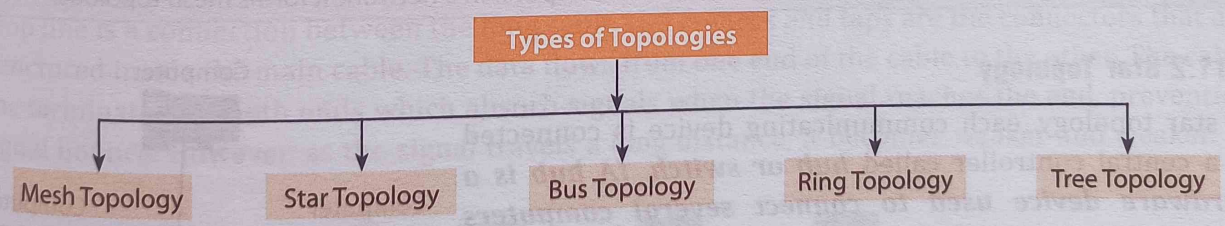


Fig. 7.19: Classification of Network Topologies

7.11.1 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.

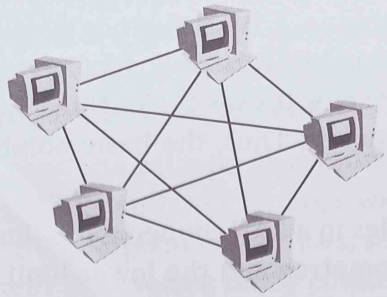


Fig. 7.20: Mesh Topology

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.

7.11.2 Star Topology

In star topology, each communicating device is connected to a central controller called ***hub or switch. (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.

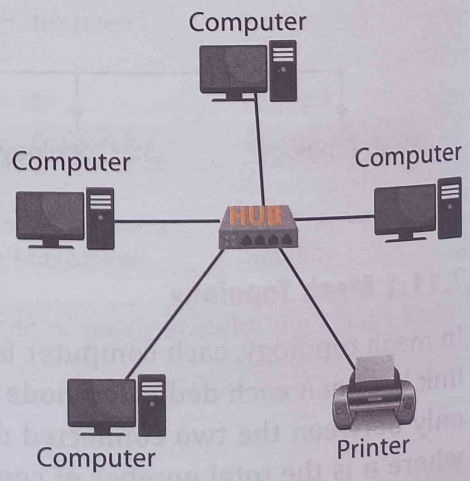


Fig. 7.21: Star Topology

The most popular and widely used **LAN** technology, **Ethernet**, currently operates in Star Topology. The central node can be either a broadcasting device (hub) which means data will be transmitted to all the nodes in the network, or a unicast device (switch) meaning the node can identify the destination and forward data to that node only.

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 be 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 the 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.

7.11.3 Bus Topology

Bus topology is a multipoint configuration, *i.e.*, several devices are connected to a main long cable (usually co-axial 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. The cable has terminators at both ends which absorb signals when the signal reaches the end, preventing signal bounce. However, as the signal travels a long distance, it becomes weaker and weaker.

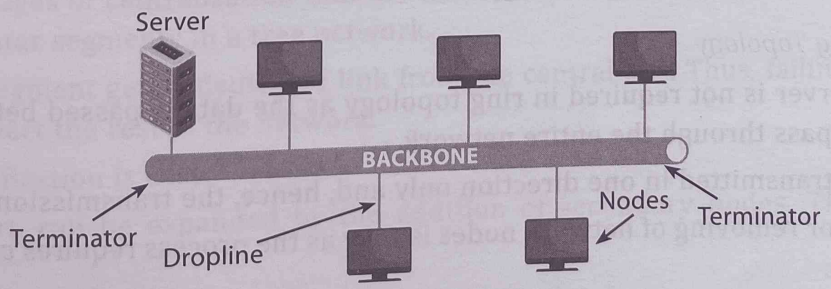


Fig. 7.22: Bus Topology

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 as several nodes can transmit data to each other at a time.

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

7.11.4 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.

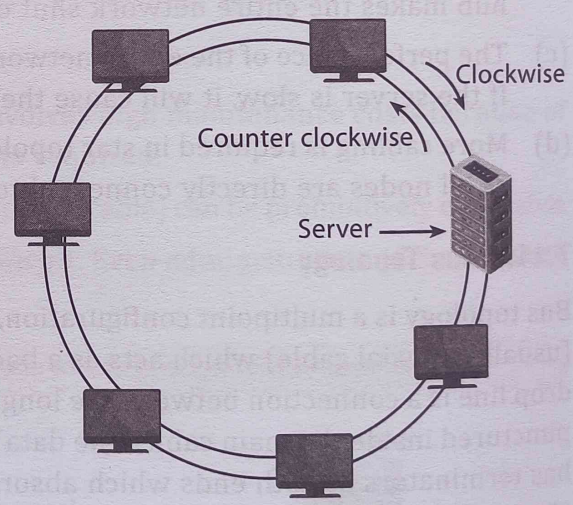


Fig. 7.23: Ring Topology

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, 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.

7.11.5 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.

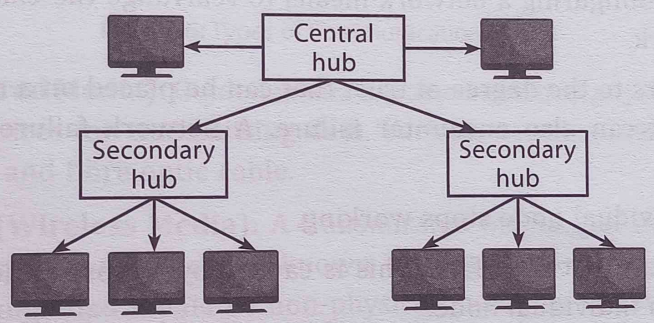


Fig. 7.24: Tree Topology

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 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. 7.25 shows a P-P link in a network.

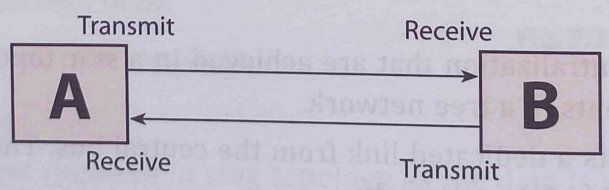


Fig. 7.25: A Point-to-Point Link

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.

7.12 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:

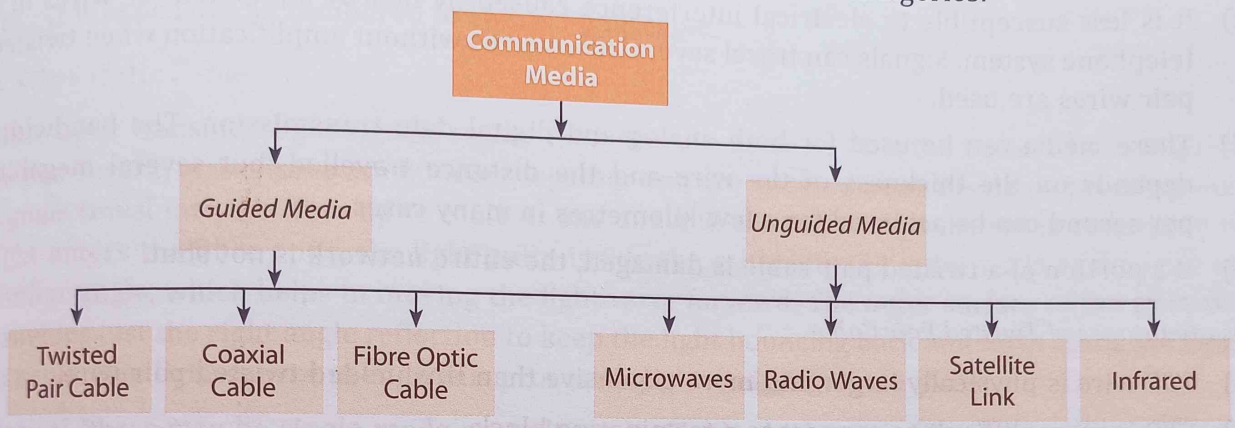


Fig. 7.26: Types of Communication Media

- **Guided Media (Wired Media):** Guided media are 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.
- **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.

7.12.1 Guided Media or Wired Networking Technologies

1. 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.

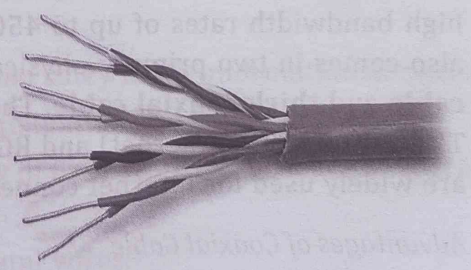


Fig. 7.27: Twisted Pair Cable

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 Unshielded 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 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.

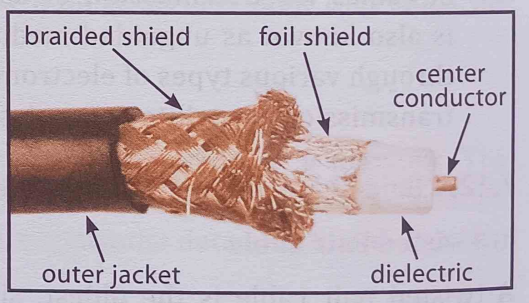


Fig. 7.28: Coaxial Cable

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) A thick coaxial cable does not bend easily and thus is 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.

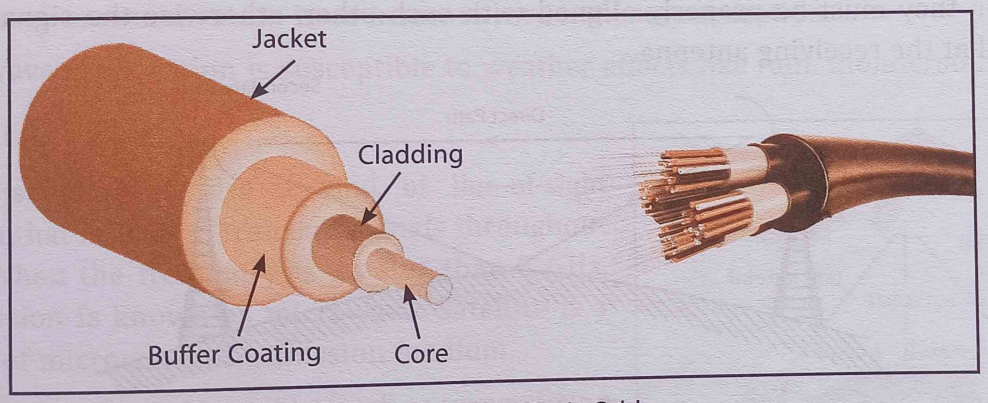


Fig. 7.29: Fibre Optic Cable

Advantages of Fibre Optic Cable

(a) Fibre optic cable 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 the fields of research and development.

Disadvantages of Fibre Optic Cable

(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, it can be easily broken.

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

7.12.2 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.

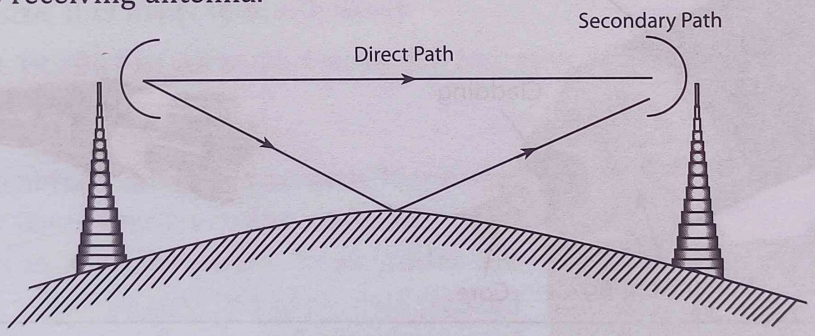


Fig. 7.30: Microwave

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

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.

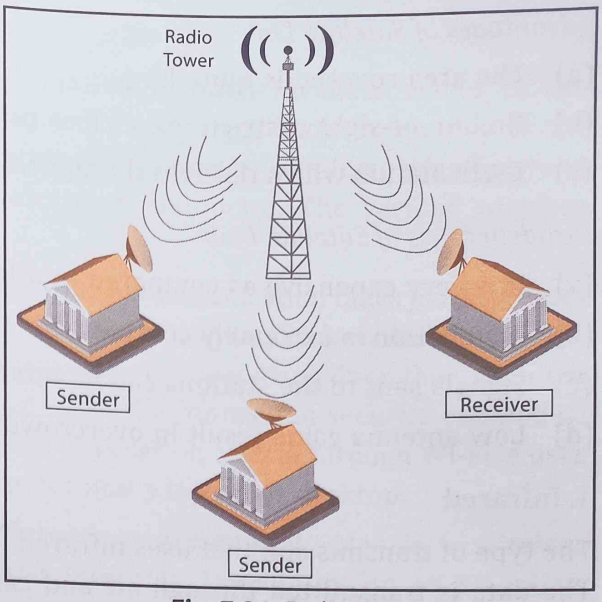


Fig. 7.31: Radio Waves

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

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.

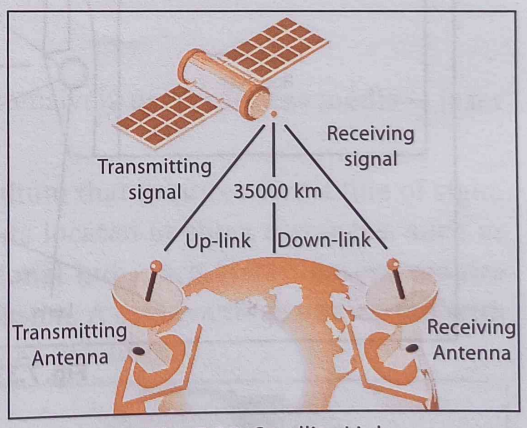


Fig. 7.32: Satellite Link

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.

POINT TO REMEMBER

Geostationary satellites orbiting the Earth are used to deliver broadband internet service, similar to the way satellites are used for television and telephone signals. These satellites use microwaves for communication between a satellite dish placed at our home and the hub of satellite internet service providers.

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.

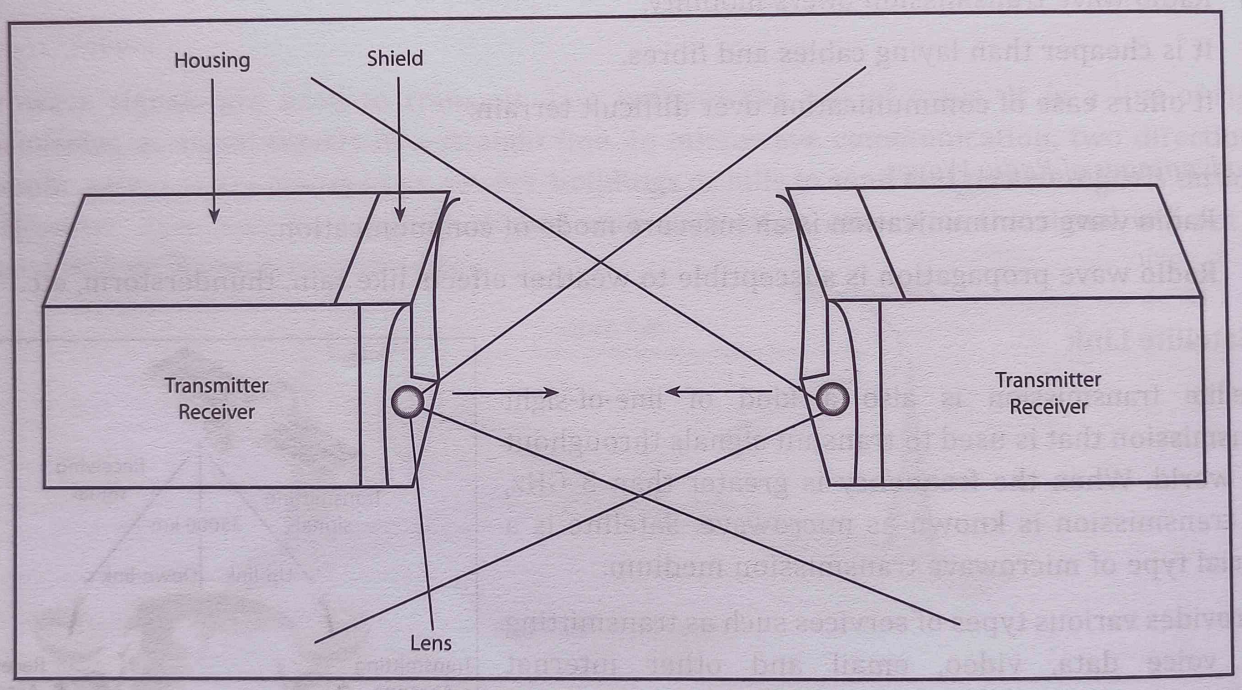


Fig. 7.33: Infrared Transmission System

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.

The difference between Wi-Fi and Wi-Max lies in their utility. Wi-Fi is used to form small wireless networks (WLANs) whereas Wi-Max uses a larger spectrum to deliver connections to various devices on the network. Wi-Max has a higher data transfer rate and can span over a large area. That is why it is used in MAN applications.

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.

(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).

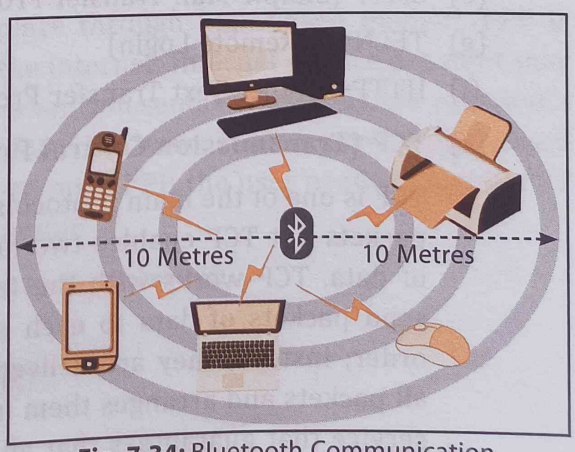


Fig. 7.34: Bluetooth Communication

Transmission of information using Bluetooth 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.

7.13 NETWORK PROTOCOLS

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 over a network.

For example, using library books.

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

Protocols also define:

- How computers identify one another on a network.
- The form to which the data should be converted for transmission.
- How to decide whether the data received is for that node or to be forwarded to another node.
- How to ensure that all the data reaches the destination without any loss.
- How to rearrange the packets and process them at the destination.

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 3)
(g) TELNET (Remote Login) (h) HTTP (Hyper Text Transfer Protocol)
(i) HTTPs (Hyper Text Transfer Protocol Secure)

(a) **TCP (Transmission Control 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.

Originally PPP was often used for dial-up connections. Nowadays it is still used for DSL with PPPoE (PPP over Ethernet) and PPPoA (PPP over ATM).

(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.

IMAP (Internet Mail Access Protocol) is used for accessing and storing emails from a mail server over a TCP/IP connection.

(f) **POP3 (Post Office Protocol 3)**

The POP3 (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 protocol allows a user to communicate with a remote machine. 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 from or sharing files to the remote system with the help of command line interface. With Telnet, a user logs in as a regular user with whatever privileges that 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.

(h) **HTTP (Hyper Text Transfer Protocol)**

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 protocol are:

1. It is a stateless protocol; this means that http server need not keep track of any command and each command is independent of any other 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.

(i) **HTTPs (Hyper Text Transfer Protocol Secure)**

HTTPs stands for Hyper Text Transfer Protocol Secure. It is a protocol for securing communication between two systems, *e.g.*, the browser and the web server. HTTP transfers data between the browser and the web server in the hypertext format, whereas https transfers data in the encrypted format. Thus, https prevents hackers from reading and modifying data during the transfer between the browser and the web server. Even if hackers manage to intercept a communication, they will not be able to use it because the message is encrypted.

7.14 PROTOCOLS FOR CHAT, AUDIO AND VIDEO CONFERENCING

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

7.14.1 IRC (Internet Relay Chat) – Protocol for Chatting

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.

7.14.2 VoIP (Voice over Internet Protocol) – Protocol for Audio

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 three main causes for the evolution of the VoIP 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.

7.14.3 Protocols for Video Conferencing

Video conferencing 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 video conference typically must have a computer, a camera, a microphone, a video screen, a sound system and internet connectivity.

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, saving time and money.

The most popular software used for video conferencing is:

(a) Google Meet (b) Ekiga

(c) Skype

Some protocols of video conferencing are:

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

1. H.323

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

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 video conferencing 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.

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.

7.15 WIRELESS/MOBILE COMMUNICATION

7.15.1 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 with 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.

7.15.2 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.

7.15.3 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.*, video conferencing.

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

7.15.4 WLL (Wireless in Local Loop)

WLL provides 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.

7.16 MOBILE TELECOMMUNICATION TECHNOLOGIES—1G, 2G, 3G, 4G & 5G

➢ 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, CDMA One.

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, video conferencing, 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, video conferencing, 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.

➢ 5G Technology

The fifth generation or 5G is currently under development. It is expected to be a milestone in the success of Internet of Things (IoT) and Machine-to-Machine (M2M) communication. M2M is direct communication between devices—wired and wireless. 5G is expected to allow data transfer in Gbps, which is much faster than 4G. It is expected to be able to support all the devices of the future such as connected vehicles and the IoT.

7.17 INTRODUCTION TO WEB SERVICES

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

7.17.1 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.

7.17.2 Hyper Text Markup Language (HTML)

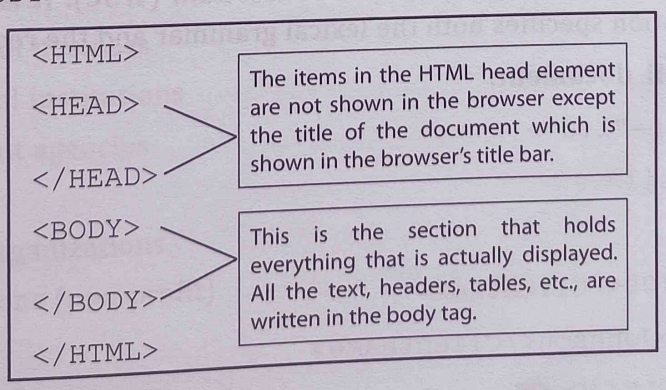
HTML is a language that is used to create web pages which are then displayed by web browsers. This language tells the browser how to display text, pictures and links on the screen. HTML is a language that supports multimedia documents and consists of audio, video, graphics, pictures, etc. It also helps 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:

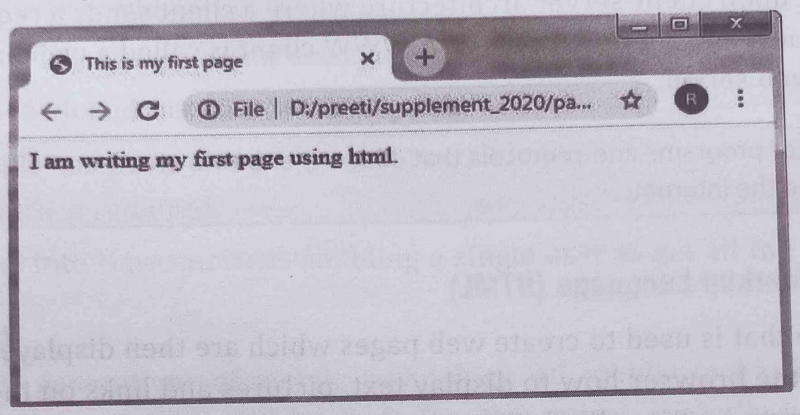
1. `<HTML> . . .</HTML>`
2. `<HEAD> . . .</HEAD>`
3. `<BODY> . . .</BODY>`



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:



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

7.17.3 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_Detail>
<Client>
<Clientid>C100</Clientid>
<Clientname>Johnson</Clientname>
<Company>APPLE</Company>
</Client>
```

```
<Client>
<Clientid>C101</Clientid>
<Clientname>McGraw</Clientname>
<Company>HCL</Company>
</Client>
</Client_Detail>
</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.

7.17.4 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 the 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

7.17.5 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 cbse.nic.in.

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

7.17.6 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 in the range of 0 to 255. Some examples of IP addresses are: 192.168.1.2, 10.24.1.3 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).

```
C:\WINDOWS\system32\cmc.exe
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>
```

7.17.7 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.

7.17.8 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.

7.17.9 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.

7.17.10 Web Server

A web server is a server that stores web pages and when a web client sends any request to a server, the 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 it 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.

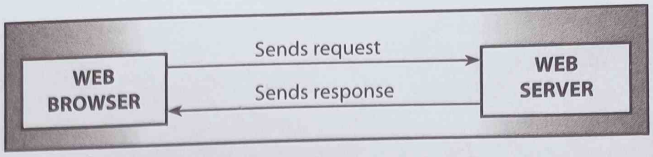


Fig. 7.35: Sending and Receiving Request

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.

7.17.11 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 hosts. 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.

7.17.12 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 (letter addressing) because it is much easier to remember than the IP address (number addressing). 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, Windows 10, 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.

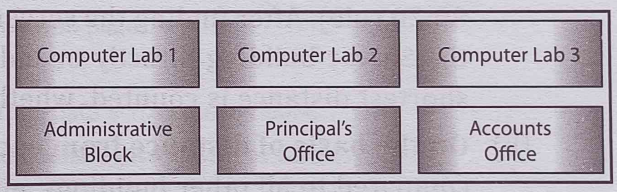
7.18 SETTING UP A COMPUTER NETWORK—AN EXAMPLE

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.

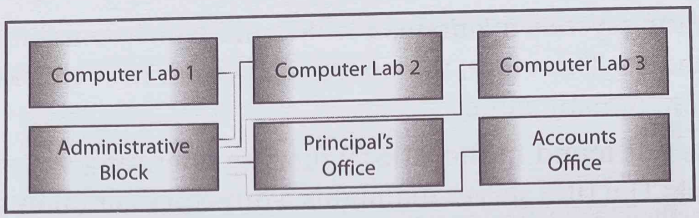


An educational society (say XYZ Educational Society), with its head office in Chennai (Tamil Nadu) and schools in various parts of the globe, is setting up a new senior secondary school, 'SF School', in Bahadurgarh (Haryana). The 'SF School' will have 3 computer labs with 30 computers in each lab, one 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 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.
- The MAC address, also known as the physical or hardware address, is a unique permanent value associated with a network adapter called a NIC. It is used to physically identify a machine on the network.
- IP address, also known as Internet Protocol address, is a unique address that can be used to uniquely identify each node in a network.
- Unlike MAC address, IP address can change if a node is removed from one network and connected to another network.
- The internet is a global network of computing devices.
- The World Wide Web (WWW), or web in short, is an ocean of information, stored in the form of trillions of interlinked web pages and web resources.
- Sir Tim Berners-Lee, a British computer scientist, invented the revolutionary World Wide Web in 1990.
- A set of rules that governs internet is called protocol.
- TCP protocol is responsible for sequential arrangement of packets.
- IP protocol is responsible for addressing and routing packets on the internet.
- FTP protocol is used to share files across networks.
- TELNET is a remote login where a user can login on remote 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.
- 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) The first network that planted the seed of internet was ..... .

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

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

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

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

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

(l) Interspace is a ..... .

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

(n) The technique of switching in which data is divided into smaller fragments is called ..... .

(o) ..... is a dedicated link between the sender and the receiver.

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

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

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

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 helps us to send and receive messages through video conferencing.

(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.

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 the use of Bridge in the network?

(i) To connect LANs (ii) To separate LANs

(iii) To control network speed (iv) All of these

(c) Each IP packet must contain:

(i) Only Source address (ii) Only Destination address

(iii) Source and Destination address (iv) Source or Destination address

(d) Which of these is not a communication channel?

(i) Satellite (ii) Microwave (iii) Radio wave (iv) WAN

(e) MAN Stands for ..... .

(i) Metropolitan Area Network (ii) Main Area Network

(iii) Metropolitan Access Network (iv) Metro Access Network

(f) Which of these is not an example of unguided media?

(i) Optical Fibre Cable (ii) Radio wave (iii) Bluetooth (iv) Satellite

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

(h) Which of the following is the smallest network?
(i) WAN (ii) MAN (iii) LAN (iv) PAN

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

(j) "One device per connection" is an advantage of:
(i) Star topology (ii) Tree topology (iii) Bus topology (iv) Ring topology

(k) Ping command is used to:
(i) Test a keyboard (ii) Test a network device
(iii) Test power cable (iv) Debug an application

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) was the first network that came into existence in 1969 and was sponsored by US Department of Defence.

NSFNET, developed by the National Science Foundation, was a high capacity network and strictly used for academic and engineering research. NSFNET along with ARPANET became the 'backbone' of the internet.

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 four types of networks:

(a) Personal Area Network (PAN) (b) Local Area Network (LAN)
(c) Metropolitan Area Network (MAN) (d) Wide Area Network (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. Rearrange the following terms in increasing order of data transfer rates:
Gbps, Mbps, Tbps, Kbps, Bps

Ans. Bps, Kbps, Mbps, Gbps, Tbps

[CBSE D 2015]

7. Differentiate between FTP and HTTP.

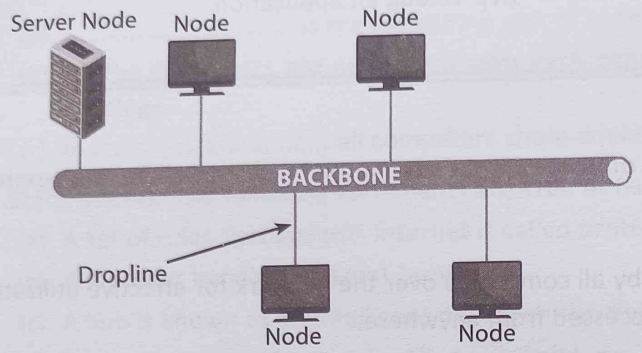
Ans. FTP—File Transfer Protocol is used to transfer files over the internet.
HTTP—Hyper Text Transfer Protocol is a protocol which allows the use of HTML to browse web pages on the World Wide Web.

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]

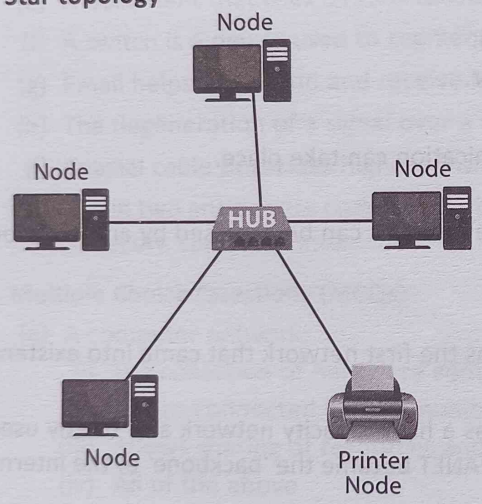
Ans. (a) *Wired:* Optical Fibre
(b) *Wireless:* Infrared for shorter distances or Microwave for longer distances.

9. Illustrate the layout for connecting five nodes in a Bus and a Star topology of Networks.

Ans. **Bus topology**



Star topology



10. 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 100 m to 500 m.

11. 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

12. Why are fibre optic cables becoming popular?

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

13. 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

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

Ans. Modem is an electronic device that enables a computer to transmit data over telephone lines. Modem stands for Modulator Demodulator. It converts digital signals to analog signals at the sender's end, called modulation, and analog signals back to digital signals at the receiver's end, called demodulation.

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

15. What is remote login? What is Telnet?

Ans. Remote login is the process of accessing a remote computer over a network 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.

16. 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.

17. 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) **PPP:** Point-to-Point Protocol
(d) **TCP/IP:** Transmission Control Protocol/Internet Protocol
(e) **SMTP:** Simple Mail Transfer Protocol
(f) **POP:** Post Office Protocol
(g) **IMAP:** Internet Mail Access Protocol

18. 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. TCP/IP protocols describe how data is packaged, addressed, transmitted, routed and how it is assembled at the receiver's side.

19. 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.

20. 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.

21. 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.

22. 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. HTML displays data and describes the structure of a web page whereas XML stores and transfers data.

23. 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. It allows individuals and organizations to post a website onto the internet that can be accessed by everyone on the web.

24. 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 (hub or switch as central device).

25. 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.

26. 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.

27. 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.

28. 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

29. 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.

30. What is a communication channel? Give examples of communication channels.

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.

Examples of wired communication channels:

(a) Twisted Pair Cables (b) Coaxial Cables (c) Fibre-optic Cables

Examples of wireless communication channels:

(a) Microwaves (b) Radio Waves (c) Satellites

31. 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.

32. Differentiate between star topology and bus topology.

Ans. The main points of difference between star topology 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.

33. 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. It broadcasts dataframe to every other port without considering whether it is destined for a particular destination or not.

(e) **Switch:** A switch is a small hardware device that joins multiple computers together within one local area network (LAN). It examines the destination address and sends the dataframe only to the intended computer.

34. 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.

35. 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.

36. 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

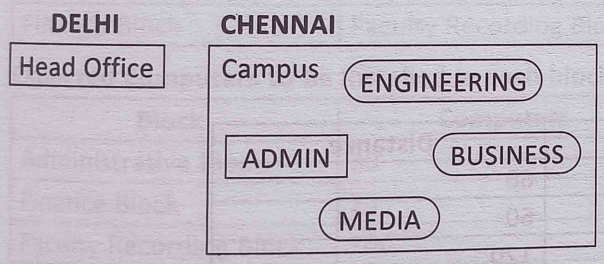
1. What is internet?
2. What is network?
3. What are the various types of topologies?
4. What is the range of frequency for radio waves?
5. 18 Gbps is equal to how many bits per second?
6. Write short notes on the following:
   (a) Bandwidth (b) Bluetooth
   (c) DNS (d) Data transfer rate
   (e) HTTP
7. Two universities in different states want to transfer information. Which type of network do they need to use for this?
8. Draw a network layout of star topology and bus topology connecting five computers.
9. Rohit, a Class XI student, has just started understanding the basics of internet and web technologies. He is a bit confused about the terms "World Wide Web" and "Internet". Help him understand both the terms with the help of suitable examples of each.
10. Describe bus topology and star topology.
11. Define the following terms:
    (a) Baud (b) Communication channel
    (c) Hub (d) Repeater
12. Define GSM and GPRS wireless communication system.
13. What is modem? Define the functioning of internal modem and external modem.
14. Expand and explain the following terms:
    (a) PPP (b) POP3
    (c) VoIP (d) IRC
15. Describe the following networking devices:
    (a) Routers (b) Bridges (c) Gateways
16. What are Wi-Fi cards? Explain.
17. What is a communication protocol? What is its role in networking?
18. What is https? How does it work?
19. What is Ethernet? What is Ethernet Card?
20. What are hubs? How are active hubs different from passive hubs?
21. What are the facilities provided by the Server in a network environment?
22. Which communication medium is to be suggested for very effective and fast communication in guided medium?
23. In a harsh industrial environment, which cable would you like to use?
24. Which media have the ability to communicate over oceans?
25. What is the difference between microwave and radio wave transmission?

26. Which transmission medium is useful for sparsely populated areas?
27. Which network topology is easy to expand?
28. Which device filters the data and which device can handle different protocol?
29. What is a network? What are its goals and applications?
30. 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
31. Explain the role of HTTP protocol.
32. Differentiate between Hub and Switch.
33. Differentiate between Circuit and Packet Switching.
34. What is the role of a switch in a network?
35. Differentiate between MAC and IP address.
36. Explain briefly:
    (a) HTTP (b) TCP/IP (c) FTP
37. What is computing? How is it different from mobile computing?
38. When would you prefer (i) hubs over repeaters, (ii) bridges over hubs, and (iii) switches over other networking devices?
39. Differentiate between web server and web browser. Write any two popular web browsers. [CBSE Sample Paper 2020-21]
40. Name the protocol that is used to send emails. [CBSE Sample Paper 2020-21]

CASE-BASED/SOURCE-BASED INTEGRATED QUESTIONS

1. Perfect Edu. Services Ltd. is an educational organization. It is planning to set up its India campus at Chennai with its head office at Delhi. The Chennai campus has four main buildings—ADMIN, ENGINEERING, BUSINESS and MEDIA.

   You, as a network expert, have to suggest the best network-related solutions for their problems raised in (a) to (d), keeping in mind the distances between the buildings and other given parameters.



Shortest distance between various buildings:

ADMIN to ENGINEERING	55 m
ADMIN to BUSINESS	90 m
ADMIN to MEDIA	50 m
ENGINEERING to BUSINESS	55 m
ENGINEERING to MEDIA	50 m
BUSINESS to MEDIA	45 m
DELHI Head Office to CHENNAI Campus	2175 m
Number of Computers installed at various buildings is as follows:	
ADMIN	110
ENGINEERING	75
BUSINESS	40
MEDIA	12
DELHI Head Office	20

(a) Suggest the most appropriate location for the server inside the Chennai campus (out of the 4 buildings) to get the best connectivity for maximum number of computers. Justify your answer.

(b) Suggest and draw the cable layout to efficiently connect various buildings within the Chennai campus for connecting the computers.

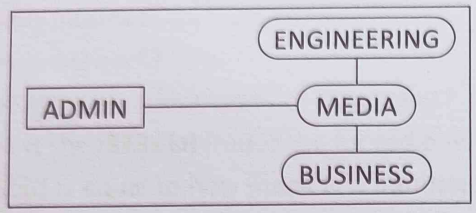
(c) Which hardware device will you suggest to be procured by the company to be installed to protect and control the internet use within the campus?

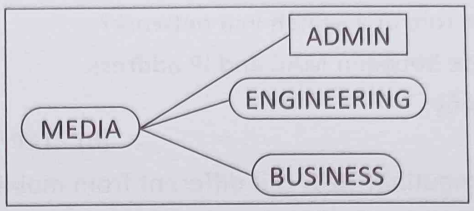
(d) Which of the following will you suggest to establish online face-to-face communication between the people in the Admin Office of the Chennai campus and Delhi Head Office?

(i) Cable TV (ii) Email (iii) Video conferencing (iv) Text Chat

Ans. (a) ADMIN (due to maximum number of computers) or MEDIA (due to shorter distance from other buildings)

(b) Any one of the following:

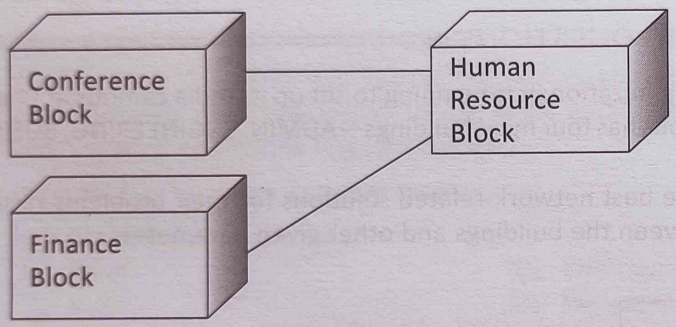




(c) Firewall or Router

(d) (iii) Video conferencing

2. Tech Up Corporation (TUC) is a professional consultancy company. The company is planning to set up new offices in India with its hub at Hyderabad. As a network adviser, you have to understand their requirements and suggest to them the best available solutions. [CBSE D 2014]



Block-to-Block distance (in Mtrs.):

Block (From)	Block (To)	Distance
Human Resources	Conference	60
Human Resources	Finance	60
Conference	Finance	120

Expected Number of Computers to be installed in each block:

Block	Computers
Human Resources	125
Conference	25
Finance	60

(a) What will be the most appropriate block where TUC should plan to install their server?

(b) Draw a block-to-block cable layout to connect all the buildings in the most appropriate manner for efficient communication.

(c) What will be the best possible connectivity out of the following to connect the new set-up of offices in Bengaluru with its London base office?

(i) Infrared (ii) Satellite Link (iii) Ethernet Cable

(d) Which of the following devices will you suggest to connect each computer in each of the above buildings?

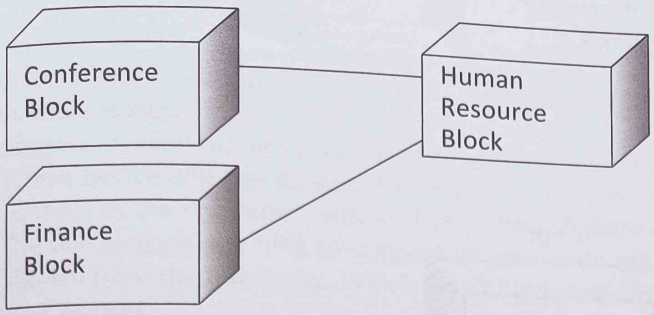
(i) Gateway (ii) Switch (iii) Modem

(e) Write names of **any two** popular Open Source Software which are used as Operating Systems.

(f) Write **any two** important characteristics of cloud computing.

Ans. (a) Human resources will be the most appropriate block where TUC should plan to install the server.

(b)



(c) Ethernet Cable

(d) Switch

(e) Linux and Open Solaris

(f) **Cost reduction:** Unlike on-site hosting, the price of deploying applications in the cloud can be less due to lower hardware costs from more effective use of physical resources.

Choice of applications: This allows flexibility for cloud users to experiment and choose the best option for their needs. Cloud computing also allows a business to use, access and pay only for what they use, with a fast implementation time.

3. Rovenza Communication International (RCI) is an online corporate training provider company for IT-related courses. The company is setting up their new campus in Kolkata. You, as a network expert, have to study the physical locations of various blocks and the number of computers to be installed. In the planning phase, provide the best possible answer for the queries (a) to (d) raised by them.

Block-to-Block distance (in Mtrs.):

From	To	Distance
Administrative Block	Finance Block	60
Administrative Block	Faculty Recording Block	120
Finance Block	Faculty Recording Block	70

Expected Computers to be installed in each block:

Block	Computers
Administrative Block	30
Finance Block	20
Faculty Recording Block	100

(a) Suggest the most appropriate block where RCI should plan to install the server.

(b) Suggest the most appropriate block-to-block cable layout to connect all three blocks for efficient communication.

(c) Which type of network out of the following is formed by connecting the computers of these three blocks?

(i) LAN (ii) MAN (iii) WAN

(d) Which wireless channel out of the following should be opted by RCI to connect to students from all over the world?

(i) Infrared (ii) Microwave (iii) Satellite

Ans. (a) Faculty recording block (due to maximum number of computers)

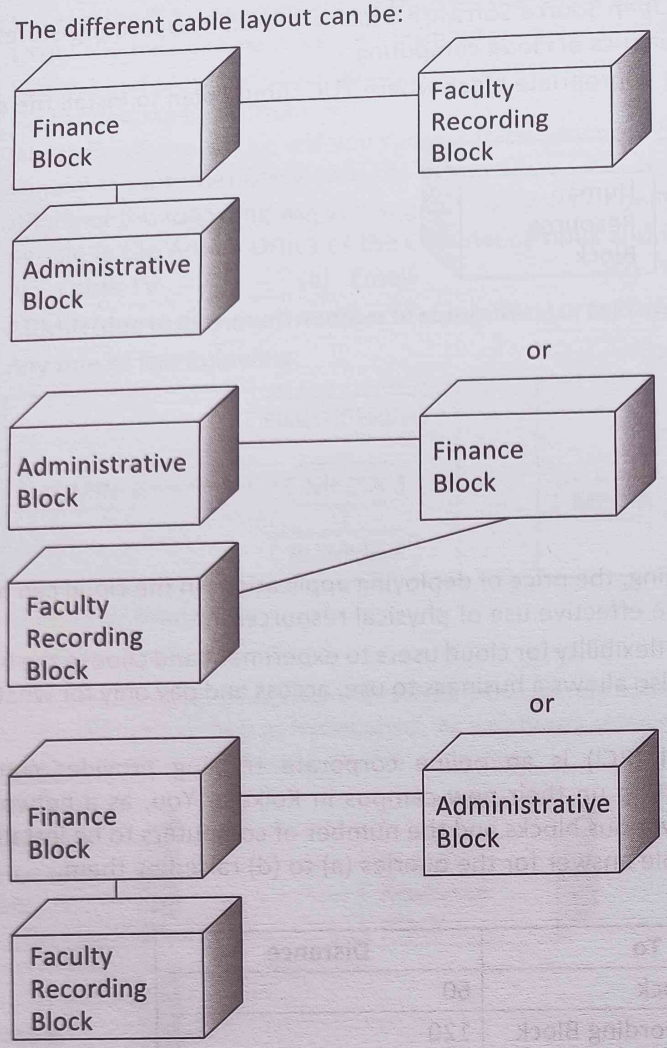
or

Finance (due to shorter distance from the other buildings)

or

Administrative block (due to name or nature of the building)

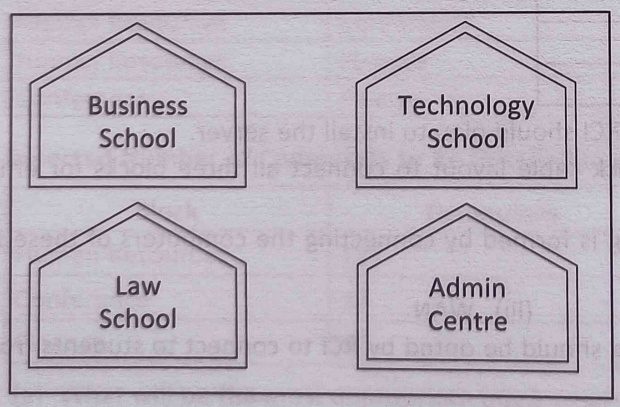
(b) The different cable layout can be:



(c) (i) LAN

(d) (iii) Satellite

4. Great Studies University is setting up its academic schools at Sunder Nagar and planning to set up a network. The university has 3 academic schools and one administration centre as shown in the diagram below:



Centre-to-centre distance between various buildings:

Law School to Business School	60 m
Law School to Technology School	90 m
Law School to Admin Centre	115 m
Business School to Technology School	40 m
Business School to Admin Centre	45 m
Technology School to Admin Centre	25 m

Number of computers in each of the Schools/Centre:

Law School	25
Technology School	50
Admin Centre	125
Business School	35

(a) Suggest the most suitable place (*i.e.*, schools/centre) to install the server of this university with a suitable reason.
(b) Suggest an ideal topology for connecting these schools/centre for a wired connectivity.
(c) Which device will you suggest to be placed/installed in each of these schools/centre to efficiently connect all the computers within these schools/centre?
(d) The university is planning to connect its admission office in the closest big city, which is more than 350 km from the university. Which type of network out of LAN, MAN or WAN will be formed? Justify your answer.

Ans. (a) Admin Centre because Admin Centre has the maximum number of computers, or Business School because it is closest to all other centres (minimum cable length required).
(b) BUS topology is the most suitable cable layout.
(c) Switch
(d) WAN is the preferred network for this purpose because 350 km is more than the range of LAN and MAN.

5. University of Correspondence in Allahabad is setting up a network between its different wings. There are 4 wings named Science (S), Journalism (J), Arts (A) and Home Science (H).

Distance between various wings:

Wing A to Wing S	100 m
Wing A to Wing J	200 m
Wing A to Wing H	400 m
Wing S to Wing J	300 m
Wing S to Wing H	100 m
Wing J to Wing H	450 m

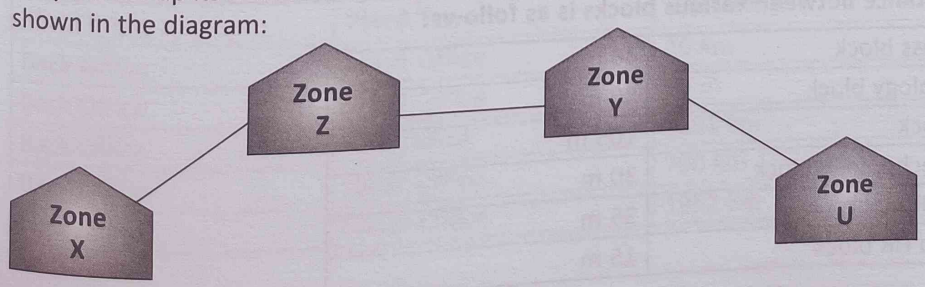
Number of Computers:

Wing A	150
Wing S	10
Wing J	5
Wing H	50

(a) Suggest the most suitable Topology for networking the computers of all wings.
(b) Name the wing where the Server is to be installed. Justify your answer.
(c) Suggest the placement of the Hub/Switch in the network.
(d) Mention how economic technology will provide internet accessibility to all wings.

Ans. (a) Star Topology can be used to network the computers of all wings.
(b) The Server should be installed in Wing A as Wing A has the maximum number of computers and installing the server in this wing will help to reduce the network traffic.
(c) Hub/Switch will be required in all the wings.
(d) The economic way to provide internet accessibility to all the wings is to use the proxy server at Wing A and connect to the internet through a dial-up network.

6. Sony has set up its Branch at Srinagar for its office and web-based activities. It has four Zones of buildings as shown in the diagram:



Branch-to-branch distance is:

Zone X to Zone Z	40 m
Zone Z to Zone Y	60 m
Zone Y to Zone X	135 m
Zone Y to Zone U	70 m
Zone X to Zone U	165 m
Zone Z to Zone U	80 m

Number of Computers:

Zone X	50
Zone Z	130
Zone Y	40
Zone U	15

(a) Suggest the most suitable cable layout or Networking Topology of connections between the Zones.

(b) Suggest the most suitable place (*i.e.*, Zone) to house the ERP and BI Server of this organization with a suitable reason, with justification.

(c) Suggest the placement of the following devices with justification:

(i) Repeater (ii) Hub/Switch

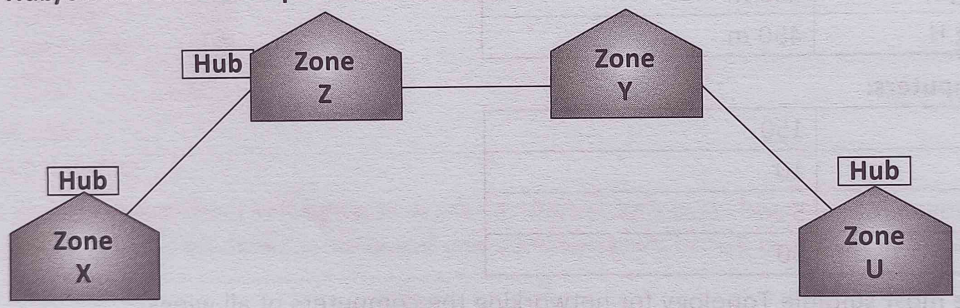
(d) Which is the most economic type of cable for the selected topology?

Ans. (a) Bus Topology

(b) The most suitable place (*i.e.*, Zone) to house the ERP and BI Server is Zone Z as it has the most number of computers; thus, cabling cost will be reduced and most traffic will be local.

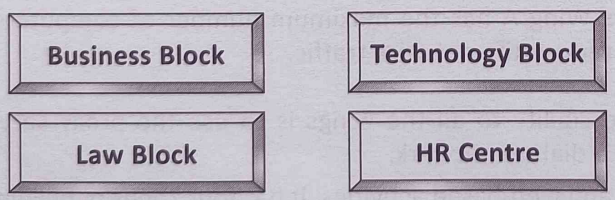
(c) **Repeater:** As per the suggested layout, separate repeaters need not be installed as each building/zone will be having a hub that acts as a repeater.

Hub/switch should be placed in each zone.



(d) An economic type of cable is dial-up or broadband as it can connect two computers at an economic rate though it provides lesser speed than other expensive methods.

7. Quick Learn University is setting up its academic blocks at Prayag Nagar and planning to set up a network. The university has 3 academic blocks and one human resource centre as shown in the diagram given below:



Centre-to-centre distance between various blocks is as follows:

Law block to business block	40 m
Law block to technology block	80 m
Law block to HR block	105 m
Business block to technology block	30 m
Business block to HR block	35 m
Technology block to HR block	15 m

Number of computers in each of the buildings is as follows:

Law block	15
Technology block	40
HR centre	115
Business block	25

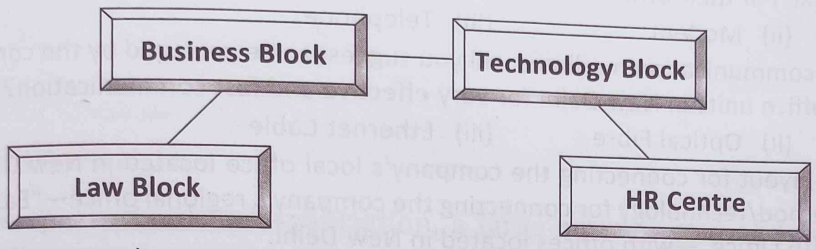
(a) Suggest a cable layout of connection between the blocks.

(b) Suggest the most suitable place to house the server of the organization with suitable reason.

(c) Which device should be placed/installed in each of these blocks to efficiently connect all the computers within these blocks.

(d) The university is planning to link its sales counters situated in various parts of the same city. Which type of network out of LAN, MAN or WAN will be formed?

Ans. (a)



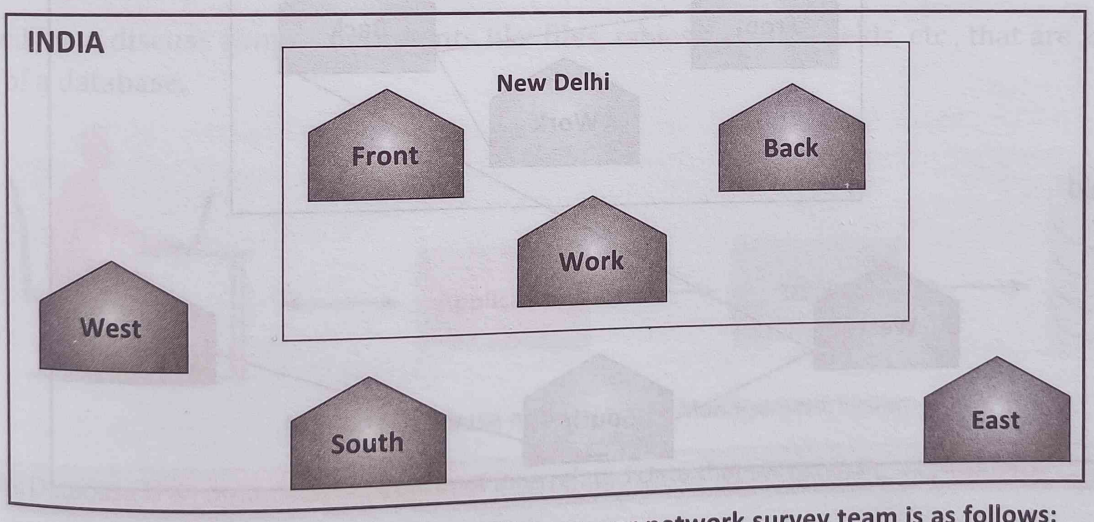
(b) HR centre because it consists of the maximum number of computers to house the server.

(c) Switch should be placed in each of these blocks.

(d) WAN because LAN and MAN cannot cover more than 250 km.

8. Bhartiya Connectivity Association is planning to expand their office in four major cities in India to provide regional IT infrastructure support in the field of Education & Culture. The company has planned to set up their head office in New Delhi at three locations and have named their New Delhi offices as "Front Office", "Back Office" and "Work Office". The company has three more regional offices—"South Office", "East Office" and "West Office"—located in other major cities of India.

A rough layout of the same is as follows:



Approximate distance between these offices as per network survey team is as follows:

Place From	Place To	Distance
Back Office	Front Office	10 km
Back Office	Work Office	70 m
Back Office	East Office	1291 km
Back Office	West Office	790 km
Back Office	South Office	1952 km

In continuation of the above, the company experts have planned to install the following number of computers in each of their offices:

Back Office	100
Front Office	20
Work Office	50
East Office	50
West Office	50
South Office	50

(a) Suggest network type (out of LAN, MAN, WAN) for connecting each of the following sets of their offices:
(i) Back Office and Work Office (ii) Back Office and South Office

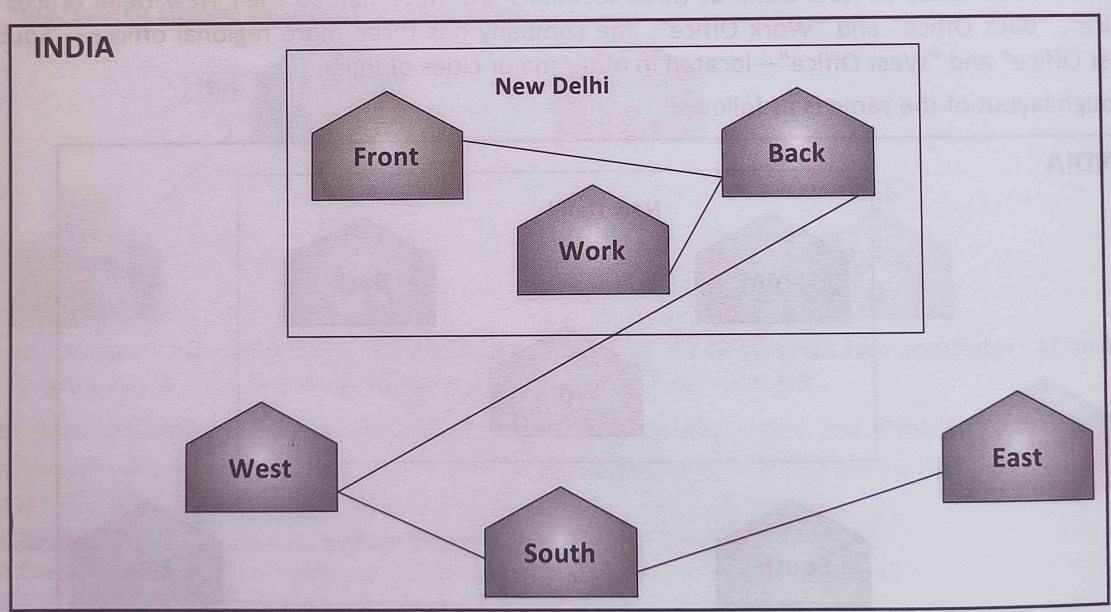
(b) Which device out of the following will you suggest to be produced by the company for connecting all the computers within each of their offices?
(i) Switch/Hub (ii) Modem (iii) Telephone

(c) Which of the following communication mediums will you suggest to be procured by the company for connecting their local office units in New Delhi for very effective and fast communication?
(i) Telephone Cable (ii) Optical Fibre (iii) Ethernet Cable

(d) Suggest a cable/wiring layout for connecting the company's local office located in New Delhi. Also, suggest an effective method/technology for connecting the company's regional office—"East Office", "West Office" and "South Office"—with offices located in New Delhi.

Ans. (a) Back Office and Work Office—MAN
Back Office and South Office—WAN

(b) Switch/Hub

(c) Optical Fibre

(d) Cable/Wiring Layout: